茨城大学重点研究

「地域に密着した世界的 ICT イノベーションの創出」

茨城大学工学部附属
ICT グローカル教育研究センター

２０１７年度

報告書

茨城大学重点研究プロジェクト「地域に密着した世界的 ICT イノベーションの創出」
平成 29 年度報告書刊行にあたって

プロジェクト代表　　黒澤　馨

ICT グローカル教育研究センターは，平成 26 年 7 月に 5 つ目の工学部附属教育研究センターとして活動を開始しました．本センターは，「情報セキュリティ・インテリジェント分野」・「社会・環境インフラ分野」・「ビッグデータ活用分野」・「ソーシャルコミュニティ・弱者支援分野」の 4 分野で構成され，各分野における『地域に密着した世界的 ICT イノベーションの創出』を目指しています．

当センターの平成 29 年度の研究業績は，著書・原著論文 31 編，特許 2 件，国際会議発表 49 件，解説 1 件，学会発表 69 件，競争的資金獲得（科学研究費補助金）12 件でした．

今後も，地域密着型の世界的 ICT イノベーションを創出する研究開発の推進に戦略的に取り組みながら，theory meets practice を実現するため，グローバル（世界的規模）な視点とローカル（地域的）な視点をもって地域課題の解決に取り組んでいきます．

本冊子は，重点研究「地域に密着した世界的 ICT イノベーションの創出」における当センター構成員の平成 29 年度の成果を中心にまとめましたので，是非ご一読頂けましたら幸甚に存じます．

構成員一同，茨城大学重点研究として地域社会の更なる発展に貢献していく所存でございますので，今後も引き続き，当センターへのご理解とご支援を宜しくお願い申し上げます．

「地域に密着した世界的 ICT イノベーションの創出」
プロジェクト参加教員

（１）情報セキュリティ・インテリジェント分野における研究開発

黒澤馨　　（工学部情報工学科・教授）
大瀧保広　（IT 基盤センター・准教授）
藤芳明生　（工学部情報工学科・准教授）
米山一樹　（工学部情報工学科・准教授）
芝軒太郎　（工学部情報工学科・講師）

（２）社会・環境インフラ分野における研究開発

上田賀一　（工学部情報工学科・教授）
桑原祐史　（工学部都市システム工学科・教授）
齋藤修　　（工学部・特命教授）
外岡秀行　（工学部情報工学科・教授）
羽渕裕真　（工学部情報工学科・教授）
山田稔　　（工学部都市システム工学科・教授）
石田智行　（工学部情報工学科・講師）
小澤佑介　（工学部情報工学科・助教）
高橋竜一　（工学部情報工学科・助教）
堀田大貴　（工学部情報工学科・助教）

（３）ビッグデータ活用分野における研究開発

新納浩幸　（工学部情報工学科・教授）
岡田信一郎（工学部情報工学科・講師）
古宮嘉那子（工学部情報工学科・講師）
佐々木稔　（工学部情報工学科・講師）

（４）ソーシャルコミュニティ・弱者支援分野における研究開発

鎌田賢　　（工学部情報工学科・教授）
米倉達広　（工学部情報工学科・教授）
野口宏　　（IT 基盤センター・講師）
小花聖輝　（工学部共通講座・助教）

－目次－

1. 活動概要

ICT グローカル教育研究センター　平成２９年度活動概要

１．　研究開発・資金獲得計画

１．　計画名：情報セキュリティ・インテリジェント分野における研究開発

（１）　実施概要：

- クラウドにおける情報セキュリティに関する研究
- 暗号プロトコルの設計論と安全性証明に関する研究
- 読字障害児童向け音声付教科書の開発
- 共創型人間－機械インタフェースの提案と障害者支援

（２）　実施予定時期：　平成 29 年 4 月 1 日～平成 30 年 3 月 31 日

（３）　実施体制

- 責任者：黒澤馨
- メンバ：大瀧保広，藤芳明生，米山一樹，芝軒太郎

（４）資金獲得計画：科研費等の各種外部資金獲得を目指す

（５）実施における課題：特になし

２．　計画名：社会・環境インフラ分野における研究開発

（１）　実施概要：

- ITS のための高信頼化通信の研究
- 組込みシステムの協調解析と品質計測手法の開発
- 衛星リモートセンシングに関する研究
- 高齢者を支援するインタラクションシステムの研究
- 総合防災管理支援システムの開発

（２）　実施予定時期：　平成 29 年 4 月 1 日～平成 30 年 3 月 31 日

（３）　実施体制

- 責任者：上田賀一
- メンバ：桑原祐史，齋藤修，外岡秀行，羽渕裕真，山田稔，石田智行，小澤佑介，高橋竜一，堀田大貴

（４）資金獲得計画：科研費等の各種外部資金獲得を目指す

（５）実施における課題：特になし

３．　計画名：ビッグデータ活用分野における研究開発

（１）　実施概要：

- 機械学習や統計学を利用した自然言語処理
- データベース学習のための支援システムの開発
- 様々なデータからの特徴抽出、分類、検索に関する研究
- 機械学習を用いた知識処理の研究

（２）　実施予定時期：　平成 29 年 4 月 1 日～平成 30 年 3 月 31 日

（３）　実施体制

- 責任者：新納浩幸
- メンバ：岡田信一郎，古宮嘉那子，佐々木稔

（４）資金獲得計画：科研費等の各種外部資金獲得を目指す

（５）実施における課題：特になし

４．　計画名：ソーシャルコミュニティ・弱者支援分野における研究開発

（１）　実施概要：

- 画像の自然な拡大・縮小・変形のための関数の開発
- 地域情報化の研究
- 階層型データモデル機能・データベースデータモデル機能に関する研究

（２）　実施予定時期：　平成 29 年 4 月 1 日～平成 30 年 3 月 31 日

（３）　実施体制

- 責任者：鎌田賢
- メンバ：米倉達広，野口宏，小花聖輝

（４）資金獲得計画：科研費等の各種外部資金獲得を目指す

（５）実施における課題：特になし

５．　計画名：各種論文誌・国際会議等での研究発表
（１）　実施概要：各種論文誌・国際会議等において研究発表を行う
（２）　実施予定時期：　平成 29 年 4 月 1 日～平成 30 年 3 月 31 日
（３）　実施体制
・　責任者：黒澤馨
・　メンバ：上田賀一，鎌田賢，桑原祐史，齋藤修，新納浩幸，外岡秀行，羽渕裕真，
山田稔，米倉達広，大瀧保広，藤芳明生，米山一樹，石田智行，岡田信一郎，
古宮嘉那子，佐々木稔，芝軒太郎，野口宏，小澤佑介，小花聖輝，
高橋竜一，堀田大貴
（４）資金獲得計画：科研費等の各種外部資金獲得を目指す
（５）実施における課題：特になし

６．　計画名：各種学会・国際会議等での委員
（１）　実施概要：各種学会・国際会議等での委員として活動する
（２）　実施予定時期：　平成 29 年 4 月 1 日～平成 30 年 3 月 31 日
（３）　実施体制
・　責任者：黒澤馨
・　メンバ：上田賀一，鎌田賢，桑原祐史，齋藤修，新納浩幸，外岡秀行，羽渕裕真，
山田稔，米倉達広，大瀧保広，藤芳明生，米山一樹，石田智行，岡田信一郎，
古宮嘉那子，佐々木稔，芝軒太郎，野口宏，小澤佑介，小花聖輝，
高橋竜一，堀田大貴
（４）資金獲得計画：特になし
（５）実施における課題：特になし

７．　計画名：当教育研究センター構成メンバによる勉強会
（１）　実施概要：当教育研究センター構成メンバによる勉強会を実施する
（２）　実施予定時期：　平成 29 年 4 月 1 日～平成 30 年 3 月 31 日
（３）　実施体制
・　責任者：黒澤馨
・　メンバ：上田賀一，鎌田賢，桑原祐史，齋藤修，新納浩幸，外岡秀行，羽渕裕真，
山田稔，米倉達広，大瀧保広，藤芳明生，米山一樹，石田智行，岡田信一郎，
古宮嘉那子，佐々木稔，芝軒太郎，野口宏，小澤佑介，小花聖輝，
高橋竜一，堀田大貴
（４）資金獲得計画：特になし
（５）実施における課題：特になし

○実施結果

１．　計画名：情報セキュリティ・インテリジェント分野における研究開発
（１）　実施結果：
- クラウドにおける情報セキュリティに関する研究
：アクセス情報も秘匿するキーワード検索可能暗号を研究開発
- 暗号プロトコルの設計論と安全性証明に関する研究
：エンドツーエンド暗号化通信の数理的安全性モデルを研究開発
- 読字障害児童向け音声付教科書の開発
：文字認知が困難な児童生徒の能動的読書を可能にするマルチモーダル教科書等を研究開発
- 共創型人間－機械インタフェースの提案と障害者支援
:双腕協調タスクモデルに基づく 5 指駆動型筋電電動義手の提案と義手処方支援を研究開発

２．　計画名：社会・環境インフラ分野における研究開発
（１）　実施結果：
- ITS のための高信頼化通信の研究
：疑似雑音符号系列による知的照明光通信ネットワークを研究開発

- 組込みシステムの協調解析と品質計測手法の開発
  ：社会インフラシステム向けソフトウェアプラットフォーム等を研究開発
- 衛星リモートセンシングに関する研究
  ：衛星データの評価検証技術，高付加価値を持つ衛星データの生成技術，衛星データの新たな利用技術等を研究開発
- 衛星リモートセンシングデータを用いた地域環境変遷の情報化に関する研究
  ：生活環境圏における CO_2 濃度の地域性に着目した新たな緑地評価指標を研究開発
- 総合防災管理支援システムの開発
  ：大規模自然災害時の円滑な情報共有に資する市町村型共通基盤等を研究開発
- ディジタル変復調や光無線通信システム等の開発
  ：海中可視光ワイヤレス給電通信のための高電力効率変調法を研究開発

３．　計画名：ビッグデータ活用分野における研究開発

（１）　実施結果：

- 機械学習や統計学を利用した自然言語処理
  ：外れ値検出手法からの重み設定による共変量シフト下における語義曖昧性解消の領域適応等を研究開発
- データベース学習のための支援システムの開発
  ：SQL 実習支援システム、リレーショナルデータモデル演習システムによる実際の授業での運用
- 様々なデータからの特徴抽出、分類、検索に関する研究
  ：局所的な周辺文脈を利用した日本語の教師なし All-words 型語義曖昧性解消等を研究開発
- 機械学習を用いた知識処理の研究
  ：状況やデータの性質を意識して，大量なデータから，知識のパターンやルールを取り出して活用する方法等を研究開発

４．　計画名：ソーシャルコミュニティ・弱者支援分野における研究開発

（１）　実施結果：

- 画像の自然な拡大・縮小・変形のための関数の開発
  ：可変張力つき 2 変数スプラインの導出とその画像補間等を研究開発
- 地域情報化の研究
  ：メディアを利用した地域の ICT 化推進と地域の情報発信等を研究開発
- 階層型データモデル機能・データベースデータモデル機能に関する研究
  ：分散キャンパスを用いたファイルバックアップシステム等を研究開発
- ウェブシステムや並列・分散処理等に関する研究
  ：次世代コンピュータシステム等を研究開発

５．　計画名：各種論文誌・国際会議等での研究発表

（１）　実施結果：

■著書・論文誌：延べ **３１件**

Kaoru Kurosawa, Le Trieu Phong, "Anonymous and leakage resilient IBE and IPE", Des. Codes Cryptography 85(2): 273-298, 2017 年 11 月.ほか３０件

■特許：延べ **２件**

吉田麗生，小林鉄太郎，川原祐人，冨士仁，米山一樹，“鍵配送システム及び方法、鍵生成装置、代表ユーザ端末、サーバ装置、ユーザ端末並びにプログラム”，2017 年 5 月．ほか 1 件

■国際会議：延べ **４９件**

Kaoru Kurosawa, Rie Habuka, "More Efficient Construction of Bounded KDM Secure Encryption", ACNS 2017: 354-372, 2017 年 7 月．ほか４８件

■その他（研究発表等）：延べ ６９件

黒澤馨，根本雄輝，“Fully Secure な紛失キーワード検索”，情報セキュリティ研究会 ISEC2017-2，2017 年 5 月．ほか６８件.

６．　計画名：各種学会・国際会議等での委員

（１）　実施結果：

No.	教員名	内容等
1	上田賀一教授	日本ソフトウェア科学会・ソフトウェア工学の基礎ワークショップ 2017，プログラム委員
2	上田賀一教授	情報処理学会・組込みシステムシンポジウム 2017，プログラム委員
3	黒澤馨教授	Indocrypt 2017 プログラム委員
4	黒澤馨教授	電子情報通信学会 安全･安心な生活とＩＣＴ研究専門委員会 専門委員
5	黒澤馨教授	IET Information Security, Associate Editor
6	黒澤馨教授	International Journal of Applied Cryptography, Associate Editor
7	黒澤馨教授	Journal of Mathematical Cryptology, Associate Editor
8	鎌田賢教授	Associate editor, IEEE Transactions on Industrial Electronics
9	鎌田賢教授	Secretary of the journal, Sampling Theory in Signal and Image Processing
10	鎌田賢教授	Program committee, The 6th International Workshop on Web Services and Social Media
11	桑原祐史教授	土木学会 地球環境委員会 委員
12	桑原祐史教授	土木学会 地球環境委員会 地球環境研究論文集編集小委員会 委員
13	桑原祐史教授	日本リモートセンシング学会 対外協力委員会 委員
14	桑原祐史教授	日本リモートセンシング学会 対外協力委員会 JpGU 小委員会 委員長
15	桑原祐史教授	日本リモートセンシング学会 国土防災リモートセンシング研究会 会長
16	桑原祐史教授	日本沿岸域学会 論文編集委員会 委員
17	桑原祐史教授	土木学会 茨城会 幹事
18	桑原祐史教授	NPO 法人 CO_2濃度マップ普及協会 理事
19	外岡秀行教授	(国研)産業技術総合研究所 客員研究員
20	外岡秀行教授	(一社)日本リモートセンシング学会 評議員
21	外岡秀行教授	(一社)日本リモートセンシング学会 事務局情報管理担当
22	外岡秀行教授	(一財)宇宙システム開発利用推進機構 ISS 搭載型ハイパースペクトルセンサ等研究開発技術委員会委員
23	外岡秀行教授	(一財)宇宙システム開発利用推進機構 次世代地球観測衛星利用委員会委員
24	羽渕裕真教授	電子情報通信学会ワイドバンドシステム(WBS)研究専門委員会　顧問
25	羽渕裕真教授	電子情報通信学会ＩＴＳ研究専門委員会　顧問
26	羽渕裕真教授	電子情報通信学会基礎境界ソサイエティ　ＷＢＳ代表委員
27	羽渕裕真教授	IEEE ITS Tokyo Chapter 委員
28	羽渕裕真教授	IEEE VTS Tokyo Chapter 委員
29	羽渕裕真教授	Associate Editor, IEICE Transaction in Fundamentals, Special section on WideBand Systems
30	羽渕裕真教授	Associate Editor, IEICE Transaction in Fundamentals, Special section on Intelligent Transport Systems
31	羽渕裕真教授	Associate Editor, IEICE Transaction in Fundamentals, Special section on Signal Design and its Applications in Communications
32	羽渕裕真教授	Associate Editor, IEICE Transaction in Fundamentals,　Special section on Information Theory and Its Applications

No.	教員名	内容等
33	羽渕裕真教授	Technical Program Committee Member, IEEE Asia Pacific Wireless Communications Symposium (IEEE VCS APWCS2017)
34	羽渕裕真教授	Program Committee Member, International Workshop on Signal Design and its Applications in Communications (IEEE IWSDA 2017)
35	羽渕裕真教授	Technical Program Committee Member, International Conference on ITS Telecommunications (ITST 2017)
36	羽渕裕真教授	Technical Program Committee Member, IEEE GLOBECOM Workshop on Optical Wireless Communications
37	羽渕裕真教授	Technical Program Committee Member, IEEE International Conference on Communication, Networks and Satellite (COMNETSAT 2017)
38	羽渕裕真教授	Technical Program Committee Member, International Conference on Advances in Computing, Communications and Informatics (ICACCI 2017)
39	羽渕裕真教授	Technical Program Committee Member, International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC 2017)
40	羽渕裕真教授	地上テレビジョン放送の高度化技術に関する研究開発運営委員会（日本放送協会 放送技術研究所）
41	大瀧保広准教授	電子情報通信学会 情報セキュリティ研究専門委員会 委員
42	大瀧保広准教授	電子情報通信学会 基礎境界ソサイエティ Fundamental Review 誌 編集委員会 委員
43	藤芳明生准教授	電子情報通信学会 英文論文誌 D 編集委員
44	藤芳明生准教授	電子情報通信学会 会誌編集委員会 編集特別幹事（５月まで）
45	米山一樹准教授	日本応用数理学会 数理的技法による情報セキュリティ(FAIS)研究部会 幹事
46	米山一樹准教授	電子情報通信学会 2018 年英文論文誌小特集編集委員会 編集幹事
47	米山一樹准教授	電子情報通信学会 2019 年英文論文誌小特集編集委員会 編集幹事
48	石田智行講師	水戸市個人情報保護審議会委員
49	石田智行講師	日立市地域情報化推進会議　委員
50	石田智行講師	日本バーチャルリアリティ学会テレイマージョン技術研究委員会 幹事
51	石田智行講師	日本バーチャルリアリティ学会学会誌委員会 幹事
52	石田智行講師	第 21 回日本バーチャルリアリティ学会大会プログラム委員
53	石田智行講師	可視化情報学会 可視化情報全国講演会 2016 実行委員
54	石田智行講師	Track Chair, The 11th International Conference on Broadband and Wireless Computing Communication and Applications (BWCCA-2016)
55	石田智行講師	Track Chair, The 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2016)
56	石田智行講師	Program Committee, The 31th IEEE International Conference on Advanced Information Networking and Applications (AINA-2016)
57	石田智行講師	Program Committee, International Workshop on Disaster and Emergency Information Network Systems (IWDENS-2017)
58	石田智行講師	Workshop Co-Chair, International Workshop on Network-based Virtual Reality and Tele-existence (INVITE-2016)
59	石田智行講師	日立市総合計画後期基本計画策定委員会委員
60	岡田信一郎講師	電子情報通信学会 東京支部運営委員 支部委員
61	古宮嘉那子講師	ICT-IPSC　2017 プログラム委員
62	古宮嘉那子講師	情報処理学会　自然言語研究会 運営委員
63	芝軒太郎講師	計測自動制御学会システムインテグレーション（SI）部門ロボティクス部会委員
64	芝軒太郎講師	日本ロボット学会会誌編集委員
65	野口宏講師	学術情報処理研究編集委員
66	小澤佑介助教	TPC member, 7th IEEE GLOBECOM Workshop on Optical Wireless Communications (OWC'17)

No.	教員名	内容等
67	小澤佑介助教	TPC member, 2nd International conference and exhibition on Visible Light Communications 2018 (ICEVLC2018)
68	小澤佑介助教	Steering Committee, 2nd International conference and exhibition on Visible Light Communications 2018 (ICEVLC2018)
69	小花聖輝助教	WSSM-2017 Workshop Co-chair
70	小花聖輝助教	電子情報通信学会　サイバーワールド時限研究専門委員会　幹事

✧　外部資金獲得結果（継続研究課題を含む）

・継続研究課題

種別	教員	研究課題
基盤(A), 分担	藤芳明生准教授	理数系をはじめとするデジタル教科書をバリアフリー化するシステムの研究
基盤(B), 代表	藤芳明生准教授	文字認知が困難な児童生徒の能動的読書を可能にするマルチモーダル教科書の開発と評価
基盤(B), 分担	石田智行講師	大規模災害時の劣悪通信環境で繋がる次世代ネバー・ダイ・ネットワークとその応用
基盤(C), 代表	桑原祐史教授	生活環境圏における CO2 濃度の地域性に着目した新たな緑地評価指標の提案
基盤(C), 代表	羽渕裕真教授	疑似雑音符号系列による知的照明光通信ネットワークの創出
基盤(C), 代表	石田智行講師	大規模自然災害時の円滑な情報共有に資する市町村型共通基盤に関する研究
若手(B), 代表	古宮嘉那子講師	局所的な周辺文脈を利用した日本語の教師なし All-words 型語義曖昧性解消

・今年度新規採択課題

種別	教員	研究課題
基盤(A), 分担	古宮嘉那子講師	日本語歴史コーパスに対する統語・意味情報アノテーション
基盤(C), 代表	黒澤馨教授	アクセス情報も秘匿するキーワード検索可能暗号
若手(B), 代表	米山一樹准教授	エンドツーエンド暗号化通信の数理的安全性モデルに関する研究
若手(B), 代表	芝軒太郎講師	双腕協調タスクモデルに基づく 5 指駆動型筋電電動義手の提案と義手処方支援
若手(B), 代表	小澤佑介助教	海中可視光ワイヤレス給電通信のための高電力効率変調法に関する研究

・共同研究

教員名	共同研究課題
上田賀一教授	社会インフラシステム向けソフトウェアプラットフォームに関する研究
桑原祐史教授	生活環境圏における CO2 濃度の計測と実証
桑原祐史教授	平成 29 年度鳥獣被害防止対策に係る委託研究
桑原祐史教授	AI 技術を利用した水害対処の研究
桑原祐史教授	沢渡川流域の雨量モニタリングに基づく精緻な流量解析手法の研究
外岡秀行教授	路面状態センシング方式と放射分光応用に関する研究
外岡秀行教授	ドローン搭載熱赤外カメラによるソーラパネル点検に関する研究
新納浩幸教授，古宮嘉那子講師，佐々木稔講師	all-words WSD システムの構築および分類語彙表と岩波国語辞典の対応表作成への利用
新納浩幸教授，古宮嘉那子講師，佐々木稔講師	国立国語共同研究プロジェクト　「コーパスアノテーションの拡張・統合・自動化に関する基礎研究」
米山一樹准教授	NTT セキュアプラットフォーム研究所 クラウドベースの非同期メッセージングシステムに適合する暗号プロトコルの共同研究
米倉達広教授・石田智行講師	広聴業務等におけるスマートフォン等の身近な ICT ツールの活用
石田智行講師	かみね動物園 Android スマホアプリの再構築
石田智行講師	AR（拡張現実）技術を利用した博物館デジタルアーカイブに関する研究開発
石田智行講師	動物園業務総合管理支援システムの研究開発
小澤佑介助教	ギガビット自由空間光伝送装置の研究開発
小澤佑介助教	光電子倍増管を用いた適応型水中光無線通信の研究

・受託研究

教員名	受託研究課題
桑原祐史教授	気候変動に伴う沿岸地域の脆弱性評価と適応策の費用便益分析に関する研究
外岡秀行教授	ASTER の TIR データの品質管理に係る研究（(一財)宇宙システム開発利用推進機構）
外岡秀行教授	平成 29 年度 地球観測用小型赤外カメラ(CIRC)に関する校正検証（(国研)宇宙航空研究開発機構/JAXA）

・その他

・今年度新規採択課題

種別	教員	研究課題
茨城大学研究拠点認定，代表	桑原祐史教授	分野横断型環境情報の生成・公開と観測技術の開発

・継続研究課題

種別	教員	研究課題
茨城大学推進研究プロジェクト，代表	桑原祐史教授	少数民族村落の孤立回避を目的としたネパール国中山間部の環境モニタリング
奨学寄附金，代表	古宮嘉那子講師	意味処理に関する先行テーマの策定（追加）

7． 計画名：当教育研究センター構成メンバによる勉強会

（2） 実施結果：

・平成 29 年度 2 月および 4 月に着任した新任教員による勉強会を実施した.

その他（参考資料、報告書など）

（注）このページに収まらない場合は、必要に応じてページを追加する。

２．人材育成

１．　計画名：各種学会等での発表を通した学生の研究開発力と国際力の向上
（１）　実施概要：本教育研究センターに関連する研究開発の学生による積極的な対外発表および国際会議等への論文採択による学生の研究開発力と国際力の向上を図る
（２）　実施予定時期：平成 29 年 4 月 1 日～平成 30 年 3 月 31 日
（３）　実施体制
・ 責任者：黒澤馨
・ メンバ：上田賀一，鎌田賢，桑原祐史，齋藤修，新納浩幸，外岡秀行，羽渕裕真，山田稔，米倉達広，大瀧保広，藤芳明生，米山一樹，石田智行，岡田信一郎，古宮嘉那子，佐々木稔，芝軒太郎，野口宏，小澤佑介，小花聖輝，高橋竜一，堀田大貴
（４）　資金獲得計画：科研費等の各種外部資金獲得を目指す
（５）　実施における課題：特になし

２．　計画名：各種講座やセミナー等による地域人材の育成
（１）　実施概要：地域への還元や地域への貢献を目的とし，各種講座やセミナー等を通して地域人材を育成し，ひとづくりを図る
（２）　実施予定時期：平成 29 年 4 月 1 日～平成 30 年 3 月 31 日
（３）　実施体制
・ 責任者：黒澤馨
・ メンバ：上田賀一，鎌田賢，桑原祐史，齋藤修，新納浩幸，外岡秀行，羽渕裕真，山田稔，米倉達広，大瀧保広，藤芳明生，米山一樹，石田智行，岡田信一郎，古宮嘉那子，佐々木稔，芝軒太郎，野口宏，小澤佑介，小花聖輝，高橋竜一，堀田大貴
（４）　資金獲得計画：特になし
（５）　実施における課題：特になし

３．　計画名：各種発表会等による技術講演・技術交流
（１）　実施概要：本教育研究センターを構成する教員の各種研究開発技術について，各種発表会等による技術講演・技術交流を通して人材育成を図る
（２）　実施予定時期：平成 29 年 4 月 1 日～平成 30 年 3 月 31 日
（３）　実施体制
・ 責任者：黒澤馨
・ メンバ：上田賀一，鎌田賢，桑原祐史，齋藤修，新納浩幸，外岡秀行，羽渕裕真，山田稔，米倉達広，大瀧保広，藤芳明生，米山一樹，石田智行，岡田信一郎，古宮嘉那子，佐々木稔，芝軒太郎，野口宏，小澤佑介，小花聖輝，高橋竜一，堀田大貴
（４）　資金獲得計画：特になし
（５）　実施における課題：特になし

○実施結果（中間報告時と年度末に、実施結果を記載してください。）

１．　計画名：各種学会等での発表を通した学生の研究開発力と国際力の向上
（１）　実施結果：下記論文誌・国際会議等で学生が発表を行った.
・ 著書：Takahiro Inui, Masaki Kohana, Shusuke Okamoto, and Masaru Kamada, "IoT Technologies: State of the Art and a Software Development Framework", Chapter 1 (pp.3-18) in Fatos Xhafa, Fang-Yie Leu and Li-Ling Hung (eds.), Smart Sensors Networks- Communication Technologies and Intelligent Applications, Academic Press, 2017 年 6 月.
・ 原著論文：Haruna Kokubo, Taro Shibanoki, Takaaki Chin and Toshio Tsuji, "Obstacle Avoidance Method for Electric Wheelchairs Based on a Multi-Layered Non-Contact Impedance Model", Journal of Robotics, Networking and Artificial Life, 2017 年 6 月.

- 原著論文：佐久間東陽，亀山哲，小野理，木塚俊和，三上英敏，“Landsat-8 OLI 地表面反射率プロダクトを用いた釧路川流域における未利用農地分布図の作成”，日本リモートセンシング学会誌，2017 年 9 月.
- 原著論文：Jumpei Okumura, Yusuke Kozawa, Yohtaro Umeda, Hiromasa Habuchi, “Hybrid PWM/DPAM Dimming Control for Digital Color Shift Keying Using RGB-LED Array”, IEEE Journal on Selected Areas in Communications, 2018 年 1 月.
- 原著論文：Miki Kuroki, Michitoshi Niibori, Tomoyuki Ishida, Tatsuhiro Yonekura, “Implementation of information collecting tools using mobile terminals useful for efficient infrastructure maintenance”, International Journal of Space-Based and Situated Computing (IJSSC), 2018 年 2 月.
- 原著論文: Misaki Iyobe, Tomoyuki Ishida, Akihiro Miyakawa, Yoshitaka Shibata, “Implementation of a Mobile Traditional Crafting Application using Kansei Retrieval Method”, IT CoNvergence PRActice (INPRA), 2018 年 3 月.
- 原著論文：榑林雄飛，外岡秀行，“高分解能衛星画像の影解析及び反復的 3D モデリングによる建物の高さ推定”，日本リモートセンシング学会誌 (印刷中).
- 国際会議論文：Asahi SAKUMA, Satoshi KAMEYAMA, Satoru ONO, Toshikazu KIZUKA, Hidetoshi MIKAMI, "The detection and evaluation of unused agricultural land using Landsat-8 OLI and DEM in Kushiro River watershed Japan", International Symposium on Remote Sensing 2017, 2017 年 5 月.
- 国際会議論文：Wudabalaqiqige, Yuji KUWAHARA Analysis of social and environmental issues caused by exploitation of center pivot in Alukeerqin Qi, Inner Mongolia Autonomous", International Symposium on Remote Sensing 2017, 2017 年 5 月.
- 国際会議論文：Hirotaka IIDA, Shinichirou OKUDE, Naohiro MANAGO, Yuji KUWAHARA, Hiroaki KUZE, "Measurement of carbon dioxide concentration using DOAS method in the human activity area in Ibaraki, Japan", International Symposium on Remote Sensing 2017, 2017 年 5 月.
- 国際会議論文：Moena Asaki, Hideyuki Tonooka, "Updates of cross-calibration results of ALOS-2/CIRC using GOES-14/Imager", Proc. of International Symposium on Remote Sensing 2017 (ISRS 2017), 2017 年 5 月.
- 国際会議論文：Moena Asaki, Hideyuki Tonooka, Fumihiro Sakuma, "Time-series radiometric comparison of ASTER band 11 and Terra/MODIS band 29 in a low temperature range", Proc. of International Symposium on Remote Sensing 2017 (ISRS 2017), 2017 年 5 月.
- 国際会議論文：Jumpei Yamamoto, Hideyuki Tonooka, "Application of deep learning to cloud discrimination for ASTER Level 1T imagery", Proc. of International Symposium on Remote Sensing 2017 (ISRS 2017), 2017 年 5 月.
- 国際会議論文：Kaoru Kurosawa, Rie Habuka, "More Efficient Construction of Bounded KDM Secure Encryption", ACNS 2017, 2017 年 7 月.
- 国際会議論文：Yuki Koshino and Masaru Kamada, "Sparse approximation of ion-mobility spectrometry profiles by binomial splines", Proceedings of the12th International Conference on Sampling Theory and Applications (SampTA 2017), 654-657, 2017 年 7 月.
- 国際会議論文：Osamu Goto, Michitoshi Niibori and Masaru Kamada, "A block-based structure editor for the English language", In: L. Barolli et al. (eds.), Advances in Network-based Information Systems (Proceedings of the 20th International Conference on Network-based Information Systems, NBiS-2017), Lecture Notes on Data Engineering and Communications Technologies 7, 1051-1060, Springer, 2017 年 8 月.
- 国際会議論文：Yukiya Yamaguchi, Ryosuke Iiya, Michitoshi Niibori, Erjing Zhou, Masaru Kamada, Osamu Saitou and Susumu Shibusawa, "A web application for passengers to watch coming buses in rural areas", In: L. Barolli et al. (eds.), Advances in Network-based Information Systems (Proceedings of the 20th International Conference on Network-based Information Systems, NBiS-2017), Lecture Notes on Data Engineering and Communications Technologies 7, 1061-1069, Springer, 2017 年 8 月.
- 国際会議論文：Shuji Ogawa, Michitoshi Niibori, Tatsuhiro Yonekura and Masaru Kamada, "An HTML5 implementation of Web-Com for recording chalk annotations and talk voices onto web pages", In: L. Barolli et al. (eds.), Advances in Network-based Information Systems (Proceedings of the 20th International Conference on Network-based Information Systems, NBiS-2017), Lecture Notes on Data Engineering and Communications Technologies 7, 1070-1075, Springer, 2017 年 8 月.
- 国際会議論文：Akira Sakuraba, Tomoyuki Ishida, Koji Hashimoto, Yoshitaka Shibata, "Ultra Definition Display Environment for Disaster Management GIS", The 12th International Workshop on Network-based Virtual Reality and Tele-existence (INVITE'2017), 2017 年 8 月.

- 国際会議論文：Miki Kuroki, Michitoshi Niibori, Tomoyuki Ishida, Tatsuhiro Yonekura, "A study on the operation of infrastructure management system with citizens", The 12th International Workshop on Network-based Virtual Reality and Tele-existence (INVITE'2017), 2017 年 8 月.
- 国際会議論文：Keisuke Osawa, Hiromasa Habuchi, Yusuke Kozawa, "A Theoretical Analysis of Visible-Light Variable N-parallel Code-Shift-Keying in LOS Indoor Environments", The Eighth International Workshop on Signal Design and Its Applications in Communications (IWSDA'17), 2017 年 9 月.
- 国際会議論文：Ran Sun, Hiromasa Habuchi, Yusuke Kozawa, "Impact of Framed-DOOK Optical Wireless System using Error Correcting Codes", The Eighth International Workshop on Signal Design and Its Applications in Communications (IWSDA'17), 2017 年 9 月
- 国際会議論文：Takashi Tokunaga, Hiromasa Habuchi, Yusuke Kozawa, "New Two-Layered Pseudo-Noise Code for Optical-Wireless Code-Shift Keying/SCDMA", The Eighth International Workshop on Signal Design and Its Applications in Communications (IWSDA'17), 2017 年 9 月
- 国際会議論文：Fumio Narisawa, Yoshikazu Ueda, "Safety Verification Method for Priority-based Real-time Software", The 16th International Conference on Intelligent Software Methodologies, Tools, and Techniques (SOMET 2017) , 2017 年 9 月.
- 国際会議論文：Masayuki Ishikawa, Hiromasa Habuchi, "On Suitable Pseudo-Noise Code for Optical-Wireless Hierarchical CSK-MPPM System", IEEE 6th Global Conference on Consumer Electronics (GCCE2017), 2017 年 10 月.
- 国際会議論文：Tomohiro Okawa, Hiromasa Habuchi, "Rigorous Communication Success Probability of MC-CDMA with MPOMS Codes for Radio-On-Demand WSN", IEEE 6th Global Conference on Consumer Electronics (GCCE2017), 2017 年 10 月.
- 国際会議論文：Yuto Asano, Hiromasa Habuchi, Yusuke Kozawa, "Improved Synchronization Scheme for Indoor Visible-Light Differential On-Off Keying", IEEE 6th Global Conference on Consumer Electronics (GCCE2017), 2017 年 10 月.
- 国際会議論文：Takashi Tokunaga, Hiromasa Habuchi, Yusuke Kozawa, Ran Sun, "SCDMA Capability of High-Density Code-Shift Keying using Dual MPOMs in Optical-Wireless Channel", 27th International Telecommunication Networks and Applications Conference (ITNAC2017) , 2017 年 11 月.
- 国際会議論文：Ran Sun, Hiromasa Habuchi, Yusuke Kozawa, "Proposal of Optical Wireless Turbo Coded APPM System", 27th International Telecommunication Networks and Applications Conference (ITNAC2017) , 2017 年 11 月.
- 国際会議論文: Ryota Kimoto, Yusuke Kozawa, Yohtaro Umeda, Hiromasa Habuchi, "Inverse pulse position modulation schemes for simultaneous visible light wireless information and power transfer", 27th International Telecommunication Networks and Applications Conference (ITNAC2017) , 2017 年 11 月.
- 国際会議論文：Tomoaki Morita, Ryo Sakai, Yohtaro Umeda, Yusuke Kozawa, "A Quadrature-modulation EPWM Transmitter That Uses Sine Wave Carriers for I and Q Channel with a 90° Hybrid", 2017 IEEE Asia Pacific Microwave Conference (APMC), 2017 年 11 月.
- 国際会議論文：Yuto Tanaka, Yohtaro Umeda, Yusuke Kozawa, "Comparison of Power Combining Methods in Power-amplifier-inserted Transversal Filter for EPWM Transmitters", 2017 IEEE Asia Pacific Microwave Conference (APMC), 2017 年 11 月.
- 国際会議論文：Tai Tomizawa, Taro Shibanoki, Takaaki Chin and Toshio Tsuji, "An EMG-based Prosthetic Hand Training System Using a Class Partial Kullback-Leibler Information", The first IEEE Life Sciences Conference (LSC2017), Sydney, 2017 年 12 月.
- 国際会議論文：Tatsuya Ooyanagi, Hayato Ito, Misaki Iyobe, Tomoyuki Ishida, "Proposal of an Integrated Common Platform for Zoo Operation Support", Proc. of the 23rd International Symposium on Artificial Life and Robotics, pp.576-581, 2018 年 1 月.
- 国際会議論文：Hayato Ito, Tatsuya Ohyanagi, Misaki Iyobe, Tomoyuki Ishida, "Proposal of a Historical Materials Presentation AR System for Local Activities and History Education", Proc. of the 23rd International Symposium on Artificial Life and Robotics, 2018 年 1 月.
- 国際会議論文：Misaki Iyobe, Tomoyuki Ishida, Akihiro Miyakawa, Yoshitaka Shibata, "Kansei Retrieval Method by Principal Component Analysis of Japanese Traditional Crafts", Proc. of the 23rd International Symposium on Artificial Life and Robotics, pp.588-591, 2018 年 1 月.
- 国際会議論文：Yusuke Matsuda, Yusuke Kozawa, Yohtaro Umeda, “Experimental Evaluation of Hybrid PWM/DPAM Dimming Control Method for Digital Color Shift Keying using RGB-LED Array”, Proc. of the RISP International Workshop on Nonlinear Circuits, Communication and Signal Processing (NCSP’18), 2018 年 3 月.

- 国際会議論文： Keisuke Osawa, Hiromasa Habuchi, Yusuke Kozawa, ” Performance Evaluation of Hybrid VN-CSK/PAM for Lighting Constrained Visible Light Communications”, Proc. of the RISP International Workshop on Nonlinear Circuits, Communication and Signal Processing (NCSP’18), 2018 年 3 月.
- 国際会議論文：Ran Sun, Hiromasa Habuchi, Yusuke Kozawa, “Error Correcting Codes in Underwater RGB-LED Parallel Communication: Turbo or LDPC?”, Proc. of the RISP International Workshop on Nonlinear Circuits, Communication and Signal Processing (NCSP’18), 2018 年 3 月.
- その他（研究会等）：黒澤馨，根本雄輝，“Fully Secure な紛失キーワード検索”，情報セキュリティ研究会 ISEC2017-2，2017 年 5 月.
- その他（研究会等）：徳永岳，羽渕裕真，小澤佑介，“光無線 CSK/SCDMA のための二重拡散符号設計に関する一検討”，電子情報通信学会ＷＢＳ研究会，2017 年 5 月.
- その他（研究会等）：浅野裕太，羽渕裕真，小澤佑介，“光無線差動符号化 OOK のためのフレーム同期信号設計に関する一検討”，電子情報通信学会ＷＢＳ研究会，2017 年 5 月.
- その他（研究会等）：木元亮太，小澤佑介，楳田洋太郎，羽渕裕真，“水中可視光ワイヤレス給電通信システムのための交流/直流分離フィルタ設計に関する基礎的検討”，電子情報通信学会ＷＢＳ研究会，2017 年 7 月.
- その他（研究会等）：大澤圭佑，羽渕裕真，小澤佑介，“VN-CSK 照明光通信における環境光雑音の影響”，電子情報通信学会ＷＢＳ研究会，2017 年 7 月.
- その他（研究会等）：孫冉，羽渕裕真，小澤佑介，“光無線通信におけるブロック誤り訂正符号を用いるフレーム化 DOOK の効果”，電子情報通信学会ＷＢＳ研究会，2017 年 7 月.
- その他（研究会等）：高橋正行，岡田信一郎，“SQL 実習支援システムにおける反復学習回数削減法の実装と評価”情報処理学会 コンピュータと教育研究会 140 回研究発表会, 2017 年 7 月.
- その他（研究会等）：山本匠，楳田洋太郎，小澤佑介，“並列出力 MASH 方式 ΔΣ 変調器を用いた直交変調型包絡線パルス幅変調方式送信機”，電子情報通信学会 ICD 研究会，2017 年 8 月.
- その他（研究会等）：加茂巧，楳田洋太郎，小澤佑介，“ウェーバー方式イメージ抑圧法を用いた全ディジタル化 Low-IF 方式送信機のマルチキャリア送信特性”，電子情報通信学会 ICD 研究会，2017 年 8 月.
- その他（研究会等）：遊佐宣彦，佐々木稔，古宮嘉那子，新納浩幸，“単義語と共起する多義語に対する分散表現を利用した語義分析”，言語資源活用ワークショップ 2017，2017 年 9 月.
- その他（研究会等）：金子顕之，古宮嘉那子，佐々木稔，新納浩幸，“深層学習と合議を用いた極性分類”，第 11 回テキストアナリティクス・シンポジウム，2017 年 9 月.
- その他（研究会等）：薄井翔，上田賀一，小飼敬， 高橋竜一，堀田大貴，“制御ルールの並びに着目した反例分析手法の提案”，日本ソフトウェア科学会第 34 回大会，2017 年 9 月.
- その他（研究会等）：長岡源樹，上田賀一，堀田大貴，高橋竜一，“データ依存グラフを利用したデータフロー図の差異検出手法”，日本ソフトウェア科学会第 34 回大会，2017 年 9 月.
- その他（研究会等）：松田勇介，小澤佑介，楳田洋太郎，“PWM/DPAM ハイブリッド型調光制御法を用いたデジタル制御型カラーシフトキーイングの実験的評価”，電子情報通信学会 WBS 研究会，2017 年 10 月.
- その他（研究会等）：森田智明，酒井涼，楳田洋太郎，小澤佑介，“同相の正弦波を I, Q チャネルの搬送波に用い 90 度ハイブリッドを信号合成に用いる直交変調型 EPWM 送信機”，電子情報通信学会 MW 研究会，2017 年 10 月.
- その他（研究会等）：田中裕人，楳田洋太郎，小澤佑介，“EPWM 送信機への応用に向けた電力増幅器挿入型トランスバーサルフィルタにおける電力合成法の比較”，電子情報通信学会 MW 研究会，2017 年 10 月.
- その他（研究会等）：徳永岳，羽渕裕真，小澤佑介，孫冉，“MPOMs の二重符号化を用いる光 CSK/SCDMA の性能評価”，電子情報通信学会ＷＢＳ研究会，2017 年 10 月.
- その他（研究会等）：大川智広，羽渕裕真，“変形擬直交 M 系列対を用いるオンデマンド型 WSN のリバースリンクにおけるノード間同期誤差の影響”，電子情報通信学会ＷＢＳ研究会，2017 年 10 月.
- その他（研究会等）：孫冉，羽渕裕真，小澤佑介，“ASK-PPM を用いる光無線ターボシステムの一検討”，電子情報通信学会ＷＢＳ研究会，2017 年 10 月.
- その他（研究会等）：大澤圭佑，羽渕裕真，小澤佑介，“VN-CSK 照明光通信における受信機位置による BER 性能変化”，電子情報通信学会ＷＢＳ研究会，2017 年 10 月.
- その他（研究会等）：石川真行，羽渕裕真，小澤佑介，“光無線 CSK-MPPM 方式における疑似雑音符号について”，電子情報通信学会ＷＢＳ研究会，2017 年 10 月.

- その他（研究会等）: 石田智行，内田法彦，柴田義孝，“防災情報システム構築に係る実績と今後の展望”，第 33 回テレイマージョン技術研究会研究会，2017 年 11 月.
- その他（研究会等）: 朝木萌奈, 外岡秀行, 佐久間史洋，“低温域における ASTER/TIR 校正精度の時系列評価”，日本リモートセンシング学会第 63 回学術講演会, 2017 年 11 月.
- その他（研究会等）: 樗林雄飛, 外岡秀行，“高分解能衛星画像の影解析及び 3D モデリングによる建物の高さ推定値の確度の検討”，日本リモートセンシング学会第 63 回学術講演会, 2017 年 11 月.
- その他（研究会等）: 山本純平, 外岡秀行，“アンサンブル学習型ディープラーニングモデルを用いた ASTER 雲量情報の評価”，日本リモートセンシング学会第 63 回学術講演会, 2017 年 11 月.
- その他（研究会等）: 平井暁裕, 外岡秀行，“マルチスペクトル画像と周辺のハイパースペクトル画像の組み合わせによる鉱物同定”，日本リモートセンシング学会第 63 回学術講演会, 2017 年 11 月.
- その他（研究会等）: 室伏拓実, 外岡秀行，“米国ネバダ州 Alkali Lake における 3 バンド放射温度計の放射率測定試験”，日本リモートセンシング学会第 63 回学術講演会, 2017 年 11 月.
- その他（研究会等）: 黒澤馨，中村有志，“消失した(p,q)の挟み撃ち復元法”，SCIS 2018，1D1-5，2018 年 1 月.
- その他（研究会等）: 黒澤馨，羽深理恵，“ゲート情報を秘匿可能な効率のよい Garbled Gate の Closed Form 表現”，SCIS 2018，2A2-5，2018 年 1 月.
- その他（研究会等）: 黒澤馨，根本雄輝，“再利用可能な Oblivious 擬似ランダム関数”，SCIS 2018, 3A1-4，2018 年 1 月.
- その他（研究会等）: 黒澤馨，夛田隼人、上田明長，“BHHO 暗号の Tight な KDM 安全性”，SCIS 2018, 3B2-2，2018 年 1 月.
- その他（研究会等）: 黒澤馨, 上田明長、夛田隼人, “補助入力付き離散対数問題を解く Cheon アルゴリズムの一般化”，SCIS 2018, 3B3-5，2018 年 1 月.
- その他（研究会等）: 萩野谷一二，古宮嘉那子，黒澤馨，“角度に基づく格子基底の判定条件：α-reduced”，SCIS 2018, 3A4-3，2018 年 1 月.
- その他（研究会等）: 安藤毅宙，米山一樹，“シグマプロトコルの合成における複製可能性について”，暗号と情報セキュリティシンポジウム, 2018 年 1 月.
- その他（研究会等）: 寺田槙太郎，米山一樹，“同種写像に基づく Unified Model 認証鍵交換プロトコル”，暗号と情報セキュリティシンポジウム, 2018 年 1 月.
- その他（研究会等）: 金井佑篤，米山一樹，“ORAM におけるアクセスタイミングの秘匿について”，暗号と情報セキュリティシンポジウム, 2018 年 1 月.
- その他（研究会等）: 木村翔吾，米山一樹，“検証可能フォワード安全動的検索可能暗号の改良”，暗号と情報セキュリティシンポジウム, 2018 年 1 月.
- その他（研究会等）: 師成，米山一樹，“LINE Encryption Version 1.0 の ProVerif による検証”，暗号と情報セキュリティシンポジウム, 2018 年 1 月.
- その他（研究会等）: 伊與部美咲，石田智行，宮川明大，柴田義孝，“感性検索法による AR 伝統工芸プレゼンテーションシステムの構築”，第 34 回テレイマージョン技術研究会研究会，2018 年 3 月.
- その他（研究会等）: 大柳達哉，石田智行，“蓄積された経験データを用いた災害支援エキスパートシステムの提案”，第 34 回テレイマージョン技術研究会研究会，2018 年 3 月.
- その他（研究会等）: 阪本隼士，大柳達哉，石田智行，“マーカレス AR 技術によるインバウンド対応型スマートフォン AR アプリの構築”，第 34 回テレイマージョン技術研究会研究会，2018 年 3 月.
- その他（研究会等）: 中井僚，石田智行，“災害対策本部におけるインタラクティブ情報共有環境を用いた意思決定支援システムの構築”，第 34 回テレイマージョン技術研究会研究会，2018 年 3 月.
- その他（研究会等）: 星野将吾，石田智行，“地理情報システムを使用した消防団活動支援システムの構築”，第 34 回テレイマージョン技術研究会研究会，2018 年 3 月.
- その他（研究会等）: Lu Yangzhicheng，石田智行，宮川明大，柴田義孝，“ヘッドマウントディスプレイによる高臨場感伝統工芸システムの構築”，第 34 回テレイマージョン技術研究会研究会，2018 年 3 月.
- その他（研究会等）: 富澤太，芝軒太郎，中村豪，陳隆明，辻敏夫，“義手と動作イメージの整合性を実現可能な相互学習型訓練システム”，第 27 回　ライフサポート学会　フロンティア講演会，2018 年 3 月.
- その他（研究会等）: 清藤拓実，古宮嘉那子，佐々木稔，新納浩幸，“係り受け関係を用いた短単位の単語ベクトルから長単位の単語ベクトルの合成”，言語処理学会第 24 回年次大会，2018 年 3 月.

- その他（研究会等）：平林照雄，鈴木類，古宮嘉那子，浅原正幸，佐々木稔，新納浩幸，“『岩波国語辞典』の語義タグを用いた all-words の語義曖昧性解消”，言語処理学会第 24 回年次大会，2018 年 3 月．
- その他（研究会等）：遊佐宣彦，佐々木稔，古宮嘉那子，新納浩幸，"係り受け関係にある単語と単義語の分散表現を用いた語義曖昧性解消"，言語処理学会第 24 回年次大会，2018 年 3 月．
- その他（研究会等）：熊谷佳奈，古宮嘉那子，新納浩幸，“nwjc2vec の効果的な fine-tuning のためのパラメータ設定”，言語処理学会第 24 回年次大会，2018 年 3 月．
- その他（研究会等）：白静，古宮嘉那子，新納浩幸，“ターゲット領域のキーワード含有率を事例の重みとした感情分析の領域適応”，言語処理学会第 24 回年次大会，2018 年 3 月．
- その他（研究会等）：山木翔馬，新納浩幸，“教師あり・教師なし学習により構築した語義の分散表現を用いた語義曖昧性解消に関する一考察”，言語処理学会第 24 回年次大会，2018 年 3 月．
- その他（研究会等）：日置千仁，岡田信一郎，“学習失敗時の救済を目的とした効果的な反復学習を促す得点計算法の改良案の提案”，2018 年電子情報通信学会総合大会，2018 年 3 月．
- その他（研究会等）：石川真行，羽渕裕真，小澤佑介，“CSK-MPPM を用いる光無線路車間通信における路車間距離による同期誤差特性”，電子情報通信学会 WBS 研究会，2018 年 3 月．
- その他（研究会等）：浅野裕太，羽渕裕真，小澤佑介，“光無線フレーム化 DOOK システムの同期性能を考慮した BER 特性の検討”，電子情報通信学会 WBS 研究会，2018 年 3 月．
- その他（研究会等）：大川智広，羽渕裕真，橋浦康一郎，“光無線フレーム化 DOOK システムの同期性能を考慮した BER 特性の検討”，電子情報通信学会 WBS 研究会，2018 年 3 月．
- その他（研究会等）：孫冉，羽渕裕真，小澤佑介，“水中通信路における可視光差動オンオフキーイングの通信路容量”，2018 年電子情報通信学会総合大会，2018 年 3 月．
- その他（研究会等）：大澤圭佑，羽渕裕真，小澤佑介，“可視光ハイブリッド VN-CSK/PAM におけるビット誤り率と情報伝送効率のトレードオフ”，2018 年電子情報通信学会総合大会，2018 年 3 月．

２．　計画名：各種講座やセミナー等による地域人材の育成

（１）　　実施結果：特になし

３．　計画名：各種発表会等による技術講演・技術交流

（１）　　実施結果：

講演者	講演内容
上田賀一教授	茨城県立古河第二高等学校（ソフトウェアを実現する仕事，5 月 8 日）【模擬授業】
羽渕裕真教授	静岡大学創造科学技術大学院（光ワイヤレス通信のこれまでとこれから，７月２４日）【招待講演】
羽渕裕真教授	茨城キリスト教学園中学校（職業講話，９月８日）【講師】

その他（参考資料、報告書など）

2. 研究報告

【平成 29 年度参加教員発表の代表的な学術論文誌】

Int. J. Inf. Secur.
DOI 10.1007/s10207-017-0389-6

SPEICAL ISSUE PAPER

Multi-cast key distribution: scalable, dynamic and provably secure construction

Kazuki Yoneyama[1] · **Reo Yoshida**[2] · **Yuto Kawahara**[2] · **Tetsutaro Kobayashi**[2] · **Hitoshi Fuji**[2] · **Tomohide Yamamoto**[2]

Abstract In this paper, we propose a two-round dynamic multi-cast key distribution (DMKD) protocol under the star topology with a central authentication server. Users can share a common session key without revealing any information of the session key to the server and can join/leave to/from the group at any time even after establishing the session key. Our protocol is scalable because communication and computation costs of each user are independent from the number of users. Also, our protocol is still secure if either private key or session-specific randomness of a user is exposed. Furthermore, time-based backward secrecy is guaranteed by renewing the session key for every time period even if the session key is exposed. We introduce the first formal security definition for DMKD under the star topology in order to capture such strong exposure resilience and time-based backward secrecy. We prove that our protocol is secure in our security model in the standard model.

Keywords Multi-cast key distribution · Exposure resilience · Star topology · Backward secrecy

1 Introduction

HTML5 is an emerging technology for next-generation web applications [4]. Actually, web browser vendors support this new technology. Google said its Chrome browser would begin blocking Internet ads using Adobe's Flash tech, likely prompting advertisers to abandon the video format [25]. Similarly, Mozilla, the Firefox vendor, is encouraging developers to adopt HTML5 and not to use Flash [10].

In HTML5, we have a simple method using WebRTC [3] for a *full-mesh real-time communication topology* [37]. WebRTC provides the confidentiality of real-time transport protocol (RTP) [30] by using a key exchange and encrypted transport protocol, DTLS-SRTP [13], which has been suggested in IETF Draft [28]. In order to make the full-mesh-encrypted communication topology, WebRTC needs full-mesh DTLS key exchanges to establish all SRTP sessions. In brief, WebRTC clients must exchange the keys with $n-1$ users in the n clients case. This is very inefficient. Such key exchange protocols under the mesh topology are generally called group key exchange (GKE).

In this paper, we consider the *star topology* instead of the mesh topology for establishing the session key. In the star topology, each user communicates with a central authentication server, and users do not directly communicate with. Thus, it is possible to reduce costs of clients without depending on n, and therefore, WebRTC clients can do the key exchange part very efficiently. Key exchange protocols under the star (or tree) topology are generally called multi-cast key distribution (MKD) or group key management. Though the star topology can reduce the cost for clients, moving most of the burden to the server makes the server a natural target for a concentrated attack. Thus, the star topology is useful if the system is still secure when some part of secret information of the server is exposed by some attack.

1.1 Our contribution

In this paper, we propose a new *provably secure two-round dynamic* MKD (DMKD) protocol under the star topology with a central authentication server. Because of the star topol-

An extended abstract of this paper appeared in ProvSec 2016 [40].

✉ Kazuki Yoneyama
kazuki.yoneyama.sec@vc.ibaraki.ac.jp

[1] Ibaraki University, Ibaraki, Japan

[2] NTT Secure Platform Laboratories, Tokyo, Japan

Published online: 04 August 2017

ogy, each user does not directly communicate with other users. Instead, the central server communicates with users and distributes information for establishing the session key. If the server was malicious under the star topology, the session key could be known for the server by impersonating a user. Thus, we suppose that the server is honest-but-curious, and even the server must not know any information of the session key.

Each user has public information, called a *static public key (SPK)*, and the corresponding secret information, called a *static secret key (SSK)*. The SPK is also expected to be certified with user's ID through an infrastructure such as PKI. A user who wants to share a *session key* with other users exchanges *ephemeral public keys (EPKs)* that are generated from the corresponding session-specific randomness, called *ephemeral secret keys (ESKs)*, via the server.

The highlight of our protocol is as follows.

- *Dynamic group* Our protocol allows users to share the session key in the dynamic group manner. It means that, after establishing the session key among a group of users in a distribution phase, a set of users can join/leave the group without executing a new distribution phase among the new group. Users generate and keep state information for the join and leave phases at the end of the distribution phase. The join and leave phases of our protocol need smaller computation and communication costs than the distribution phase thanks to state information. Also, since the session key is refreshed after the join/leave phases, any information of the new session key is not exposed to leaving users.
- *Strong exposure resilience* In real-world applications, there are several situations that secret information is exposed. For example, if a pseudo-random number generator implemented in a system is poor, ESKs may be guessed to the adversary. Also, when some devices containing SSKs are lost, then a malicious person may use SSKs to know the session key generated by the owner. Furthermore, the government may order the server to reveal the SSK. Thus, it is desirable that DMKD protocols are resilient to secret key exposure attacks. Our protocol is secure even if either of SSKs or ESKs used to generate the session key are exposed. We call security when ESKs are exposed *ephemeral key exposure resilience*, and security when SSKs (including the server's) are exposed *strong server key forward secrecy*. To achieve ephemeral key exposure resilience, we use *the twisted pseudo-random function (PRF) trick* [15,21].
  Since our protocol adopts the star topology, the crack of the central server must be considered. If the server is attacked, all secret information may be leaked. Hence, we need *server key forward secrecy* which guarantees that even if all secret keys of the server are leaked, secrecy of session keys which are established before leakage of the server key is protected. Also, forward secrecy has two levels: one is weak forward secrecy and the other is strong forward secrecy. Weak forward secrecy guarantees secrecy of a session key only in the case that the adversary does not modify messages in the session. On the other hand, strong forward secrecy can guarantee secrecy of a session key even if the adversary modifies messages in the session. Thus, strong forward secrecy is more desirable than weak forward secrecy. Our protocol satisfies strong server key forward secrecy, while most of AKE protocols only satisfy weak forward secrecy.
  Moreover, our protocol guarantees a distinguished security property, called *time-based backward secrecy*. It means that if the session key is exposed at a time frame, the exposed session key is revoked when a new time frame begins. Time-based backward secrecy is very useful to resist real-time session key exposure attacks like malwares. We achieve time-based backward secrecy by formalizing the notion of the time frame in the security model and proposing a method to update the session key with a minimum cost.
- *Scalability* Most of previous GKE protocols are constructed under the mesh topology. A user must combine information from users in order to establish the session key with contributions of all users. Thus, the user needs to broadcast a message to all users (i.e. computation and communication costs depend on the number of users), or the round complexity depends on the number of users. Hence, if we adopt the mesh topology, it is difficult to achieve scalability. On the other hand, our DMKD protocol is constructed under the star topology. Though the server needs computation and communication costs depending on the number of users, users can share the session key with constant costs. The load of the server is actually not a problem because the server can be very powerful in computational resource and communication bandwidth. Conversely, users may have poor resources like a mobile device, and thus, scalability is very important in reality.

Also, we propose a first formal security model for DMKD. Our security model captures the star topology and several exposure resilience. In particular, to grasp time-based backward secrecy, the notion of time frames is formulated to define session freshness.

1.2 Related work

We revisit several related work of this work. We show a comparison among related works and our DMKD protocol in Table. 1.

Table 1 Comparison among related works and our DMKD protocol

	Topology	Exposure resilience?	Trust on central server	# of users	Computational complexity for user	Communication complexity for user
[1]	Mesh	No	None	3	$\mathcal{O}(n)$	$\mathcal{O}(n)$
[34]	Mesh	Yes	None	3	$\mathcal{O}(2^n)$	$\mathcal{O}(n)$
[38]	Mesh	No	None	General	$\mathcal{O}(n)$	$\mathcal{O}(n)$
[23]	Star	No	Fully trusted	General	$\mathcal{O}(\log n)$	$\mathcal{O}(\log n)$
[33]	Star	No	Semi-honest	General	$\mathcal{O}(1)$	$\mathcal{O}(n)$
Ours	Star	Yes	Semi-honest	General	$\mathcal{O}(1)$	$\mathcal{O}(1)$

1.2.1 Group key exchange

The first provably secure GKE protocol is proposed by Bresson et al. [7]. Their security model follows the ordinary indistinguishability-based 2-party AKE security model by Bellare and Rogaway [2]. Their protocol is not dynamic (i.e. the group member is fixed before starting sessions). Then, several dynamic GKE (DGKE) protocols and security models are proposed [5,6]. These protocols need a linear number of rounds. After that, several constant-round DGKE protocols are studied [12,20,38]. The seminal work of one-round GKE is the pairing-based tripartite AKE protocol introduced by Joux [17]. However, it is unauthenticated and subject to man-in-the-middle attacks. Many authenticated tripartite AKE protocols are studied [1].

Several flavours of security models are proposed to capture advanced security properties like forward secrecy against outside adversary [19] (i.e. assuming that the adversary is not part of the group), insider security [18] and key compromise impersonation resilience [16] (i.e. no adversary with the long-term private key of Alice can impersonate Bob to Alice without knowledge of Bob's long-term private key). Exposure resilience of GKE protocols is firstly considered in the security model by Manulis et al. [14,24]. Their model is based on the eCK model for 2-party AKE [22] and guarantees ephemeral key exposure resilience and weak forward secrecy. This security model is extended by Suzuki and Yoneyama [34] to grasp session state exposure. These protocols do not satisfy strong forward secrecy. Some GKE protocols satisfy strong forward secrecy as in [39]. Their protocol uses the compiler to provide strong forward secrecy for 2-party AKE [11]. Since these GKE protocols are considered under the mesh topology, no central server is required, but costs of users depend on the number of users. Also these are not for general group setting, but for three-party setting.

1.2.2 Multi-cast key distribution

Since the main application of MKD is mobile ad hoc networks (MANETs), most of MKD protocols use tree topology. The advantage of the tree-based MKD is that total communication complexity is reduced to $\mathcal{O}(\log n)$. For example, MKD protocols based on logical key hierarchies (LKH) [8,9,31,36] have been well studied. In LKH protocols, a binary tree of depth d having exactly n leaf nodes is constructed where n is the number of users such that $2^{d-1} < n < 2^d$. The n leaf nodes of the binary tree correspond to the n users. There is a key associated with every node in the tree where $k(X)$ is the key for node X. The group key is $k(R)$ where R is the root node of the tree. User U is given the $d+1$ keys belonging to the nodes that lie on the unique path from U to R. Therefore, each user needs to have $\mathcal{O}(\log n)$ keys.

There are few papers studying MKD in the star topology [23,27,29,33]. The motivation of previous star topology-based MKD protocols is to reduce the rekeying cost of tree topology-based MKD protocols. For example, in the protocol in [23] there is no need for rekeying when a member joins and leaves the group. However, the secret key is calculated by the key server and then is unicast to every group member separately. Therefore, it increases the burden on the server. In another star topology-based MKD schemes like in [29], secret keys are calculated by the group members. This eliminates the need to unicast the secret keys to every member separately, henceforth reducing the load on the server. However, most of these protocols have no formal security proof, and the central server must be fully trusted. Sun et al. [33] propose a provably secure star topology-based MKD protocol with the semi-honest central server. Their security model does not capture exposure resilience, and their protocol is not scalable because communication complexity for uses depends on the number of users. A formal security model for MKD protocols is introduced by Micciancio and Panjwani [26]. However, their model allows the server to know the session key shared by users. Also, exposure resilience is not considered.

2 Preliminaries

2.1 Notations

Throughout this paper we use the following notations. If Set is a set, then by $m \in_R \mathsf{Set}$ we denote that m is sampled

uniformly from Set. If **ALG** is an algorithm, then by $y \leftarrow \mathbf{ALG}(x; r)$ we denote that y is output by **ALG** on input x and randomness r (if **ALG** is deterministic, r is empty).

2.2 Pseudo-random function and twisted pseudo-random function trick

Let κ be a security parameter and $\mathsf{F} = \{F_\kappa : Dom_\kappa \times Kspace_\kappa \rightarrow Rng_\kappa\}_\kappa$ be a function family with a family of domains $\{Dom_\kappa\}_\kappa$, a family of key spaces $\{Kspace_\kappa\}_\kappa$ and a family of ranges $\{Rng_\kappa\}_\kappa$.

Definition 1 (*Pseudo-random Function*) We say that function family $\mathsf{F} = \{F_\kappa\}_\kappa$ is the PRF family, if for any PPT distinguisher $\mathcal{D}$, $|\Pr[1 \leftarrow \mathcal{D}^{F_\kappa(\cdot)}] - \Pr[1 \leftarrow \mathcal{D}^{RF_\kappa(\cdot)}]| \leq negl$, where $RF_\kappa : Dom_\kappa \rightarrow Rng_\kappa$ is a truly random function.

Next, we show the notion of the twisted PRF [15]. The twisted PRF $tPRF$ is a function that $tPRF : \{0,1\}^\kappa \times Kspace_\kappa \times \{0,1\}^\kappa \times Kspace_\kappa \rightarrow Rng_\kappa$. We construct $tPRF(a, a', b, b') := F_\kappa(a, b) \oplus F_\kappa(b', a')$ with PRF F_κ, where $a, b' \in \{0,1\}^\kappa$ and $a', b \in Kspace_\kappa$. The twisted PRF is used to guarantee that $tPRF(a, a', b, b')$ looks random even if either (a, a') or (b, b') is exposed.

Lemma 1 (Theorem 1 in [21]) *If F_κ is PRF, then*

- $[(a, a'), tPRF(a, a', b, b')]$ *is indistinguishable from* $[(a, a'), R]$ *where R is randomly chosen from Rng_κ, and*
- $[(b, b'), tPRF(a, a', b, b')]$ *is indistinguishable from* $[(b, b'), R]$ *where R is randomly chosen from Rng_κ.*

2.3 Target collision resistant hash function

We say a function $TCR : Dom \rightarrow Rng$ is a target collision resistant (TCR) hash function if the following condition holds for security parameter κ: for any PPT adversary $\mathcal{A}$, $\Pr[x \in_R Dom; x' \leftarrow \mathcal{A}(x) \text{ s.t. } x \neq x' \wedge TCR(x) = TCR(x')] \leq negl$.

2.4 Public key encryption

Definition 2 (*Syntax for Public Key Encryption Schemes*) A PKE scheme consists of the following 3-tuple (**Gen**, **Enc**, **Dec**):

- **Gen** : a key generation algorithm which on input 1^κ, where κ is the security parameter, outputs a pair of public and secret keys (pk, sk).
- **Enc** : an encryption algorithm which takes as input public key pk and plaintext m outputs ciphertext CT.
- **Dec** : a decryption algorithm which takes as input secret key sk and ciphertext CT outputs plaintext m or rejection symbol $\perp$.

Definition 3 (*Chosen-Ciphertext Security for Public Key Encryption*) A PKE scheme is CCA-secure if the following property holds for security parameter κ: for any adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, $|\Pr[(pk, sk) \leftarrow \mathbf{Gen}(1^\kappa); (m_0, m_1, state) \leftarrow \mathcal{A}_1^{\mathcal{DO}(sk,\cdot)}(pk); b \in_R \{0,1\}; CT^* \leftarrow \mathbf{Enc}(pk, m_b); b' \leftarrow \mathcal{A}_2^{\mathcal{DO}(sk,\cdot)}(pk, CT^*, state); b' = b] - 1/2| \leq negl(\kappa)$, where $\mathcal{DO}$ is the decryption oracle which outputs m or $\perp$ on receiving CT and $state$ is state information (possibly including pk, m_0 and m_1) which $\mathcal{A}$ wants to preserve. $\mathcal{A}$ cannot submit the ciphertext $CT = CT^*$ to $\mathcal{DO}$.

The CCA security means that the adversary can pose queries to decryption oracle $\mathcal{DO}$ after receiving the challenge ciphertext because $\mathcal{A}_2$ can access $\mathcal{DO}$.

2.5 Ciphertext-policy attribute-based encryption

Definition 4 (*Syntax for Ciphertext-Policy Attribute-based Encryption Schemes*) A CP-ABE scheme consists of the following 4-tuple (**Setup**, **Der**, **AEnc**, **ADec**):

$(Params, msk) \leftarrow \mathbf{Setup}(1^\kappa, att)$: a setup algorithm which on inputs 1^κ and att, where κ is the security parameter and att is an attribute universe description, outputs a public parameter $Params$ and a master secret key msk.
$usk_A \leftarrow \mathbf{Der}(Params, msk, A)$: a key derivation algorithm which on input $Params$, msk and attribute A outputs a user secret key usk_A.
$CT \leftarrow \mathbf{AEnc}(Params, P, m)$: an encryption algorithm which on input $Params$, an access structure P and a plaintext m outputs a ciphertext CT.
$m \leftarrow \mathbf{ADec}(Params, usk_A, CT)$: a decryption algorithm which on input usk_A and CT outputs plaintext m if A satisfies P.

Definition 5 (*Chosen-Ciphertext Security for Ciphertext-Policy Attribute-based Encryption*) A CP-ABE scheme is CCA-secure if the following property holds for security parameter κ: for any PPT adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, $|\Pr[(Params, msk) \leftarrow \mathbf{Setup}(1^\kappa, att); (m_0, m_1, P^*, s) \leftarrow \mathcal{A}_1^{\mathcal{EO}(Params,msk,\cdot),\mathcal{DO}(Params,usk_\cdot,\cdot)}(Params); b \in_R \{0,1\}; CT^* \leftarrow \mathbf{AEnc}(Params, P^*, m_b); b' \leftarrow \mathcal{A}_2^{\mathcal{EO}(Params,msk,\cdot),\mathcal{DO}(Params,usk_\cdot,\cdot)}(Params, CT^*, s); b' = b] - 1/2| \leq negl$, where $\mathcal{EO}$ is the key extraction oracle, $\mathcal{DO}$ is the decryption oracle, and s is state information that $\mathcal{A}$ wants to preserve from $\mathcal{A}_1$ to $\mathcal{A}_2$. $\mathcal{A}$ cannot submit sets of attributes which satisfy P^* to $\mathcal{EO}$ and the ciphertext CT^* to $\mathcal{DO}$.

We say a CP-ABE scheme is CPA-secure if $\mathcal{A}$ does not access $\mathcal{DO}$. Also, we say a CP-ABE scheme is selectively secure if the adversary must commit P^* before **Setup**.

2.6 Message authentication codes

Definition 6 (*Syntax for Message Authentication Codes*) A MAC scheme consists of the following 3-tuple (**MGen**, **Tag**, **Ver**):

MGen : a key generation algorithm which on input 1^κ, where κ is the security parameter, outputs a MAC key mk.
Tag : a tagging algorithm which on input mk and plaintext m outputs an authentication tag σ.
Ver : a verification algorithm which on input mk, m and σ outputs 1 if accepts, 0 otherwise.

Definition 7 (*Unforgeability against Chosen-Message Attacks for Message Authentication Codes*) A MAC scheme is UF-CMA if the following property holds for security parameter κ: for any PPT forger $\mathcal{A}$, $\Pr[mk \leftarrow \mathbf{MGen}(1^\kappa); (m^*, \sigma^*) \leftarrow \mathcal{A}^{\mathcal{MO}(mk,\cdot)}; 1 \leftarrow \mathbf{Ver}(mk, m^*, \sigma^*)] \leq negl$, where $\mathcal{MO}$ is the MAC oracle. $\mathcal{A}$ cannot submit m^* to $\mathcal{MO}$.

2.7 Decisional Diffie–Hellman assumption

Definition 8 (*Decisional Diffie–Hellman Assumption*) Let p be a prime, and let g be a generator of a finite cyclic group G of order p. We define two experiments: $\mathsf{Exp}_{g,p}^{ddh\text{-}real}(\mathcal{D})$ and $\mathsf{Exp}_{g,p}^{ddh\text{-}rand}(\mathcal{D})$. For a distinguisher $\mathcal{D}$, inputs $(g,\ A = g^a,\ B = g^b,\ C)$ are provided, where $(a, b) \in_R (\mathbb{Z}_p)^2$. $C = g^{ab}$ in $\mathsf{Exp}_{g,p}^{ddh\text{-}real}(\mathcal{D})$ and $C = g^c$ in $\mathsf{Exp}_{g,p}^{ddh\text{-}rand}(\mathcal{D})$, where $c \in_R \mathbb{Z}_p$. Let $(g,\ A = g^a,\ B = g^b,\ C = g^{ab})$ be the tuple in $\mathsf{Exp}_{g,p}^{ddh\text{-}real}(\mathcal{D})$ and $(g,\ A = g^a,\ B = g^b,\ C = g^c)$ be the tuple in $\mathsf{Exp}_{g,p}^{ddh\text{-}rand}(\mathcal{D})$. We say that the DDH assumption in G holds for security parameter κ if for any PPT distinguisher $\mathcal{D}$ $|\Pr[\mathsf{Exp}_{g,p}^{ddh\text{-}real}(\mathcal{D}) = 1] - \Pr[\mathsf{Exp}_{g,p}^{ddh\text{-}rand}(\mathcal{D}) = 1]| \leq negl$.

3 Security definition

In this section, we introduce a new security definition of DMKD under the star topology. Our definition captures strong exposure resilience and time-based forward secrecy. The model is based on [34,35,38].

3.1 Protocol participants and initialization

Let $\mathcal{U} := \{U_1, \ldots, U_N\}$ be a set of potential protocol users. Each user U_i is modelled as a PPT Turing machine w.r.t. security parameter κ. For user U_i, we denote static secret (public) key by SSK_i (SPK_i). U_i generates its own keys, SSK_i and SPK_i, and the static public key SPK_i is linked with U_i's identity in some systems like PKI. Each user U_i and the authentication server S are connected by the unauthenticated star topology. That is, they do communications through an unicast channel over an insecure network like the Internet. Users do not directly communicate. S is also modelled as a PPT Turing machine. S has the static secret key by SSK_S and the static public key SPK_S.

3.2 Session and state information

There are three phases (Dist, Join, Leave) for DMKD. Dist means the session key distribution phase that a new group is established and a session key is generated for users in the group. Join means the user joining phase that a set of new users join an established group and a session key is re-generated for users in the new group. Leave means the user leaving phase that a set of users leave an established group and a session key is re-generated for remaining users in the group. An invocation of a phase is called a *session*. We suppose that a session contains n users $\{U_{i_1}, \ldots, U_{i_n}\}$, where $2 \leq n \leq N$. Let Π be a phase identifier such that $\Pi \in \{\mathsf{Dist}, \mathsf{Join}, \mathsf{Leave}\}$. A session owned by user instance $U_{i_\ell}^{j_\ell}$ is managed by a tuple $(\Pi, U_{i_\ell}^{j_\ell}, \{U_{i_1}^{j_1}, \ldots, U_{i_n}^{j_n}\})$. $U_{i_\ell}^{j_\ell}$ means the j_ℓth instance of U_{i_ℓ}. Sessions owned by user instances $\{U_{i_1}^{j_1}, \ldots, U_{i_{\ell-1}}^{j_{\ell-1}}, U_{i_{\ell+1}}^{j_{\ell+1}}, \ldots, U_{i_n}^{j_n}\}$ are called matching sessions of the session of $U_{i_\ell}^{j_\ell}$. Hereafter, for simplicity, we can describe U_{i_ℓ} as U_i without loss of generality. We suppose that the total number of sessions in the system is $\ell_{\max}$. We consider the notion of *time frames*. Each user U_i and S communicate to update some state information $state_i$ when the session is firstly executed in a time frame. Hereafter, U_i uses $state_i$ in sessions within the time frame. Also, we consider the session key update based on time frames. Update means the session key update phase that the shared session key is updated when a new time frame begins. If a session key is shared in the Dist/Join/Leave phase in the past time frame, the session key is updated by Update. We note that the session is not changed after Update phase, but only the session key is changed. In Dist phase, U_i^j generates ephemeral secret key ESK_i^j and sends ephemeral public key EPK_i^j to S. When S receives all EPK_i^j for $i, j = 1, \ldots, n$, then S returns messages to users. Users and S repeat some rounds, and then users finally share session key SK and complete the session. After completing the session, each user U_i updates $state_i$ to remain necessary information for Update, Join and Leave phases. $state_i$ is passed to another inactivated instance $U_i^{j'}$ to participate in the next activation of Update, Join or Leave phase. Similarly, in Update, Join and Leave phases, users and S execute some interactions and users update the session key. DMKD consists of many concurrent executions of Dist, Update, Join and Leave phases.

3.3 Adversary

The adversary $\mathcal{A}$, which is modelled as a PPT Turing machine, controls all communications between parties including session activation and registrations of users by performing the following adversary queries.

- Establish(U_i, SPK_i): This query allows $\mathcal{A}$ to introduce a new user. In response, if $U_i \notin \mathcal{U}$ (due to the uniqueness of identities) then U_i with the static public key SPK_i is added to $\mathcal{U}$. Note that $\mathcal{A}$ is not required to prove the possession of the corresponding secret key SSK_i. If a party is registered by a Establish query issued by $\mathcal{A}$, then we call the party *dishonest*. If not, we call the party *honest*.
- Send(U_i^j, $message$): This query allows $\mathcal{A}$ to send $message$ to instance U_i^j. $message$ includes $\Pi \in$ {Dist, Join, Leave}. $\mathcal{A}$ obtains the response from U_i^j. If U_i^j is an inactivated instance and $\Pi =$ {Join, Leave}, $state_i$ is passed to U_i^j.

To capture exposure of secret information, the adversary $\mathcal{A}$ is allowed to issue the following queries.

- SessionReveal(U_i^j): The adversary $\mathcal{A}$ obtains the session key SK for the session owned by U_i^j if the session is completed.
- StateReveal(U_i): The adversary $\mathcal{A}$ obtains current state information $state_i$ of U_i. State information does not include the static secret key.
- ServerReveal: This query allows the adversary $\mathcal{A}$ to obtain static secret key SSK_S of the server S.
- StaticReveal(U_i): This query allows the adversary $\mathcal{A}$ to obtain static secret key SSK_i of the user U_i.
- EphemeralReveal(U_i^j): This query allows the adversary $\mathcal{A}$ to obtain ephemeral secret key ESK_i^j of U_i^j if the session is not completed (i.e. the session key is not established yet).

3.4 Freshness

For the security definition, we need the notion of freshness.

Definition 9 (*Freshness*) Let $\mathsf{sid}^* = (\Pi, U_i^j, \{U_{i_1}^{j_1}, \ldots, U_{i_n}^{j_n}\})$ be a completed session among *honest* users $\{U_1, \ldots, U_n\}$, which is owned by U_i^j. Let $\overline{\mathsf{sid}^*}$ be a matching session of sid^*. We say session sid^* is *fresh* if none of the following conditions hold:

1. The adversary $\mathcal{A}$ issues either of SessionReveal(U_i^j) or SessionReveal($U_{i'}^{j'}$) for any $\overline{\mathsf{sid}^*}$ in the current time frame,
2. The adversary $\mathcal{A}$ issues either of SessionReveal(U_i^j) or SessionReveal($U_{i'}^{j'}$) for any $\overline{\mathsf{sid}^*}$ in the past time frame if $\mathcal{A}$ issues either of ServerReveal, StaticReveal(U_i) or StaticReveal($U_{i'}$),
3. The adversary $\mathcal{A}$ issues ServerReveal before completing sid^*,
4. The adversary $\mathcal{A}$ makes either of StateReveal(U_i) or StateReveal($U_{i'}$) in the current time frame or any of its ancestors[1],
5. The adversary $\mathcal{A}$ makes either of StaticReveal(U_i) before completing sid^* or StaticReveal($U_{i'}$) before completing $\overline{\mathsf{sid}^*}$ for any $\overline{\mathsf{sid}^*}$,
6. The adversary $\mathcal{A}$ makes both of StaticReveal(U_i) and EphemeralReveal(U_i^j), and
7. The adversary $\mathcal{A}$ makes both of StaticReveal($U_{i'}$) and EphemeralReveal($U_{i'}^{j'}$) for any $\overline{\mathsf{sid}^*}$.

We note that if both EphemeralReveal(U_i^j) and StaticReveal(U_i) are posed, then we regard that StateReveal(U_i) in the time frame for instance U_i^j is also posed because $state_i$ in the time frame is trivially derived from ESK_i^j and SSK_i.

3.5 Security experiment

For the security definition, we consider the following security experiment. Initially, the adversary $\mathcal{A}$ is given a set of honest users and makes any sequence of the queries described above. During the experiment, the adversary $\mathcal{A}$ makes the following query.

- Test(sid^*): Here, sid^* must be a fresh session. Select random bit $b \in_R \{0, 1\}$, and return the session key held by sid^* if $b = 0$, and return a random key if $b = 1$.

The experiment continues until the adversary $\mathcal{A}$ makes a guess b'. The adversary $\mathcal{A}$ *wins* the game if the test session sid^* is still fresh and if the guess of the adversary $\mathcal{A}$ is correct, i.e. $b' = b$. The advantage of the adversary $\mathcal{A}$ is defined as $\mathbf{Adv}^{\mathrm{dmkd}}(\mathcal{A}) = \Pr[\mathcal{A}\ wins] - \frac{1}{2}$. We define the security as follows.

Definition 10 (DMKD *Security*) We say that a DMKD protocol Π is *secure in the* DMKD *model* if the following conditions hold:

1. If two honest parties complete matching sessions, then, except for negligible probability, they both compute the same session key.
2. For any PPT adversary $\mathcal{A}$, $\mathbf{Adv}^{\mathrm{dmkd}}(\mathcal{A})$ is negligible in security parameter κ for the test session sid^*.

[1] We say that $state_i$ is an ancestor of $state_{i'}$ if there exists a path $(state_i, \ldots, state_{i'})$ such that each state in the path is updated to the next one.

3.6 Summary of our security definition

Here, we give an intuition of security properties captured by our security definition.

- *Ephemeral key exposure resilience* The adversary can obtain ESKs of users by EphemeralReveal queries. From the freshness definition, when the adversary does not pose StaticReveal(U_i) where U_i is the owner of the test session, then the adversary can pose EphemeralReveal(U_i^j) where the jth session of U_i is the test session. Thus, it guarantees that the session key is still secure even if $ESKs$ used to generate the session key are *totally exposed*.
- *Time-based backward secrecy* The adversary can obtain the session key of the test session by SessionReveal queries if the session key was generated at a past time frame. Generally, if the session key of the test session is exposed, the adversary easily distinguishes the real session key from a random key. In our security model, we introduce the notion of the time frame and consider the Update phase. Thus, when a new time frame begins, the session key may be updated. Hence, it guarantees that the updated session key looks independent from past session keys even in the test session.
- *Strong server key forward secrecy* The adversary can obtain both SSKs of users and the server by StaticReveal and ServerReveal queries. From the freshness definition, when the adversary does not pose EphemeralReveal queries for the test session, then the adversary can pose StaticReveal and ServerReveal for users in the test session after completion of the session.[2] Hence, it guarantees that past session keys are still secure even if SSKs of users and the server are exposed. Also, the adversary is allowed to modify messages in the test session (i.e. there is a non-matching session) regardless of posing StaticReveal or ServerReveal. Thus, while in most of AKE protocols only weak forward secrecy is guaranteed (i.e. the adversary is prohibited to pose StaticReveal for non-matching sessions), our security model guarantees strong forward secrecy.

4 New dynamic multi-cast key distribution protocol under star topology

In this section, we show a DMKD protocol under the star topology. In the Dist phase, a group of users shares a session key with the help of the central server. In the Join phase, new users can join the group that previously established the session key with lower costs than executing a Dist phase by the new group members. In the Leave phase, a subset of group users leaves from the group with lower costs than executing a Dist phase by the remaining group members. After establishing the session key, users can update the key at a new time frame. In the Update phase, the server sends information to refresh the session key to users, and users can locally update the key.

For simplicity, we show a simple setting that only one user joins/leaves the group simultaneously. We show the general setting that multiple users can join/leave the group simultaneously in Sect. 7.

4.1 Design principle

The session key in our protocol is generated from two key materials K_1 and K_2. K_1 guarantees ephemeral key exposure resilience and strong server key forward secrecy, and K_2 guarantees time-based backward secrecy. Here, we give an intuition of the design of our protocol.

The way to share K_1 is based on the ring structure and is similar to the previous dynamic group key exchange protocol (the YT protocol) [38]. In the YT protocol, each user broadcasts g^{r_i} in Round 1 and computes $g^{r_{i-1}r_i}$ and $g^{r_ir_{i+1}}$. Then, the left key $K_i^{(l)}$ based on $g^{r_{i-1}r_i}$ and the right key $K_i^{(r)}$ based on $g^{r_ir_{i+1}}$ are generated, and each user broadcasts $K_i^{(l)} \oplus K_i^{(r)}$ in Round 2. Also, a representative user generates k and broadcasts the masked k with his left key to all users. Then, each user can recover the left and right keys for all group members with his/her $K_i^{(l)}$ and $K_i^{(r)}$. Thus, they can share k and generate K_1 based on k. However, we cannot simply apply the YT protocol to our protocol. First, the YT protocol is insecure if ESKs of users are exposed, that means ephemeral key exposure resilience is not satisfied. The other problem is scalability. To broadcast messages and to compute k, both communication and computational complexity of each user depend on the number of users, and thus, if the YT protocol uses very large system, the load of users increases. Therefore, achieving both exposure resilience and scalability is not an easy task.

We can solve the first problem on ephemeral key exposure resilience by using the twisted PRF trick. We use outputs of the twisted PRF based on the SSK and the ESK instead of all randomness of users in our protocol. From Lemma 1, it is guaranteed that an output of the twisted PRF is indistinguishable from the random value unless both SSK and ESK are exposed. The freshness definition also guarantees that both SSK and ESK are not exposed in the test session. Therefore, our protocol satisfies ephemeral key exposure resilience. Also, we can solve the second problem on scalability thanks to the difference of the network topology. In the YT pro-

[2] If the adversary poses StaticReveal or ServerReveal before completion of the test session, then the session key is trivially distinguished from a random key. Also, it means that the server is honest-but-curious.

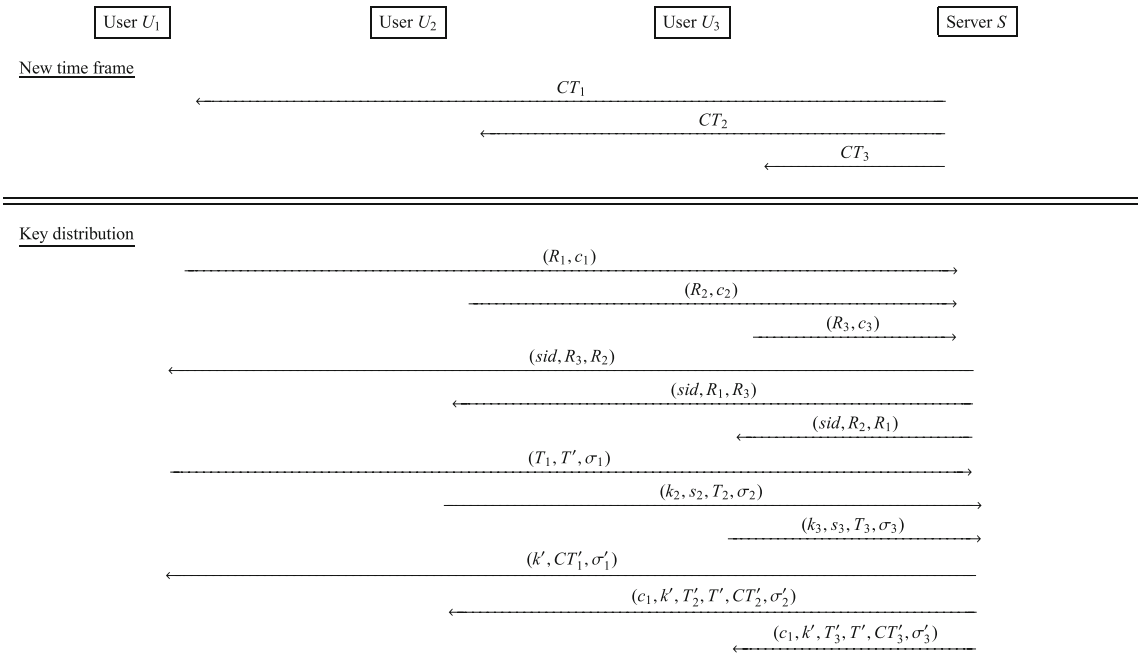

Fig. 1 Dist phase for the case of $N = 3$

tocol, each user must communicate with other users directly because of the mesh topology, and all costs inevitably depend on the number of users. On the other hand, in our protocol, each user only communicates with the server because of the star topology. Thus, we can confine commutation depending on the number of users to the server in our protocol. The server only sends a constant number of messages to each user. Therefore, communication and computational complexity of each user do not depend on the number of users, and thus, our protocol is scalable. We note that complexity of the server depends on the number of users; however, it is inevitable and not serious because the server has sufficient computational power and communication bandwidth in reality.

The other key material, K_2, is generated by the server. It is encrypted by a CP-ABE scheme with the access structure that the ID is of the recipient and the time is within the current time frame. Since for every time frame each user receives a new decryption key with attribute of his/her ID and the current time, K_2 can be decrypted if the ID of the recipient is valid and the decryption key is sent at the same time frame. The new decryption key is stored as state information. After generating the session key, when a new time frame begins, the server sends the encrypted form of new K_2 and each user locally updates the session key. Though the adversary can pose StateReveal queries, the freshness definition guarantees that state information of the test session in the current time frame or any of its ancestors is not exposed. Thus, even if the adversary obtains session keys at past time frames, the session key at the current time frame is still secure. Therefore, our protocol satisfies time-based backward secrecy.

4.2 System setup

S runs the setup algorithm **Setup** of CP-ABE and generates a public parameter $Params$ and a master secret key msk. Let p be a κ-bit prime and G be a finite cyclic group of order p with generator g, h. Let $TCR : \{0,1\}^* \to \{0,1\}^\kappa$ be a TCR hash function. Let $tPRF : \{0,1\}^\kappa \times Kspace_\kappa \times \{0,1\}^\kappa \times Kspace_\kappa \to \mathbb{Z}_p$ and $tPRF' : \{0,1\}^\kappa \times Kspace_\kappa \times \{0,1\}^\kappa \times Kspace_\kappa \to Kspace_\kappa$ be twisted PRFs. Let $F : \{0,1\}^\kappa \times G \to \mathbb{Z}_p^2$, $F' : \{0,1\}^\kappa \times \mathbb{Z}_p \to Kspace_\kappa$ and $F'' : \{0,1\}^\kappa \times Kspace_\kappa \to \{0,1\}^\kappa$, $F''' : \{0,1\}^\kappa \times Kspace_\kappa \to \mathbb{Z}_p$ be PRFs. S stores msk as SSK_S and publishes $(Params, p, G, g, h, TCR, tPRF, tPRF', F, F', F'', F''')$ as SPK_S.

There are N users $U_1 \ldots, U_N$. Each user U_i runs the key generation algorithm of PKE **Gen** and generates a public key pk_i and a secret key sk_i. Also, U_i generates secret strings for the twisted PRF (st_i, st'_i) and (st_S, st'_S), where $st_i, st_S \in_R$ Kspace_κ and $st'_i, st'_S \in_R \{0,1\}^\kappa$. U_i stores (sk_i, st_i, st'_i) as SSK_i and publishes pk_i as SPK_i.

4.3 Dist phase

A set of users $U_{i_1}, \ldots, U_{i_n}$ $(n \leq N)$ starts a new session and shares a session key. For simplicity, w.l.o.g., we suppose that $(U_{i_1}, \ldots, U_{i_n}) = (U_1, \ldots, U_n)$. We illustrate the message flow of Dist phase for the case of $N = 3$ in Fig.1.

(State Update at New Time Frame) If the session is the first session for U_i at the time frame TF,

then for the current time $time$ S generates $usk_i \leftarrow \mathbf{Der}(Params, msk, A_i)$ with attribute $A_i = (U_i, time)$ and $mk_i \leftarrow \mathbf{MGen}$ and computes $CT_i \leftarrow \mathbf{Enc}_{pk_i}(usk_i, mk_i)$. Then, S sends CT_i to U_i, and U_i obtains $(usk_i, mk_i) \leftarrow \mathbf{Dec}_{sk_i}(CT_i)$ and updates (usk_i, mk_i) in $state_i$.
(Round 1 for Users) U_i generates $\tilde{r}_i \in_R \{0,1\}^\kappa$, $\tilde{r}'_i \in_R \mathsf{Kspace}_\kappa$, $\tilde{k}_i \in_R \{0,1\}^\kappa$, $\tilde{k}'_i \in_R \mathsf{Kspace}_\kappa$, $\tilde{s}_i \in_R \{0,1\}^\kappa$ and $\tilde{s}'_i \in_R \mathsf{Kspace}_\kappa$ as ESK_i and computes $r_i = tPRF(\tilde{r}_i, \tilde{r}'_i, st_i, st'_i)$, $k_i = tPRF(\tilde{k}_i, \tilde{k}'_i, st_i, st'_i)$ and $s_i = tPRF(\tilde{s}_i, \tilde{s}'_i, st_i, st'_i)$. Then, U_i computes $R_i = g^{r_i}$ and $c_i = g^{k_i} h^{s_i}$ and sends (R_i, c_i) to S.
(Round 1 for Server) On receiving (R_i, c_i) from all users, S computes $sid = TCR(c_1, \ldots, c_n)$ and chooses a representative user from $(U_1, \ldots, U_n)$. Here, w.l.o.g., we suppose that U_1 is the representative user. For $i \in [1, n]$, S sends (sid, R_{i-1}, R_{i+1}) to U_i. Also, S notices that U_1 is the representative user.
(Round 2 for Users) For $i \in [2, n]$, on receiving (sid, R_{i-1}, R_{i+1}), U_i computes $K_i^{(l)} = F(sid, R_{i-1}^{r_i})$, $K_i^{(r)} = F(sid, R_{i+1}^{r_i})$ and $T_i = K_i^{(l)} \oplus K_i^{(r)}$. Then, U_i computes $\sigma_i \leftarrow \mathbf{Tag}_{mk_i}(R_i, c_i, R_{i-1}, R_{i+1}, k_i, s_i, T_i, U_i, sid)$ and sends $(k_i, s_i, T_i, \sigma_i)$ to S.
On receiving (sid, R_n, R_2), U_1 computes $K_1^{(l)} = F(sid, R_n^{r_1})$, $K_1^{(r)} = F(sid, R_2^{r_1})$, $T_1 = K_1^{(l)} \oplus K_1^{(r)}$ and $T' = K_1^{(l)} \oplus (k_1 || s_1)$. Then, U_1 computes $\sigma_1 \leftarrow \mathbf{Tag}_{mk_1}(R_1, c_1, R_n, R_2, T_1, T', U_1, sid)$ and sends (T_1, T', σ_1) to S.
(Round 2 for Server) On receiving (T_1, T', σ_1) and $(k_i, s_i, T_i, \sigma_i)$, S verifies $\mathbf{Ver}_{mk_1}(R_1, c_1, R_n, R_2, T_1, T', U_1, sid, \sigma_1)$ and $\mathbf{Ver}_{mk_i}(R_i, c_i, R_{i-1}, R_{i+1}, k_i, s_i, T_i, U_i, sid, \sigma_i)$, and if the verification fails, then aborts. Also, for $i \in [2, n]$, S checks if $c_i = g^{k_i} h^{s_i}$ holds, and if the verification fails, then aborts. S generates $\tilde{k}_S \in_R \{0,1\}^\kappa$, $\tilde{k}'_S \in_R \mathsf{Kspace}_\kappa$, $\tilde{K}_1 \in_R \{0,1\}^\kappa$ and $\tilde{K}'_1 \in_R Kspace_\kappa$ as ESK_S and computes $k_S = tPRF(\tilde{k}_S, \tilde{k}'_S, st_S, st'_S)$, $K_1 = tPRF'(\tilde{K}_1, \tilde{K}'_1, st_S, st'_S)$ and $k' = (\bigoplus_{2 \le i \le n} k_i) \oplus k_S$. For $i \in [2, n]$, S computes $T'_i = \bigoplus_{1 \le j \le i-1} T_j$. For $i \in [1, n]$, S computes $CT'_i \leftarrow \mathbf{AEnc}(Params, P_i, K_1)$ with access structure $P_i := (ID = U_i) \wedge (time \in TF)$. S computes $\sigma'_1 \leftarrow \mathbf{Tag}_{mk_1}(R_1, c_1, R_n, R_2, T_1, T', U_1, sid, k', CT'_1)$ and sends (k', CT'_1, σ'_1) to U_1. For $i \in [2, n]$, S computes $\sigma'_i \leftarrow \mathbf{Tag}_{mk_i}(R_i, c_i, R_{i-1}, R_{i+1}, k_i, s_i, T_i, U_i, sid, c_1, k', T'_i, T', CT'_i)$ and sends $(c_1, k', T'_i, T', CT'_i, \sigma'_i)$ to U_i.
(Session Key Generation and Post-computation) For $i \in [2, n]$, on receiving $(c_1, k', T'_i, T', CT'_i, \sigma'_i)$, U_i verifies $\mathbf{Ver}_{mk_i}(R_i, c_i, R_{i-1}, R_{i+1}, k_i, s_i, T_i, U_i, sid, c_1, k', T'_i, T', CT'_i, \sigma'_i)$, and if the verification fails, then aborts. U_i computes $K_1^{(l)} = T'_i \oplus K_i^{(l)}$ and $k_1 || s_1 = T' \oplus K_1^{(l)}$, and checks if $c_1 = g^{k_1} h^{s_1}$ holds, and if the verification fails, then aborts. U_i decrypts $K_1 \leftarrow \mathbf{ADec}_{usk_i}(CT'_i, P_i)$, computes $K_2 = F'(sid, k' \oplus k_1)$ and outputs the session key $SK = F''(sid, K_1) \oplus F''(sid, K_2)$. As state information, U_i adds sid, $H_i^{(l)} = R_{i-1}^{r_i}$, $H_i^{(r)} = R_{i+1}^{r_i}$ and $r = F'''(sid, K_1) \oplus F'''(sid, K_2)$ to $state_i$.
On receiving (k', CT'_1, σ'_1), U_1 verifies $\mathbf{Ver}_{mk_1}(R_1, c_1, R_n, R_2, T_1, T', U_1, sid, k', CT'_1, \sigma'_1)$, and if the verification fails, then aborts. U_1 decrypts $K_1 \leftarrow \mathbf{ADec}_{usk_1}(CT'_1, P_1)$, computes $K_2 = F'(sid, k' \oplus k_1)$ and outputs the session key $SK = F''(sid, K_1) \oplus F''(sid, K_2)$. As state information, U_1 adds sid, $H_1^{(l)} = R_n^{r_1}$, $H_1^{(r)} = R_2^{r_1}$ and $r = F'''(sid, K_1) \oplus F'''(sid, K_2)$ to $state_1$.

4.4 Join phase

A user $U_{i_{n+1}}$ joins an established session by $U_1, \ldots, U_n$. W.l.o.g., we suppose that $U_{i_{n+1}} = U_{n+1}$.

In the Join phase, users U_i for $i \in [2, n-1]$ can reduce computation than the Dist phase. They do not need to compute g^{r_i}. The ring structure to compute K_1 still works because r in $state_i$ is used to connect the ring instead of using r_i. We illustrate the message flow of Join phase for the case of $N = 3$ in Fig.2.

(State Update at New Time Frame) If the session is the first session for U_i at the time frame TF', then for the current time $time$ S generates $usk_i \leftarrow \mathbf{Der}(Params, msk, A_i)$ with attribute $A_i = (U_i, time)$ and $mk_i \leftarrow \mathbf{MGen}$ and computes $CT_i \leftarrow \mathbf{Enc}_{pk_i}(usk_i, mk_i)$. Then, S sends CT_i to U_i, and U_i obtains $(usk_i, mk_i) \leftarrow \mathbf{Dec}_{sk_i}(CT_i)$ and updates (usk_i, mk_i) in $state_i$.
(Round 1 for Users) For $i \in \{1, n, n+1\}$, U_i generates $\tilde{r}_i \in_R \{0,1\}^\kappa$, $\tilde{r}'_i \in_R \mathsf{Kspace}_\kappa$, $\tilde{k}_i \in_R \{0,1\}^\kappa$, $\tilde{k}'_i \in_R \mathsf{Kspace}_\kappa$, $\tilde{s}_i \in_R \{0,1\}^\kappa$ and $\tilde{s}'_i \in_R \mathsf{Kspace}_\kappa$ as ESK_i and computes $r_i = tPRF(\tilde{r}_i, \tilde{r}'_i, st_i, st'_i)$, $k_i = tPRF(\tilde{k}_i, \tilde{k}'_i, st_i, st'_i)$ and $s_i = tPRF(\tilde{s}_i, \tilde{s}'_i, st_i, st'_i)$. U_i computes $R_i = g^{r_i}$ and $c_i = g^{k_i} h^{s_i}$ and sends (R_i, c_i) to S.
For $i \in [2, n-1]$, U_i generates $\tilde{k}_i \in_R \{0,1\}^\kappa$, $\tilde{k}'_i \in_R \mathsf{Kspace}_\kappa$, $\tilde{s}_i \in_R \{0,1\}^\kappa$ and $\tilde{s}'_i \in_R \mathsf{Kspace}_\kappa$ as ESK_i and computes $k_i = tPRF(\tilde{k}_i, \tilde{k}'_i, st_i, st'_i)$ and $s_i = tPRF(\tilde{s}_i, \tilde{s}'_i, st_i, st'_i)$. U_i computes $c_i = g^{k_i} h^{s_i}$ and sends c_i to S.
(Round 1 for Server) On receiving (R_i, c_i) for $i \in \{1, n, n+1\}$ and c_i for $i \in [2, n-1]$, S computes $sid = TCR(c_1, \ldots, c_{n+k})$ and chooses a representative user from $i \in \{1, n, n+1\}$. Here, w.l.o.g., we suppose that U_1 is the representative user. S sends (sid, R_n, R_1) to U_{n+1}. For $i \in \{1, 2\}$, S sends (sid, R_{i-1}) to U_i where $R_0 = R_{n+1}$. For $i \in [3, n-2]$, S sends sid to U_i. Also, S notices that U_1 is the representative user.
(Round 2 for Users) On receiving (sid, R_{n+1}), U_1 computes $K_1^{(l)} = F(sid, R_{n+1}^{r_1})$, $K_1^{(r)} = F(sid, R_1^r)$, $T_1 = K_1^{(l)} \oplus K_1^{(r)}$ and $T' = K_1^{(l)} \oplus (k_1 || s_1)$. U_1 computes

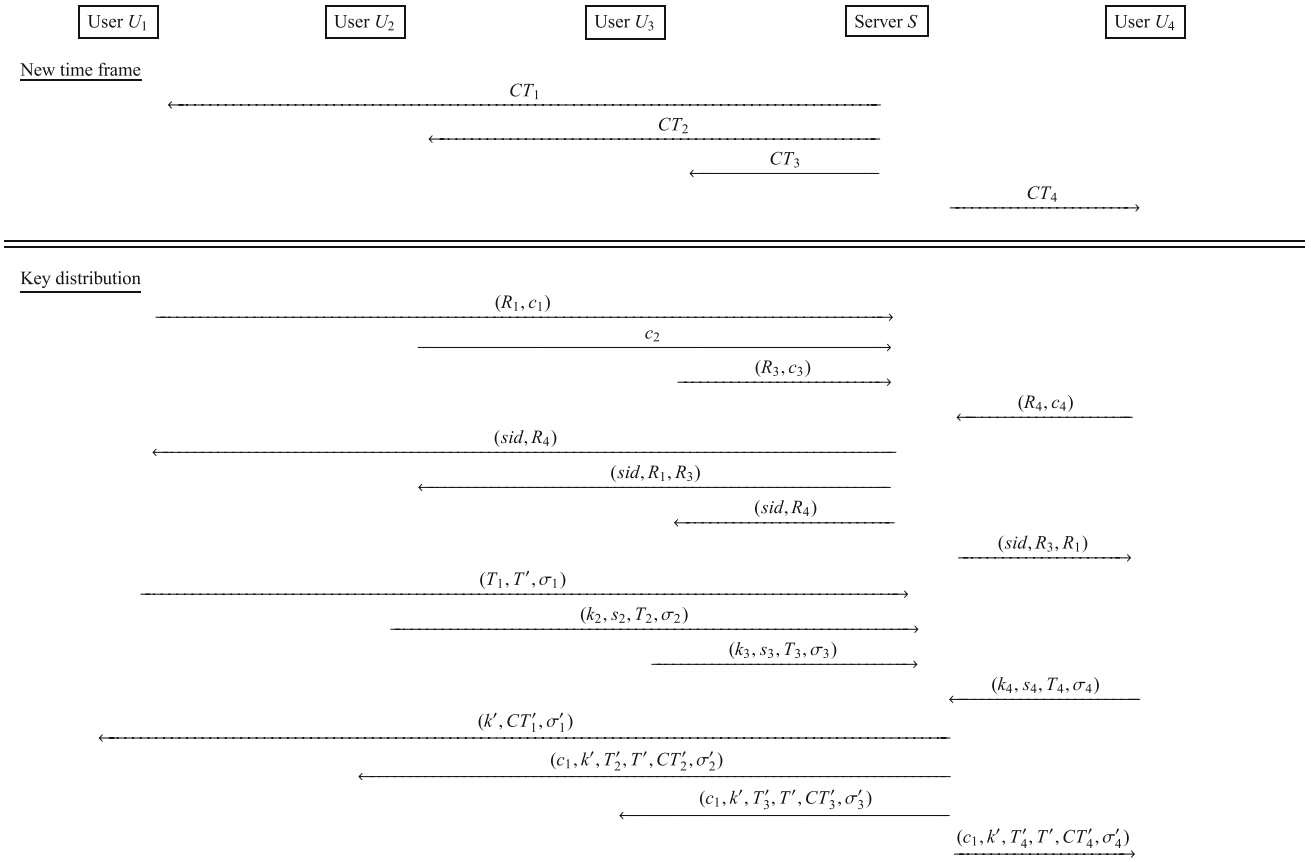

Fig. 2 Join phase for the case of $N = 3$

$\sigma_1 \leftarrow \mathbf{Tag}_{mk_1}(R_1, c_1, R_{n+1}, T_1, T', U_1, sid)$ and sends (T_1, T', σ_1) to S.

On receiving (sid, R_1), U_2 computes $K_2^{(l)} = F(sid, R_1^r)$, $K_2^{(r)} = F(sid, g^r)$ and $T_2 = K_2^{(l)} \oplus K_2^{(r)}$. U_2 computes $\sigma_2 \leftarrow \mathbf{Tag}_{mk_2}(c_2, R_1, k_2, s_2, T_2, U_2, sid)$ and sends $(k_2, s_2, T_2, \sigma_2)$ to S.

For $i \in [3, n-2]$, on receiving sid, U_i computes $\sigma_i \leftarrow \mathbf{Tag}_{mk_i}(c_i, k_i, s_i, U_i, sid)$ and sends (k_i, s_i, σ_i) to S.

On receiving (sid, R_n), U_{n-1} computes $K_{n-1}^{(l)} = F(sid, g^r)$, $K_{n-1}^{(r)} = F(sid, R_n^r)$ and $T_{n-1} = K_{n-1}^{(l)} \oplus K_{n-1}^{(r)}$. U_{n-1} computes $\sigma_{n-1} \leftarrow \mathbf{Tag}_{mk_{n-1}}(c_{n-1}, R_n, k_{n-1}, s_{n-1}, T_{n-1}, U_{n-1}, sid)$ and sends $(k_{n-1}, s_{n-1}, T_{n-1}, \sigma_{n-1})$ to S.

On receiving (sid, R_{n+1}), U_n computes $K_n^{(l)} = F(sid, R_n^r)$, $K_n^{(r)} = F(sid, R_{n+1}^{r_n})$ and $T_n = K_n^{(l)} \oplus K_n^{(r)}$. U_n computes $\sigma_n \leftarrow \mathbf{Tag}_{mk_n}(R_n, c_n, R_{n+1}, k_n, s_n, T_n, U_n, sid)$ and sends $(k_n, s_n, T_n, \sigma_n)$ to S.

On receiving (sid, R_n, R_1), U_{n+1} computes $K_{n+1}^{(l)} = F(sid, R_n^{r_{n+1}})$, $K_{n+1}^{(r)} = F(sid, R_1^{r_{n+1}})$ and $T_{n+1} = K_{n+1}^{(l)} \oplus K_{n+1}^{(r)}$. U_{n+1} computes $\sigma_{n+1} \leftarrow \mathbf{Tag}_{mk_{n+1}}(R_{n+1}, c_{n+1}, R_n, R_1, k_{n+1}, s_{n+1}, T_{n+1}, U_{n+1}, sid)$ and sends $(k_{n+1}, s_{n+1}, T_{n+1}, \sigma_{n+1})$ to S.

(Round 2 for Server) On receiving (T_1, T', σ_1) from U_1, $(k_i, s_i, T_i, \sigma_i)$ for $i \in \{2\} \cup [n-1, n+1]$ and (k_i, s_i, σ_i) for $i \in [3, n-2]$, S verifies authentication tags, and if the verification fails, then aborts. Also, for $i \in [2, n+1]$, S checks if $c_i = g^{k_i} h^{s_i}$ holds, and if the verification fails, then aborts. S generates $\tilde{k}_S \in_R \{0,1\}^\kappa$, $\tilde{k}'_S \in_R \mathsf{Kspace}_\kappa$, $\tilde{K}_1 \in_R \{0,1\}^\kappa$ and $\tilde{K}'_1 \in_R Kspace_\kappa$ as ESK_S and computes $k_S = tPRF(\tilde{k}_S, \tilde{k}'_S, st_S, st'_S)$, $K_1 = tPRF'(\tilde{K}_1, \tilde{K}'_1, st_S, st'_S)$ and $k' = (\bigoplus_{2 \le i \le n+k} k_i) \oplus k_S$. For $i \in [2, n+1]$, S computes $T'_i = \bigoplus_{1 \le j \le i-1} T_j$, where for $i \in [3, n-1]$, T_i is treated as empty (i.e. $T'_3 = \cdots = T'_{n-1}$). For $i \in [1, n+1]$, S computes $CT'_i \leftarrow \mathbf{AEnc}(Params, P_i, K_1)$ with access structure $P_i := (ID = U_i) \wedge (time \in TF)$.

S computes $\sigma'_1 \leftarrow \mathbf{Tag}_{mk_1}(R_1, c_1, R_{n+1}, T_1, T', U_1, sid, k', CT'_1)$ and sends (k', CT'_1, σ'_1) to U_1.

S computes $\sigma'_2 \leftarrow \mathbf{Tag}_{mk_2}(c_2, R_1, k_2, s_2, T_2, U_2, sid, c_1, k', T'_2, T', CT'_2)$ and sends $(c_1, k', T'_2, T', CT'_2, \sigma'_2)$ to U_2.

For $i \in [3, n-2]$, S computes $\sigma'_i \leftarrow \mathbf{Tag}_{mk_i}(c_i, k_i, s_i, U_i, sid, c_1, k', T'_i, T', CT'_i)$ and sends $(c_1, k', T'_i, T', CT'_i, \sigma'_i)$ to U_i.

S computes $\sigma'_{n-1} \leftarrow \mathbf{Tag}_{mk_{n-1}}(c_{n-1}, R_n, k_{n-1}, s_{n-1},$

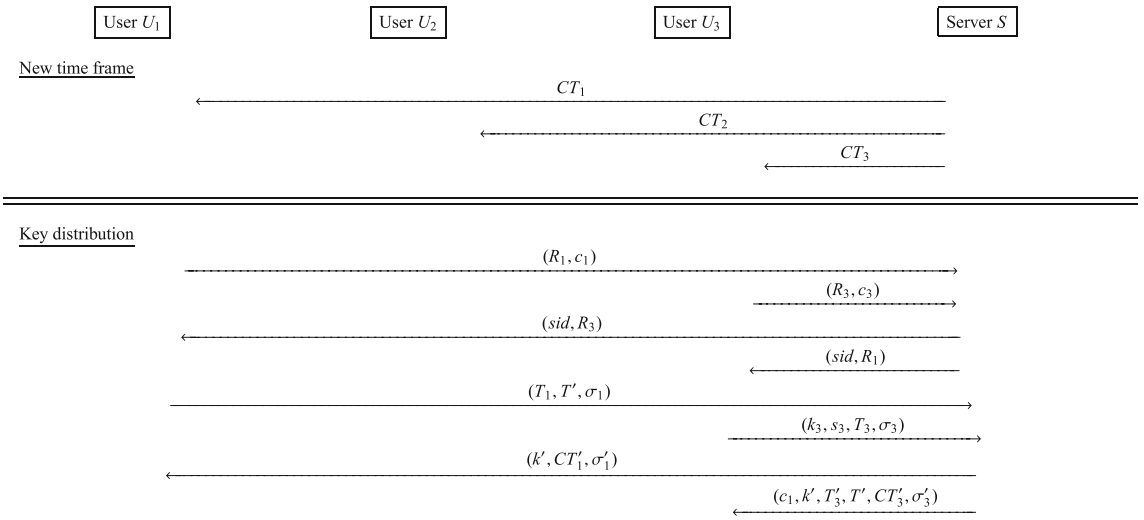

Fig. 3 Leave phase for the case of $N = 3$ when U_2 is the leaving user

T_{n-1}, $U_{n-1}, sid, c_1, k', T'_{n-1}$, T', CT'_{n-1}) and sends $(c_1, k', T'_{n-1}, T', CT'_{n-1}, \sigma'_{n-1})$ to U_{n-1}.
S computes $\sigma'_n \leftarrow \mathbf{Tag}_{mk_n}(R_n, c_n, R_{n+1}, k_n, s_n, T_n, U_n, sid, c_1, k', T'_n, T', CT'_n)$ and sends $(c_1, k', T'_n, T', CT'_n, \sigma'_n)$ to U_n.
S computes $\sigma'_{n+1} \leftarrow \mathbf{Tag}_{mk_{n+1}}(R_{n+1}, c_{n+1}, R_n, R_1, k_{n+1}, s_{n+1}, T_{n+1}, U_{n+1}, sid, c_1, k', T'_{n+1}, T', CT'_{n+1})$ and sends $(c_1, k', T'_{n+1}, T', CT'_{n+1}, \sigma'_{n+1})$ to U_{n+1}.
(Session Key Generation and Post-computation) For $i \in [2, n+1]$, on receiving $(c_1, k', T'_i, T', CT'_i, \sigma'_i)$, U_i verifies the authentication tag, and if the verification fails, then aborts. U_i computes $K_1^{(l)} = T'_i \oplus K_i^{(l)}$ where for $i \in [3, n-1]$ $K_1^{(l)} = T'_i \oplus g^r$ and $k_1 || s_1 = T' \oplus K_1^{(l)}$ and checks if $c_1 = g^{k_1} h^{s_1}$ holds, and if the verification fails, then aborts. U_i decrypts $K_1 \leftarrow \mathbf{ADec}_{usk_i}(CT'_i, P_i)$, computes $K_2 = F'(sid, k' \oplus k_1)$ and outputs the session key $SK = F''(sid, K_1) \oplus F''(sid, K_2)$. As state information, U_i updates $r = F'''(sid, K_1) \oplus F'''(sid, K_2)$ in $state_i$. Also, U_n updates $H_n^{(r)} = R_{n+1}^{r_n}$ in $state_n$. U_{n+1} adds sid, $H_{n+1}^{(l)} = R_n^{r_{n+1}}$ and $H_{n+1}^{(r)} = R_1^{r_{n+1}}$ to $state_{n+1}$. On receiving (k', CT'_1, σ'_1), U_1 verifies the authentication tag, and if the verification fails, then aborts. U_1 decrypts $K_1 \leftarrow \mathbf{ADec}_{usk_1}(CT'_1, P_1)$, computes $K_2 = F'(sid, k' \oplus k_1)$ and outputs the session key $SK = F''(sid, K_1) \oplus F''(sid, K_2)$. As state information, U_1 updates sid, $H_1^{(l)} = R_{n+1}^{r_1}$ and $r = F'''(sid, K_1) \oplus F'''(sid, K_2)$ in $state_1$.

4.5 Leave phase

A user U_j leaves an established session by $U_1, \ldots, U_n$.

In the Leave phase, users $U_i \in \mathcal{I} \backslash \{U_{j-1}, U_j, U_{j_1+1}\}$ can reduce computation than the Dist phase. They do not need to compute g^{r_i}. The ring structure to compute K_1 still works because $H_i^{(l)}$ and $H_i^{(r)}$ in $state_i$ are used to connect the ring instead of using $g^{r_{i-1} r_i}$ and $g^{r_i r_{i+1}}$. We illustrate the message flow of Leave phase for the case of $N = 3$ in Fig.3.

(State Update at New Time Frame) If the session is the first session for U_i at the time frame TF', then for the current time $time$ S generates $usk_i \leftarrow \mathbf{Der}(Params, msk, A_i)$ with attribute $A_i = (U_i, time)$ and $mk_i \leftarrow \mathbf{MGen}$ and computes $CT_i \leftarrow \mathbf{Enc}_{pk_i}(usk_i, mk_i)$. Then, S sends CT_i to U_i, and U_i obtains $(usk_i, mk_i) \leftarrow \mathbf{Dec}_{sk_i}(CT_i)$ and updates (usk_i, mk_i) in $state_i$.
(Round 1 for Users) $U_i \in \{U_{j-1}, U_{j+1}\}$ generates $\tilde{r}_i \in_R \{0,1\}^\kappa$, $\tilde{r}'_i \in_R \mathsf{Kspace}_\kappa$, $\tilde{k}_i \in_R \{0,1\}^\kappa$, $\tilde{k}'_i \in_R \mathsf{Kspace}_\kappa$, $\tilde{s}_i \in_R \{0,1\}^\kappa$ and $\tilde{s}'_i \in_R \mathsf{Kspace}_\kappa$ as ESK_i and computes $r_i = tPRF(\tilde{r}_i, \tilde{r}'_i, st_i, st'_i)$, $k_i = tPRF(\tilde{k}_i, \tilde{k}'_i, st_i, st'_i)$ and $s_i = tPRF(\tilde{s}_i, \tilde{s}'_i, st_i, st'_i)$. Then, U_i computes $R_i = g^{r_i}$ and $c_i = g^{k_i} h^{s_i}$ and sends (R_i, c_i) to S.
$U_i \in \mathcal{I} \backslash \{U_{j-1}, U_j, U_{j+1}\}$ generates $\tilde{k}_i \in_R \{0,1\}^\kappa$, $\tilde{k}'_i \in_R \mathsf{Kspace}_\kappa$, $\tilde{s}_i \in_R \{0,1\}^\kappa$ and $\tilde{s}'_i \in_R \mathsf{Kspace}_\kappa$ as ESK_i and computes $k_i = tPRF(\tilde{k}_i, \tilde{k}'_i, st_i, st'_i)$ and $s_i = tPRF(\tilde{s}_i, \tilde{s}'_i, st_i, st'_i)$. Then, U_i computes $c_i = g^{k_i} h^{s_i}$ and sends c_i to S.
(Round 1 for Server) On receiving (R_i, c_i) from $U_i \in \{U_{j-1}, U_{j+1}\}$ and c_i from $U_i \in \mathcal{I} \backslash \{U_{j-1}, U_j, U_{j+1}\}$, for i such that $U_i \in \mathcal{I} \backslash \{U_j\}$, S computes $sid = TCR(\{c_i\}_{\mathcal{I} \backslash \{U_j\}})$ and chooses a representative user from $U_i \in \{U_{j-1}, U_{j+1}\}$. Here, w.l.o.g., we suppose that U_{j-1} is the representative user. S sends (sid, R_{j+1}) to U_{j-1}. S sends (sid, R_{j-1}) to U_{j+1}. Then, S sends sid to $U_i \in \mathcal{I} \backslash \{U_{j-1}, U_j, U_{j+1}\}$. Also, S notices that U_{j-1} is the representative user.
(Round 2 for Users) On receiving (sid, R_{j+1}), U_{j-1} computes $K_{j-1}^{(l)} = F(sid, H_{j-1}^{(l)})$, $K_{j-1}^{(r)} = F(sid, R_{j+1}^{r_{j-1}})$,

$T_{j-1} = K_{j-1}^{(l)} \oplus K_{j-1}^{(r)}$ and $T' = K_{j-1}^{(l)} \oplus (k_{j-1}||s_{j-1})$. U_{j-1} computes $\sigma_{j-1} \leftarrow \mathbf{Tag}_{mk_{j-1}}(R_{j-1}, c_{j-1}, R_{j+1}, T_{j-1}, T', U_{j-1}, sid)$ and sends $(T_{j-1}, T', \sigma_{j-1})$ to S.

On receiving (sid, R_{j-1}), U_{j+1} computes $K_{j+1}^{(l)} = F(sid, R_{j-1}^{r_{j+1}})$, $K_{j+1}^{(r)} = F(sid, H_{j+1}^{(r)})$ and $T_{j+1} = K_{j+1}^{(l)} \oplus K_{j+1}^{(r)}$. U_{j+1} computes $\sigma_{j+1} \leftarrow \mathbf{Tag}_{mk_{j+1}}(R_{j+1}, c_{j+1}, R_{j-1}, k_{j+1}, s_{j+1}, T_{j+1}, U_{j+1}, sid)$ and sends $(k_{j+1}, s_{j+1}, T_{j+1}, \sigma_{j+1})$ to S.

On receiving sid, $U_i \in \mathcal{I}\backslash\{U_{j-1}, U_j, U_{j+1}\}$ computes $K_i^{(l)} = F(sid, H_i^{(l)})$, $K_i^{(r)} = F(sid, H_i^{(r)})$ and $T_i = K_i^{(l)} \oplus K_i^{(r)}$. U_i computes $\sigma_i \leftarrow \mathbf{Tag}_{mk_i}(c_i, k_i, s_i, T_i, U_i, sid)$ and sends $(k_i, s_i, T_i, \sigma_i)$ to S.

(Round 2 for Server) On receiving $(T_{j-1}, T', \sigma_{j-1})$ from U_{j-1} and $(k_i, s_i, T_i, \sigma_i)$ from other users, S verifies the authentication tag, and if the verification fails, then aborts. Also, for $U_i \in \mathcal{I}\backslash\{U_{j-1}, U_j\}$, S checks if $c_i = g^{k_i} h^{s_i}$ holds, and if the verification fails, then aborts. S generates $\tilde{k}_S \in_R \{0,1\}^\kappa$, $\tilde{k}'_S \in_R \mathsf{Kspace}_\kappa$, $\tilde{K}_1 \in_R \{0,1\}^\kappa$ and $\tilde{K}'_1 \in_R Kspace_\kappa$ as ESK_S and computes $k_S = tPRF(\tilde{k}_S, \tilde{k}'_S, st_S, st'_S)$ and $K_1 = tPRF'(\tilde{K}_1, \tilde{K}'_1, st_S, st'_S)$. For i such that $U_i \in \mathcal{I}\backslash\{U_{j-1}, U_j\}$, S computes $k' = (\bigoplus\{k_i\}) \oplus k_S$. For i such that $U_i \in \mathcal{I}\backslash\{U_j\}$ and $i < j-1$, S computes $T'_i = \bigoplus_{1 \le \ell \le i-1, j-1 \le \ell \le n} T_\ell$, where T_j is empty. For i such that $U_i \in \mathcal{I}\backslash\{U_j\}$ and $j+1 \le i$, S computes $T'_i = \bigoplus_{j-1 \le \ell \le i-1} T_\ell$, where T_j is empty. For $U_i \in \mathcal{I}\backslash\{U_j\}$, S computes $CT'_i \leftarrow \mathbf{AEnc}(Params, P_i, K_1)$ with access structure $P_i := (ID = U_i) \wedge (time \in TF)$.

S computes $\sigma'_{j-1} \leftarrow \mathbf{Tag}_{mk_{j-1}}(R_{j-1}, c_{j-1}, R_{j+1}, T_{j-1}, T', U_{j-1}, sid, k', CT'_{j-1})$ and sends $(k', CT'_{j-1}, \sigma'_{j-1})$ to U_{j-1}.

S computes $\sigma'_{j+1} \leftarrow \mathbf{Tag}_{mk_{j+1}}(R_{j+1}, c_{j+1}, R_{j-1}, k_{j+1}, s_{j+1}, T_{j+1}, U_{j+1}, sid, c_{j-1}, k', T'_{j+1}, T', CT'_{j+1})$ and sends $(c_{j-1}, k', T'_{j+1}, T', CT'_{j+1}, \sigma'_{j+1})$ to U_{j+1}.

For $U_i \in \mathcal{I}\backslash\{U_{j-1}, U_j, U_{j+1}\}$, S computes $\sigma'_i \leftarrow \mathbf{Tag}_{mk_i}(c_i, k_i, s_i, T_i, U_i, sid, c_{j-1}, k', T'_i, T', CT'_i)$ and sends $(c_{j-1}, k', T'_i, T', CT'_i, \sigma'_i)$ to U_i.

(Session Key Generation and Post-computation) On receiving $(c_{j-1}, k', T'_i, T', CT'_i, \sigma'_i)$, $U_i \in \mathcal{I}\backslash\{U_{j-1}, U_j\}$ verifies the authentication tag, and if the verification fails, then aborts. U_i computes $K_{j-1}^{(l)} = T'_i \oplus K_i^{(l)}$ and $k_{j-1}||s_{j-1} = T' \oplus K_{j-1}^{(l)}$ and checks if $c_{j-1} = g^{k_{j-1}} h^{s_{j-1}}$ holds, and if the verification fails, then aborts. U_i decrypts $K_1 \leftarrow \mathbf{ADec}_{usk_i}(CT'_i, P_i)$, computes $K_2 = F'(sid, k' \oplus k_{j-1})$ and outputs the session key $SK = F''(sid, K_1) \oplus F''(sid, K_2)$. As state information, U_i updates $sid, r = F'''(sid, K_1) \oplus F'''(sid, K_2)$ in $state_i$.

On receiving $(k', CT'_{j-1}, \sigma'_{j-1})$, U_{j-1} verifies the authentication tag, and if the verification fails, then aborts. U_{j-1} decrypts $K_1 \leftarrow \mathbf{ADec}_{usk_{j-1}}(CT'_{j-1}, P_{j-1})$, computes $K_2 = F'(sid, k' \oplus k_{j-1})$ and outputs the session key $SK = F''(sid, K_1) \oplus F''(sid, K_2)$. As state information, U_1 updates $sid, r = F'''(sid, K_1) \oplus F'''(sid, K_2)$ in $state_1$.

Additionally, U_{j-1} updates $H_{j-1}^{(r)} = R_{j+1}^{r_{j-1}}$ in $state_{j-1}$, and U_{j+1} updates $H_{j+1}^{(l)} = R_{j-1}^{r_{j+1}}$ in $state_{j+1}$.

4.6 Update phase

When a new time frame begins, a set of users $U_{i_1}, \ldots, U_{i_n}$ $(n \le N)$ update the session key SK shared by them in the Dist/Join/Leave phase at the past time frame to a new session key SK'. For simplicity, w.l.o.g., we suppose that $(U_{i_1}, \ldots, U_{i_n}) = (U_1, \ldots, U_n)$.

(State Update at New Time Frame) If the session is the first session for U_i at the time frame TF, then for the current time $time$ S generates $usk_i \leftarrow \mathbf{Der}(Params, msk, A_i)$ with attribute $A_i = (U_i, time)$ and $mk_i \leftarrow \mathbf{MGen}$ and computes $CT_i \leftarrow \mathbf{Enc}_{pk_i}(usk_i, mk_i)$. Then, S sends CT_i to U_i, and U_i obtains $(usk_i, mk_i) \leftarrow \mathbf{Dec}_{sk_i}(CT_i)$ and updates (usk_i, mk_i) in $state_i$.

(Information for Update) S generates $\tilde{K}_1 \in_R \{0,1\}^\kappa$ and $\tilde{K}'_1 \in_R Kspace_\kappa$ and computes $K_1 = tPRF'(\tilde{K}_1, \tilde{K}'_1, st_S, st'_S)$ and $CT'_i \leftarrow \mathbf{AEnc}(Params, P_i, K_1)$ with access structure $P_i := (ID = U_i) \wedge (time \in TF)$. Then, S sends CT'_i to U_i.

(Session Key Update) On receiving CT'_i, U_i decrypts $K_1 \leftarrow \mathbf{ADec}_{usk_i}(CT'_i, P_i)$ and outputs the updated session key $SK' = F''(sid, K_1) \oplus SK$.

5 Complexity for users

5.1 Computational complexity

We consider dominant operations like modular exponentiations and operations for public key crypto and ignore other light-weight operations like XORs and operations for secret key crypto.

In the Dist phase, online computations (i.e. from Round 1 to post-computations) for a user are g^{r_i} and $g^{k_i} h^{s_i}$ for Round 1, $R_{i-1}^{r_i}$ and $R_{i+1}^{r_i}$ for Round 2, and $g^{k_1} h^{s_1}$ and the decryption of CT'_i for the session key generation. In the Join phase, maximum online computations for a user are g^{r_i} and $g^{k_i} h^{s_i}$ for Round 1, $R_{i-1}^{r_i}$ and $R_{i+1}^{r_i}$ for Round 2, and $g^{k_1} h^{s_1}$ and the decryption of CT'_i for the session key generation. In the Leave phase, maximum online computations for a user are g^{r_i} and $g^{k_i} h^{s_i}$ for Round 1, $R_{i-1}^{r_i}$ for Round 2, and $g^{k_1} h^{s_1}$ and the decryption of CT'_i for the session key generation. In the Update phase, the online computation for a user is the decryption of CT'_i for the session key update.

Therefore, for all phases, computational complexity of users is constant for the number of users.

5.2 Communication complexity

In the Dist phase, sent and received information for a user in online (i.e. from Round 1 to post-computations) are (R_i, c_i) and (sid, R_{i-1}, R_{i+1}) for Round 1, and $(k_i, s_i, T_i, \sigma_i)$ and $(c_1, k', T'_i, T', CT'_i, \sigma'_i)$ for Round 2. In the Join phase, maximum sent and received information for a user in online are (R_i, c_i) and (sid, R_{i-1}, R_{i+1}) for Round 1, and $(k_i, s_i, T_i, \sigma_i)$ and $(c_1, k', T'_i, T', CT'_i, \sigma'_i)$ for Round 2. In the Leave phase, maximum sent and received information for a user in online are (R_i, c_i) and (sid, R_{i-1}) for Round 1, and $(k_i, s_i, T_i, \sigma_i)$ and $(c_{j-1}, k', T'_{j+1}, T', CT'_{j+1}, \sigma'_{j+1})$ for Round 2. In the Leave phase, received information for a user in online is CT'_i for the session key update.

Therefore, for all phases, communication complexity of users is constant for the number of users.

6 Security

Theorem 1 *We assume that TCR satisfies the TCR property, tPRF and tPRF′ are twisted PRFs, F, F′, F″ and F‴ are PRFs,* (**Gen**, **Enc**, **Dec**) *is a CCA-secure PKE,* (**Setup**, **Der**, **AEnc**, **ADec**) *is a selective CCA-secure CP-ABE,* (**MGen**, **Tag**, **Ver**) *is an UF-CMA MAC scheme, and the DDH assumption in G holds. Then, our scheme is secure in the* DMKD *model.*

Here, we show a proof sketch. The proof can be divided four cases: (1) the test session is in the Dist phase, (2) the test session is in the Join phase, (3) the test session is in the Leave phase, and (4) the test session is in the Update phase. For Cases (1), (2) and (3), secrecy of the session key is guaranteed by secrecy of K_1. Thus, we use the game hopping proof technique [32], and finally, K_1 is replaced with a random value. To prevent malicious behaviours of the adversary, we show that the probability that messages in the test session are modified is negligible thanks to the security of PKE and MAC and the DDH assumption. For Case (4), secrecy of the session key is guaranteed by secrecy of K_2. Thus, K_2 is replaced with a random value similar to other cases. In this case, we rely on the security of CP-ABE to prevent malicious behaviours of the adversary.

Proof We prove Theorem 1 for all four cases as follows.

6.1 Case of Dist phase

We change the interface of oracle queries and the computation of the session key. These instances are gradually changed over hybrid experiments, depending on specific subcases. In the last hybrid experiment, the session key in the test session does not contain information of the bit b. Thus, the adversary clearly only outputs a random guess. We denote these hybrid experiments by $\mathbf{H}_0, \ldots, \mathbf{H}_7$, and the advantage of the adversary $\mathcal{A}$ when participating in experiment $\mathbf{H}_i$ by $\mathbf{Adv}(\mathcal{A}, \mathbf{H}_i)$.

6.1.1 Hybrid experiment $\mathbf{H}_0$

This experiment denotes the real experiment for DMKD security, and in this experiment the environment for $\mathcal{A}$ is as defined in the protocol. Thus, $\mathbf{Adv}(\mathcal{A}, \mathbf{H}_0)$ is the same as the advantage of the real experiment.

6.1.2 Hybrid experiment $\mathbf{H}_1$

If sid in two sessions are identical, the experiment halts.

When randomness in generating c_i is identical or the TCR property of H is broken, sid in two sessions may be identical. However, such an event occurs with negligible probability. Thus, $|\mathbf{Adv}(\mathcal{A}, \mathbf{H}_1) - \mathbf{Adv}(\mathcal{A}, \mathbf{H}_0)|$ is negligible.

6.1.3 Hybrid experiment $\mathbf{H}_2$

The experiment selects user instances $\{U_{i_1}^{j_1}, \ldots, U_{i_n}^{j_n}\})$ and the owner U_i^j randomly in advance. If $\mathcal{A}$ poses Test query to a session except $\{U_{i_1}^{j_1}, \ldots, U_{i_n}^{j_n}\})$ owned by U_i^j, the experiment halts.

Since the guess of the test session matches with $\mathcal{A}$'s choice with probability $1/\ell_{max}$ where ℓ_{max} is the total number of sessions in the system, $\mathbf{Adv}(\mathcal{A}, \mathbf{H}_2) \geq (1/\ell_{max}) \cdot \mathbf{Adv}(\mathcal{A}, \mathbf{H}_1)$.

6.1.4 Hybrid experiment $\mathbf{H}_3$

If $\mathcal{A}$ modifies a message in the test session and the session is complete, the experiment halts. We denote such an event Bad.

Bad may occur only if either of the following events occur:

- Bad_1 : $\mathcal{A}$ obtains information of mk_i from CT_i.
- Bad_2 : $\mathcal{A}$ forges σ_i for a modified message.
- Bad_3 : $\mathcal{A}$ forges σ'_i for a modified message.
- Bad_4 : $\mathcal{A}$ finds (k'_i, s'_i) such that $c_i = g^{k_i} h^{s_i} = g^{k'_i} h^{s'_i}$ and $(k'_i, s'_i) \neq (k_i, s_i)$.

Since $\mathbf{H}_2$ does not differ from $\mathbf{H}_3$ if Bad does not occur, from the Difference Lemma [32] $|\mathbf{Adv}(\mathcal{A}, \mathbf{H}_3) - \mathbf{Adv}(\mathcal{A}, \mathbf{H}_2)| \leq \Pr[\mathsf{Bad}]$. We show $\Pr[\mathsf{Bad}]$ is negligible.

First, we show that if Bad_1 occurs, we can construct an adversary B breaking the CCA security of (**Gen**, **Enc**,

Dec). B receives the public key pk^* and sets pk^* to SPK_i. When $\mathcal{A}$ poses $\mathsf{Send}(U_i^{j'}, CT_i)$ for sessions other than the test session, B poses CT_i to $\mathcal{DO}$ and continues to simulate the experiment with received (usk_i, mk_i). When $\mathcal{A}$ poses $\mathsf{Send}(S, init)$ for the test session, B chooses mk_0 and mk_1 and obtains the challenge ciphertext CT^* encrypting (usk, mk_0) or (usk, mk_1). Then, B sends CT^* as CT_i to $\mathcal{A}$. After that, if $\mathcal{A}$ poses Send containing a MAC tag of a modified message with $mk_{b'}$, then B outputs $b = b'$. Therefore, if $\mathcal{A}$ obtains information of mk_i from CT_i, B can break the CCA security.

Next, we show that if Bad_2 or Bad_3 occurs, we can construct a forger B breaking unforgeability of (**MGen**, **Tag**, **Ver**). When $\mathcal{A}$ poses $\mathsf{Send}(U_i^j, (sid, R_{i-1}, R_{i+1}))$ or $\mathsf{Send}(U_i^j, (k_i, s_i, T_i, \sigma_i))$ for the test session, B poses messages to $\mathcal{MO}$ and continues to simulate the experiment with the received MAC tag. It means that mk_i is set as the challenge MAC key. When $\mathcal{A}$ poses Send containing a forged MAC tag σ^* for mk_i, then B outputs σ^*. Therefore, if $\mathcal{A}$ forges σ_i or σ_i' for a modified message, B can break UF-CMA.

Finally, we show that if Bad_4 occurs, we can construct a distinguisher B breaking the DDH assumption. B receives the tuple (g, A, B, C) and sets $g = g, h = A$ to SPK_S. When $\mathcal{A}$ poses $\mathsf{Send}(U_i^j, init)$ for the test session, B chooses (k_i, s_i), computes $c_i = g^{k_i} h^{s_i}$ and returns (R_i, c_i) to $\mathcal{A}$. After that, if $\mathcal{A}$ poses $\mathsf{Send}(S, (k_i', s_i', T_i, \sigma_i))$ such that $c_i = g^{k_i'} h^{s_i'}$ and $(k_i', s_i') \neq (k_i, s_i)$, then B computes $a = \frac{k_i' - k_i}{s_i' - s_i}$. B verifies if $B^a = C$, and if so, outputs 1, otherwise outputs 0. Therefore, if $\mathcal{A}$ finds (k_i', s_i') such that $c_i = g^{k_i} h^{s_i} = g^{k_i'} h^{s_i'}$ and $(k_i', s_i') \neq (k_i, s_i)$, B can break the DDH assumption.

Hence, $\Pr[\mathsf{Bad}]$ is negligible and $|\mathbf{Adv}(\mathcal{A}, \mathbf{H}_3) - \mathbf{Adv}(\mathcal{A}, \mathbf{H}_2)|$ is negligible.

6.1.5 Hybrid experiment $\mathbf{H}_4$

The computation of (r_i, k_i, s_i, k_S) for all users in the test session is changed. Instead of computing tPRF, it is changed as choosing (r_i, k_i, s_i, k_S) randomly.

From the freshness definition (Definition 9) $\mathcal{A}$ cannot pose both of $\mathsf{StaticReveal}(U_i)$ and $\mathsf{EphemeralReveal}(U_i^j)$, and both of $\mathsf{StaticReveal}(U_{i'})$ and $\mathsf{EphemeralReveal}(U_{i'}^{j'})$ for any $\overline{\mathsf{sid}^*}$. Hence, $\mathcal{A}$ cannot see either of $(\tilde{r}_i, \tilde{r}_i')$ or (st_i, st_i'). From Lemma 1 $r_i = tPRF(\tilde{r}_i, \tilde{r}_i', st_i, st_i')$ is indistinguishable from randomly chosen r_i. Similarly, $k_i = tPRF(\tilde{k}_i, \tilde{k}_i', st_i, st_i')$, $k_S = tPRF(\tilde{k}_S, \tilde{k}_S', st_S, st_S')$ and $s_i = tPRF(\tilde{s}_i, \tilde{s}_i', st_i, st_i')$ are indistinguishable from randomly chosen k_i, k_S and s_i, respectively.

Therefore, $|\mathbf{Adv}(\mathcal{A}, \mathbf{H}_4) - \mathbf{Adv}(\mathcal{A}, \mathbf{H}_3)|$ is negligible.

6.1.6 Hybrid experiment $\mathbf{H}_5$

The computation of $R_{i-1}^{r_i}$ and $R_{i+1}^{r_i}$ in the test session is changed. Instead of computing exponentiations, it is changed as choosing R and R' randomly.

In this experiment, r_{i-1}, r_i and r_{i+1} are randomly chosen and $\mathcal{A}$ cannot see r_{i-1}, r_i and r_{i+1}. From the definition of DDH assumption (Definition 8) $R = R_{i-1}^{r_i}$ is indistinguishable from randomly chosen R. Similarly, $R' = R_{i+1}^{r_i}$ is indistinguishable from randomly chosen R'.

Therefore, $|\mathbf{Adv}(\mathcal{A}, \mathbf{H}_5) - \mathbf{Adv}(\mathcal{A}, \mathbf{H}_4)|$ is negligible.

6.1.7 Hybrid experiment $\mathbf{H}_6$

The computation of $K_i^{(l)}$ and $K_i^{(r)}$ in the test session is changed. Instead of computing PRF, it is changed as choosing $K_i^{(l)}$ and $K_i^{(r)}$ randomly.

In this experiment, $R_{i-1}^{r_i}$ and $R_{i+1}^{r_i}$ are randomly chosen. From the definition of PRF (Definition 1) $K_i^{(l)} = F(sid, R_{i-1}^{r_i})$ is indistinguishable from randomly chosen $K_i^{(l)}$. Similarly, $K_i^{(r)} = F(sid, R_{i+1}^{r_i})$ is indistinguishable from randomly chosen $K_i^{(r)}$.

Therefore, $|\mathbf{Adv}(\mathcal{A}, \mathbf{H}_6) - \mathbf{Adv}(\mathcal{A}, \mathbf{H}_5)|$ is negligible.

6.1.8 Hybrid experiment $\mathbf{H}_7$

The computation of K_2 in the test session is changed. Instead of computing PRF, it is changed as choosing K_2 randomly.

In this experiment, $k' = (\bigoplus_{2 \leq i \leq n} k_i) \oplus k_S$ is random because k_i and k_S are randomly chosen. Also, k_1 is randomly chosen, and thus, $k' \oplus k_1$ is random. From the definition of PRF 1 $K_2 = F'(sid, k' \oplus k_1)$ is indistinguishable from randomly chosen K_2.

Therefore, $|\mathbf{Adv}(\mathcal{A}, \mathbf{H}_7) - \mathbf{Adv}(\mathcal{A}, \mathbf{H}_6)|$ is negligible.

6.1.9 Hybrid experiment $\mathbf{H}_8$

The computation of $K_2' = F''(sid, K_2)$ in the test session is changed. Instead of computing PRF, it is changed as choosing K_2' randomly.

In this experiment, K_2 is random. From the definition of PRF 1 $K_2' = F''(sid, K_2)$ is indistinguishable from randomly chosen K_2'.

Therefore, $|\mathbf{Adv}(\mathcal{A}, \mathbf{H}_8) - \mathbf{Adv}(\mathcal{A}, \mathbf{H}_7)|$ is negligible.

6.1.10 Bounding the advantage in $\mathbf{H}_8$

In $\mathbf{H}_8$, $F''(sid, K_2)$ is replaced with random K_2'. Hence, $SK = F''(sid, K_1) \oplus K_2'$ is also random. Then, regardless of the challenge bit b for the test session, when $\mathcal{A}$ poses Test query, a random session key is returned.

Therefore, $\mathbf{Adv}(\mathcal{A}, \mathbf{H}_8)$ is negligible.

6.2 Case of Join phase

The proof is almost the same as the case of the Dist phase. The difference is to add a hybrid experiment between $\mathbf{H}_4$ and $\mathbf{H}_5$. In this experiment, the computation of r in the test session is changed. Instead of computing PRF, it is changed as choosing r randomly.

From the freshness definition (Definition 9) $\mathcal{A}$ cannot pose either StateReveal(U_i) or StateReveal($U_{i'}$) in the current time frame or any of its ancestors. Also, though $\mathcal{A}$ can pose SessionReveal($U_{i'}^{j'}$) for sessions other than the test session, $r = F'''(sid, K_1) \oplus F'''(sid, K_2)$ is independent of $SK = F''(sid, K_1) \oplus F''(sid, K_2)$ from the definition of PRF. Hence, $\mathcal{A}$ cannot see r. Therefore, the difference between this experiment and the previous experiment is negligible.

6.3 Case of Leave phase

The proof is almost the same as the case of the Dist phase. The difference is to add a hybrid experiment between $\mathbf{H}_5$ and $\mathbf{H}_6$. In this experiment, the computation of $H_i^{(r)}$ and $H_i^{(l)}$ in the test session is changed. Instead of computing exponentiations, it is changed as choosing H and H' randomly.

From the freshness definition (Definition 9) $\mathcal{A}$ cannot pose either StateReveal(U_i) or StateReveal($U_{i'}$) in the current time frame or any of its ancestors. Also, since if both EphemeralReveal(U_i^j) and StaticReveal(U_i) are posed, then we regard that StateReveal(U_i) in the time frame for instance U_i^j is also posed, the adversary cannot see r_{i-1}, r_i and r_{i+1} corresponding to $H_i^{(r)}$ and $H_i^{(l)}$ from Lemma 1. From the definition of DDH assumption (Definition 8) $H_i^{(l)} = R_{i-1}^{r_i}$ is indistinguishable from randomly chosen H'. Similarly, $H_i^{(r)}$ is indistinguishable from randomly chosen H. Therefore, the difference between this experiment and the previous experiment is negligible.

6.4 Case of Update phase

We denote these hybrid experiments by $\mathbf{H}_0, \ldots, \mathbf{H}_4$, and the advantage of the adversary $\mathcal{A}$ when participating in experiment $\mathbf{H}_i$ by $\mathbf{Adv}(\mathcal{A}, \mathbf{H}_i)$.

6.4.1 Hybrid experiment $\mathbf{H}_0$

This experiment denotes the real experiment for DMKD security, and in this experiment the environment for $\mathcal{A}$ is as defined in the protocol. Thus, $\mathbf{Adv}(\mathcal{A}, \mathbf{H}_0)$ is the same as the advantage of the real experiment.

6.4.2 Hybrid experiment $\mathbf{H}_1$

If sid in two sessions are identical, the experiment halts.

As the case of the Join phase, $|\mathbf{Adv}(\mathcal{A}, \mathbf{H}_1) - \mathbf{Adv}(\mathcal{A}, \mathbf{H}_0)|$ is negligible.

6.4.3 Hybrid experiment $\mathbf{H}_2$

The experiment selects user instances $\{U_{i_1}^{j_1}, \ldots, U_{i_n}^{j_n}\}$ and the owner U_i^j randomly in advance. If $\mathcal{A}$ poses Test query to a session except $\{U_{i_1}^{j_1}, \ldots, U_{i_n}^{j_n}\}$ owned by U_i^j, the experiment halts.

As the case of the Join phase, $\mathbf{Adv}(\mathcal{A}, \mathbf{H}_2) \geq (1/\ell_{max}) \cdot \mathbf{Adv}(\mathcal{A}, \mathbf{H}_1)$.

6.4.4 Hybrid experiment $\mathbf{H}_3$

The computation of CT_i' in the test session is changed. Instead of encrypting K_1, it is changed as encrypting randomly chosen K_1'.

From the freshness definition (Definition 9) $\mathcal{A}$ can pose SessionReveal(U_i^j) or SessionReveal($U_{i'}^{j'}$) for any $\overline{\text{sid}^*}$ in the past time frame, but cannot pose StaticReveal(U_i), StaticReveal($U_{i'}$) for any $\overline{\text{sid}^*}$, ServerReveal, StateReveal(U_i) and StateReveal($U_{i'}$) in the current time frame. Hence, $\mathcal{A}$ cannot see usk_i or $usk_{i'}$. We show that if $\mathcal{A}$ distinguishes $\mathbf{H}_3$ from $\mathbf{H}_2$, we can construct an adversary B breaking the selective CCA security of (**Setup**, **Der**, **AEnc**, **ADec**). First, B outputs $P^* := (ID = U_i) \wedge (time \in TF)$ for the test session. Then, B receives the public parameter $Params$ and sets $Params$ to SPK_S. When $\mathcal{A}$ poses Send($U_{i'}^{j'}, CT_{i'}'$) for $U_{i'} \neq U_i$, B poses $A_{i'}$ to $\mathcal{EO}$ where $A_{i'} := (U_{i'}, time)$ and continues to simulate the experiment with received $usk_{i'}$. When $\mathcal{A}$ poses Send($U_i^{j'}, CT_i'$) for sessions other than the test session, B poses CT_i' to $\mathcal{DO}$ and continues to simulate the experiment with received K_1. When $\mathcal{A}$ poses Send($S, init$) for the test session, B computes $K_0^* = tPRF'(\tilde{K}_1, \tilde{K}_1', st_S, st_S')$ and randomly chosen K_1^* and obtains the challenge ciphertext CT^* encrypting K_0^* or K_1^*. Then, B sends CT^* as CT_i' to $\mathcal{A}$. After that, if $\mathcal{A}$ outputs b', then B outputs $b = b'$. If $b = 0$ holds, the environment for $\mathcal{A}$ is identical to $\mathbf{H}_2$, and otherwise, the environment for $\mathcal{A}$ is identical to $\mathbf{H}_3$. Therefore, if $\mathcal{A}$ distinguishes $\mathbf{H}_3$ from $\mathbf{H}_2$, B can break the selective CCA security.

Hence, $|\mathbf{Adv}(\mathcal{A}, \mathbf{H}_3) - \mathbf{Adv}(\mathcal{A}, \mathbf{H}_2)|$ is negligible.

6.4.5 Hybrid experiment $\mathbf{H}_4$

The computation of $K_1' = F''(sid, K_1)$ in the test session is changed. Instead of computing PRF, it is changed as choosing K_1' randomly.

In this experiment, K_1 is random. From the definition of PRF (Definition 1) $K_1' = F''(sid, K_1)$ is indistinguishable from randomly chosen K_1'.

Therefore, $|\mathbf{Adv}(\mathcal{A}, \mathbf{H}_4) - \mathbf{Adv}(\mathcal{A}, \mathbf{H}_3)|$ is negligible.

6.4.6 Bounding the advantage in $\mathbf{H}_4$

In $\mathbf{H}_4$, $F''(sid, K_1)$ is replaced with random K_1'. Though $\mathcal{A}$ can obtain SK in the past time frame, $SK' = K_1' \oplus SK$ is random. Then, regardless of the challenge bit b for the test session, when $\mathcal{A}$ poses Test query, a random session key is returned.

Therefore, $\mathbf{Adv}(\mathcal{A}, \mathbf{H}_4)$ is negligible. □

7 General setting of our protocol

In this section, we show the general setting that multiple users can join/leave the group simultaneously.

7.1 System setup

The system setup is the same as the simple case.

7.2 Dist phase

The Dist phase is the same as the simple case.

7.3 Join phase

A new set of users $U_{i_{n+1}}, \ldots, U_{i_{n+k}}$ join an established session by $U_1, \ldots, U_n$. W.l.o.g., we suppose that $(U_{i_{n+1}}, \ldots, U_{i_{n+k}}) = (U_{n+1}, \ldots, U_{n+k})$.

In the Join phase, users U_i for $i \in [2, n-1]$ can reduce computation than the Dist phase. They do not need to compute g^{r_i}. The ring structure to compute K_1 still works because r in $state_i$ is used to connect the ring instead of using r_i.

(State Update at New Time Frame) If the session is the first session for U_i at the time frame TF', then for the current time $time$ S generates $usk_i \leftarrow \mathbf{Der}(Params, msk, A_i)$ with attribute $A_i = (U_i, time)$ and $mk_i \leftarrow \mathbf{MGen}$ and computes $CT_i \leftarrow \mathbf{Enc}_{pk_i}(usk_i, mk_i)$. Then, S sends CT_i to U_i, and U_i obtains $(usk_i, mk_i) \leftarrow \mathbf{Dec}_{sk_i}(CT_i)$ and updates (usk_i, mk_i) in $state_i$.

(Round 1 for Users) For $i \in \{1\} \cup [n, n+k]$, U_i generates $\tilde{r}_i \in_R \{0,1\}^\kappa$, $\tilde{r}_i' \in_R \mathsf{Kspace}_\kappa$, $\tilde{k}_i \in_R \{0,1\}^\kappa$, $\tilde{k}_i' \in_R \mathsf{Kspace}_\kappa$, $\tilde{s}_i \in_R \{0,1\}^\kappa$ and $\tilde{s}_i' \in_R \mathsf{Kspace}_\kappa$ as ESK_i and computes $r_i = tPRF(\tilde{r}_i, \tilde{r}_i', st_i, st_i')$, $k_i = tPRF(\tilde{k}_i, \tilde{k}_i', st_i, st_i')$ and $s_i = tPRF(\tilde{s}_i, \tilde{s}_i', st_i, st_i')$. U_i computes $R_i = g^{r_i}$ and $c_i = g^{k_i} h^{s_i}$ and sends (R_i, c_i) to S.

For $i \in [2, n-1]$, U_i generates $\tilde{k}_i \in_R \{0,1\}^\kappa$, $\tilde{k}_i' \in_R \mathsf{Kspace}_\kappa$, $\tilde{s}_i \in_R \{0,1\}^\kappa$ and $\tilde{s}_i' \in_R \mathsf{Kspace}_\kappa$ as ESK_i and computes $k_i = tPRF(\tilde{k}_i, \tilde{k}_i', st_i, st_i')$ and $s_i = tPRF(\tilde{s}_i, \tilde{s}_i', st_i, st_i')$. U_i computes $c_i = g^{k_i} h^{s_i}$ and sends c_i to S.

(Round 1 for Server) On receiving (R_i, c_i) for $i \in \{1\} \cup [n, n+k]$ and c_i for $i \in [2, n-1]$, S computes $sid = TCR(c_1, \ldots, c_{n+k})$ and chooses a representative user from $i \in \{1\} \cup [n, n+k]$. Here, w.l.o.g., we suppose that U_1 is the representative user. For $i \in [n+1, n+k]$, S sends (sid, R_{i-1}, R_{i+1}) to U_i where $R_{n+k+1} = R_1$. For $i \in \{1, 2\}$, S sends (sid, R_{i-1}) to U_i where $R_0 = R_{n+k}$. For $i \in [3, n-2]$, S sends sid to U_i. Also, S notices that U_1 is the representative user.

(Round 2 for Users) On receiving (sid, R_{n+k}), U_1 computes $K_1^{(l)} = F(sid, R_{n+k}^{r_1})$, $K_1^{(r)} = F(sid, g^{r_1 r})$, $T_1 = K_1^{(l)} \oplus K_1^{(r)}$ and $T' = K_1^{(l)} \oplus (k_1 || s_1)$. U_1 computes $\sigma_1 \leftarrow \mathbf{Tag}_{mk_1}(R_1, c_1, R_{n+k}, T_1, T', U_1, sid)$ and sends (T_1, T', σ_1) to S.

On receiving (sid, R_1), U_2 computes $K_2^{(l)} = F(sid, R_1^r)$, $K_2^{(r)} = F(sid, g^r)$ and $T_2 = K_2^{(l)} \oplus K_2^{(r)}$. U_2 computes $\sigma_2 \leftarrow \mathbf{Tag}_{mk_2}(c_2, R_1, k_2, s_2, T_2, U_2, sid)$ and sends $(k_2, s_2, T_2, \sigma_2)$ to S.

For $i \in [3, n-2]$, on receiving sid, U_i computes $\sigma_i \leftarrow \mathbf{Tag}_{mk_i}(c_i, k_i, s_i, U_i, sid)$ and sends (k_i, s_i, σ_i) to S.

On receiving (sid, R_n), U_{n-1} computes $K_{n-1}^{(l)} = F(sid, g^r)$, $K_{n-1}^{(r)} = F(sid, R_n^r)$ and $T_{n-1} = K_{n-1}^{(l)} \oplus K_{n-1}^{(r)}$. U_{n-1} computes $\sigma_{n-1} \leftarrow \mathbf{Tag}_{mk_{n-1}}(c_{n-1}, R_n, k_{n-1}, s_{n-1}, T_{n-1}, U_{n-1}, sid)$ and sends $(k_{n-1}, s_{n-1}, T_{n-1}, \sigma_{n-1})$ to S.

On receiving (sid, R_{n+1}), U_n computes $K_n^{(l)} = F(sid, R_n^r)$, $K_n^{(r)} = F(sid, R_{n+1}^{r_n})$ and $T_n = K_n^{(l)} \oplus K_n^{(r)}$. U_n computes $\sigma_n \leftarrow \mathbf{Tag}_{mk_n}(R_n, c_n, R_{n+1}, k_n, s_n, T_n, U_n, sid)$ and sends $(k_n, s_n, T_n, \sigma_n)$ to S.

For $i \in [n+1, n+k]$, on receiving (sid, R_{i-1}, R_{i+1}), U_i computes $K_i^{(l)} = F(sid, R_{i-1}^{r_i})$, $K_i^{(r)} = F(sid, R_{i+1}^{r_i})$ and $T_i = K_i^{(l)} \oplus K_i^{(r)}$. U_i computes $\sigma_i \leftarrow \mathbf{Tag}_{mk_i}(R_i, c_i, R_{i-1}, R_{i+1}, k_i, s_i, T_i, U_i, sid)$ and sends $(k_i, s_i, T_i, \sigma_i)$ to S.

(Round 2 for Server) On receiving (T_1, T', σ_1) from U_1, $(k_i, s_i, T_i, \sigma_i)$ for $i \in \{2\} \cup [n-1, n+k]$ and (k_i, s_i, σ_i) for $i \in [3, n-2]$, S verifies authentication tags, and if the verification fails, then aborts. Also, for $i \in [2, n+k]$, S checks if $c_i = g^{k_i} h^{s_i}$ holds, and if the verification fails, then aborts. S generates $\tilde{k}_S \in_R \{0,1\}^\kappa$, $\tilde{k}_S' \in_R \mathsf{Kspace}_\kappa$, $\tilde{K}_1 \in_R \{0,1\}^\kappa$ and $\tilde{K}_1' \in_R Kspace_\kappa$ as ESK_S and computes $k_S = tPRF(\tilde{k}_S, \tilde{k}_S', st_S, st_S')$, $K_1 = tPRF'(\tilde{K}_1, \tilde{K}_1', st_S, st_S')$ and $k' = (\bigoplus_{2 \le i \le n+k} k_i) \oplus k_S$.

For $i \in [2, n+k]$, S computes $T_i' = \bigoplus_{1 \le j \le i-1} T_j$,

where for $i \in [3, n-1]$, T_i is treated as empty (i.e. $T'_3 = \cdots = T'_{n-1}$). For $i \in [1, n+k]$, S computes $CT'_i \leftarrow \mathbf{AEnc}(Params, P_i, K_1)$ with access structure $P_i := (ID = U_i) \wedge (time \in TF)$.
S computes $\sigma'_1 \leftarrow \mathbf{Tag}_{mk_1}(R_1, c_1, R_{n+k}, T_1, T', U_1, sid, k', CT'_1)$ and sends (k', CT'_1, σ'_1) to U_1.
S computes $\sigma'_2 \leftarrow \mathbf{Tag}_{mk_2}(c_2, R_1, k_2, s_2, T_2, U_2, sid, c_1, k', T'_2, T', CT'_2)$ and sends $(c_1, k', T'_2, T', CT'_2, \sigma'_2)$ to U_2.
For $i \in [3, n-2]$, S computes $\sigma'_i \leftarrow \mathbf{Tag}_{mk_i}(c_i, k_i, s_i, U_i, sid, c_1, k', T'_i, T', CT'_i)$ and sends $(c_1, k', T'_i, T', CT'_i, \sigma'_i)$ to U_i.
S computes $\sigma'_{n-1} \leftarrow \mathbf{Tag}_{mk_{n-1}}(c_{n-1}, R_n, k_{n-1}, s_{n-1}, T_{n-1}, U_{n-1}, sid, c_1, k', T'_{n-1}, T', CT'_{n-1})$ and sends $(c_1, k', T'_{n-1}, T', CT'_{n-1}, \sigma'_{n-1})$ to U_{n-1}.
S computes $\sigma'_n \leftarrow \mathbf{Tag}_{mk_n}(R_n, c_n, R_{n+1}, k_n, s_n, T_n, U_n, sid, c_1, k', T'_n, T', CT'_n)$ and sends $(c_1, k', T'_n, T', CT'_n, \sigma'_n)$ to U_n.
For $i \in [n+1, n+k]$, S computes $\sigma'_i \leftarrow \mathbf{Tag}_{mk_i}(R_i, c_i, R_{i-1}, R_{i+1}, k_i, s_i, T_i, U_i, sid, c_1, k', T'_i, T', CT'_i)$ and sends $(c_1, k', T'_i, T', CT'_i, \sigma'_i)$ to U_i.
(Session Key Generation and Post-computation) For $i \in [2, n+k]$, on receiving $(c_1, k', T'_i, T', CT'_i, \sigma'_i)$, U_i verifies the authentication tag, and if the verification fails, then aborts. U_i computes $K_1^{(l)} = T'_i \oplus K_i^{(l)}$ where for $i \in [3, n-1]$ $K_1^{(l)} = T'_i \oplus g^r$ and $k_1 || s_1 = T' \oplus K_1^{(l)}$ and checks if $c_1 = g^{k_1} h^{s_1}$ holds, and if the verification fails, then aborts. U_i decrypts $K_1 \leftarrow \mathbf{ADec}_{usk_i}(CT'_i, P_i)$, computes $K_2 = F'(sid, k' \oplus k_1)$ and outputs the session key $SK = F''(sid, K_1) \oplus F''(sid, K_2)$. As state information, U_i updates $r = F'''(sid, K_1) \oplus F'''(sid, K_2)$ in $state_i$. Also, U_n updates $H_n^{(r)} = R_{n+1}^{r_n}$ in $state_n$.
For $i \in [n+1, n+k]$, U_i adds sid, $H_i^{(l)} = R_{i-1}^{r_i}$ and $H_i^{(r)} = R_{i+1}^{r_i}$ to $state_i$.
On receiving (k', CT'_1, σ'_1), U_1 verifies the authentication tag, and if the verification fails, then aborts. U_1 decrypts $K_1 \leftarrow \mathbf{ADec}_{usk_1}(CT'_1, P_1)$, computes $K_2 = F'(sid, k' \oplus k_1)$ and outputs the session key $SK = F''(sid, K_1) \oplus F''(sid, K_2)$. As state information, U_1 updates sid, $H_1^{(l)} = R_{n+k}^{r_1}$ and $r = F'''(sid, K_1) \oplus F'''(sid, K_2)$ in $state_1$.

7.4 Leave phase

A set of users $\mathcal{R} = (U_{j_1}, \ldots, U_{j_m})$ leave an established session by $U_1, \ldots, U_n$. Let $\mathcal{N} = (U_{j_1-1}, U_{j_1+1}, U_{j_2-1}, U_{j_2+1}, \ldots, U_{j_m-1}, U_{j_m+1})$ be a set of users neighbouring leaved users. W.l.o.g., we suppose that $U_1 \in \mathcal{N}$.

In the Leave phase, users $U_i \in \mathcal{I} \backslash (\mathcal{R} \cup \mathcal{N})$ can reduce computation than the Dist phase. They do not need to compute g^{r_i}. The ring structure to compute K_1 still works because $H_i^{(l)}$ and $H_i^{(r)}$ in $state_i$ are used to connect the ring instead of using $g^{r_{i-1} r_i}$ and $g^{r_i r_{i+1}}$.

(State Update at New Time Frame) If the session is the first session for U_i at the time frame TF', then for the current time $time$ S generates $usk_i \leftarrow \mathbf{Der}(Params, msk, A_i)$ with attribute $A_i = (U_i, time)$ and $mk_i \leftarrow \mathbf{MGen}$ and computes $CT_i \leftarrow \mathbf{Enc}_{pk_i}(usk_i, mk_i)$. Then, S sends CT_i to U_i, and U_i obtains $(usk_i, mk_i) \leftarrow \mathbf{Dec}_{sk_i}(CT_i)$ and updates (usk_i, mk_i) in $state_i$.
(Round 1 for Users) $U_i \in \mathcal{N}$ generates $\tilde{r}_i \in_R \{0,1\}^\kappa$, $\tilde{r}'_i \in_R \mathsf{Kspace}_\kappa$, $\tilde{k}_i \in_R \{0,1\}^\kappa$, $\tilde{k}'_i \in_R \mathsf{Kspace}_\kappa$, $\tilde{s}_i \in_R \{0,1\}^\kappa$ and $\tilde{s}'_i \in_R \mathsf{Kspace}_\kappa$ as ESK_i and computes $r_i = tPRF(\tilde{r}_i, \tilde{r}'_i, st_i, st'_i)$, $k_i = tPRF(\tilde{k}_i, \tilde{k}'_i, st_i, st'_i)$ and $s_i = tPRF(\tilde{s}_i, \tilde{s}'_i, st_i, st'_i)$. Then, U_i computes $R_i = g^{r_i}$ and $c_i = g^{k_i} h^{s_i}$ and sends (R_i, c_i) to S.
$U_i \in \mathcal{I} \backslash (\mathcal{R} \cup \mathcal{N})$ generates $\tilde{k}_i \in_R \{0,1\}^\kappa$, $\tilde{k}'_i \in_R \mathsf{Kspace}_\kappa$, $\tilde{s}_i \in_R \{0,1\}^\kappa$ and $\tilde{s}'_i \in_R \mathsf{Kspace}_\kappa$ as ESK_i and computes $k_i = tPRF(\tilde{k}_i, \tilde{k}'_i, st_i, st'_i)$ and $s_i = tPRF(\tilde{s}_i, \tilde{s}'_i, st_i, st'_i)$. Then, U_i computes $c_i = g^{k_i} h^{s_i}$ and sends c_i to S.
(Round 1 for Server) On receiving (R_i, c_i) from $U_i \in \mathcal{N}$ and c_i from $U_i \in \mathcal{I} \backslash (\mathcal{R} \cup \mathcal{N})$, for i such that $U_i \in \mathcal{I} \backslash \mathcal{R}$, S computes $sid = TCR(\{c_i\}_{\mathcal{I} \backslash \mathcal{R}})$, chooses a representative user from $U_i \in \mathcal{N}$. Here, w.l.o.g., we suppose that U_1 is the representative user. For i such that $U_i \in \mathcal{N}$ and $U_{i+1} \in \mathcal{R}$, S sends (sid, R_j) to U_i where j is the minimum index such that $U_j \in \mathcal{N}$ and $j > i$. For i such that $U_i \in \mathcal{N}$ and $U_{i-1} \in \mathcal{R}$, S sends $(sid, R_{j'})$ to U_i where j is the maximum index such that $U_{j'} \in \mathcal{N}$ and $j' < i$. Then, S sends sid to $U_i \in \mathcal{I} \backslash (\mathcal{R} \cup \mathcal{N})$. Also, S notices that U_1 is the representative user.
(Round 2 for Users) For U_1, if $U_j = U_3$ and $U_{j'} = U_{n-1}$ hold, then on receiving (sid, R_3, R_{n-1}), U_1 computes $K_1^{(l)} = F(sid, R_{n-1}^{r_1})$, $K_1^{(r)} = F(sid, R_3^{r_1})$, $T_1 = K_1^{(l)} \oplus K_1^{(r)}$ and $T' = K_1^{(l)} \oplus (k_1 || s_1)$. For U_1, if $U_{j'} = U_{n-1}$ and $U_2 \in \mathcal{N}$ hold, then on receiving (sid, R_{n-1}), U_1 computes $K_1^{(l)} = F(sid, R_{n-1}^{r_1})$, $K_1^{(r)} = F(sid, H_1^{(r)})$, $T_1 = K_1^{(l)} \oplus K_1^{(r)}$ and $T' = K_1^{(l)} \oplus (k_1 || s_1)$. For U_1, if $U_j = U_3$ and $U_n \in \mathcal{N}$ hold, then on receiving (sid, R_3), U_1 computes $K_1^{(l)} = F(sid, H_1^{(l)})$, $K_1^{(r)} = F(sid, R_3^{r_1})$, $T_1 = K_1^{(l)} \oplus K_1^{(r)}$ and $T' = K_1^{(l)} \oplus (k_1 || s_1)$. U_1 computes $\sigma_1 \leftarrow \mathbf{Tag}_{mk_1}(R_1, c_1, (R_3, R_{n-1},) T_1, T', U_1, sid)$ and sends (T_1, T', σ_1) to S.
On receiving (sid, R_j), U_i such that $U_i \in \mathcal{N}$ and $U_{i+1} \in \mathcal{R}$ hold computes $K_i^{(l)} = F(sid, H_i^{(l)})$, $K_i^{(r)} = F(sid, R_j^{r_i})$ and $T_i = K_i^{(l)} \oplus K_i^{(r)}$. U_i computes $\sigma_i \leftarrow \mathbf{Tag}_{mk_i}(R_i, c_i, R_j, k_i, s_i, T_i, U_i, sid)$ and sends $(k_i, s_i, T_i, \sigma_i)$ to S.
On receiving $(sid, R_{j'})$, U_i such that $U_i \in \mathcal{N}$ and $U_{i-1} \in \mathcal{R}$ hold computes $K_i^{(l)} = F(sid, R_{j'}^{r_i})$, $K_i^{(r)} =$

$F(sid, H_i^{(r)})$ and $T_i = K_i^{(l)} \oplus K_i^{(r)}$. U_i computes $\sigma_i \leftarrow \mathbf{Tag}_{mk_i}(R_i, c_i, R_{j'}, k_i, s_i, T_i, U_i, sid)$ and sends $(k_i, s_i, T_i, \sigma_i)$ to S.

On receiving sid, $U_i \in \mathcal{I}\backslash(\mathcal{R} \cup \mathcal{N})$ computes $K_i^{(l)} = F(sid, H_i^{(l)})$, $K_i^{(r)} = F(sid, H_i^{(r)})$ and $T_i = K_i^{(l)} \oplus K_i^{(r)}$. U_i computes $\sigma_i \leftarrow \mathbf{Tag}_{mk_i}(c_i, k_i, s_i, T_i, U_i, sid)$ and sends $(k_i, s_i, T_i, \sigma_i)$ to S.

(Round 2 for Server) On receiving (T_1, T', σ_1) from U_1 and $(k_i, s_i, T_i, \sigma_i)$ from other users, S verifies the authentication tag, and if the verification fails, then aborts. Also, for $U_i \in \mathcal{I}\backslash(U_1 \cup \mathcal{R})$, S checks if $c_i = g^{k_i} h^{s_i}$ holds, and if the verification fails, then aborts. S generates $\tilde{k}_S \in_R \{0,1\}^\kappa$, $\tilde{k}'_S \in_R \mathsf{Kspace}_\kappa$, $\tilde{K}_1 \in_R \{0,1\}^\kappa$ and $\tilde{K}'_1 \in_R Kspace_\kappa$ as ESK_S and computes $k_S = tPRF(\tilde{k}_S, \tilde{k}'_S, st_S, st'_S)$ and $K_1 = tPRF'(\tilde{K}_1, \tilde{K}'_1, st_S, st'_S)$. For i such that $U_i \in \mathcal{I}\backslash(U_1 \cup \mathcal{R})$, S computes $k' = (\bigoplus\{k_i\}) \oplus k_S$. For i such that $U_i \in \mathcal{I}\backslash\mathcal{R}$, S computes $T'_i = \bigoplus_{1 \le j \le i-1} T_j$, where for j such that $U_j \in \mathcal{R}$, T_j is empty. For $U_i \in \mathcal{I}\backslash\mathcal{R}$, S computes $CT'_i \leftarrow \mathbf{AEnc}(Params, P_i, K_1)$ with access structure $P_i := (ID = U_i) \wedge (time \in TF)$.

S computes $\sigma'_1 \leftarrow \mathbf{Tag}_{mk_1}(R_1, c_1, (R_3, R_{n-1},) T_1, T', U_1, sid, k', CT'_1)$ and sends (k', CT'_1, σ'_1) to U_1.

For i such that $U_i \in \mathcal{N}$ and $U_{i+1} \in \mathcal{R}$, S computes $\sigma'_i \leftarrow \mathbf{Tag}_{mk_i}(R_i, c_i, R_j, k_i, s_i, T_i, U_i, sid, c_1, k', T'_i, T', CT'_i)$ and sends $(c_1, k', T'_i, T', CT'_i, \sigma'_i)$ to U_i.

For i such that $U_i \in \mathcal{N}$ and $U_{i-1} \in \mathcal{R}$, S computes $\sigma'_i \leftarrow \mathbf{Tag}_{mk_i}(R_i, c_i, R_{j'}, k_i, s_i, T_i, U_i, sid, c_1, k', T'_i, T', CT'_i)$ and sends $(c_1, k', T'_i, T', CT'_i, \sigma'_i)$ to U_i.

For $U_i \in \mathcal{I}\backslash(\mathcal{R} \cup \mathcal{N})$, S computes $\sigma'_i \leftarrow \mathbf{Tag}_{mk_i}(c_i, k_i, s_i, T_i, U_i, sid, c_1, k', T'_i, T', CT'_i)$ and sends $(c_1, k', T'_i, T', CT'_i, \sigma'_i)$ to U_i.

(Session Key Generation and Post-computation) On receiving $(c_1, k', T'_i, T', CT'_i, \sigma'_i)$, $U_i \in \mathcal{I}\backslash(U_1 \cup \mathcal{R})$ verifies the authentication tag, and if the verification fails, then aborts. U_i computes $K_1^{(l)} = T'_i \oplus K_i^{(l)}$ and $k_1 || s_1 = T' \oplus K_1^{(l)}$ and checks if $c_1 = g^{k_1} h^{s_1}$ holds, and if the verification fails, then aborts. U_i decrypts $K_1 \leftarrow \mathbf{ADec}_{usk_i}(CT'_i, P_i)$, computes $K_2 = F'(sid, k' \oplus k_1)$ and outputs the session key $SK = F''(sid, K_1) \oplus F''(sid, K_2)$. As state information, U_i updates $sid, r = F'''(sid, K_1) \oplus F'''(sid, K_2)$ in $state_i$. For i such that $U_i \in \mathcal{N}$ and $U_{i+1} \in \mathcal{R}$, U_i updates $H_i^{(r)} = R_j^{r_i}$ in $state_i$. For i such that $U_i \in \mathcal{N}$ and $U_{i-1} \in \mathcal{R}$, U_i updates $H_i^{(l)} = R_{j'}^{r_i}$ in $state_i$.

On receiving (k', CT'_1, σ'_1), U_1 verifies the authentication tag, and if the verification fails, then aborts. U_1 decrypts $K_1 \leftarrow \mathbf{ADec}_{usk_1}(CT'_1, P_1)$, computes $K_2 = F'(sid, k' \oplus k_1)$ and outputs the session key $SK = F''(sid, K_1) \oplus F''(sid, K_2)$. As state information, U_1 updates $sid, r = F'''(sid, K_1) \oplus F'''(sid, K_2)$ in $state_1$. If $U_2 \in \mathcal{R}$, then U_1 updates $H_1^{(r)} = R_j^{r_1}$ in $state_1$. If $U_n \in \mathcal{R}$, then U_1 updates $H_1^{(l)} = R_{j'}^{r_1}$ in $state_1$.

7.5 Update phase

The Update phase is the same as the simple case.

7.6 Complexity for users

Computational complexity of the general scheme is the same as the simple scheme. The Dist phase and the Update phase are the same as the simple scheme. In the Join phase, maximum online computations for a user are g^{r_i} and $g^{k_i} h^{s_i}$ for Round 1, $R_{i-1}^{r_i}$ and $R_{i+1}^{r_i}$ for Round 2, and $g^{k_1} h^{s_1}$ and the decryption of CT'_i for the session key generation. In the Leave phase, maximum online computations for a user are g^{r_i} and $g^{k_i} h^{s_i}$ for Round 1, $R_{i-1}^{r_i}$ for Round 2, and $g^{k_1} h^{s_1}$ and the decryption of CT'_i for the session key generation. Hence, for all phases, computational complexity of users is constant for the number of users.

Communication complexity of the general scheme is also the same as the simple scheme. The Dist phase and the Update phase are the same as the simple scheme. In the Join phase, maximum sent and received information for a user in online are (R_i, c_i) and (sid, R_{i-1}, R_{i+1}) for Round 1, and $(k_i, s_i, T_i, \sigma_i)$ and $(c_1, k', T'_i, T', CT'_i, \sigma'_i)$ for Round 2. In the Leave phase, maximum sent and received information for a user in online are (R_i, c_i) and (sid, R_{i-1}) for Round 1, and $(k_i, s_i, T_i, \sigma_i)$ and $(c_{j-1}, k', T'_{j+1}, T', CT'_{j+1}, \sigma'_{j+1})$ for Round 2. Hence, for all phases, communication complexity of users is constant for the number of users.

7.7 Security

Since the Dist phase and the Update phase are the same as the simple scheme, the security proof is also the same. Here, we discuss the security of the Join phase and the Leave phase.

For the Join phase, new k users join the group in the general scheme, while a single user joins the group in the simple scheme. However, in the security proof, $R_{i-1}^{r_i}$ and $R_{i+1}^{r_i}$ for new users are similarly changed to random values as in the hybrid experiment $\mathbf{H}_4$ of Sect. 6.1. Also, r for $i \in [2, n-1]$ is changed to a random value as in Sect. 6.2. Hence, we can prove the security of the Join phase in the general scheme by the same way as the simple scheme.

For the Leave phase, m users leave the group in the general scheme, while a single user leaves the group in the simple scheme. However, in the security proof, $H_i^{(r)}$ and $H_i^{(l)}$ for remaining users are similarly changed to random values as

in Sect. 6.3. If all secret keys for m users are exposed, the adversary cannot distinguish this transition from the definition of DDH assumption (Definition 8). Hence, we can prove the security of the Leave phase in the general scheme by the same way as the simple scheme.

Acknowledgements This work is supported in part by JSPS KAKENHI Grant Number 15H06063.

Compliance with ethical standards

This paper follows ethical rules of the journal as follows: Originality: This paper extends our earlier extended abstract [40]. The earlier abstract introduces a new security model and construction of multi-cast key distribution (MKD). This submission adds following new results: 1. Though the earlier abstract does not give the security proof of the proposed scheme, we show the security proof formally. 2. In the earlier abstract, the proposed MKD scheme only captures a simple setting (i.e. only one user joins/leaves the group simultaneously) because of simplicity, and it is just described that an extension to the general setting will be possible. In this paper, we give a concrete protocol of MKD in the general setting (i.e. multiple users can join/leave the group simultaneously). This manuscript is the authors' original work and has not been published nor has it been submitted simultaneously elsewhere.

Conflicts of interest This paper does not receive any funding because the work is done as an academic research.

Research involving human participants and/or animals This paper does not involve any human participants and animals.

Informed consent Any informed consent is not necessary for this paper because it does not involve any human participants and animals.

References

1. Al-Riyami, S.S., Paterson, K.G.: Tripartite authenticated key agreement protocols from pairings. In: IMA International Conference 2003, pp. 332–359 (2003)
2. Bellare, M., Rogaway, P.: Entity authentication and key distribution. In: CRYPTO 1993, pp. 232–249 (1993)
3. Bergkvist, A., Burnett, D.C., Jennings, C., Narayanan, A., Aboba, B.: WebRTC 1.0: real-time communication between browsers. In: InfoQ (2015)
4. Berjon, R., Leithead, T., Navara, E.D., O'Connor, E., Pfeiffer, S.: HTML5. In: W3C working draft (2012)
5. Bresson, E., Chevassut, O., Pointcheval, D.: Provably authenticated group Diffie–Hellman key exchange—the dynamic case. In: Boyd C. (ed.) Advances in Cryptology—ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, 9–13 Dec 2001 Proceedings, Lecture Notes in Computer Science, vol. 2248, pp. 290–309. Springer (2001)
6. Bresson, E., Chevassut, O., Pointcheval, D.: Dynamic group Diffie–Hellman key exchange under standard assumptions. In: Knudsen L.R. (ed.) Advances in Cryptology—EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, 28 April–2 May 2002, Proceedings, Lecture Notes in Computer Science, vol. 2332, pp. 321–336. Springer (2002)
7. Bresson, E., Chevassut, O., Pointcheval, D., Quisquater, J.: Provably authenticated group Diffie–Hellman key exchange. In: Reiter M.K., Samarati P. (eds.) CCS 2001, Proceedings of the 8th ACM Conference on Computer and Communications Security, Philadelphia, Pennsylvania, USA, 6–8 Nov 2001, pp. 255–264. ACM (2001)
8. Canetti, R., Garay, J.A., Itkis, G., Micciancio, D., Naor, M., Pinkas, B.: Multicast security: A taxonomy and some efficient constructions. In: Proceedings IEEE INFOCOM '99, The Conference on Computer Communications, Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies, The Future Is Now, New York, NY, USA, 21–25 March 1999, pp. 708–716. IEEE (1999)
9. Caronni, G., Waldvogel, M., Sun, D., Plattner, B.: Efficient security for large and dynamic multicast groups. In: 7th Workshop on Enabling Technologies (WETICE '98), Infrastructure for Collaborative Enterprises, 17–19 June 1998, Palo Alto, CAUSA, Proceedings, pp. 376–383. IEEE Computer Society (1998)
10. Chesters, J.: Mozilla blocks flash, encourages HTML5 adoption. In: InfoQ (2015)
11. Cremers, C.J.F., Feltz, M.: Beyond eCK: perfect forward secrecy under actor compromise and ephemeral-key reveal. In: ESORICS 2012, pp. 734–751 (2012)
12. Dutta, R., Barua, R.: Constant round dynamic group key agreement. In: Zhou J., Lopez v, Deng R.H., Bao F. (eds.) Information Security, 8th International Conference, ISC 2005, Singapore, 20–23 Sept 2005, Proceedings, Lecture Notes in Computer Science, vol. 3650, pp. 74–88. Springer (2005)
13. Fischl, J., Tschofenig, H., Rescorla, E.: Framework for establishing a secure real-time transport protocol (SRTP), security context using datagram transport layer security (DTLS). In: IEFT RFC pp. 5763. (2010)
14. Fujioka, A., Manulis, M., Suzuki, K., Ustaoglu, B.: Sufficient condition for ephemeral key-leakage resilient tripartite key exchange. In: ACISP 2012, pp. 15–28 (2012)
15. Fujioka, A., Suzuki, K., Xagawa, K., Yoneyama, K.: Strongly secure authenticated key exchange from factoring, codes, and lattices. Des. Codes Cryptogr. **76**(3), 469–504 (2015)
16. Gorantla, M.C., Boyd, C., Nieto, J.M.G.: Modeling key compromise impersonation attacks on group key exchange protocols. In: Public Key Cryptography, pp. 105–123 (2009)
17. Joux, A.: A One round protocol for tripartite Diffie–Hellman. In: ANTS 2000, pp. 385–394 (2000)
18. Katz, J., Shin, J.S.: Modeling insider attacks on group key-exchange protocols. In: ACM Conference on Computer and Communications Security, pp. 180–189 (2005)
19. Katz, J., Yung, M.: Scalable protocols for authenticated group key exchange. In: CRYPTO, pp. 110–125 (2003)
20. Kim, H., Lee, S., Lee, D.H.: Constant-round authenticated group key exchange for dynamic groups. In: Lee P.J. (ed.) Advances in Cryptology—ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, 5–9 Dec 2004, Proceedings, Lecture Notes in Computer Science, vol. 3329, pp. 245–259. Springer (2004)
21. Kurosawa, K., Furukawa, J.: 2-pass key exchange protocols from cpa-secure KEM. In: Benaloh J. (ed.) Topics in Cryptology—CT-RSA 2014—The Cryptographer's Track at the RSA Conference 2014, San Francisco, CA, USA, 25–28 Feb 2014. Proceedings, Lecture Notes in Computer Science, vol. 8366, pp. 385–401. Springer (2014)
22. LaMacchia, B.A., Lauter, K.E., Mityagin, A.: Stronger security of authenticated key exchange. In: Susilo W., Liu J.K., Mu Y. (eds.) Provable Security, First International Conference, ProvSec 2007, Wollongong, Australia, 1–2 Nov 2007, Proceedings, Lecture Notes in Computer Science, vol. 4784, pp. 1–16. Springer (2007)
23. Lin, I., Tang, S., Wang, C.: Multicast key management without rekeying processes. Comput. J. **53**(7), 939–950 (2010)

24. Manulis, M., Suzuki, K., Ustaoglu, B.: Modeling leakage of ephemeral secrets in tripartite/group key exchange. In: Lee D.H., Hong S. (eds.) Information, Security and Cryptology—ICISC 2009, 12th International Conference, Seoul, Korea, 2–4 Dec 2009, Revised Selected Papers, Lecture Notes in Computer Science, vol. 5984, pp. 16–33. Springer (2009)
25. Marshall, J.: Google Chrome Will Begin Blocking Flash Web Ads. In: The Wall Street Journal: (2015)
26. Micciancio, D., Panjwani, S.: Optimal communication complexity of generic multicast key distribution. In: Cachin C., Camenisch J. (eds.) Advances in Cryptology—EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2–6 May 2004, Proceedings, Lecture Notes in Computer Science, vol. 3027, pp. 153–170. Springer (2004)
27. Mittal, N., Kumar, V.: An efficient and secure multicast key management scheme based on star topology. Int. J. Comput. Sci. Inf. Technol. **5**(3), 3777–3783 (2014)
28. Rescorla, E.: WebRTC Security architecture, draft-ietf-rtcweb-security-arch-11. In: IETF Draft (2015)
29. Saravanan, K., Purusothaman, T.: Efficient star topology based multicast key management algorithm. J. Comput. Sci. **8**(6), 951–956 (2012)
30. Schulzrinne, H., Casner, S.L., Frederick, R., Jacobson, V.: RTP: A transport protocol for real-time applications. In: IEFT RFC 3550 (2003)
31. Sherman, A.T., McGrew, D.A.: Key establishment in large dynamic groups using one-way function trees. IEEE Trans. Softw. Eng. **29**(5), 444–458 (2003)
32. Shoup, V.: Sequences of games: a tool for taming complexity in security proofs. In: Cryptology ePrint Archive: 2004/332 (2004)
33. Sun, H., He, B., Chen, C., Wu, T., Lin, C., Wang, H.: A provable authenticated group key agreement protocol for mobile environment. Inf. Sci. **321**, 224–237 (2015)
34. Suzuki, K., Yoneyama, K.: Exposure-resilient one-round tripartite key exchange without random oracles. In: Jr. M.J.J., Locasto M.E., Mohassel P., Safavi-Naini R. (eds.) Applied Cryptography and Network Security—11th International Conference, ACNS 2013, Banff, AB, Canada, 25–28 June 2013. Proceedings, Lecture Notes in Computer Science, vol. 7954, pp. 458–474. Springer (2013)
35. Suzuki, K., Yoneyama, K.: Exposure-resilient one-round tripartite key exchange without random oracles. IEICE Trans. **97–A**(6), 1345–1355 (2014)
36. Waldvogel, M., Caronni, G., Sun, D., Weiler, N., Plattner, B.: The versakey framework: versatile group key management. IEEE J. Sel. Areas Commun. **17**(9), 1614–1631 (1999)
37. Westerlund, M., Wenger, S.: RTP Topologies, draft-ietf-avtcore-rtp-topologies-update-07. In: IETF Draft (2015)
38. Yang, G., Tan, C.H.: Dynamic group key exchange revisited. In: Heng S., Wright R.N., Goi B. (eds.) Cryptology and Network Security—9th International Conference, CANS 2010, Kuala Lumpur, Malaysia, 12–14 Dec 2010. Proceedings, Lecture Notes in Computer Science, vol. 6467, pp. 261–277. Springer (2010)
39. Yang, Z., Zhang, D.: Towards modelling perfect forward secrecy for one-round group key exchange. I. J. Netw. Secur. **18**(2), 304–315 (2016)
40. Yoneyama, K., Yoshida, R., Kawahara, Y., Kobayashi, T., Fuji, H., Yamamoto, T.: Multi-cast key distribution: scalable, dynamic and provably secure construction. ProvSec **2016**, 207–226 (2016)

Artif Life Robotics
DOI 10.1007/s10015-017-0369-y

ORIGINAL ARTICLE

Implementation of a decision support system using an interactive large-scale high-resolution display

Tomoyuki Ishida[1] · Yusuke Hirohara[1] · Nobuyuki Kukimoto[2] · Yoshitaka Shibata[3]

Received: 28 February 2017 / Accepted: 7 June 2017

Abstract In this research, we propose and evaluate a decision support system using an interactive large-scale high-resolution display. This decision support system supports the summarization and decision-making of a large amount of disaster information during the occurrence of a large-scale natural disaster. Municipal employees at the disaster control headquarters can display disaster information on the large-scale display with a touch or flick on a laptop or tablet. To evaluate the operability, readability, functionality, and necessity of the decision support system, we surveyed 23 municipal employees in the disaster prevention division using a questionnaire. The system received a great evaluation in all the evaluation items.

Keywords Decision support system · Tiled display system · Disaster information-sharing · Disaster management · Disaster control headquarters

This work was presented in part at the 22nd International Symposium on Artificial Life and Robotics, Beppu, Oita, January 19–21, 2017.

✉ Tomoyuki Ishida
tomoyuki.ishida.49@vc.ibaraki.ac.jp

Yusuke Hirohara
mikado0903h@gmail.com

Nobuyuki Kukimoto
kukimoto@atinde.com

Yoshitaka Shibata
shibata@iwate-pu.ac.jp

[1] Ibaraki University, Hitachi, Ibaraki, Japan

[2] ATINDE Inc., Yukuhashi, Fukuoka, Japan

[3] Iwate Prefectural University, Takizawa, Iwate, Japan

1 Introduction

When large-scale natural disasters, such as the Great East Japan Earthquake, and local natural disasters, such as typhoons, occur, disaster response measures are taken at the municipality level, not at the country or prefecture level. When a natural disaster occurs, disaster control headquarters and disaster alert headquarters are established by the local government. As control centers, these headquarters should gather the necessary disaster information from the control tower without delay to take timely and appropriate disaster response measures. However, many local governments' disaster control headquarters have not introduced systems for summarizing and sharing the disaster information. Currently, local government's disaster control headquarters typically use blackboards and vellum papers to summarize and share disaster information. The disaster control headquarters is the primary decision-making body during the occurrence of a natural disaster. By summarizing and sharing disaster information using blackboards and vellum papers, they risk missing important information. Therefore, to solve this issue, we must provide modern tools for information collection and sharing in disaster control headquarters.

2 Related work

The Cabinet Office's comprehensive disaster prevention information system [1–3] supports early assessment of the damage situation as well as prompt and accurate decision-making during the occurrence of a large-scale natural disaster. In addition, this system can share geospatial information about the disaster among relevant administrative departments. However, although this system has a huge

Published online: 12 June 2017

budget, its cost effectiveness has been questioned from various quarters. In addition, the system provides no means to cooperate with the municipalities, so it is impossible to share detailed information with each municipality. Furthermore, it is a large-scale system that requires a huge budget. Therefore, it is difficult for municipalities to introduce this system.

The Ministry of Internal Affairs and Communications' public information commons [4] is an information infrastructure aimed at summarizing and sharing disaster information, which is then transmitted to residents promptly and accurately. Residents can obtain information from the public information commons through various media, such as television, radio, mobile phone, and a Web portal. However, the public information commons is designed to allow the disaster information to be shared with the prefecture in order to assess the situation in each municipality. It is, therefore, difficult to share disaster information with other municipalities.

3 Purpose of the research

In this research, we construct a decision support system for disaster countermeasures using an interactive large-scale high-resolution display. This system allows registered information to be quickly shared with the disaster control headquarters. It also displays digitized disaster information and valuable "big data" information posted on SNS and elsewhere on a large display in the disaster control headquarters. Consequently, the system supports the summarization and decision-making of a large amount of disaster information. The large display provides a large-scale display environment that uses an inexpensive commercially available liquid crystal display as a platform for simultaneously displaying a variety of content. In addition, it offers a decision-making system that considers a diverse range of disaster information (about house collapses, medical institutions, relief supplies, and traffic) and media (e.g., videos, pictures, Web pages, and documents). The decision-making system displays disaster information on the large-scale display with a touch or flick from a laptop or tablet.

4 System configuration

The configuration of our system is shown in Fig. 1. The system comprises a disaster information interactive sharing agent, disaster information input agent, disaster information application server, and disaster information database server.

In addition, we introduced a tiled display system, allowing us to construct an interactive large-scale high-resolution

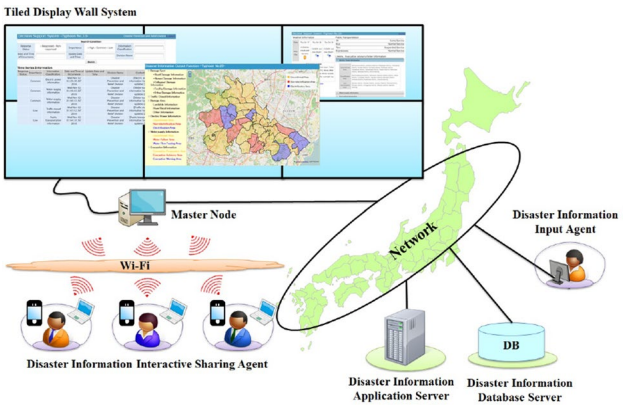

Fig. 1 System configuration

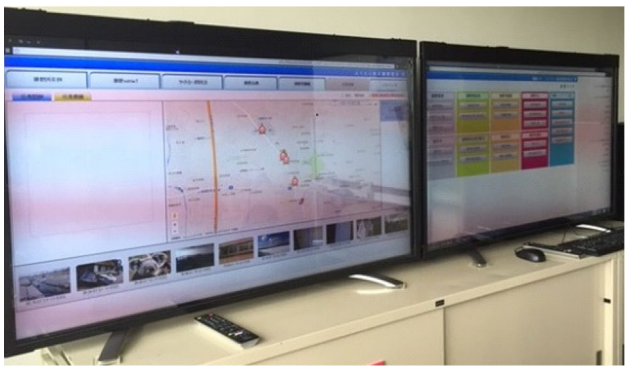

Fig. 2 Tiled display system

touch-enabled display. A tiled display wall was used to display high-resolution data on the large-scale display [5–8]. The tiled display wall system is used for constructing remote collaboration environments, such as a high-presence video conferencing system and a multi-point remote operation system.

We developed the interactive large-scale display environment by employing a tiled display system at the disaster control headquarters. The tiled display system used in this research is shown in Fig. 2.

When a large-scale natural disaster occurs, many stakeholders gather at the disaster control headquarters. Figure 3 shows the disaster control headquarters established in Takizawa City, Iwate Prefecture, when the Great East Japan Earthquake occurred. In such situations, large-scale displays play an important role in allowing members gathered at the disaster control headquarters to share the damage information and make appropriate decisions.

In addition, we surveyed multiple local governments and confirmed the necessity of large-scale displays. In the survey, municipal employees expressed an opinion that "we are sharing information on the blackboard at present,

Fig. 3 Actual disaster control headquarters for the Great East Japan Earthquake

so that we can respond quickly to disasters by using large-scale displays."

5 Decision support system

When a natural disaster occurs, the disaster control headquarters should summarize the huge amount of disaster information received both from the relevant administrative departments and from residents and assess the damage status. Therefore, we constructed a decision support system to summarize the disaster information registered by the disaster information registration system and support information-sharing and decision-making.

The disaster control headquarters needs the information summarized in Table 1 for decision-making and can confirm this information at a glance using the decision support system. This information is obtained mainly from firefighters, police, and municipal employees. On the other hand, casualty and damage information acquired from residents is also very important for decision-making by the disaster headquarters as this information is very up to date. The information received from residents is mainly reported to the disaster control headquarters via telephone.

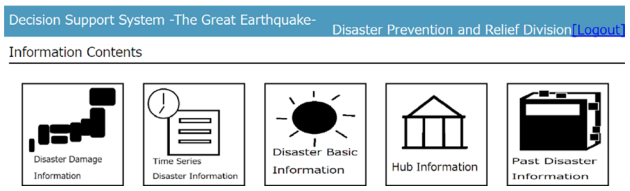

Fig. 4 Screenshot of the main screen of the decision support system

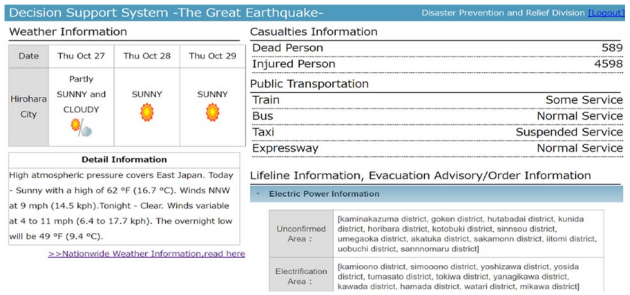

Fig. 5 Screenshot of the basic disaster information-sharing system

5.1 Main screen of the decision support system

The main screen of the decision support system is shown in Fig. 4. The decision support system is used on the interactive large-scale display established at the local government's disaster control headquarters. When the user selects an item on the main screen, the selected content is reflected on the interactive large-scale display.

5.2 Basic disaster information-sharing system

A screenshot of the basic disaster information-sharing system is shown in Fig. 5. This system can share information from the casualty, public transport, electrical, water, and evacuation order registration systems. The basic disaster information-sharing system supports decision-making, such as arranging water supply vehicles or recommending evacuation.

Table 1 Necessary information for decision-making

Type of disaster information	Information provider
Public transport information	Railway and bus companies
Casualty information	Firefighters, police, municipal employees, and residents
Medical institution information	Medical institutions
Damage information	Firefighters, police, municipal employees, and residents
Road block information	Firefighters, police, municipal employees, residents
River information	Firefighters, police, municipal employees, and residents
Shelter information	Municipal employees
Electrical information	Power company
Water supply information	Municipal water department and residents

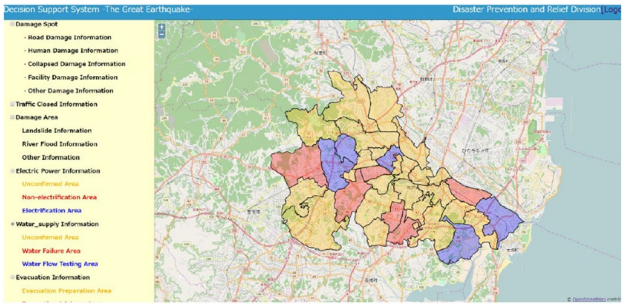

Fig. 6 Screenshot of the disaster damage information-sharing system (water supply information)

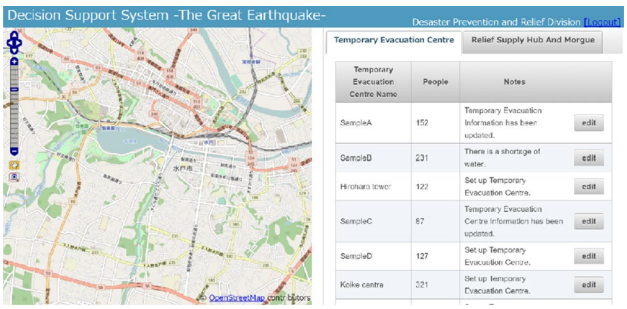

Fig. 7 Screenshot of the hub information-sharing system

5.3 Disaster damage information-sharing system

A screenshot of the disaster damage information-sharing system is shown in Fig. 6. This system can share information from the disaster damage, road block, damage area, electrical, water supply, and evacuation order information registration systems. The disaster damage information-sharing system supports decision-making, such as requests to the self-defense force for cooperation or dispatch of municipal employees.

5.4 Hub information-sharing system

A screenshot of the hub information-sharing system is shown in Fig. 7. The hub information-sharing system can share information from the temporary evacuation center, relief supply hub, and morgue information registration systems. It supports decision-making, such as dispatching municipal employees to the evacuation center or distribution of relief supplies.

5.5 Time-series disaster information-sharing system

A screenshot of the time-series disaster information-sharing system is shown in Fig. 8. This system can share all

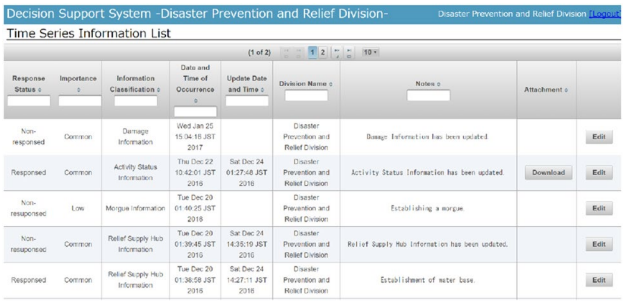

Fig. 8 Screenshot of the time-series disaster information-sharing system

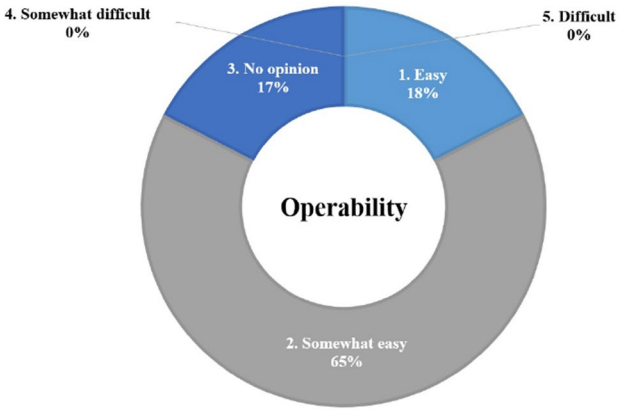

Fig. 9 Operability evaluation [total number of municipal employees (n) = 23]

the disaster information registered in the disaster information registration system. In addition, it supports decision-making by enabling prompt measures to be taken based on damage information presented in the time-series form.

6 Evaluation

To evaluate the operability, readability, functionality, and necessity of the decision support system, we surveyed 23 municipal employees of the disaster prevention division through a questionnaire.

6.1 Operability of the decision support system

The operability evaluation results for the decision support system are shown in Fig. 9. With regard to the operability of the decision support system, approximately 80% of the subjects answered “easy” or “somewhat easy” and none of the subjects answered “somewhat difficult”

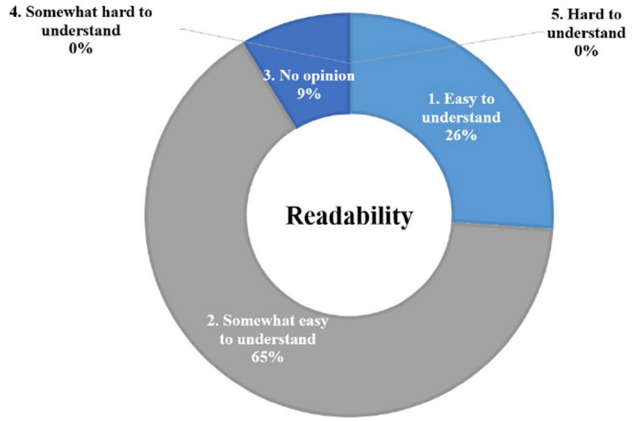

Fig. 10 Readability evaluation ($n = 23$)

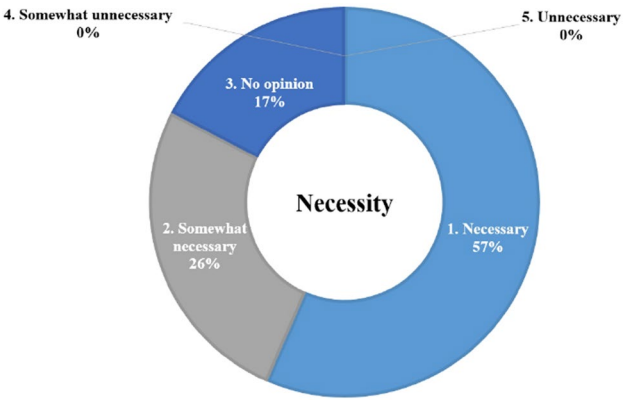

Fig. 12 Necessity evaluation ($n = 23$)

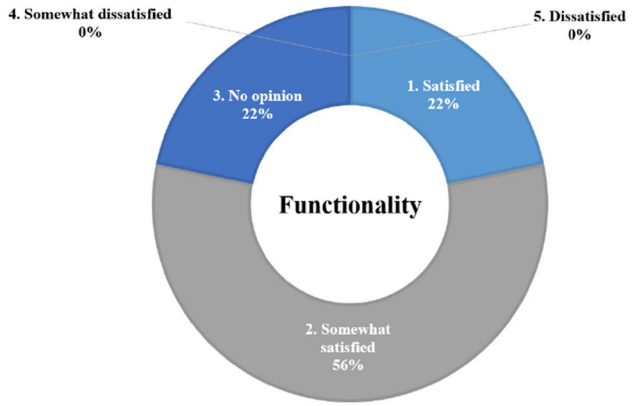

Fig. 11 Functionality evaluation ($n = 23$)

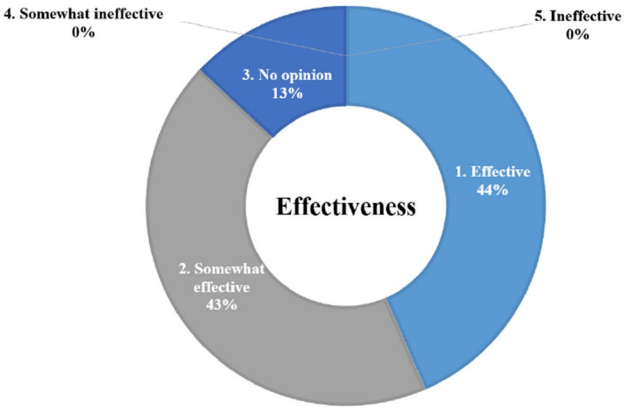

Fig. 13 Effectiveness evaluation for the large-scale display ($n = 23$)

or "difficult." Therefore, the results of the questionnaire indicate that the decision support system is easy in terms of operability.

6.2 Readability of the decision support system

The readability evaluation results for the decision support system are shown in Fig. 10. With respect to the readability of the decision support system, approximately 90% of the subjects answered "easy to understand" or "somewhat easy to understand" and none of the subjects answered "somewhat hard to understand" or "hard to understand." Therefore, the results of questionnaire indicate that the decision support system is easy in terms of readability.

6.3 Functionality of the decision support system

The functionality evaluation results for the decision support system are shown in Fig. 11. With regard to the functionality of the decision support system, approximately 70% of the subjects answered "satisfied" or "somewhat satisfied," and none of the subjects answered "somewhat dissatisfied" or "dissatisfied." Therefore, the results of the questionnaire indicate that the decision support system serves its function well.

6.4 Necessity of the decision support system

The necessity evaluation results for the decision support system are shown in Fig. 12. Regarding the necessity of the decision support system, about 80% of the subjects answered "necessary" or "somewhat necessary", and none of the subjects answered "somewhat unnecessary" or "unnecessary". Therefore, the results of the questionnaire indicate that the decision support system is needed.

6.5 Effectiveness of the large-scale display

The effectiveness evaluation results for the large-scale display are shown in Fig. 13. Regarding the effectiveness of the large-scale display, about 90% of the subjects answered

"effective" or "somewhat effective", and none of the subjects answered "somewhat ineffective" or "ineffective". Therefore, the results of the questionnaire indicate that the large-scale display is effective.

7 Conclusions

In this research, we constructed and evaluated a decision support system to formulate disaster countermeasures using an interactive large-scale high-resolution display. The system enabled rapid sharing of registered information at the disaster control headquarters, displaying a range of disaster information on the large-scale display from diverse information sources and media.

To evaluate the operability, readability, functionality, and necessity of the decision support system, 23 municipal employees of the disaster prevention division were surveyed through a questionnaire. The system received a great evaluation in all the evaluation items.

Acknowledgements This research was supported by a research Grant from the Telecommunications Advancement Foundation (TAF) of Japan and JSPS KAKENHI Grant Number JP16K00119.

References

1. Cabinet Office of Japan (2011) Employment of comprehensive disaster prevention information system towards sharing of information. http://www.bousai.go.jp/oukyu/higashinihon/4/pdf/naikakufu2.pdf. Accessed 10 Feb 2017
2. Cabinet Office of Japan (2012) Maintenance cost of comprehensive disaster prevention information system (administration projects review sheet, 2012). http://www.cao.go.jp/yosan/kanshi_korituka/pdf/sheet_6.pdf. Accessed 10 Feb 2017
3. Cabinet Office of Japan (2012) Cabinet secretariat and head office of cabinet office project reviews "disclosure process". http://www.cao.go.jp/yosan/kanshi_korituka/pdf/6.pdf. Accessed 10 Feb 2017
4. Shinetsu Bureau of Telecommunications (2013) Utilization guideline of the "Public Information Commons" and the Disaster Information Platform (third edition). http://www.soumu.go.jp/main_content/000263444.pdf. Accessed 10 Feb 2017
5. Ebara Y, Noda S, Sakuraba A, Shibata Y (2014), Experimental evaluation on transmission and display of ultra-resolution video on tiled display wall in JGN-X testbed. In: Proceedings of the 17th International Conference on Network-Based Information Systems (NBiS2014), Salerno, Italy, Sep. 10–12, 2014, pp 393–398
6. Ebara Y, Noda S, Sakuraba A, Shibata Y (2013) An Experiment on ultra-resolution video transmission with tiled display wall in wide-area network. In: Proceedings of the 16th International Conference on Network-Based Information Systems (NBiS2013), Gwangju, Korea, Sep. 4–6, 2013, pp 317–322
7. Ebara Y (2013) Experimental study on camera setting for telecommunication environment with tiled display wall. In: Proceedings of the 8th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Compiegne (3PGCIC-2013), France, Oct. 28–30, 2013, pp 563–568
8. Ebara Y (2012) Approaches to display of ultra-resolution video streaming by multi-transmission on tiled display environment. In: Proceedings of the 15th International Conference on Network-Based Information Systems (NBiS2012), Melbourne, Australia, Sep. 26–28, 2012, pp 540–545

Cross-lingual Product Recommendation System Using Collaborative Filtering

Kanako Komiya[†], Minoru Sasaki[†], Hiroyuki Shinnou[†] and Yoshiyuki Kotani[††]

We developed a cross-lingual recommender system using collaborative filtering with English-Japanese translation pairs of product names to help non-Japanese buyers who speak English when they are visiting Japanese shopping websites. Customer purchase histories at an English shopping site and those at another Japanese shopping site were used for the experiments. Two experiments were conducted to evaluate the system. They were (1) two-fold cross validation where half of the translation pairs were masked and (2) experiments where all of the translation pairs were used. The precisions, recalls, and mean reciprocal ranks (MRRs) of the system were evaluated to assess the general performance of the recommender system in the first set of experiments. We investigated the effect formatting the translation pairs and the performance according to the type of feature value of the vectors (binary versus rating values). In contrast, the kind of items that were recommended in a more realistic scenario were shown in the second experiment. The results reveal that masked items were found more efficiently than when the bestseller recommender system was used and, further, that items only on the Japanese site that seemed to be related to the buyers' interests could be found by the system in the more realistic scenario.

Key Words: *Cross-lingual, Recommendation, Collaborative Filtering, Translation Pair*

1 Introduction

Japanese pop culture such as that exemplified by manga, anime, and gaming has gained popularity with the younger generation in recent years. In addition, e-commerce has become widely used throughout the world and had enabled people to purchase products from abroad. However, there are some cases in which non-Japanese buyers are unable to find the products they want through Japanese shopping websites because the websites require Japanese queries. It is particularly difficult to translate product names such as the titles of anime or movies using machine translation. We developed a cross-lingual recommender system using collaborative filtering with English-Japanese translation pairs of product names to alleviate this problem. Even if non-Japanese buyers cannot formulate Japanese queries on Japanese shopping websites, the recommender system should capture their interests from their purchase histories and recommend

[†] Ibaraki University
[††] Tokyo University of Agriculture and Technology

Journal of Natural Language Processing Vol. 24 No. 4 September 2017

various products that they want.

Since we had no customer purchase histories for shopping sites in both English and Japanese, the customer purchase histories at an English shopping site and those at another Japanese shopping site were used together for the experiments. The precisions, recalls, and mean reciprocal ranks (MRRs) of four types of systems were evaluated to investigate the performance of the cross-lingual recommendation. Two kinds of experiments were conducted to evaluate the system: (1) two-fold cross validation, where half of the translation pairs were masked and (2) experiments where all the translation pairs were used. The experiments reveal that the system with collaborative filtering outperformed a bestseller recommender system and products only at the Japanese site that seemed to be related to buyers' interests could be found by the system.

This paper is structured as follows. Section 2 reviews related work on recommendations and other trials to solve the problem where non-Japanese buyers cannot buy some products via Japanese shopping sites. Section 3 explains the outline of the recommendation system that we developed. Section 4 describes the data we used, Section 5 demonstrates two processes to achieve our system, and Section 6 explains the experimental settings. We present the results in Section 7 and discuss them in Section 8. Finally, we conclude the paper in Section 9.

2 Related Work

Recommender systems, which involve recommending items such as products, pages, and articles, have been studied intensively in recent years. Methods of recommendation can be categorized into two types, i.e., content based and collaborative filtering based recommendations. We focused on the latter type in the current study.

There has been a large amount of work on the similarities between users for collaborative filtering. For example, (Symeonidis, Tiakas, and Manolopoulos 2010) defined similarities that took into consideration the strength of links between users on social network services (SNSs) and they used a graph based on similarities between links on SNSs and customer purchase histories.

In addition, (Kawamae, Sakano, Yamada, and Ueda 2009) proposed collaborative filtering based on the relationships between users who tended to purchase products ahead of other users by considering changes in users' interests. (Chang and Quiroga 2010) proposed a method of recommendation using bookmark data and content from Wikipedia to consider the serendipity of recommendations. (Musto, Semeraro, Gemmis, and Lops 2015) proposed content-based recommendation and (Ozsoy 2016) proposed an item recommendation system using the technique of word embedding.

Our purpose is to help the non-Japanese users of Japanese shopping sites who speak English to purchase products that are sold only on Japanese shopping sites. One way to solve this problem is to use machine translation techniques. However, it is difficult for machines to translate the titles of the books or movies because they contain few literal translations. In addition, machine translation techniques cannot be used, especially when we have no parallel corpora. (Tsuji, Nemoto, Luangpiensamut, Abe, Kimura, Komiya, Fujimoto, and Kotani 2012) proposed transliteration from Japanese product names to alphabetical queries to address this problem. We developed a cross-lingual recommender system and exploited another way of recommending products that are only sold on a Japanese shopping site to non-Japanese users. We believe that these two methods could be used together.

To our knowledge, the closest work to ours is the cross-lingual paper or keyword recommender systems proposed by (Uchiyama, Nanba, Aizawa, and Sagara 2011) and (Takasu 2010). However, they recommended papers or keywords for the abstracts of papers rather than products such as books and movies, and they did not use translation pairs but parallel corpora instead.

Recommendations using Linked Open Data (LOD) also correlate with our system because they also use no parallel corpora. (Pham, Jung, Nguyen, and Kim 2016) and (Mirizzi, Noia, Ostuni, and Ragone 2015) made cross-lingual recommendations using LOD without using collaborative filtering. However, we extracted the translation pairs from Wikipedia.

In addition, this research has a close relation to cross-domain recommender systems. According to (Cantador and Cremonesi 2014), our research belongs to linked-domain recommendation.

The contributions of this paper are as follows. (1) We achieved a cross-lingual recommendation system without any parallel corpora. We conducted linked-domain recommendation using simple collaborative filtering with only translation pairs and customer purchase histories at two shopping sites in different languages. (2) We assessed our system using cross validation of the translation pairs. This contribution enabled the cross-lingual recommender systems to be evaluated. In addition to the evaluation of the system, we showed some examples in a more realistic scenario.

3 Recommendation System to Help Non-Japanese Buyers

Figure 1 depicts the data flow diagram of the recommender system using collaborative filtering with translation pairs. Hereafter, buyers from Japanese shopping sites are referred to as "Japanese users," and buyers from English shopping sites are referred to as "English users."

As Figure 1 shows, Japanese items are recommended for each English user when the customer purchase history of that user is input into the system. The system performs two processes, item

Journal of Natural Language Processing Vol. 24 No. 4 September 2017

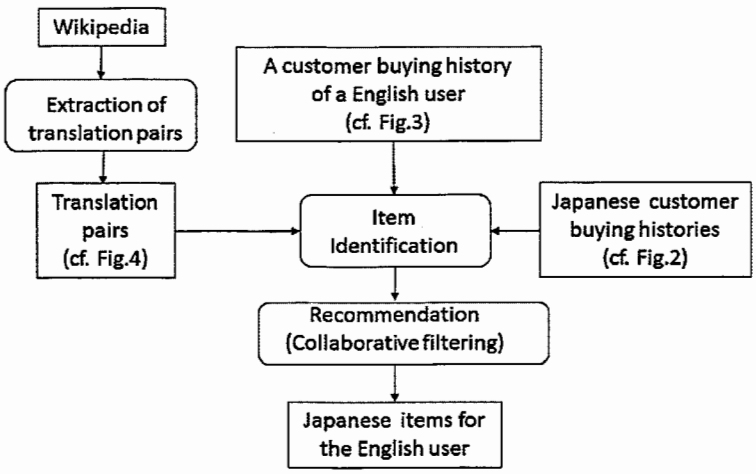

Fig. 1 Data flow diagram

identification and recommendation, that is, (1) the items at an English shopping site are identified as those at a Japanese shopping site using translation pairs extracted from Wikipedia and (2) the items at the Japanese shopping site are recommended using collaborative filtering.

4 Data

Two kinds of data, i.e., the customer purchase histories at English and Japanese shopping sites and English-Japanese translation pairs, were necessary to recommend items at a Japanese shopping site to non-Japanese buyers. Because we had no customer purchase histories of a shopping site in both English and Japanese, customer purchase histories from an English shopping site and those from another Japanese shopping site were used together in the experiments.

The review data of the Rakuten Ichiba in Rakuten Data Release[1] and MovieLens 10 M Dataset of GroupLens Research (Harper and Konstan 2015)[2] were used for the customer purchase histories on Japanese and English shopping sites, respectively. GroupLens Research has data on the movies. However, the Rakuten Data Release contains data on products in various genres. Therefore, the reviews from Rakuten Books,[3] which includes data on movies and books, were extracted for the experiments. We used the reviews as the customer purchase histories because they could only be written by users who had bought the items. We used not only movie data

[1] http://rit.rakuten.co.jp/opendata.html
[2] http://www.grouplens.org/
[3] http://books.rakuten.co.jp/

but also book data because the original stories of some movies were first written as books and movies are often novelized. The customer purchase histories we used are transactions that consist of three items of data: user IDs, product names, and their ratings. The ratings were graded by each user on a scale from one to five. Hereafter, items that were bought at both the English and Japanese sites are referred to as "common items." and are important because our system uses collaborative filtering.

The numbers of transactions, users, and transactions per user of the original data and the data of common items according to language are listed in Table 1 (in the column labeled "Without").

The English-Japanese translation pairs were collected from Japanese Wikipedia[4] using regular expressions.[5] Because the translation pairs consisted of Japanese movie titles extracted from their original titles, they included not only English translations but also translations into other languages such as French, Spanish, and Chinese. Table 1 lists the number of translation pairs, number of item types[6] in the original data, number of item types with translations in the original data, and common items (in the column labeled "Without").

Table 1 Statistics of the original data and data of the common items

Format		Without		With	
Language		Japanese	English	Japanese	English
Original	Transactions	352,692	442,849	346,104	442,845
Original	Users	82,176	62,839	81,159	62,839
Original	Transactions/user	4.29	7.05	4.26	7.05
Common Items	Transactions	794	10,947	2,553	32,623
Common Items	Users	705	2,835	1,935	7,372
Common Items	Transactions/user	1.13	3.86	1.32	4.43
Translation pairs		14,327		14,324	
Original	Types of items	235,777		196,326	
Original	Types of items with translation	2,633		4,081	
Common Items	Types of items with translation	236		506	

[4] http://ja.wikipedia.org/wiki/ (accessed 2012/12/20)

[5] Wikipedia data only contain translation pairs for famous items. It is desirable to use methods that generate more translation pairs to alleviate the sparsity of the data. For example, image recognition could be used in the future.

[6] We used the word "type" to distinguish the number of types from the number of tokens, i.e., the frequency. For example, the number of item types equals that of the product IDs if the products have them.

Journal of Natural Language Processing Vol. 24 No. 4 September 2017

5 Item Identification and Recommendation

As Figure 1 illustrates, the recommender system using collaborative filtering with translation pairs consists of two processes: item identification and recommendation using collaborative filtering. We used collaborative filtering with item overlap as Figure 2 shows (see (Cantador and Cremonesi 2014)).

5.1 Item Identification

The same items at the two sites are identified using English-Japanese translation pairs because they have different product names according to the language. Figures 3, 4 and 5 have examples of Japanese customer purchase histories, English customer purchase histories, and the translation

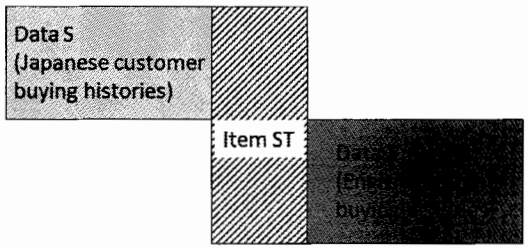

Fig. 2 Collaborative filtering with item overlap

```
User ID  Product name  Ratings
1  【予約】【楽天限定（国内）】 Crystal Ball × NYLON JAPAN ドリームコラボ・ラブリー トート
バッグ付 （ホワイト×ブラック ） 4
1  TSUMORI CHISATO 2010-11 AUTUMN & WINTER COLLECTION  5
1  【楽天管理商品】  4
2  ななちゃんとどうぶつさんワンワンワン  2
2  【送料無料】チャレンジミッケ！（5）  4
2  【送料無料】【ポイント4倍対象商品】Mr.Children / SENSE  1
```

```
User ID  Product name  Ratings
1  crystalballnylonjapan ドリームコラボラブリートートバッグ付  4
1  tsumorichisato201011autumnwintercollection  5
2  ななちゃんとどうぶつさんワンワンワン  2
2  チャレンジミッケ  4
2  mrchildrensense  1
```

Fig. 3 Examples of Japanese customer purchase histories

```
User ID  Product name  Ratings
1  Chasing Amy  5
1  Mr. Smith Goes to Washington  3
1  Return of the Jedi  5
1  Nadja  2
1  Weekend at Bernie's  3
1  Brothers McMullen, The  3
-------------------------------------------
User ID  Product name  Ratings
1  chasingamy  5
1  mrsmithgoestowashington  3
1  returnofjedi  5
1  nadja  2
1  weekendatbernies  3
1  brothersmcmullen  3
```

Fig. 4 Examples of English customer purchase histories

```
ナイトライダー        Knight Rider
最後の猿の惑星        BATTLE FOR THE PLANET OF THE APES
バラッド        The Elephant's Child
猿の惑星・征服        CONQUEST OF THE PLANET OF THE APES
東京オリンピック        Tokyo Olympiad
宇宙の旅        2001: A Space Odyssey
-------------------------------------------
ナイトライダー        knightrider
最後の猿の惑星        battleforplanetofapes
バラッド        elephantschild
猿の惑星征服        conquestofplanetofapes
東京オリンピック        tokyoolympiad
宇宙の旅        2001spaceodyssey
```

Fig. 5 Examples of translation pairs

pairs. The ones above the lines are the original text. As Figures 3 shows, Japanese customer purchase histories contain noise like "【送料無料】" (freight free), "（予約）" (pre-order), and "(Book 2)." These expressions should be removed to identify the product names. In addition, the formats of product names are varied: *The Godfather* in the translation pair list is *Godfather, The* in the customer purchase histories of the English shopping site. This kind of difference

Journal of Natural Language Processing Vol. 24 No. 4 September 2017

often prevents the products from being correctly identified. Therefore, we formatted the product names to improve product identification and called this process "formatting."

The procedures of this process are as follows.

(1) Expressions within brackets are removed to remove expressions such as "【送料無料】" (freight free), "（予約）" (pre-order), and "(Book 2)."
(2) All the Japanese one-byte characters are converted into two-byte characters.
(3) All the two-byte Latin characters used on Japanese shopping sites are converted into one-byte characters.
(4) All the Latin characters are converted into lower case.
(5) Articles are removed.
(6) Punctuation, marks such as apostrophes, and marks used on Japanese shopping sites such as "*" and "♪" are removed.
(7) Expressions like "special edition," "Blu-ray Disc Video," and "DVD コレクターズ BOX1" (DVD collectors BOX1) are removed using a stop words list, which included 65 words.

The text under the lines in Figures 3, 4 and 5 are formatted examples.

In addition, Table 1 shows that the number of the original data items decreased[7] but the number of common items increased as a results of the formatting. It also shows that the formatting decreased the number of translation pairs and the type of items in the original data, but increased the number of types of items with a translation.

After formatting, the items at the English shopping site are identified as those at the Japanese shopping site using the translation pairs extracted from Wikipedia. There are some items that have no translation, but they have no impact on the collaborative filtering. In this study, we demonstrate the effect of the item identification formatting.

5.2 Recommendation

We used collaborative filtering for the recommendations. Note that ordinary collaborative filtering can be used now that the items at the English shopping site are identified on the Japanese shopping site. The steps of this process are as follows.

(1) Vectors for English and Japanese users are generated. The features of the user vectors are the indices of the products and their values are binary, i.e., bought or not, or their ratings.
(2) Similarities between the English and Japanese users are calculated. Cosine similarities are used.

[7] All the words in some transactions are removed by formatting.

(3) Japanese users who are similar to English users are selected.

(4) Items that the Japanese users bought are recommended to the English users. (All the items bought by a Japanese user who is the most similar to an English user are recommended before any items bought by the Japanese user who is the second-most similar to him/her. If the feature values are ratings, items are recommended in order of the ratings for Japanese users.)

6 Experiments

Since the purpose of our research is to recommend items at a Japanese shopping site to non-Japanese buyers, we wanted to recommend items that were only sold at a Japanese shopping site to non-Japanese buyers. However, we could not automatically evaluate the performance of the recommender system using the customer purchase histories of products that were sold only at a Japanese shopping site because there were no customer purchase histories where English users purchased items at a Japanese site.

Therefore, two kinds of experiment were carried out to evaluate the system. They were (1) two-fold cross validation, where half of the translation pairs were masked and (2) experiments in which all the translation pairs were used. The former experiment assesses the general performance of the recommender system. In contrast, the latter experiments show what kinds of items were recommended in a more realistic scenario. The system in both sets of experiments recommended items from the Japanese shopping site to English users. A bestseller recommender system, in which the bestsellers at a Japanese shopping site were recommended in order of the number of times they were sold, was implemented and compared with the proposed method. The frequency with which an item was sold was calculated using all the customer purchase histories at the Japanese shopping site.[8] The Japanese customer purchase histories we used in these two kinds of experiments are summarized in Table 1. In the experiments, if a Japanese product name had multiple translations, we used all the translations. The items that were in the input vector were not recommended because we believe that most users do not purchase items that they already have.

[8] The bestseller baseline emphasizes popular products. We used this baseline, although it is unknown whether the data we used contain many of such products. This is because we think that our system can at least recommend items to those who purchase items that are not popular products.

Journal of Natural Language Processing Vol. 24 No. 4 September 2017

6.1 Cross Validation of Translation Pairs

In this experiment, two-fold cross validation, where half of the translation pairs are masked, was conducted. The items whose translation pair was masked were assumed to be the items sold only at a Japanese site. Only common items were used both in Japanese and English customer purchase histories because the other items on the two sites are too different from each other to assess the system using cross validation. The experiment consisted of five steps.

(1) Only common items were collected for the experiment.

(2) Half of the translation pairs were masked for the recommendation phase.[9]

(3) The common items with masked translations were masked for the test with respect to the English vectors.

(4) The system recommended items at a Japanese shopping site to English users.

(5) The system then checks if the recommended items have been bought by the English user using the uncovered translation pairs.

The system recommended not only items with masked translation pairs but also items with unmasked translation pairs. In addition, the translation pairs were divided into two groups without looking for the list of common items. Therefore, the number of masked items differ in the two validations. The item-based precisions and recalls at 1[10] (one recommended item per item) and at 10[11] (10 recommended items per item), the user-based precisions at 1 and at 10, and the MRRs[12] of the system were evaluated to assess the general performance of the recommender system. As the number of masked items differed in the two validations, micro-averaged precisions and recalls were assessed and F-measures were calculated based on them. However, macro-averaged MRRs were assessed because it is a criterion about ranks.

6.2 More Realistic Scenario

This experiment shows what kind of items were recommended in a more realistic scenario using all the translation pairs. Therefore, not only common items but also the items bought only by Japanese buyers were recommended. We present the examples and discuss them in Section 8 because the items only sold at a Japanese shopping site could not be automatically checked.

In addition, common items in English vectors were masked for the test and item-based preci-

[9] Note that not the customer buying histories but the translation pairs were divided for cross validation.
[10] The system recommended one item for one masked item.
[11] The system recommended ten items for one masked item.
[12] The system recommended any number of items for one masked item.

sions at 1 and recalls were evaluated for reference.[13] Cross validation of the items in the English vectors was conducted; half of the common items were masked and checked to determine if they were recommended by the system. Binary purchase values were used in this experiment. Two methods were used for the evaluations: strict and lenient evaluation methods. The system output is only correct in the strict evaluation when the masked item was recommended to users who bought it. However, the system output is correct in the lenient evaluation when the recommended item was bought by any of the users in the test set.

7 Results

Tables 2, 3, and 4 summarize item-based precisions, recalls, and F-measures, user-based precisions, and MRRs of experiments with cross validation of translation pairs. In addition, Table 5 shows item-based precisions, recalls, and F-measures of experiment in realistic scenario. "−" and "+" in the "Format" column means that the recommendations were performed without and with formatting, respectively. "Binary" and "value" in the Feature column means that the feature values for the recommendations were binary or rating values. "CF" in the tables means collaborative filtering. "1" and "10" in the "N of Answers" column means that the results at 1 and 10, respectively. Bestseller (English) in Table 5 means the case that only English items

Table 2 Item-based precision, recall, and F-measure of experiment with cross validation of the translation pairs

Format	Feature	Method	N of Answers	Precision	Recall	F-measure
−	binary	CF	1	0.55% (6/1,097)	0.15% (6/3,906)	0.24%
−	value	CF	1	0.55% (6/1,097)	0.15% (6/3,906)	0.24%
−		Bestseller	1	1.66% (65/3,906)	1.66% (65/3,906)	1.66%
+	binary	CF	1	6.39% (616/9,642)	5.27% (616/11,690)	5.78%
+	value	CF	1	6.56% (632/9,641)	5.41% (632/11,690)	5.93%
+		Bestseller	1	3.08% (360/11,690)	3.08% (360/11,690)	3.08%
−	binary	CF	10	0.53% (6/1,138)	0.15% (6/3,906)	0.24%
−	value	CF	10	0.70% (8/1,138)	0.20% (8/3,906)	0.32%
−		Bestseller	10	2.76% (1,086/39,386)	27.80% (1,086/3,906)	5.02%
+	binary	CF	10	6.12% (933/15,242)	7.98% (933/11,690)	6.93%
+	value	CF	10	6.12% (932/15,241)	7.97% (932/11,690)	6.92%
+		Bestseller	10	3.32% (3,880/117,013)	33.19% (3,880/11,690)	6.03%

[13] These experiments were conducted not to assess the performance of the system but to show some examples in a more realistic scenario.

Journal of Natural Language Processing Vol. 24 No. 4 September 2017

Table 3 User-based precision of the experiment with cross validation of the translation pairs

Format	Feature	Method	N of Answers	Precision
−	binary	CF	1	0.39%
−	value	CF	1	0.39%
−		Bestseller	1	1.08%
+	binary	CF	1	6.72%
+	value	CF	1	6.81%
+		Bestseller	1	1.41%
−	binary	CF	10	0.34%
−	value	CF	10	0.50%
−		Bestseller	10	18.51%
+	binary	CF	10	9.42%
+	value	CF	10	9.38%
+		Bestseller	10	16.17%

Table 4 MRR and rank of the experiment with cross validation of the translation pairs

Format	Featrue	Method	MRR	Rank
−	binary	CF	0.0181	55.31th
−	value	CF	0.0182	54.89th
−		Bestseller	0.0480	20.83th
+	binary	CF	0.1556	6.43th
+	value	CF	0.1355	7.38th
+		Bestseller	0.0584	17.12th

Table 5 Item-based precision, recall, and F-measure of the experiment in a realistic scenario

Method	Strictness	Precision	Recall	F-measure
CF	Strict	1.58% (74/4,678)	1.48% (74/4,998)	1.53
Bestseller	Strict	0.00% (0/4,998)	0.00% (0/4,998)	0.00
Bestseller (English)	Strict	0.90% (45/4,998)	0.90% (45/4,998)	0.90
CF	Lenient	14.92% (698/4,678)	13.97% (698/4,998)	14.43
Bestseller	Lenient	0.00% (0/4,998)	0.00% (0/4,998)	0.00

recommended. (This system could not recommend items sold only at a Japanese site.)

We defined the item-based precision, user-based precision, and recall as follows:

$$Precision_{item} = \frac{N_{item}}{Np_{item}} \tag{1}$$

$$Precision_{user} = \frac{N_{user}}{Np_{user}} \tag{2}$$

$$Recall_{item} = \frac{N_{item}}{Nr} \tag{3}$$

where N_{item}, Np_{item}, N_{user}, Np_{user}, and Nr correspond to the number of correct items output by the system, number of items output by the system, number of users the correct items are recommended to, number of all users to whom items are recommended by the system, and number of all masked items. Here, $\frac{1}{k}$ is added to N_{user} when one item is correct (k is the number of items that are masked for the user in question). Thus, user-based precision can be 100% only when all the items of all the users are correctly recommended.

In addition, MRR was calculated as:

$$MRR = \frac{1}{N}\sum_{i=1}^{N}\frac{1}{rank(i)} \tag{4}$$

where N denotes the number of test data (users) and $rank(i)$ denotes the highest ranking of the correct products that are recommended to user i. When none of the items recommended to user i are correct, $rank(i)$ is zero.

The rank of Table 4 shows the rank of the correct items that are generally recommended.

8 Discussion

8.1 Cross Validation of Translation Pairs

Table 2 shows that the collaborative filtering system outperformed the bestseller recommender system with respect to all criteria except for recall at 10 when item-based precisions, recalls, and F-measures are compared. In addition, although the recalls at 10 of bestseller recommender system (27.80% without formatting and 33.19% with formatting) substantially outperformed those of the collaborative filtering system (0.15% and 0.20% without formatting and 7.98% and 7.97% with formatting), this is only because the bestseller recommender system recommended many items; it recommended more than 34 times (without formatting) or seven times (with formatting) as many items as the collaborative filtering system recommended. Table 2 also shows that formatting makes the results better regardless of the method. In addition, the results improved with respect to all criteria except for the precision of the collaborative filtering system when the number of recommended items was increased from 1 to 10. The results are almost the same as for the precisions of the collaborative filtering system. Moreover, the results are almost identical to each other when the feature values were binary or ratings.

Table 3 shows that the bestseller recommender system was better in the use-based precision at 1 when the titles were not formatted,[14] but the collaborative filtering system was better when

[14] The results are very low.

Journal of Natural Language Processing Vol. 24 No. 4 September 2017

the titles were formatted. The same table shows that the bestseller recommender system was better at user-based precision at 10 regardless of formatting. The collaborative filtering system with formatting was the best when the user-based precisions at 1 are compared and the bestseller system was the best when the user-based precisions at 10 are compared. These results indicate that the collaborative filtering system recommended fewer correct products but did so more quickly. In addition, the results are almost identical to each other when the feature values were binary or rating values.

Moreover, Tables 2 and 3 show that the collaborative filtering system was better for the item-based precision at 10 but the bestseller system was better for the user-based precision at 10. These results indicate that the collaborative filtering system was better for the user who bought many items and that the bestseller system tends to recommend the correct products more for the user who buys fewer items. The original collaborative filtering has a cold start problem and this is also the case here.

Finally, Table 4 show that, as for MRR, the collaborative filtering system outperforms the bestseller system when the titles are formatted. In addition, formatting makes the results better regardless of the method. Moreover, the results are almost identical to each other yet again whether the feature values were binary or ratings. The collaborative filtering system with formatting when binary values were used was the best system. Table 4 shows that for the 6.43th item, the collaborative system recommends was generally correct although for the 17.12th item the bestseller recommender system recommends is generally correct. This indicates that the bestseller recommender system has to wait more than twice as long as the collaborative filtering system to make a sale.

8.2 More Realistic Scenario

Table 5 shows that the performance of the collaborative filtering system is low. In particular, the low values for lenient evaluations of the recommendations from the Japanese shopping site to English users indicate how different they are. The reason for the poor performances of recommendations from the Japanese shopping site is the difference in the items that the two shopping sites sell.

However, none of the items the bestseller recommender system recommended were bought by any English users. In addition, not only the strict precision and recall but also those of the lenient evaluation were 0%. Moreover, the bestseller recommender system could correctly recommend only 45 items even if the system recommended only items with translation pairs. These results reveal that naive collaborative filtering could better recommend items that the English buyers

bought than the bestseller recommender system.

Since the purpose of our research was to recommend items at a Japanese shopping site to non-Japanese buyers, the system is successful if it can recommend products that seem to be related with buyers' interests at only the Japanese site, even if the precision or recalls are low.

Therefore, we finally present examples of the recommender system outputs. For users who bought *Fantasia*, *Wizard of Oz, The*, *Pinocchio*, *Alice in Wonderland*, *Snow White and the Seven Dwarfs*, *Beauty and the Beast*, and *Cinderella*, the system recommended *The Aristocats*, *The Little Mermaid*, *Dumbo*, ねむれるもりのびじょ (*Sleeping Beauty*), *Alice's Adventures in Wonderland*, 101 ぴきわんちゃん (*101 Dalmatians*), しらゆきひめ (*Snow White*), 風の谷のナウシカ 7 巻セット (*Nausicaä of the Valley of the Wind Set: Volumes 1 to 7*), *Peter Pan*, *Toy Story 3*, and プーさんをさがせ (*Look and Find Pooh*). Here, the English names were the products that had translation pairs and the Japanese names were those that did not have them. In addition, バック・トゥ・ザ・フューチャー Part 3 (*Back to the Future Part 3*) or バックトゥザフューチャー 25th アニバーサリー (*Back to the Future 25th Anniversary*) were recommended to users who bought *Back to the Future*. These results indicate that even if the recommended items were determined to be incorrect by the system, they included many correct answers.

In addition, *Nausicaä of the Valley of the Wind Set: Volumes 1 to 7* and *Back to the Future 25th Anniversary* were products that were sold only at the Japanese shopping site. They also seemed to be related to buyers' interests. Therefore, we think that simple collaborative filtering between two shopping sites in different languages could provide many effective recommendations. These items could not be recommended by the bestseller recommender system at all.[15]

However, *Back to the Future Part 3* was also sold at the English shopping site, as was *Back to the Future Part III*. The system could not identify that they were the same product. We think that more accurate translation pairs will lead to fewer errors of that nature. Formatting using the edit distance was tried, but it increased erroneous translations: 天使と悪魔 (*Angels & Demons*) was identified as 天使と小悪魔 (literally meaning angels and demons, but they are totally different work). More precise formatting of product names should be investigated in the future.

Finally, collaborative filtering has some limitations such as sparsity, scalability, and synonymy. (Sarwar, Karypis, Konstan, and Riedl 2000) used singular value decomposition to reduce dimensionality. We think that this technique could be used together with our method because it is

[15] For example, the top-5 bestsellers were 1. *One Piece* (Japanese manga), 2. *This Is It* (CD) 3. *Cath Kidston "HELLO !" FROM LONDON*, 4. 鋼の錬金術師 (Japanese manga, English title is *Fullmetal Alchemist*), and 5. 体脂肪計タニタの社員食堂 (a Japanese cookbook).

Journal of Natural Language Processing Vol. 24 No. 4 September 2017

effective in some domains. In addition, we plan to perform domain adaptation in a scenario in which we use a small number of English customer purchase histories in addition to Japanese customer purchase histories in the future.

9 Conclusion

We developed a system that recommends products at a Japanese shopping site to non-Japanese users using naive collaborative filtering. The same items on both Japanese and English sites were identified using translation pairs because the items had different product names according to the language. Our experiments reveal that the collaborating filtering system outperformed the bestseller recommender system. They also reveal that products only at the Japanese site that seemed to be related to the buyers' interests could be found by the system. In addition, even if the recommended items were determined to be incorrect by the system, they included many answers that seemed to be correct. We think that simple collaborative filtering between two shopping sites in different languages could provide many effective recommendations.

Acknowledgment

This paper is the revised version of (Komiya, Shibata, and Kotani 2014), which is published in the proceedings of the CICLING 2014. We would like to thank Rakuten, Inc. and the National Institute of Informatics which provide us the "Rakuten Data Release." This work was partially supported by JSPS KAKENHI Grant Number 15K16046.

Reference

Cantador, I. and Cremonesi, P. (2014). "Tutorial on Cross-Domain Recommender Systems." In *Proceedings of RecSys '14*, pp. 401–402.

Chang, P.-C. and Quiroga, L. M. (2010). "Using Wikipedia's Content for Cross-Website Page Recommendations that Consider Serendipity." In *Proceedings of International Conference on Technologies and Applications of Artificial Intelligence*, pp. 293–298.

Harper, F. M. and Konstan, J. A. (2015). "The MovieLens Datasets: History and Context." *ACM Transactions on Interactive Intelligent Systems (TiiS)*, **5** (4), pp. 19:1–19:19.

Kawamae, N., Sakano, H., Yamada, T., and Ueda, N. (2009). "Collaborative Filtering Focusing on the Dynamics and Precedence of User Preference." *The Transactions of the Institute*

of Electronics, Information and Communication Engineers D (In Japanese), **J92-D** (6), pp. 767–776.

Komiya, K., Shibata, S., and Kotani, Y. (2014). "Cross-lingual Product Recommendation Using Collaborative Filtering With Translation Pairs." In *Proceedings of Cicling 2014, Part II, LNCS8404*, pp. 141–152.

Mirizzi, R., Noia, T. D., Ostuni, V. C., and Ragone, A. (2015). "Linked Open Data for content-based recommender systems." *Politecnico di Bari*, **5** (4), pp. 19:1–19:24.

Musto, C., Semeraro, G., Gemmis, M. D., and Lops, P. (2015). "Word Embedding techniques for Content-based Recommender Systems: An Emprical Evaluation." In *Proceedings of the 2015 of the 9th ACM Conference on Recommender Systems*, No. 23.

Ozsoy, M. G. (2016). "From Word Embedding to Item Recommendation." In *arXiv.org.* **arXiv: 1601.01356v2**.

Pham, X. H., Jung, J. J., Nguyen, N. T., and Kim, P. (2016). "Ontology-based Multilingual Search in Recommendation Systems." *Acta Polytechnica Hungarica*, **13** (2), pp. 195–207.

Sarwar, B., Karypis, G., Konstan, J., and Riedl, J. (2000). "Application of Dimensionality Reduction in Recommender System—A Case Study." In *Proceedings of ACM WebKDD 2000 Workshop.*

Symeonidis, P., Tiakas, E., and Manolopoulos, Y. (2010). "Transitive Node Similarity for Link Prediction in Social Networks with Positive and Negative Links." In *Proceedings of The ACM Conference Series on Recommender Systems 2010*, pp. 183–190.

Takasu, A. (2010). "Cross-Lingual Keyword Recommendation Using Latent Topics." In *Proceedings of HetRec '10*, pp. 52–56.

Tsuji, R., Nemoto, Y., Luangpiensamut, W., Abe, Y., Kimura, T., Komiya, K., Fujimoto, K., and Kotani, Y. (2012). "The Transliteration from Alphabet Queries to Japanese Product Names." In *Proceedings of PACLIC 2012*, pp. 490–496.

Uchiyama, K., Nanba, H., Aizawa, A., and Sagara, T. (2011). "OSUSUME: Cross-lingual Recommender System for Research Papers." In *Proceedings of the 2011 Workshop on Context-awareness in Retrieval and Recommendation*, pp. 39–42.

Kanako Komiya: received her Ph.D. degree in Tokyo University of Agriculture and Technology in 2009. After being a postdoctoral fellow in Tokyo Institute of Technology and an assistant professor in Tokyo University of Agriculture and Technology, she is currently a lecturer in Ibaraki University. She is interested

in natural language processing. She is a member of IPSJ, JSAI, and ANLP.

Minoru Sasaki: received his Ph.D. degree in Tokushima University. After being a research assistant in Ibaraki University, he is currenly a lecturer in Ibaraki University. His research interests include information retrieval and natural language processing. He is a member of IPSJ and ANLP.

Hiroyuki Shinnou: received his Ph.D. degree in Tokyo Institute of Technology. After being a researcher in Fuji Xerox Co., Ltd. and Panasonic Corporation and a research assistant, a lecturer, and an associate professor in Ibaraki University, he is currently a professor in Ibaraki University. His research interests include Bayes statistics, machine learning and natural language processing. He is a member of IPSJ, JSAI, and ANLP.

Yoshiyuki Kotani: received his Ph.D. degree in the University of Tokyo. He is currently a professor emeritus at the Tokyo University of Agriculture and Technology. His research interests include artificial intelligence, game programming, and natural language processing. He is a member of IPSJ and JSAI.

(Received November 29, 2016)
(Revised April 16, 2017)
(Accepted June 7, 2017)

3. プロジェクト業績

研究論文等発表一覧

【著書】

1). 新納浩幸(訳), “ニューラルネットワーク自作入門”, 株式会社マイナビ出版, 2017 年 4 月.
2). 小澤佑介, “LED の利用動向特集「LED を使った可視光通信とはなにか”, 電気計算(2017 年 5 月号 Vol. 85, No. 5), 2017 年 5 月.
3). Takahiro Inui, Masaki Kohana, Shusuke Okamoto, and Masaru Kamada, ″IoT Technologies: State of the Art and a Software Development Framework″, Chapter 1 (pp.3-18) in Fatos Xhafa, Fang-Yie Leu and Li-Ling Hung (eds.), Smart Sensors Networks- Communication Technologies and Intelligent Applications, Academic Press, 2017 年 6 月.
4). 藤芳明生, “形式言語・オートマトン入門”, 数理工学社, 2017 年 8 月.
5). 情報技術協会(石田智行), “VR／AR技術の開発動向と最新応用事例, 第13章第4節「AR技術によるバーチャル伝統工芸システムの開発」担当”, 情報技術協会, 2018 年 2 月.
6). Taro Shibanoki and Toshio Tsuji, ″Discrimination of Dual-arm Motions Using a Joint Posterior Probability Neural Network for Human-robot Interfaces″, Handbook of Research on Biomimetics and Biomedical Robotics, (Maki K. Habib, Ed.), IGI Global, USA, accepted.

【原著論文】

1). 藤芳衛, 藤芳明生, 石田透, “重度視覚障害を有する教職員等の点字教材の自立的作図を可能にする Bplot (コマンド記述方式)”, 日本教育工学会論文誌, 2017 年 5 月.
2). Akio Fujiyoshi, ″A Practical Algorithm for the Uniform Membership Problem of Labeled Multidigraphs of Tree-Width 2 for Spanning Tree Automata″, International Journal of Foundations of Computer Science, 2017 年 6 月.
3). Tomoyuki Ishida, Yusuke Hirohara, Nobuyuki Kukimoto, Yoshitaka Shibata, ″Implementation of a decision support system using an interactive large-scale high-resolution display″, Springer Journal of Artificial Life and Robotics, 2017 年 6 月.
4). Taro Shibanoki, Go Nakamura, Takaaki Chin and Toshio Tsuji, ″A Voice Signal-Based Manipulation Method for the Bio-Remote Environment Control System Based on Candidate Word Discriminations″, Journal of Robotics, Networking and Artificial Life, 2017 年 6 月.
5). Haruna Kokubo, Taro Shibanoki, Takaaki Chin and Toshio Tsuji, ″Obstacle Avoidance Method for Electric Wheelchairs Based on a Multi-Layered Non-Contact Impedance Model″, Journal of Robotics, Networking and Artificial Life, 2017 年 6 月.
6). Go Nakamura, Taro Shibanoki, Yuichiro Honda, Futoshi Mizobe, Akito Masuda, Takaaki Chin and Toshio Tsuji, ″A human reaching movement model for Myoelectric Prosthesis Control″, Journal of Robotics, Networking and Artificial Life, 2017 年 6 月.
7). Minoru Sasaki, ″Word Sense Disambiguation Based On Global Co-Occurrence Information Using Non-Negative Matrix Factorization″, Journal of Computer Science Applications and Information Technology, 2017 年 7 月.
8). 箭内春樹, 熊野直子, 田村誠, 横木裕宗, 桑原祐史, “伊勢湾台風を事例とする高潮浸水被害額推計手法の検証”, 土木学会 土木学会論文集 G(地球環境), 2017 年 8 月.
9). Kazuki Yoneyama, Reo Yoshida, Yuto Kawahara, Tetsutaro Kobayashi, Hitoshi Fuji, Tomohide Yamamoto, ″Multi-cast key distribution: scalable, dynamic and provably secure construction″, Springer International Journal of Information Security, 2017 年 8 月.
10). Kazuki Yoneyama, ″Computational Soundness of Asymmetric Bilinear Pairing-based Protocols″, IEICE Trans. on Fundamentals, 2017 年 9 月.
11). 佐久間東陽, 亀山哲, 小野理, 木塚俊和, 三上英敏, “Landsat-8 OLI 地表面反射率プロダクトを用いた釧路川流域における未利用農地分布図の作成”, 日本リモートセンシング学会誌, 2017 年 9 月.
12). Kanako Komiya, Minoru Sasaki, Hiroyuki Shinnou, Yoshiyuki Kotani, ″Cross-lingual Product Recommendation System Using Collaborative Filtering″, 自然言語処理, 2017 年 9 月.
13). Noriki Uchida, Shoma Takeuchi, Tomoyuki Ishida, Yoshitaka Shibata, “Mobile Traffic Accident Prevention System

based on Chronological Changes of Wireless Signals and Sensors", Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 2017 年 9 月.

14). Tomoyoshi Ono, Kazuki Yoneyama, "On Randomness Exposure Resilience of Group Signatures", IEICE Trans. on Information and Systems, 2017 年 10 月.
15). Kaoru Kurosawa, Le Trieu Phong, "Anonymous and leakage resilient IBE and IPE", Des. Codes Cryptography, 2017 年 11 月.
16). Tomoyuki Ishida, Yusuke Hirohara, Noriki Uchida, Yoshitaka Shibata, "Implementation of an Integrated Disaster Information Cloud System for Disaster Control", Journal of Internet Services and Information Security (JISIS), 2017 年 11 月.
17). Go Nakamura, Taro Shibanoki, Yuichi Kurita, Yuichiro Honda, Akito Masuda, Futoshi Mizobe, Takaaki Chin, and Toshio Tsuji, "A Virtual Myoelectric Prosthesis Training System Capable of Providing Instructions on Hand Operations", International Journal of Advanced Robotic Systems (IJARS), in press.
18). 新納浩幸, 浅原正幸, 古宮嘉那子, 佐々木稔, "nwjc2vec:国語研日本語ウェブコーパスから構築した単語の分散表現データ", 自然言語処理, 2017 年 12 月.
19). Yukou Kobayashi, Naoto Yanai, Kazuki Yoneyama, Takashi Nishide, Goichiro Hanaoka, Kwangjo Kim, Eiji Okamoto, "Provably Secure Gateway Threshold Password-based Authenticated Key Exchange Secure against Undetectable On-line Dictionary Attack", IEICE Trans. on Fundamentals, 2017 年 12 月.
20). Jumpei Okumura, Yusuke Kozawa, Yohtaro Umeda, Hiromasa Habuchi, "Hybrid PWM/DPAM Dimming Control for Digital Color Shift Keying Using RGB-LED Array", IEEE Journal on Selected Areas in Communications, 2018 年 1 月.
21). Akira Sakuraba, Tomoyuki Ishida, Koji Hashimoto, Yoshitaka Shibata, "Design and Implementation of Disaster Management GIS System Based on Ultra High Definition Display Environment", International Journal of Space-Based and Situated Computing (IJSSC), 2018 年 2 月.
22). Miki Kuroki, Michitoshi Niibori, Tomoyuki Ishida, Tatsuhiro Yonekura, "Implementation of information collecting tools using mobile terminals useful for efficient infrastructure maintenance", International Journal of Space-Based and Situated Computing (IJSSC), 2018 年 2 月.
23). 堀田大貴, 平山秀昭, 早瀬健夫, 田原康之, 大須賀昭彦, "決定木学習を利用したビジネスプロセス実行ログ検証のための論理式の生成", 電子情報通信学会論文誌, 2018 年 3 月.
24). Misaki Iyobe, Tomoyuki Ishida, Akihiro Miyakawa, Yoshitaka Shibata, "Implementation of a Mobile Traditional Crafting Application using Kansei Retrieval Method", IT CoNvergence PRActice (INPRA), 2018 年 3 月.
25). 樽林雄飛, 外岡秀行, "高分解能衛星画像の影解析及び反復的 3D モデリングによる建物の高さ推定", 日本リモートセンシング学会誌 (印刷中).

【特許】

1). 吉田麗生, 小林鉄太郎, 川原祐人, 冨士仁, 米山一樹, "鍵配送システム及び方法、鍵生成装置、代表ユーザ端末、サーバ装置、ユーザ端末並びにプログラム", 2017 年 5 月.
2). 吉田麗生, 川原祐人, 小林鉄太郎, 冨士仁, 米山一樹, "匿名ブロードキャスト方法、鍵交換方法、匿名ブロードキャストシステム、鍵交換システム、通信装置、プログラム", 2017 年 9 月.

【国際会議発表】

1). Kanako Komiya, Shota Suzuki, Minoru Sasaki, Hiroyuki Shinnou, and Manabu Okumura, "Domain Adaptation for Word Sense Disambiguation Using Word Embeddings". CICLING2017, 2017 年 4 月.
2). Asahi SAKUMA, Satoshi KAMEYAMA, Satoru ONO, Toshikazu KIZUKA, Hidetoshi MIKAMI, "The detection and evaluation of unused agricultural land using Landsat-8 OLI and DEM in Kushiro River watershed Japan", International Symposium on Remote Sensing 2017, 2017 年 5 月.
3). Wudabalaqiqige, Yuji KUWAHARA Analysis of social and environmental issues caused by exploitation of center pivot in Alukeerqin Qi, Inner Mongolia Autonomous", International Symposium on Remote Sensing 2017 , 2017 年 5 月.
4). Hirotaka IIDA, Shinichirou OKUDE, Naohiro MANAGO, Yuji KUWAHARA, Hiroaki KUZE, "Measurement of

carbon dioxide concentration using DOAS method in the human activity area in Ibaraki, Japan", International Symposium on Remote Sensing 2017, 2017 年 5 月.

5). Moena Asaki, Hideyuki Tonooka, "Updates of cross-calibration results of ALOS-2/CIRC using GOES-14/Imager", Proc. of International Symposium on Remote Sensing 2017 (ISRS 2017), 2017 年 5 月.
6). Moena Asaki, Hideyuki Tonooka, Fumihiro Sakuma, "Time-series radiometric comparison of ASTER band 11 and Terra/MODIS band 29 in a low temperature range", Proc. of International Symposium on Remote Sensing 2017 (ISRS 2017), 2017 年 5 月.
7). Jumpei Yamamoto, Hideyuki Tonooka, "Application of deep learning to cloud discrimination for ASTER Level 1T imagery", Proc. of International Symposium on Remote Sensing 2017 (ISRS 2017), 2017 年 5 月.
8). Kaoru Kurosawa, Rie Habuka, "More Efficient Construction of Bounded KDM Secure Encryption", ACNS 2017, 2017 年 7 月.
9). Yuki Koshino and Masaru Kamada, "Sparse approximation of ion-mobility spectrometry profiles by binomial splines", Proceedings of the12th International Conference on Sampling Theory and Applications (SampTA 2017), 654-657, 2017 年 7 月.
10). Osamu Goto, Michitoshi Niibori and Masaru Kamada, "A block-based structure editor for the English language", In: L. Barolli et al. (eds.), Advances in Network-based Information Systems (Proceedings of the 20th International Conference on Network-based Information Systems, NBiS-2017), Lecture Notes on Data Engineering and Communications Technologies 7, 1051-1060, Springer, 2017 年 8 月.
11). Yukiya Yamaguchi, Ryosuke Iiya, Michitoshi Niibori, Erjing Zhou, Masaru Kamada, Osamu Saitou and Susumu Shibusawa, "A web application for passengers to watch coming buses in rural areas", In: L. Barolli et al. (eds.), Advances in Network-based Information Systems (Proceedings of the 20th International Conference on Network-based Information Systems, NBiS-2017), Lecture Notes on Data Engineering and Communications Technologies 7, 1061-1069, Springer, 2017 年 8 月.
12). Shuji Ogawa, Michitoshi Niibori, Tatsuhiro Yonekura and Masaru Kamada, "An HTML5 implementation of Web-Com for recording chalk annotations and talk voices onto web pages", In: L. Barolli et al. (eds.), Advances in Network-based Information Systems (Proceedings of the 20th International Conference on Network-based Information Systems, NBiS-2017), Lecture Notes on Data Engineering and Communications Technologies 7, 1070-1075, Springer, 2017 年 8 月.
13). Tomoyuki Ishida, Yusuke Hirohara, Noriki Uchida, Yoshitaka Shibata, "Implementation of a Community-Based Disaster Prevention Information System", The 12th International Workshop on Network-based Virtual Reality and Tele-existence (INVITE'2017), 2017 年 8 月.
14). Akira Sakuraba, Tomoyuki Ishida, Koji Hashimoto, Yoshitaka Shibata, "Ultra Definition Display Environment for Disaster Management GIS", The 12th International Workshop on Network-based Virtual Reality and Tele-existence (INVITE'2017), 2017 年 8 月.
15). Miki Kuroki, Michitoshi Niibori, Tomoyuki Ishida, Tatsuhiro Yonekura, "A study on the operation of infrastructure management system with citizens", The 12th International Workshop on Network-based Virtual Reality and Tele-existence (INVITE'2017), 2017 年 8 月.
16). Noriki Uchida, Tomoyuki Ishida, Yoshitaka Shibata, "Delay Tolerant Networking with Antenna Directional Controls with the Weight Function for the Multiple Vehicular Communication", The 12th International Workshop on Network-based Virtual Reality and Tele-existence (INVITE'2017), 2017 年 8 月.
17). Hiroyuki Shinnou, Kanako Komiya, Minoru Sasaki, "Domain Adaptation for Document Classification by Alternately Using Semi-supervised Learning and Feature Weighted Learning". PACLING2017, 2017 年 8 月.
18). Shusuke Okamoto, Masaki Kohana, "Running a MPI Program on Web Browsers", 2017 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, 2017 年 8 月.
19). Masaki Kohana, Hiroki Sakaji, Akio Kobayashi, Shusuke Okamoto, "A Topic Trend on P2P Based Social Media", The 6th International Workshop on Web Services and Social Media (WSSM-2017), 2017 年 8 月.
20). Akio Kobayashi, Hiroki Sakaji, Masaki Kohana, "A Method for Extracting Correct Links from Automatic Created Links on Folksonomy", The 6th International Workshop on Web Services and Social Media (WSSM-2018), 2017 年 8 月.

21). Keisuke Osawa, Hiromasa Habuchi, Yusuke Kozawa, "A Theoretical Analysis of Visible-Light Variable N-parallel Code-Shift-Keying in LOS Indoor Environments", The Eighth International Workshop on Signal Design and Its Applications in Communications (IWSDA'17), 2017 年 9 月.
22). Ran Sun, Hiromasa Habuchi, Yusuke Kozawa, "Impact of Framed-DOOK Optical Wireless System using Error Correcting Codes", The Eighth International Workshop on Signal Design and Its Applications in Communications (IWSDA'17), 2017 年 9 月
23). Takashi Tokunaga, Hiromasa Habuchi, Yusuke Kozawa, "New Two-Layered Pseudo-Noise Code for Optical-Wireless Code-Shift Keying/SCDMA", The Eighth International Workshop on Signal Design and Its Applications in Communications (IWSDA'17), 2017 年 9 月
24). Fumio Narisawa, Yoshikazu Ueda, "Safety Verification Method for Priority-based Real-time Software", The 16th International Conference on Intelligent Software Methodologies, Tools, and Techniques (SOMET 2017) , 2017 年 9 月.
25). Masayuki Ishikawa, Hiromasa Habuchi, "On Suitable Pseudo-Noise Code for Optical-Wireless Hierarchical CSK-MPPM System", IEEE 6th Global Conference on Consumer Electronics (GCCE2017), 2017 年 10 月.
26). Tomohiro Okawa, Hiromasa Habuchi, "Rigorous Communication Success Probability of MC-CDMA with MPOMS Codes for Radio-On-Demand WSN", IEEE 6th Global Conference on Consumer Electronics (GCCE2017), 2017 年 10 月.
27). Yuto Asano, Hiromasa Habuchi, Yusuke Kozawa, "Improved Synchronization Scheme for Indoor Visible-Light Differential On-Off Keying", IEEE 6th Global Conference on Consumer Electronics (GCCE2017), 2017 年 10 月.
28). Takashi Tokunaga, Hiromasa Habuchi, Yusuke Kozawa, Ran Sun, "SCDMA Capability of High-Density Code-Shift Keying using Dual MPOMs in Optical-Wireless Channel", 27th International Telecommunication Networks and Applications Conference (ITNAC2017) , 2017 年 11 月.
29). Ran Sun, Hiromasa Habuchi, Yusuke Kozawa, "Proposal of Optical Wireless Turbo Coded APPM System", 27th International Telecommunication Networks and Applications Conference (ITNAC2017) , 2017 年 11 月.
30). Ryota Kimoto, Yusuke Kozawa, Yohtaro Umeda, Hiromasa Habuchi, "Inverse pulse position modulation schemes for simultaneous visible light wireless information and power transfer", 27th International Telecommunication Networks and Applications Conference (ITNAC2017) , 2017 年 11 月.
31). Daniel Prusa, Akio Fujiyoshi, "Rank-reducing Two-dimensional Grammars for Document Layout Analysis", The 14th IAPR International Conference on Document Analysis and Recognition, 2017 年 11 月.
32). Kentaro Koike, Misaki Iyobe, Tomoyuki Ishida, Noriki Uchida, Kaoru Sugita, Yoshitaka Shibata, "Proposal of an Open Data Visualization System for Disaster Prevention and Disaster Reduction", The 12th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2017 年 11 月.
33). Noriki Uchida, Tomoyuki Ishida, Yoshitaka Shibata, "Adaptive Array Antenna Systems with Machine Learning based Image Recognitions for Vehicular Delay Tolerant Networking", The 12th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2017 年 11 月.
34). Hiroyuki Shinnou, Kanako Komiya, Minoru Sasaki, and Shinsuke Mori, "Japanese all-words WSD system using the Kyoto Text Analysis ToolKit", PACLIC 2017, 2017 年 11 月.
35). Tomoaki Morita, Ryo Sakai, Yohtaro Umeda, Yusuke Kozawa, "A Quadrature-modulation EPWM Transmitter That Uses Sine Wave Carriers for I and Q Channel with a 90° Hybrid", 2017 IEEE Asia Pacific Microwave Conference (APMC), 2017 年 11 月.
36). Yuto Tanaka, Yohtaro Umeda, Yusuke Kozawa, "Comparison of Power Combining Methods in Power-amplifier-inserted Transversal Filter for EPWM Transmitters", 2017 IEEE Asia Pacific Microwave Conference (APMC), 2017 年 11 月.
37). Wakaha Ogata, Kaoru Kurosawa, "Efficient No-dictionary Verifiable Searchable Symmetric Encryption", Financial Cryptography 2017, 498-516, 2017 年 12 月
38). Tai Tomizawa, Taro Shibanoki, Takaaki Chin and Toshio Tsuji, "An EMG-based Prosthetic Hand Training System Using a Class Partial Kullback-Leibler Information", The first IEEE Life Sciences Conference (LSC2017), Sydney, 2017 年 12 月.
39). Kazuki Yoneyama, Shogo Kimura, "Verifiable and Forward Secure Dynamic Searchable Symmetric Encryption with

Storage Efficiency″, International Conference on Information and Communications Security (ICICS 2017), 2017 年 12 月.

40). Tatsuya Ooyanagi, Hayato Ito, Misaki Iyobe, Tomoyuki Ishida, ″Proposal of an Integrated Common Platform for Zoo Operation Support″, Proc. of the 23rd International Symposium on Artificial Life and Robotics, pp.576-581, 2018 年 1 月.

41). Hayato Ito, Tatsuya Ohyanagi, Misaki Iyobe, Tomoyuki Ishida, ″Proposal of a Historical Materials Presentation AR System for Local Activities and History Education″, Proc. of the 23rd International Symposium on Artificial Life and Robotics, 2018 年 1 月.

42). Misaki Iyobe, Tomoyuki Ishida, Akihiro Miyakawa, Yoshitaka Shibata, ″Kansei Retrieval Method by Principal Component Analysis of Japanese Traditional Crafts″, Proc. of the 23rd International Symposium on Artificial Life and Robotics, pp.588-591, 2018 年 1 月.

43). Yuki Watanabe, Masanao Kobayashi, Noboru Nakamichi, Rieko Inaba, Shinya Watanabe, Takashi Hasuike, Takeo Tatsumi, Tomoharu Ugawa, Yasuhiro Ohtaki, Yoshifumi Yamamoto, Kei Onishi, Toshio Matsuura, Hiroshi Ishikawa, “Transition of Information Studies on Japanese Secondary Education -Meta text analysis of the Government Course Guidelines-”, Proc. of the 16th Annual Hawaii International Conference on Education(HICOE18), 2018 年 1 月.

44). Ryuichi Takahashi, Yasuo Tsurugai, Yoshiaki Fukazawa, “Discovery of Latent Requirements by Using Web Service Composition Techniques”, 2018 HKICEAS: Hong Kong International Conference on Engineering and Applied Sciences, 2018 年 1 月.

45). Taro Shibanoki, Masaki Watanabe, Go Nakamura, Takaaki Chin and Toshio Tsuji, “A Training Method for the Speech Controlled Environmental Control System Based on Candidate Word Discriminations”, Proceedings of the 2018 International Conference on Artificial Life and Robotics (ICAROB2018), 2018 年 2 月.

46). Yusuke Matsuda, Yusuke Kozawa, Yohtaro Umeda, “Experimental Evaluation of Hybrid PWM/DPAM Dimming Control Method for Digital Color Shift Keying using RGB-LED Array”, Proc. of the RISP International Workshop on Nonlinear Circuits, Communication and Signal Processing (NCSP’18), 2018 年 3 月.

47). Kanako Komiya, Minoru Sasaki, and Hiroyuki Shinnou, “Distributed Representation vs. Context Vector: Comparison of Features for Japanese Onomatopoeia Classification”, CICLING 2018, 2018 年 3 月.

48). Keisuke Osawa, Hiromasa Habuchi, Yusuke Kozawa, “Performance Evaluation of Hybrid VN-CSK/PAM for Lighting Constrained Visible Light Communications”, Proc. of the RISP International Workshop on Nonlinear Circuits, Communication and Signal Processing (NCSP’18), 2018 年 3 月.

49). Ran Sun, Hiromasa Habuchi, Yusuke Kozawa, “Error Correcting Codes in Underwater RGB-LED Parallel Communication: Turbo or LDPC? ”, Proc. of the RISP International Workshop on Nonlinear Circuits, Communication and Signal Processing (NCSP’18), 2018 年 3 月.

【解説】

1). 土田聡, 外岡秀行, 小野晃, “衛星搭載光学センサの放射量校正 第 4 回(前半) 代替校正”, 日本リモートセンシング学会誌, Vol. 37, No. 2, pp. 139-146, 2017 年 4 月.

【学会発表 (国内, 国際)】

1). 黒澤馨, 根本雄輝, “Fully Secure な紛失キーワード検索”, 情報セキュリティ研究会 ISEC2017-2, 2017 年 5 月.

2). 徳永岳, 羽渕裕真, 小澤佑介, “光無線 CSK/SCDMA のための二重拡散符号設計に関する一検討”, 電子情報通信学会WBS研究会, 2017 年 5 月.

3). 浅野裕太, 羽渕裕真, 小澤佑介, “光無線差動符号化 OOK のためのフレーム同期信号設計に関する一検討”, 電子情報通信学会WBS研究会, 2017 年 5 月.

4). 新納 浩幸, 古宮 嘉那子, 佐々木 稔, “順方向多層 LSTM と分散表現を用いた教師あり学習による語義曖昧性解消”, 情報処理学会 研究報告自然言語処理(NLP), 2017 年 7 月.

5). 木元亮太, 小澤佑介, 楳田洋太郎, 羽渕裕真, “水中可視光ワイヤレス給電通信システムのための交流/直流分離フィルタ設計に関する基礎的検討”, 電子情報通信学会WBS研究会, 2017 年 7 月.

6). 大澤圭佑, 羽渕裕真, 小澤佑介, “VN-CSK 照明光通信における環境光雑音の影響”, 電子情報通信学会WBS

研究会, 2017 年 7 月.

7). 孫冉, 羽渕裕真, 小澤佑介, “光無線通信におけるブロック誤り訂正符号を用いるフレーム化 DOOK の効果”, 電子情報通信学会WBS研究会, 2017 年 7 月.
8). 高橋正行, 岡田信一郎, “SQL 実習支援システムにおける反復学習回数削減法の実装と評価”情報処理学会 コンピュータと教育研究会 140 回研究発表会, 2017 年 7 月.
9). 山本匠, 楳田洋太郎, 小澤佑介, “並列出力 MASH 方式ΔΣ変調器を用いた直交変調型包絡線パルス幅変調方式送信機”, 電子情報通信学会 ICD 研究会, 2017 年 8 月.
10). 加茂巧, 楳田洋太郎, 小澤佑介, “ウェーバー方式イメージ抑圧法を用いた全ディジタル化 Low-IF 方式送信機のマルチキャリア送信特性”, 電子情報通信学会 ICD 研究会, 2017 年 8 月.
11). 新納浩幸, 古宮嘉那子, 佐々木稔, “nwjc2vec の fine-tuning”, 言語資源活用ワークショップ 2017, 2017 年 9 月.
12). 遊佐宣彦, 佐々木稔, 古宮嘉那子, 新納浩幸, “単義語と共起する多義語に対する分散表現を利用した語義分析”, 言語資源活用ワークショップ 2017, 2017 年 9 月.
13). 金子顕之, 古宮嘉那子, 佐々木稔, 新納浩幸, “深層学習と合議を用いた極性分類”, 第 11 回テキストアナリティクス・シンポジウム, 2017 年 9 月.
14). 薄井翔, 上田賀一, 小飼敬, 高橋竜一, 堀田大貴, “制御ルールの並びに着目した反例分析手法の提案”, 日本ソフトウェア科学会第 34 回大会, 2017 年 9 月.
15). 長岡源樹, 上田賀一, 堀田大貴, 高橋竜一, “データ依存グラフを利用したデータフロー図の差異検出手法”, 日本ソフトウェア科学会第 34 回大会, 2017 年 9 月.
16). 新納浩幸, 古宮嘉那子, 佐々木稔, “nwjc2vec の fine-tuning”, 国語研言語資源活用ワークショップ, P-B-4, 2017 年 9 月.
17). 松田勇介, 小澤佑介, 楳田洋太郎, “PWM/DPAM ハイブリッド型調光制御法を用いたデジタル制御型カラーシフトキーイングの実験的評価”, 電子情報通信学会 WBS 研究会, 2017 年 10 月.
18). 森田智明, 酒井涼, 楳田洋太郎, 小澤佑介, “同相の正弦波を I, Q チャネルの搬送波に用い 90 度ハイブリッドを信号合成に用いる直交変調型 EPWM 送信機”, 電子情報通信学会 MW 研究会, 2017 年 10 月.
19). 田中裕人, 楳田洋太郎, 小澤佑介, “EPWM 送信機への応用に向けた電力増幅器挿入型トランスバーサルフィルタにおける電力合成法の比較”, 電子情報通信学会 MW 研究会, 2017 年 10 月.
20). 徳永岳, 羽渕裕真, 小澤佑介, 孫冉, “MPOMs の二重符号化を用いる光 CSK/SCDMA の性能評価”, 電子情報通信学会WBS研究会, 2017 年 10 月.
21). 大川智広, 羽渕裕真, “変形擬直交 M 系列対を用いるオンデマンド型 WSN のリバースリンクにおけるノード間同期誤差の影響”, 電子情報通信学会WBS研究会, 2017 年 10 月.
22). 孫冉, 羽渕裕真, 小澤佑介, “ASK-PPM を用いる光無線ターボシステムの一検討”, 電子情報通信学会WBS研究会, 2017 年 10 月.
23). 大澤圭佑, 羽渕裕真, 小澤佑介, “VN-CSK 照明光通信における受信機位置による BER 性能変化”, 電子情報通信学会WBS研究会, 2017 年 10 月.
24). 石川真行, 羽渕裕真, 小澤佑介, “光無線 CSK-MPPM 方式における疑似雑音符号について”, 電子情報通信学会WBS研究会, 2017 年 10 月.
25). 石田智行, 内田法彦, 柴田義孝, “防災情報システム構築に係る実績と今後の展望”, 第 33 回テレイマージョン技術研究会研究会, 2017 年 11 月.
26). 外岡秀行, “熱赤外分光特性を利用した雪氷リモートセンシングの可能性”, 日本リモートセンシング学会第 63 回学術講演会, 2017 年 11 月.
27). 外岡秀行, 朝木萌奈, 酒井理人, 粂田綾香, 中右浩二, “ALOS-2/CIRC のラジオメトリック校正係数の算出”, 日本リモートセンシング学会第 63 回学術講演会, 2017 年 11 月.
28). 朝木萌奈, 外岡秀行, 佐久間史洋, “低温域における ASTER/TIR 校正精度の時系列評価”, 日本リモートセンシング学会第 63 回学術講演会, 2017 年 11 月.
29). 樽林雄飛, 外岡秀行, “高分解能衛星画像の影解析及び 3D モデリングによる建物の高さ推定値の確度の検討”, 日本リモートセンシング学会第 63 回学術講演会, 2017 年 11 月.
30). 山本純平, 外岡秀行, “アンサンブル学習型ディープラーニングモデルを用いた ASTER 雲量情報の評価”, 日本リモートセンシング学会第 63 回学術講演会, 2017 年 11 月.

31). 平井暁裕, 外岡秀行, “マルチスペクトル画像と周辺のハイパースペクトル画像の組み合わせによる鉱物同定”, 日本リモートセンシング学会第 63 回学術講演会, 2017 年 11 月.
32). 室伏拓実, 外岡秀行, “米国ネバダ州 Alkali Lake における 3 バンド放射温度計の放射率測定試験”, 日本リモートセンシング学会第 63 回学術講演会, 2017 年 11 月.
33). 野口宏, 大瀧保広, 鎌田賢, “ユーザ検索機能を考慮した Office365 のライセンス付与に関する考察”, 大学 ICT 推進協議会 2017 年度年次大会, 2017 年 12 月.
34). 黒澤馨, 中村有志, “消失した(p,q)の挟み撃ち復元法”, SCIS 2018, 1D1-5, 2018 年 1 月.
35). 黒澤馨, 羽深理恵, “ゲート情報を秘匿可能な効率のよい Garbled Gate の Closed Form 表現”, SCIS 2018, 2A2-5, 2018 年 1 月.
36). 黒澤馨, 根本雄輝, “再利用可能な Oblivious 擬似ランダム関数”, SCIS 2018, 3A1-4, 2018 年 1 月.
37). 黒澤馨, 夛田隼人、上田明長, “BHHO 暗号の Tight な KDM 安全性”, SCIS 2018, 3B2-2, 2018 年 1 月.
38). 黒澤馨, 上田明長、夛田隼人, “補助入力付き離散対数問題を解く Cheon アルゴリズムの一般化”, SCIS 2018, 3B3-5, 2018 年 1 月.
39). 萩野谷一二, 古宮嘉那子, 黒澤馨, “角度に基づく格子基底の判定条件: α-reduced”, SCIS 2018, 3A4-3, 2018 年 1 月.
40). 安藤毅宙, 米山一樹, “シグマプロトコルの合成における複製可能性について”, 暗号と情報セキュリティシンポジウム, 2018 年 1 月.
41). 寺田槙太郎, 米山一樹, “同種写像に基づく Unified Model 認証鍵交換プロトコル”, 暗号と情報セキュリティシンポジウム, 2018 年 1 月.
42). 金井佑篤, 米山一樹, “ORAM におけるアクセスタイミングの秘匿について”, 暗号と情報セキュリティシンポジウム, 2018 年 1 月.
43). 木村翔吾, 米山一樹, “検証可能フォワード安全動的検索可能暗号の改良”, 暗号と情報セキュリティシンポジウム, 2018 年 1 月.
44). 師成, 米山一樹, “LINE Encryption Version 1.0 の ProVerif による検証”, 暗号と情報セキュリティシンポジウム, 2018 年 1 月.
45). 小林鉄太郎, 米山一樹, 吉田麗生, 川原祐人, 山本 具英, 冨士 仁, “通信のメタデータを漏らさないグループ鍵交換”, 暗号と情報セキュリティシンポジウム, 2018 年 1 月.
46). 吉田麗生, 米山一樹, 川原祐人, 小林鉄太郎, 冨士仁, 山本具英, 岡野裕樹, 奥田哲矢, “非対話参加可能な ID ベース動的多者鍵配布プロトコルの提案とその実装評価”, 暗号と情報セキュリティシンポジウム, 2018 年 1 月.
47). 松井政裕, 岡野裕樹, 吉田麗生, 小林鉄太郎, 米山一樹, “長期秘密鍵漏洩時の動的多者鍵配布プロトコルにおける後方鍵の安全性について”, 暗号と情報セキュリティシンポジウム, 2018 年 1 月.
48). 岡野裕樹, 小林鉄太郎, 西巻陵, 吉田麗生, 米山一樹, “ビジネスチャットにおけるエンドツーエンド暗号化を実現するためのグループメッセージングプロトコルの提案”, 暗号と情報セキュリティシンポジウム, 2018 年 1 月.
49). 伊與部美咲, 石田智行, 宮川明大, 柴田義孝, “感性検索法による AR 伝統工芸プレゼンテーションシステムの構築”, 第 34 回テレイマージョン技術研究会研究会, 2018 年 3 月.
50). 大柳達哉, 石田智行, “蓄積された経験データを用いた災害支援エキスパートシステムの提案”, 第 34 回テレイマージョン技術研究会研究会, 2018 年 3 月.
51). 阪本隼士, 大柳達哉, 石田智行, “マーカレス AR 技術によるインバウンド対応型スマートフォン AR アプリの構築”, 第 34 回テレイマージョン技術研究会研究会, 2018 年 3 月.
52). 中井僚, 石田智行, “災害対策本部におけるインタラクティブ情報共有環境を用いた意思決定支援システムの構築”, 第 34 回テレイマージョン技術研究会研究会, 2018 年 3 月.
53). 星野将吾, 石田智行, “地理情報システムを使用した消防団活動支援システムの構築”, 第 34 回テレイマージョン技術研究会研究会, 2018 年 3 月.
54). Lu Yangzhicheng, 石田智行, 宮川明大, 柴田義孝, “ヘッドマウントディスプレイによる高臨場感伝統工芸システムの構築”, 第 34 回テレイマージョン技術研究会研究会, 2018 年 3 月.
55). 富澤太, 芝軒太郎, 中村豪, 陳隆明, 辻敏夫, “義手と動作イメージの整合性を実現可能な相互学習型訓練システム”, 第 27 回 ライフサポート学会 フロンティア講演会, 2018 年 3 月.
56). 清藤拓実, 古宮嘉那子, 佐々木稔, 新納浩幸, “係り受け関係を用いた短単位の単語ベクトルから長単位の単語ベクトルの合成”, 言語処理学会第 24 回年次大会, 2018 年 3 月.

57). 平林照雄, 鈴木類, 古宮嘉那子, 浅原正幸, 佐々木稔, 新納浩幸, “『岩波国語辞典』の語義タグを用いた all-words の語義曖昧性解消”, 言語処理学会第 24 回年次大会, 2018 年 3 月.
58). 遊佐宣彦, 佐々木稔, 古宮嘉那子, 新納浩幸, ″係り受け関係にある単語と単義語の分散表現を用いた語義曖昧性解消″, 言語処理学会第 24 回年次大会, 2018 年 3 月.
59). 熊谷佳奈, 古宮嘉那子, 新納浩幸, “nwjc2vec の効果的な fine-tuning のためのパラメータ設定”, 言語処理学会第 24 回年次大会, 2018 年 3 月.
60). 白静, 古宮嘉那子, 新納浩幸, “ターゲット領域のキーワード含有率を事例の重みとした感情分析の領域適応”, 言語処理学会第 24 回年次大会, 2018 年 3 月.
61). 山木翔馬, 新納浩幸, “教師あり・教師なし学習により構築した語義の分散表現を用いた語義曖昧性解消に関する一考察”, 言語処理学会第 24 回年次大会, 2018 年 3 月.
62). 新納浩幸, VAE による WSD の半教師あり学習”, 言語処理学会第 24 回年次大会, 2018 年 3 月.
63). 日置千仁, 岡田信一郎, “学習失敗時の救済を目的とした効果的な反復学習を促す得点計算法の改良案の提案”, 2018 年電子情報通信学会総合大会, 2018 年 3 月.
64). 平柳卓哉, 日置千仁, 岡田信一郎, “学習間隔に応じた得点計算法の効果の検証 -休憩期間 4 週間の結果-”, 2018 年電子情報通信学会総合大会, 2018 年 3 月.
65). 石川真行, 羽渕裕真, 小澤佑介, “CSK-MPPMを用いる光無線路車間通信における路車間距離による同期誤差特性”, 電子情報通信学会 WBS 研究会, 2018 年 3 月.
66). 浅野裕太, 羽渕裕真, 小澤佑介, “光無線フレーム化 DOOK システムの同期性能を考慮した BER 特性の検討”, 電子情報通信学会 WBS 研究会, 2018 年 3 月.
67). 大川智広, 羽渕裕真, 橋浦康一郎, “光無線フレーム化 DOOK システムの同期性能を考慮した BER 特性の検討”, 電子情報通信学会 WBS 研究会, 2018 年 3 月.
68). 孫冉, 羽渕裕真, 小澤佑介, “水中通信路における可視光差動オンオフキーイングの通信路容量”, 2018 年電子情報通信学会総合大会, 2018 年 3 月.
69). 大澤圭佑, 羽渕裕真, 小澤佑介, “可視光ハイブリッド VN-CSK/PAM におけるビット誤り率と情報伝送効率のトレードオフ”, 2018 年電子情報通信学会総合大会, 2018 年 3 月.

茨城大学重点研究

「地域に密着した世界的 ICT イノベーションの創出」

茨城大学工学部附属 ICT グローカル教育研究センター

２０１７年度報告書

発行日　　平成 30 年 3 月

発行者　　茨城大学　工学部　情報工学科
教授　黒澤　馨
〒316-8511 日立市中成沢町 4-12-1
Tel: 0294-38-5135　Fax: 0294-38-5282

茨城大学重点研究
http://www.ibaraki.ac.jp/generalinfo/activity/researching/juuten/

茨城大学工学部附属教育研究センター
http://www.eng.ibaraki.ac.jp/research/centers/index.html

ICT グローカル教育研究センター
http://www.eng.ibaraki.ac.jp/research/centers/ict/index.html