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

２０１８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 30 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 30 年度の研究業績は，特許 5 件，学術誌論文 10 件、国際会議発表 50 件，招待講演 2 件、その他（研究会等）56 件，競争的資金獲得（科学研究費補助金）15 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 30 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）
原口春海　（工学部情報工学科・准教授）
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）
笹井一人　（工学部情報工学科・准教授）
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・准教授）
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３０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 30 年 4 月 1 日～平成 31 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 30 年 4 月 1 日～平成 31 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，原口春海，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 30 年 4 月 1 日～平成 31 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 30 年 4 月 1 日～平成 31 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 30 年 4 月 1 日～平成 31 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，原口春海，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 30 年 4 月 1 日～平成 31 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，原口春海，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 30 年 4 月 1 日～平成 31 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，原口春海，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：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 CO2 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:

■特許: **5 件**

■学術誌論文: **10 件**

■国際会議論文: **50 件**

■招待講演: **2 件**

■その他（研究会等）: **56 件**

6. 計画名:各種学会・国際会議等での委員
7.
（1）実施結果:

教員名	内容等

黒澤馨教授	ACNS 2018 プログラム委員	
黒澤馨教授	Asiacrypt 2018 プログラム委員	
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	
黒澤馨教授	IET Information Security, Associate Editor	
黒澤馨教授	International Journal of Applied Cryptography, Associate Editor	
黒澤馨教授	Journal of Mathematical Cryptology, Associate Editor	
上田賀一教授	日本ソフトウェア科学会 FOSE2018 プログラム委員	
鎌田賢教授	Associate editor, IEEE Transactions on Industrial Electronics	
鎌田賢教授	Secretary of the journal, Sampling Theory in Signal and Image Processing	
鎌田賢教授	Program committee, The 6th International Workshop on Web Services and Social Media	
桑原祐史教授	土木学会 地球環境委員会 委員	
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	
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	
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	
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	
桑原祐史教授	日本沿岸域学会 論文編集委員会 委員	
桑原祐史教授	土木学会 茨城会 幹事	
桑原祐史教授	NPO 法人 CO_2濃度マップ普及協会 理事	
外岡秀行教授	(国研)産業技術総合研究所 客員研究員	
外岡秀行教授	(一社)日本リモートセンシング学会 評議員	
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	
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	
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	
羽渕裕真教授	電子情報通信学会ITS研究専門委員会 顧問	
羽渕裕真教授	電子情報通信学会東京支部 次期支部長	
羽渕裕真教授	IEEE Japan Chapter Treasure	
羽渕裕真教授	IEEE Tokyo Section Treasure	
羽渕裕真教授	IEEE ITS Tokyo Chapter 委員	
羽渕裕真教授	IEEE VTS Tokyo Chapter 委員	
羽渕裕真教授	Associate Editor, IEICE Transaction in Fundamentals, Special section on WideBand Systems	
羽渕裕真教授	Associate Editor, IEICE Transaction in Fundamentals, Special section on Intelligent Transport Systems	
羽渕裕真教授	Associate Editor, IEICE Transaction in Fundamentals, Special section on Signal Design and its Applications in Communications	
羽渕裕真教授	Technical Program Committee Member, IEEE Asia Pacific Wireless Communications Symposium (IEEE VCS APWCS2018)	
羽渕裕真教授	Technical Program Committee Member, International Conference on ITS Telecommunications (ITST 2018)	
羽渕裕真教授	Technical Program Committee Member, IEEE GLOBECOM Workshop on Optical Wireless Communications	
羽渕裕真教授	Technical Program Committee Member, 10th International Conference on Knowledge and Systems Engineering (KSE 2018)	
羽渕裕真教授	Technical Program Committee Member, 2nd International Conference on Electrical Engineering and Informatics（ICon EEI 2018）	
羽渕裕真教授	Technical Program Committee Member, IEEE International Conference on Communication, Networks and Satellite (COMNETSAT 2018)	

教員名	内容等
羽渕裕真教授	Technical Program Committee Member, International Conference on Advances in Computing, Communications and Informatics (ICACCI 2018)
羽渕裕真教授	Technical Program Committee Member, International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC 2018)
羽渕裕真教授	Technical Program Committee Member, International Conference on Advanced Technologies for Communications (ATC'18)
羽渕裕真教授	Technical Program Committee Member, The 3rd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom2019)
羽渕裕真教授	Technical Program Committee Member, IEEE ICC'19 - SPC Symposium
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）
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
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
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
米山一樹准教授	日本応用数理学会 日本応用数理学会論文誌 編集委員
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
米山一樹准教授	電子情報通信学会 2020 年英文論文誌小特集編集委員会 編集幹事
米山一樹准教授	Indocrypt2018 プログラム委員
米山一樹准教授	ACM ASIA Public-Key Cryptography Workshop 2018 プログラム委員
米山一樹准教授	ACM ASIA Public-Key Cryptography Workshop 2019 プログラム委員
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
古宮嘉那子講師	ICT-IPSC 2018 プログラム委員
古宮嘉那子講師	電子情報通信学会 言語理解とコミュニケーション研究会 (NLC) 運営委員
古宮嘉那子講師	JCSSE 2018 プログラム委員
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
芝軒太郎講師	日本ロボット学会会誌編集委員
野口宏准教授	学術情報処理研究編集委員
野口宏准教授	水戸市個人情報保護運営委員審議会

教員名	内容等
小澤佑介助教	TPC member for 8th IEEE Globecom Workshop on Optical Wireless Communications (OWC'18)
小澤佑介助教	Secretary for 8th IEEE Globecom workshop on Optical Wireless Communications (OWC18)
小澤佑介助教	日本フォトニクス協議会可視光通信分科会 幹事
小澤佑介助教	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 幹事
小澤佑介助教	IEICE Guest Editor for the IEICE transactions on fundamentals special section on Wideband Systems
小澤佑介助教	Publication chair for RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing 2019 (NCSP2019)
小花聖輝助教	WSSM-2018 Workshop Co-chair
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
新納浩幸教授	自然言語処理学会理事
新納浩幸教授	言語処理学会第 25 回年次大会 大会副委員長
佐々木稔講師	情報処理学会論文誌データベース編集委員

佐々木稔講師	情報処理学会自然言語処理研究会運営委員
佐々木稔講師	国際会議 SEMAPRO 2018 Technical Program Committee
佐々木稔講師	International Journal On Advances in Intelligent Systems, Editorial Board
佐々木稔講師	ひたちものづくりサロン代表幹事
佐々木稔講師	FM ひたち番組審議委員
髙橋竜一助教	電子情報通信学会知能ソフトウェア工学研究専門委員会　幹事補佐

✧　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（C）	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（代表）
基盤（C）	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（代表）
基盤（C）	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（代表）
若手（B）	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（代表）
基盤（A）	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（分担）
科研費(国際共同研究加速基金)出型」共同研究	古宮嘉那子講師	語義曖昧性解消結果と領域適応を利用した課題情報の抽出(代表)
若手（B）	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（代表）
若手（B）	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（代表）
若手（B）	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（代表）

・今年度新規採択課題

種別	教員	研究課題
基盤（C）	古宮嘉那子講師	複数タスクのタグがついたコーパスによる語義曖昧性解消の転移学習
基盤（C）	大瀧保広准教授	検索可能暗号の応用システムに関する研究
基盤（C）	佐々木稔講師	半教師あり学習を用いた語義曖昧性解消

基盤（B）	藤芳明生准教授	文字認知が困難な児童生徒の公平な学力評価を保証するマルチモーダル問題の開発と評価（代表）
基盤（B）	藤芳明生准教授	障害特性に合わせデジタル教科書・教材を最適にバリアフリー化するシステムの研究(分担)
基盤（C）	上田賀一教授	組込みシステムのモデルベース設計のためのハイブリッドモデル検査手法の確立

・共同研究

教員名	共同研究課題
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 30 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
古宮嘉那子講師	国立国語共同研究プロジェクト　「通時コーパスの構築と日本語史研究の新展開」
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　実運用に即したグループ鍵共有プロトコルの共同研究
米山一樹准教授	東芝　形式検証を用いた暗号プロトコルの安全性検証に関する研究
米山一樹准教授	富士通研究所　セキュリティ攻撃の動向調査
小澤佑介助教	日本フォトニクス協議会可視光通信分科会　フェーズドアレイ光学素子を用いた光空間伝送装置の研究開発
小澤佑介助教	海洋開発研究機構　イメージセンサ型可視光通信を用いた水中無線通信・測距技術の研究
新納浩幸教授	日立水戸エンジニアリング 画像認識技術を利用した作業効率改善に関する研究
新納浩幸教授	アイシン・エィ・ダブリュ株式会社　「時系列モデリング手法の開発」

佐々木稔講師	大和証券投資信託委託株式会社「AI 運用のためのニューステキストからのアルファならびにセンチメント情報自動抽出」
上田賀一教授 高橋竜一助教	日立 AMS「自動運転制御ソフトウェアのアーキテクチャに関する研究 」
湊淳教授 原口春海講師	サンテクノ「機械学習による検品ツール開発に関する予備検討」

・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 30 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）
藤芳明生准教授	音声教材の効率的な製作方法等に関する調査研究（文部科学省，NPO 法人テストと学習環境のユニバーサルデザイン研究機構より再委託）

・その他

・今年度新規採択課題

種別	教員	研究課題
茨城大学女性エンパワーメント支援制度	原口春海講師	鉄筋製造業における人的要因を考慮した作業者計画モデル
研究推進経費（Research Booster）	新納浩幸教授	文書の埋め込み表現と双方向 LSTM を用いた翻訳文書の訳語校正

・継続研究課題

種別	教員	研究課題
茨城大学研究拠点認定	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（代表）
茨城大学推進研究プロジェクト	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（代表）

8. 計画名：当教育研究センター構成メンバによる勉強会
実施結果：
・平成 30 年 9 月に、全員参加型の勉強会を実施した.

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 30 年 4 月 1 日～平成 31 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，原口春海，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 30 年 4 月 1 日～平成 31 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，原口春海，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 30 年 4 月 1 日～平成 31 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，原口春海，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。）

- 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
  - 実施結果：下記論文誌・国際会議等で学生が発表を行った.

- 国際会議論文：Akinaga Ueda, Hayato Tada, Kaoru Kurosawa: (Short Paper) How to Solve DLOG Problem with Auxiliary Input. IWSEC 2018: 104-113
- 国際会議論文：Hayato Tada, Akinaga Ueda, Kaoru Kurosawa: How to Prove KDM Security of BHHO. IWSEC 2018: 281-296
- 国際会議論文：Hiroyuki Shinnou, Xinyu Zhao and Kanako Komiya, “Domain Adaptation Using a Combination of Multiple Embeddings”, PACLIC 2018, Hong Kong, China, 1-3 December, 2018 (accepted).
- 国際会議論文：Masaya Suzuki, Kanako Komiya, Minoru Sasaki and Hiroyuki Shinnou, “Fine-tuning for Named Entity Recognition Using Part-of-Speech Tagging”, PACLIC 2018, Hong Kong, China, 1-3 December, 2018.

- **国際会議論文**: Jing Bai, Hiroyuki Shinnou and Kanako Komiya, “Domain Adaptation for Sentiment Analysis using Keywords in the Target Domain as the Learning Weight”, PACLIC 2018, Hong Kong, China, 1-3 December, 2018.
- **国際会議論文**: Aya Tanabe, Kanako Komiya, Masayuki Asahara, Minoru Sasaki and Hiroyuki Shinnou, “Detecting Unknown Word Senses in Contemporary Japanese Dictionary from Corpus of Historical Japanese”, JADH 2018, Tokyo, Japan, 9-11 September, 2018.
- **国際会議論文**: Rui Suzuki, Kanako Komiya, Masayuki Asahara, Minoru Sasaki and Hiroyuki Shinnou, “All-words Word Sense Disambiguation Using Concept Embeddings”, LREC 2018, no 100, Miyazaki Japan, 9-11 May, 2018.
- **国際会議論文**: Cheng Shi, Kazuki Yoneyama, "Verification of LINE Encryption Version 1.0 using ProVerif", International Workshop on Security (IWSEC 2018), LNCS11409, pp.158-173, Sep. 2018.
- **国際会議論文**: Shintaro Terada, Kazuki Yoneyama, "Improved Verifiable Delegated Private Set Intersection", International Symposium on Information Theory and its Applications (ISITA 2018), pp., Oct. 2018.
- **国際会議論文**: Yuma Kanai, Kazuki Yoneyama, "On Hiding Access Timings in ORAM", International Symposium on Information Theory and its Applications (ISITA 2018), pp., Oct. 2018.
- **国際会議論文**: Shotaro Naiki, Masaki Kohana, Shusuke Okamoto and Masaru Kamada: A graphical front-end interface for React.js. In: L. Barolli et al. (eds.), Advances in Network-based Information Systems (Proceedings of the 21st International Conference on Network-based Information Systems, NBiS-2018), Lecture Notes on Data Engineering and Communications Technologies 22, Springer, pp.887-896, Sep. 2018.
- **国際会議論文**: Shinya Kinoshita, Michitoshi Niibori and Masaru Kamada: An attendance management system capable of mapping participants onto the seat map. In: L. Barolli et al. (eds.), Advances in Network-based Information Systems (Proceedings of the 21st International Conference on Network-based Information Systems, NBiS-2018), Lecture Notes on Data Engineering and Communications Technologies 22, Springer, pp.897-902, Sep. 2018.
- **国際会議論文**: Tatsuya Ohyanagi, Tomoyuki Ishida, Noriki Uchida, Yoshitaka Shibata, and Hiromasa Habuchi: "Proposal of a Disaster Support Expert System Using Accumulated Empirical Data", The 12th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2018), July 2018
- **国際会議論文**: Yutaka Imaizumi, Hiromasa Habuchi, and Koichiro Hashiura : "Improved Packet Success Rate on MC-CDMA based On-demand WSN System with MPOMS", IEEE Vehicular Technology Society Asia Pacific Wireless Communications Symposium (APWCS 2018), Aug. 2018
- **国際会議論文**: Hikari Iiduka, Hiromasa Habuchi, and Yusuke Kozawa : "Proposal of VN-CSK System having Positioning Function", IEEE Vehicular Technology Society Asia Pacific Wireless Communications Symposium (APWCS 2018), Aug. 2018
- **国際会議論文**: Tomofumi Haruna, Hiromasa Habuchi, and Yusuke Kozawa : "Theoretical Analysis of Optical-Wireless Code Shift Keying System using Extended Einarsson Code", IEEE Vehicular Technology Society Asia Pacific Wireless Communications Symposium (APWCS 2018), Aug. 2018
- **国際会議論文**: Yuto Asano, Hiromasa Habuchi, and Yusuke Kozawa : "Exact Bit Error Rate Analysis for Optical-Wireless Framed-DOOK System", IEEE 7th Global Conference of Consumer Electronics (GCCE 2018), (2018-10-12)
- **国際会議論文**: Takashi Tokunaga, Hiromasa Habuchi, Yusuke Kozawa, and Ran Sun : "BER Performance Impaired by Transmission Time Offset Between Users in Optical Wireless CSK/ACDMA System Using DMPOMs", IEEE 7th Global Conference of Consumer Electronics (GCCE 2018), (2018-10-12)
- **国際会議論文**: Yutaka Imaizumi, Hiromasa Habuchi, and Yusuke Kozawa : "Enhanced On-demand WSN in terms of MC-CDMA with MPOMS", IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS 2018), pp.102-106, (2018-11-28)
- **国際会議論文**: Run Sun, Hiromasa Habuchi, and Yusuke Kozawa : "Proposal of Optical Wireless Turbo Coded System with Hybrid PPM-OOK Signalling", International Conference on Signal Processing and Communication Systems (ICSPCS 2018), (2018-12-18)

- 国際会議論文: Yuto Asano, Hiromasa Habuchi, and Yusuke Kozawa : "Frame Error Detection Performance of Optical-Wireless Advanced Framed-DOOK System", International Conference on Signal Processing and Communication Systems (ICSPCS 2018), (2018-12-19)
- 国際会議論文: Lu Yangzhicheng, Tomoyuki Ishida, Hiromasa Habuchi : "Proposal of a Furniture Layout Simulation System using Mixed Reality Technology", 24th International Symposium on Artificial Life and Robotics pp.808-811, (2019-01-24)
- 国際会議論文: Ryo Nakai, Tatsuya Ohyanagi, Tomoyuki Ishida, Hiromasa Habuchi : "Proposal of a Scalable Interactive Visualization Environment using Large Display in Emergency", 24th International Symposium on Artificial Life and Robotics pp.812-815, (2019-01-24)
- 国際会議論文: Hikari Iizuka, Ran Sun, Hiromasa Habuchi, and Yusuke Kozawa : "High Accuracy Positioning System on Indoor Optical Wireless VN-CSK System",RISP International Workshop on Nonlinear Circuits, Communication and Signal Processing (NCSP'19), (2019-03-05),
- 国際会議論文: Yuta Asano, Hiromasa Habuchi, and Yusuke Kozawa : "Effective Frame Error Detecting Scheme for Optical-Wireless Advanced Framed-DOOK System", RISP International Workshop on Nonlinear Circuits, Communication and Signal Processing (NCSP'19), (2019-03-05)
- その他(研究会等): 柴田 敏弥, 米山 一樹, "UC 安全動的検索可能暗号の拡張とフォワード安全性について", 暗号と情報セキュリティシンポジウム (SCIS 2019), Jan. 2019.
- その他(研究会等): 金井 佑篤, 米山 一樹, "複数のファイルアクセス可能な ORAM", 暗号と情報セキュリティシンポジウム (SCIS 2019), Jan. 2019.
- その他(研究会等): 寺田 槙太郎, 米山 一樹, "CSIDH に基づくパスワードベース認証鍵交換 ", 暗号と情報セキュリティシンポジウム (SCIS 2019), Jan. 2019.
- その他(研究会等): 野口 凌雅, 花谷 嘉一, 米山 一樹, "ProVerif による HEMS におけるグループ鍵管理の検証", 暗号と情報セキュリティシンポジウム (SCIS 2019), Jan. 2019.
- その他(研究会等): 師 成, 米山 一樹, "ProVerif によるスマートコントラクト決済委託プロトコルの公平性の検証", 暗号と情報セキュリティシンポジウム (SCIS 2019), Jan. 2019.
- その他(研究会等): 勝野 凌介, 米山 一樹, "IC カードとリーダ/ライタ間の認証プロトコルにおける認証再利用と暗号理論的安全性モデルの関係", 電子情報通信学会情報セキュリティ研究会, Mar. 2019.
- その他(研究会等): 白井 直輝, 米山 一樹, "検証可能委譲秘匿ビット比較演算", 電子情報通信学会情報セキュリティ研究会, Mar. 2019.
- その他(研究会等): 春名智文, 羽渕裕真, 小澤佑介 : "光無線 CSK システムへの拡張 Einarsson 符号の適用性", 電子情報通信学会ワイドバンド研究会 WBS2018-8, pp.17-22, (2018-07-06)
- その他(研究会等): 飯塚暉, 羽渕裕真, 小澤佑介 : "光無線 VN-CSK システムにおける測位性能の検討", 電子情報通信学会ワイドバンド研究会 WBS2018-9, pp.23-27, (2018-07-06)
- その他(研究会等): 今泉豊, 大川智広, 羽渕裕真, 橋浦康一郎 : "変形擬直交 M 系列対を用いるオンデマンド型 WSN におけるパケット成功率向上法", 電子情報通信学会ワイドバンド研究会, WBS2018-11, pp.35-40, (2018-07-06)
- 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 システムにおける同期シンボルによる誤り検出法の検討", 電子情報通信学会ワイドバンド研究会, WBS2018-16, pp.59-63, (2018-07-06)
- その他(研究会等): 徳永岳, 孫冉, 羽渕裕真, 小澤佑介 : "DMPOMs を用いる光無線 CSK システムにおける同期性能を考慮した誤り率性能", 電子情報通信学会ワイドバンド研究会, WBS2018-17, pp.65-70, (2018-07-06)
- その他(研究会等): 浅野裕太, 羽渕裕真, 小澤佑介 : "誤り検出可能な光無線フレーム化 DOOK システム", 革新的無線通信技術に関する横断型研究会 MIKA2018, 3-13, (2018-09-27)
- 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ハイブリッド PPM-OOK ターボ符号システム", 革新的無線通信技術に関する横断型研究会 MIKA2018, 3-14, (2018-09-27)
- その他(研究会等): 陳力源, 羽渕裕真: "SIK を用いる多視覚秘密分散法によるマルチルートネットワーク", 革新的無線通信技術に関する横断型研究会 MIKA2018, 4-2, (2018-09-27)
- その他(研究会等): 浅野裕太, 羽渕裕真, 小澤佑介:"拡張フレーム化 DOOK システムのためのフレーム誤り検出法の検討",電子情報通信学会ワイドバンド研究会,WBS2018-30 (ITS2018-13, RCC2018-

61), pp.17-21, (2018-12-06)

- その他（研究会等）：孫冉，羽渕裕真，小澤佑介 ："ハイブリッド PPM-OOK 信号形式を用いる光無線パンクチャードターボ符号システムの検討"，電子情報通信学会ワイドバンド研究会,WBS2018-72 (ITS2018-55, RCC2018-103), pp.249-253, (2018-12-07)
- その他（研究会等）：真中佳祐，陳力源，羽渕裕真，小澤佑介 ："VN-CSK 照明可視光通信における等重み(2,2)視覚復号型秘密分散法"，電子情報通信学会東京支部学生会研究発表会, (2019-03-02)
- その他（研究会等）：木口朋洋，孫冉，羽渕裕真，小澤佑介 ："光無線 PPM-OOK システムのためのフレーム同期法 "，電子情報通信学会東京支部学生会研究発表会, (2019-03-02)
- その他（研究会等）：鈴木暁大，羽渕裕真 ："フレーム ALOHA を用いる MPSC-PDMA 方式"，電子情報通信学会東京支部学生会研究発表会, (2019-03-02)
- その他（研究会等）：孫冉，羽渕裕真，小澤佑介 ："光無線通信ターボ符号システムにおける信号伝送形式の一検討"，電子情報通信学会 WBS/IT/ISEC 合同研究会, WBS2018- (IT2018- ,ISEC2018-), (2019-03-07)
- その他（研究会等）：今泉豊，羽渕裕真，橋浦康一郎 ："変形擬直交 M 系列対を用いる ROD-WSN における ノード間干渉の影響"，電子情報通信学会総合大会, (2019-03-19)
- その他（研究会等）：荒井宏，原口春海，“鉄筋製造業における切断作業の効率化に関する研究”，日本機械学会生産システム部門研究発表講演会 2019，2019 年 3 月（発表予定）
- その他（研究会等）：黒澤馨、上田明長、松橋駿斗、阪上佑介，"複数の小さな離散対数問題を解くアルゴリズム"，暗号と情報セキュリティシンポジウム (SCIS 2019), Jan. 2019.019.
- その他（研究会等）：冨田斗威、尾形わかは、黒澤馨、"標準的な仮定のもとで leakage resilient かつ CCA 安全な ID ベース KEM"，暗号と情報セキュリティシンポジウム (SCIS 2019), Jan. 2019.019.

- 計画名：各種講座やセミナー等による地域人材の育成
  - 実施結果：特になし

- 計画名：各種発表会等による技術講演・技術交流
  - 実施結果：

講演者	講演内容
原口春海講師	平成 30 年度茨大シーズ発表会「IoT 時代の作業者訓練のあり方」
	水戸英陵高等学校【模擬授業】5 月 24 日 「高校数学の数式で理解する通信ネットワーク」
黒澤馨教授	ハノイ科学大学学生向けサマーセミナー「現代暗号理論入門」

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. 研究報告

【代表的な論文】

IEICE TRANS. FUNDAMENTALS, VOL.E102–A, NO.1 JANUARY 2019

PAPER Special Section on Cryptography and Information Security

No-Dictionary Searchable Symmetric Encryption*

Wakaha OGATA[†a)], ***Member and*** **Kaoru KUROSAWA**[††b)], ***Fellow***

SUMMARY In the model of *no-dictionary* searchable symmetric encryption (SSE) schemes, the client does not need to keep the list of keywords $\mathcal{W}$. In this paper, we first show a generic method to transform any passively secure SSE scheme to a *no-dictionary* SSE scheme such that the client can verify search results even if $w \notin \mathcal{W}$. In particular, it takes only $O(1)$ time for the server to prove that $w \notin \mathcal{W}$. We next present a no-dictionary SSE scheme such that the client can hide even the search pattern from the server.

key words: *searchable symmetric encryption, dictionary, verifiable, search pattern*

1. Introduction

1.1 Background

The notion of searchable symmetric encryption (SSE) schemes was introduced by Song et al. [34]. In the store phase, a client encrypts a set of files and an index table by a symmetric encryption scheme, and then stores them on an untrusted server. In the search phase, he can efficiently retrieve the matching files for a search keyword w keeping the keyword and the files secret.

Since then, single keyword search SSE schemes [15], [16], [19], [24], [26], dynamic SSE schemes [13], [21], [22], [25], [27], [30], verifiable SSE schemes [24]–[27], [35], multiple keyword search SSE schemes [1], [7], [12], [20], [23], [36] and more [14] have been studied extensively by many researchers.

Curtmola, et al. [16], [17] gave a rigorous definition of privacy against honest but curious servers. Kurosawa and Ohtaki [24], [26] showed a definition of reliability against malicious servers who may return incorrect search results to the client, or may delete some encrypted files to save her memory space. An SSE scheme is called verifiable if it satisfies both privacy and reliability.

Let $\mathcal{D} = \{D_1, \ldots, D_N\}$ be the set of files and $\mathcal{W} = \{w_1, \ldots, w_m\}$ be the set of keywords, where each keyword w is contained in some file(s). We call $\mathcal{W}$ a dictionary.

Let $\mathcal{ID}(w) = \{j \mid D_j \text{ contains } w\}$. Then an index table $\mathcal{T}$ is defined as $\mathcal{T} = (\mathcal{ID}(w_1), \ldots, \mathcal{ID}(w_m))$, where $w_i \in \mathcal{W}$. Let $\mathcal{I}$ be an encryption of $\mathcal{T}$. In the store phase, the client sends $\mathcal{I}$ and an encryption of $\mathcal{D}$ to the server.

We say that an SSE scheme is a *no-dictionary* SSE scheme if the client does not need to keep $\mathcal{W}$. In usual SSE schemes, the client does not need to keep $\mathcal{W}$. However, there are some exceptional cases. In this paper, we study two cases in which it is non-trivial to design an efficient no-dictionary SSE scheme. (The notion of no-dictionary SSE schemes was first studied by Taketani and Ogata [35] in the setting of verifiable SSE schemes.)

1.2 No-Dictionary SSE with Search Pattern Hiding

The search pattern is the information on which past queries are the same as the current one, where a query is an encryption of a search word w. In usual SSE schemes, the search pattern is leaked to the server.

If the client keeps a dictionary $\mathcal{W}$, we can construct a search pattern hiding SSE scheme by using the technique of private information retrieval (PIR) [29], [32][†] (The cost for it is that the communication complexity and the computation complexity increase.).

In the store phase, the client stores an encrypted index table $\mathcal{I}_0 = (\mathcal{I}_0[1], \ldots, \mathcal{I}_0[m])$ such that $\mathcal{I}_0[i]$ is an encryption of $\mathcal{T}[i] (= \mathcal{ID}(w_i))$, where $w_i \in \mathcal{W}$ for each i. In the search phase, by using PIR, he obtains $\mathcal{I}_0[i]$ from the server without revealing any information on the search word $w_i \in \mathcal{W}$. This means that the search pattern is hidden from the server. He finally retrieves encryptions of all D_j such that $j \in \mathcal{T}[i]$ from the server.

If the client does not want to keep $\mathcal{W}$ (i.e. no-dictionary SSE), there is a simple way to modify the above scheme. Let b be the bit length of the longest keyword in $\mathcal{W}$, and let $\pi : \{0,1\}^{\leq b} \to \{0,1\}^{\ell}$ be an injection for some ℓ. The client constructs an extended index table $\mathcal{T}_e$ of size 2^{ℓ} such that $\mathcal{T}_e[\pi(w)] = \mathcal{ID}(w)$. Then he stores $\mathcal{I}_e = (\mathcal{I}_e[1], \ldots, \mathcal{I}_e[2^{\ell}])$ such that $\mathcal{I}_e[i]$ is an encryption of $\mathcal{T}_e[i]$ to the server, and keeps only (b, π). In this way, we can obtain a no-dictionary search-pattern hiding SSE scheme. However, $\mathcal{I}_e$ is much larger than $\mathcal{I}_0$ because $2^{\ell} \gg |\mathcal{W}|$ in general.

Manuscript received March 20, 2018.
Manuscript revised June 19, 2018.

[†]The author is with Tokyo Institute of Technology, Tokyo, 152-8552 Japan.
[††]The author is with Ibaraki University, Hitachi-shi, 316-8511 Japan.

*A part of this paper was published at Financial Cryptography and Data Security 2017 [31].

a) E-mail: ogata.w.aa@m.titech.ac.jp
b) E-mail: kaoru.kurosawa.kk@vc.ibaraki.ac.jp

DOI: 10.1587/transfun.E102.A.114

[†]The connection between SSE and PIR was suggested by Curtmola et al. [16], [17].

1.3 No-Dictionary Verifiable SSE

Consider a verifiable SSE scheme such as follows. The client stores $\mathcal{I}_1 = ((a_1, b_1, c_1), \ldots, (a_m, b_m, c_m))$ to the server such that

$$(a_i, b_i, c_i) = (F_{k_1}(w_i), F_{k_2}(w_i) + \mathcal{ID}(w_i), MAC(a_i, b_i))$$

for each $w_i \in \mathcal{W}$, where F is a pseudorandom function and k_1, k_2 are keys. To search on w, the client sends

$$(a', b') = (F_{k_1}(w), F_{k_2}(w))$$

to the server. The server finds i such that $a' = a_i$ and returns the search result with $MAC(a_i, b_i)$.

Is it a *no-dictionary* verifiable SSE scheme? The answer is no because a malicious server can cheat by saying that $a' \notin \{a_1, \ldots, a_m\}$ (namely $w \notin \mathcal{W}$) even if $a' \in \{a_1, \ldots, a_m\}$. The client has no way to check this.

We can prevent this cheating by using the extended index table $\mathcal{T}_e$ defined in Sect. 1.2. However, the encrypted $\mathcal{I}_e$ gets much larger than $\mathcal{I}_1$ (see Sect. 1.2).

For this problem, Taketani and Ogata [35] showed a *no-dictionary* verifiable SSE scheme such that the encrypted index table is almost the same size as $\mathcal{I}_1$. In this scheme, however, the server takes $O(N \log(Nm))$ time to prove that $w \notin \mathcal{W}$, where $N = |\mathcal{D}|$ and $m = |\mathcal{W}|$.

1.4 Our Contribution

In this paper, we first show a generic method to transform any passively secure SSE scheme to a *no-dictionary* verifiable SSE scheme. In the transformed scheme, the encrypted index table is only a few times larger than that of the underlying SSE scheme, and the server takes only $O(1)$ time to prove that $w \notin \mathcal{W}$, which is more efficient than the scheme in [35]. The search time for $w \in \mathcal{W}$ remains almost the same as that of the original SSE scheme. We also prove that the transformed scheme is UC-secure in Appendix similarly to [24], [26].

We next present a no-dictionary search-pattern hiding SSE scheme such that the encrypted index table is only a few times larger than $\mathcal{I}_0$ (As in the corresponding dictionary SSE scheme, the cost for it is that the communication complexity and the computation complexity increase.)[†].

We use Cuckoo Hashing [33] in both our results as a main technical tool.

1.5 Remark

In the verifiable SSE schemes of [24]–[27], the set of keywords is defined as $\mathcal{W} = \{0,1\}^\ell$. In reality, however, keywords have various length. Therefore we must use the technique of Sect. 1.2 in practice.

[†]This part was not written in the conference version [31] of this paper.

If we use an oblivious RAM (ORAM) in a dynamic SSE scheme [18] (in which the client can update files), we can hide the search pattern and the access pattern. In such a scheme, however, the client must keep the dictionary (or a corresponding list). The communication cost is also large.

2. Verifiable Searchable Symmetric Encryption

In this section, we define a no-dictionary (verifiable) SSE scheme and its security. Basically, we follow the notation used in [12], [24], [26].

- Let $\mathcal{D} = \{D_1, \ldots, D_N\}$ be the set of files.
- Let $\mathcal{W}$ be the set of keywords, where each keyword w is contained in some file(s).
- For $w \in \{0,1\}^*$, define as follows:

$$\mathcal{D}(w) = \begin{cases} \{D_i \mid D_i \text{ contains } w\} & \text{if } w \in \mathcal{W} \\ \emptyset & \text{otherwise} \end{cases}$$

- Let $C = \{C_1, \ldots, C_N\}$, where C_i is a ciphertext of D_i.
- Let

$$C(w) = \{C_i \mid C_i \text{ is a ciphertext of } D_i \in \mathcal{D}(w)\}. \quad (1)$$

Note that $C(w) = \emptyset$ if $w \notin \mathcal{W}$.

If X is a bit string, $|X|$ denotes the bit length of X. If X is a set, $|X|$ denotes the cardinality of X. "PPT" refers to probabilistic polynomial time, and "PT" refers to polynomial time.

2.1 Model

An SSE scheme has two phases, the store phase (which is executed only once) and the search phase (which is executed a polynomial number of times). In the store phase, the client encrypts all files in $\mathcal{D}$ and stores them on the server. In the search phase, the client sends a ciphertext of a word w, and the server returns $C(w)$. If there is a mechanism to verify the validity of $C(w)$, the scheme is called a verifiable SSE (vSSE).

Formally, a vSSE scheme consists of the following four polynomial-time algorithms $\mathtt{vSSE} = (\mathtt{Setup}, \mathtt{Trpdr}, \mathtt{Search}, \mathtt{Dec})$ as follows:

- $(K, \mathcal{I}, C) \leftarrow \mathtt{Setup}(1^\lambda, \mathcal{D}, \mathcal{W}, \{(w, \mathcal{D}(w)) \mid w \in \mathcal{W}\})$: a PPT algorithm that generates a key K, an encrypted index $\mathcal{I}$, and the set of encrypted files $C = \{C_1, \ldots, C_N\}$, where λ is a security parameter.
  This algorithm is run by the client in the store phase. He then stores $(\mathcal{I}, C)$ on the server.
- $t(w) \leftarrow \mathtt{Trpdr}(K, w)$: a PPT algorithm that outputs a trapdoor $t(w)$ for $w \in \{0,1\}^*$.
  This algorithm is run by the client in the search phase. $t(w)$ is sent to the server.
- $(C^*, \mathsf{Proof}) \leftarrow \mathtt{Search}(\mathcal{I}, C, t(w))$: a PT algorithm that outputs the search result C^* and Proof for the validity check.

This algorithm is run by the server in the search phase. She then returns (C^*, Proof) to the client.

- $\mathcal{D}^*/\perp \leftarrow \mathtt{Dec}(K, t(w), C^*, \mathsf{Proof})$: a PT algorithm that decrypts C^* and verifies its validity based on Proof. If not valid, output is $\perp$. This algorithm is run by the client in the search phase.

We say that a vSSE satisfies correctness if the following holds for any $K, \mathcal{D}, \mathcal{W}, \{(w, \mathcal{D}(w)) \mid w \in \mathcal{W}\}$ and any word $w \in \{0,1\}^*$.

- If

$$\begin{aligned}(K, \mathcal{I}, C) &\leftarrow \mathtt{Setup}(1^\lambda, \mathcal{D}, \mathcal{W}, \\ &\qquad \{(w, \mathcal{D}(w)) \mid w \in \mathcal{W}\}), \\ t(w) &\leftarrow \mathtt{Trpdr}(K, w), \\ (C^*, \mathsf{Proof}) &\leftarrow \mathtt{Search}(\mathcal{I}, C, t(w)), \\ \mathcal{D}^* &\leftarrow \mathtt{Dec}(K, t(w), C^*, \mathsf{Proof}),\end{aligned}$$

then

$$\mathcal{D}^* = \mathcal{D}(w).$$

We assume that C^* is equal to $C(w)(\subset C)$ as in most existing schemes.

An (not verifiable) SSE scheme is defined by omitting Proof.

2.2 Security Definition

We next define the security of vSSE schemes. Note that a search word w does not need to belong to the set $\mathcal{W}$.

Privacy. In a (v)SSE, the server should learn almost no information on $\mathcal{D}, \mathcal{W}$, and the search word w. Let $L_1(\mathcal{D}, \mathcal{W})$ denote the information that the server can learn in the store phase, and let $L_2(\mathcal{D}, \mathcal{W}, \mathbf{w}, w)$ denote that in the search phase, where w is the current search word and $\mathbf{w} = (w_1, w_2, \ldots)$ is the list of the past search words queried so far.

In most existing SSE schemes, $L_1(\mathcal{D}, \mathcal{W}) = (|D_1|, \ldots, |D_N|, |\mathcal{W}|)$, and $L_2(\mathcal{D}, \mathcal{W}, \mathbf{w}, w)$ consists of $\{j \mid D_j \in \mathcal{D}(w)\}$ and the search pattern

$$\mathtt{SPattern}((w_1, \ldots, w_{q-1}), w) = (sp_1, \ldots, sp_{q-1}),$$

where

$$sp_j = \begin{cases} 1 & \text{if } w_j = w, \\ 0 & \text{if } w_j \neq w. \end{cases}$$

The search pattern reveals which past queries are the same as w.

Let $L = (L_1, L_2)$. The client's privacy is defined by using two games: a real game $\mathbf{Game}_{real}$ and a simulation game $\mathbf{Game}^L_{sim}$, as shown in Figs. 1 and 2, respectively. $\mathbf{Game}_{real}$ is played by a challenger $\mathbf{C}$ and an adversary $\mathbf{A}$, and $\mathbf{Game}^L_{sim}$ is played by $\mathbf{C}$, $\mathbf{A}$, and a simulator $\mathbf{S}$.

Definition 1 (L-privacy): We say that a vSSE scheme has L-privacy, if there exists a PPT simulator $\mathbf{S}$ such that

$$\begin{aligned}&|\Pr[\mathbf{A} \text{ outputs } b = 1 \text{ in } \mathbf{Game}_{real}] \\ &\quad - \Pr[\mathbf{A} \text{ outputs } b = 1 \text{ in } \mathbf{Game}^L_{sim}]|\end{aligned} \tag{2}$$

is negligible for any PPT adversary $\mathbf{A}$.

1. Adversary $\mathbf{A}$ chooses $(\mathcal{D}, \mathcal{W})$ and sends them to challenger $\mathbf{C}$.
2. $\mathbf{C}$ generates $(K, \mathcal{I}, C) \leftarrow \mathtt{Setup}(1^\lambda, \mathcal{D}, \mathcal{W}, \{(w, \mathcal{D}(w)) \mid w \in \mathcal{W}\})$ and sends $(\mathcal{I}, C)$ to $\mathbf{A}$.
3. For $i = 1, \ldots, q$, do:
   a. $\mathbf{A}$ chooses a word $w_i \in \{0,1\}^*$ and sends it to $\mathbf{C}$.
   b. $\mathbf{C}$ sends the trapdoor $t(w_i) \leftarrow \mathtt{Trpdr}(K, w_i)$ back to $\mathbf{A}$.
4. $\mathbf{A}$ outputs bit b.

Fig. 1 Real game $\mathbf{Game}_{real}$.

1. Adversary $\mathbf{A}$ chooses $(\mathcal{D}, \mathcal{W})$ and sends them to challenger $\mathbf{C}$.
2. $\mathbf{C}$ sends $L_1(\mathcal{D}, \mathcal{W})$ to simulator $\mathbf{S}$.
3. $\mathbf{S}$ computes $(\mathcal{I}, C)$ from $L_1(\mathcal{D}, \mathcal{W})$, and sends them to $\mathbf{C}$.
4. $\mathbf{C}$ relays $(\mathcal{I}, C)$ to $\mathbf{A}$.
5. For $i = 1, \ldots, q$, do:
   a. $\mathbf{A}$ chooses $w_i \in \{0,1\}^*$ and sends it to $\mathbf{C}$.
   b. $\mathbf{C}$ sends $L_2(\mathcal{D}, \mathcal{W}, \mathbf{w}, w_i)$ to $\mathbf{S}$, where $\mathbf{w} = (w_1, \ldots, w_{i-1})$.
   c. $\mathbf{S}$ computes $t(w_i)$ from $L_2(\mathcal{D}, \mathcal{W}, \mathbf{w}, w_i)$ and sends it to $\mathbf{C}$.
   d. $\mathbf{C}$ relays $t(w_i)$ to $\mathbf{A}$.
6. $\mathbf{A}$ outputs bit b.

Fig. 2 Simulation game $\mathbf{Game}^L_{sim}$.

Reliability. In an SSE scheme, a malicious server might cheat a client by returning a false result $\tilde{C}^* (\neq C(w))$ during the search phase. (Weak) reliability guarantees that the client can detect such a malicious behavior. Formally, reliability is defined by game $\mathbf{Game}_{reli}$ shown in Fig. 3, which is played by an adversary $\mathbf{B} = (\mathbf{B}_1, \mathbf{B}_2)$ (malicious server) and a challenger $\mathbf{C}$. $\mathbf{B}_1$ and $\mathbf{B}_2$ are assumed to be able to communicate freely.

Definition 2 (Reliability): We say that $\mathbf{B}$ wins in $\mathbf{Game}_{reli}$ if $\mathbf{B}_1$ receives $\mathcal{D}^*_i$ such that $\tilde{\mathcal{D}}^*_i \notin \{\mathcal{D}(w_i), \perp\}$ for some i. We say that a vSSE scheme satisfies reliability if for any PPT adversary $\mathbf{B}$,

$$\Pr[\mathbf{B} \text{ wins in } \mathbf{Game}_{reli}]$$

is negligible.

For SSE schemes in which $C^* = C(w)$ is assumed to be returned as a search result, strong reliability was also defined in [26]. In strong reliability, the server has to answer a wrong pair $(\tilde{C}^*, \widetilde{\mathsf{Proof}})(\neq (C(w), \mathsf{Proof}))$ that will be accepted in the search phase to win the game.

(Store phase)
1. $\mathbf{B}_1$ chooses $(\mathcal{D}, \mathcal{W})$ and sends them to $\mathbf{C}$.
2. $\mathbf{C}$ generates $(K, \mathcal{I}, C) \leftarrow \mathtt{Setup}(1^\lambda, \mathcal{D}, \mathcal{W}, \{(w, \mathcal{D}(w)) \mid w \in \mathcal{W}\})$, and sends $(\mathcal{I}, C)$ to $\mathbf{B}_2$.

(Search phase) For $i = 1, \ldots, q$, do
1. $\mathbf{B}_1$ chooses $w_i \in \{0,1\}^*$ and sends it to $\mathbf{C}$.
2. $\mathbf{C}$ sends the trapdoor $t(w_i) \leftarrow \mathtt{Trpdr}(K, w_i)$ to $\mathbf{B}_2$.
3. $\mathbf{B}_2$ returns $(\tilde{C}_i^*, \widetilde{\mathsf{Proof}_i})$ to $\mathbf{C}$.
4. $\mathbf{C}$ computes

$$\tilde{\mathcal{D}}_i^* \leftarrow \mathtt{Dec}(K, t(w_i), \tilde{C}_i^*, \widetilde{\mathsf{Proof}_i})$$

and returns $\tilde{\mathcal{D}}_i^*$ to $\mathbf{B}_1$. $\tilde{\mathcal{D}}_i^*$ can be $\perp$.

Fig. 3 $\mathbf{Game}_{reli}$.

Definition 3 (Strong Reliability): We say that $\mathbf{B}$ strongly wins in $\mathbf{Game}_{reli}$ if there exists i, such that both $\mathtt{Dec}(K, t(w_i), \tilde{C}_i^*, \widetilde{\mathsf{Proof}_i}) \neq \perp$ and $(\tilde{C}_i^*, \widetilde{\mathsf{Proof}_i}) \neq (C(w_i), \mathsf{Proof}_i)$ hold. We say that a vSSE scheme satisfies strong reliability if for any PPT adversary $\mathbf{B}$,

$$\Pr[\mathbf{B} \text{ strongly wins in } \mathbf{Game}_{reli}]$$

is negligible.

3. Building Blocks

3.1 Cuckoo Hashing

Cuckoo Hashing [33] is a hashing algorithm with the advantage that the search time is constant. To store n keys, it uses two tables T_1 and T_2 of size m, and two independent random hash functions h_1 and h_2 with the range $\{1, \ldots, m\}$. Every key x is stored at one of two positions, $T_1(h_1(x))$ or $T_2(h_2(x))$. So we need to inspect at most two positions to search x.

It can happen that both possible places $T_1(h_1(x))$ and $T_2(h_2(x))$ of a given key x are already occupied. This problem is solved by allowing x to throw out the key (say y) occupying the position $T_1(h_1(x))$. Next, we insert y at its alternative position $T_2(h_2(y))$. If it is already occupied, we repeat the above steps until we find an empty position. If we failed after some number of trials, we choose new hash functions and rebuild the data structure.

Let $n = m(1-\epsilon)$ for some $\epsilon \in (0,1)$. Then the above algorithm succeeds with probability $1 - c(\epsilon)/m + O(1/m^2)$ for some explicit function $c(\cdot)$ [28]. The expected construction time of (T_1, T_2) is bounded above by [28]

$$2n\frac{1-e^{\epsilon-1}}{(1-e^{\epsilon-1})+\epsilon}. \tag{3}$$

3.2 Pseudo-Random Function

Let $\mathcal{R}$ be a family of all functions $f : \{0,1\}^* \to \{0,1\}^n$. We say that $F : \{0,1\}^\ell \times \{0,1\}^* \to \{0,1\}^n$ is a pseudo-random function if for any PPT distinguisher $\mathbf{D}$,

$$\left|\Pr[k \xleftarrow{\$} \{0,1\}^\ell : \mathbf{D}^{F(k,\cdot)} = 1] - \Pr[f \xleftarrow{\$} \mathcal{R} : \mathbf{D}^{f(\cdot)} = 1]\right|$$

is negligibly small.

It is well known that a pseudo-random function works as a MAC which is existentially unforgeable against chosen message attack.

4. Generic Transformation from SSE to vSSE

In this section, we show a generic method to transform any SSE which satisfies privacy to a no-dictionary verifiable SSE. In the transformed scheme, the encrypted index table is only a few times larger than that of the underlying SSE scheme, and the server takes only $O(1)$ time to prove that $w \notin \mathcal{W}$. The search time for $w \in \mathcal{W}$ remains almost the same as that of the original SSE scheme. We also prove that the transformed scheme is UC-secure in Appendix similarly to [24], [26].

4.1 Construction

Let $\mathtt{SSE}_0 = (\mathtt{Setup}_0, \mathtt{Trpdr}_0, \mathtt{Search}_0, \mathtt{Dec}_0)$ be an SSE scheme. We construct a no-dictionary verifiable SSE $\mathtt{vSSE}_1 = (\mathtt{Setup}_1, \mathtt{Trpdr}_1, \mathtt{Search}_1, \mathtt{Dec}_1)$ as follows. Let F be a pseudo-random function.

- $\mathtt{Setup}_1(1^\lambda, \mathcal{D}, \mathcal{W}, \{(w, \mathcal{D}(w)) \mid w \in \mathcal{W}\})$: Let $\mathcal{W} = \{w_1, w_2, \ldots, w_{|\mathcal{W}|}\}$.
  1. Run $\mathtt{Setup}_0(1^\lambda, \mathcal{D}, \mathcal{W}, \{(w, \mathcal{D}(w)) \mid w \in \mathcal{W}\})$ to obtain $(K_0, \mathcal{I}_0, C)$. Note that $C_i \in C$ is a ciphertext of each file $D_i \in \mathcal{D}$.
  2. Randomly choose a key k of F. We write $F_k(x)$ instead of $F(k, x)$.
  3. Compute $key_j \leftarrow F_k(0\|w_j)$ for all $w_j \in \mathcal{W}$.
  4. Construct cuckoo hash tables (T_1', T_2') of size $|\mathcal{W}|+1$ which store $\{key_j\}_{j=1}^{|\mathcal{W}|}$. Let (h_1, h_2) be the hash functions which are used to construct (T_1', T_2'). This means that
  $$T_1'(h_1(key_j)) = key_j \text{ or } T_2'(h_2(key_j)) = key_j$$
  for each key_j. When failing in constructing tables, go back to step 2.
  5. Construct two tables (T_1, T_2) of size $|\mathcal{W}| + 1$ as follows:
  For $a = 1, 2$ and $i = 1, \ldots, |\mathcal{W}|+1$, if $T_a'(i) = key_j$ for some $key_j = F_k(0\|w_j)$, then
  $$T_a(i) \leftarrow \langle key_j, F_k(a\|i\|key_j), F_k(3\|key_j\|C(w_j))\rangle.$$
  Otherwise
  $$T_a(i) \leftarrow \langle null, F_k(a\|i\|null), null\rangle.$$
  6. Output $(K = (K_0, k), \mathcal{I} = (\mathcal{I}_0, T_1, T_2, h_1, h_2), C)$.

The client sends $(\mathcal{I}, C)$ to the server, and keeps K secret.

For each $key_j = F_k(0\|w_j)$, it holds that

$$T_1(h_1(key_j)) = \langle key_j, F_k(1\|h_1(key_j)\|key_j), F_k(3\|key_j\|C(w_j))\rangle$$

or

$$T_2(h_2(key_j)) = \langle key_j, F_k(2\|h_2(key_j)\|key_j), F_k(3\|key_j\|C(w_j))\rangle.$$

- $\mathtt{Trpdr}_1((K_0, k), w)$: Compute $key \leftarrow F_k(0\|w)$ and $t_0(w) \leftarrow \mathtt{Trpdr}_0(K_0, w)$. Output $t(w) = (key, t_0(w))$.

The client sends $t(w)$ to the server, where w is a search word.

- $\mathtt{Search}_1((\mathcal{I}_0, T_1, T_2, h_1, h_2), C, t(w) = (key, token))$: Retrieve

$$\langle \alpha_1, \beta_1, \gamma_1\rangle \leftarrow T_1(h_1(key)),$$
$$\langle \alpha_2, \beta_2, \gamma_2\rangle \leftarrow T_2(h_2(key)).$$

Let

$$C^* \leftarrow \begin{cases} \mathtt{Search}_0(\mathcal{I}_0, C, token) & \text{if } key \in \{\alpha_1, \alpha_2\} \\ \emptyset & \text{otherwise} \end{cases}$$

$$\mathsf{Proof} \leftarrow \begin{cases} \gamma_1 & \text{if } key = \alpha_1 \\ \gamma_2 & \text{if } key = \alpha_2 \\ (\alpha_1, \beta_1, \alpha_2, \beta_2) & \text{otherwise} \end{cases}$$

Output (C^*, Proof).

The server returns (C^*, Proof) to the client.

- $\mathtt{Dec}_1((K_0, k), t(w) = (key, token), C^*, \mathsf{Proof})$:
  (Case 1) $\mathsf{Proof} = \gamma$.
  If $\gamma \neq F_k(3\|key\|C^*)$, then output $\perp$.
  (Case 2) $\mathsf{Proof} = (\alpha_1, \beta_1, \alpha_2, \beta_2)$.
  If $C^* \neq \emptyset$ or $key \in \{\alpha_1, \alpha_2\}$ or $\beta_1 \neq F_k(1\|h_1(key)\|\alpha_1)$ or $\beta_2 \neq F_k(2\|h_2(key)\|\alpha_2)$, then output $\perp$.
  Otherwise, compute $\mathcal{D}^* \leftarrow \mathtt{Dec}_0(K_0, token, C^*)$ and output $\mathcal{D}^*$.

The client obtains $\perp$ or $\mathcal{D}^*$.

4.2 Example

Suppose that there are 7 keywords $\mathcal{W} = \{w_1, \ldots, w_7\}$ and 8 ciphertexts $C = \{C_1, \ldots, C_8\}$ such that $C(w_j)$ are given in Table 1. In the same table, $h_1(key_j)$ and $h_2(key_j)$ are the hash values which are used to construct the cuckoo hash tables (T_1', T_2') for the set $\{key_j = F_k(0\|w_j) \mid j = 1, \ldots, 7\}$. Then T_1 and T_2 are constructed as shown in Table 2. Note that the size of each table is $8 = |\mathcal{W}| + 1$.

(Case 1) Suppose that a client searches for a keyword $w_3 \in \mathcal{W}$.

1. The client sends trapdoor $(key_3, t_0(w_3))$ to the server.
2. Since $h_1(key_3) = 6$ and $h_2(key_3) = 4$, the server retrieves

$$\langle \alpha_1, \beta_1, \gamma_1\rangle = T_1(6) = \langle key_3, F_k(1\|6\|key_3), F_k(3\|key_3\|C_1, C_4)\rangle,$$
$$\langle \alpha_2, \beta_2, \gamma_2\rangle = T_2(4) = \langle key_2, F_k(2\|4\|key_2), F_k(3\|key_2\|C_2)\rangle$$

from T_1 and T_2.
Because $\alpha_1 = key_3$, the server obtains the search result

$$C^* = (C_1, C_4) \leftarrow \mathtt{Search}_0(\mathcal{I}_0, C, t_0(w_3)),$$
$$\mathsf{Proof} = \gamma_1 = F_k(3\|key_3\|C_1, C_4),$$

and returns (C^*, Proof) to the client.
3. The client verifies if $\gamma_1 = F_k(3\|key_3\|C^*)$.

(Case 2) Suppose that the client searches for $w \notin \mathcal{W}$.

1. The client computes $key \leftarrow F_k(0\|w)$ and $t_0(w) \leftarrow \mathtt{Trpdr}_0(K_0, w)$. He sends $t(w) = (key, t_0(w))$ to the server.
2. Suppose that $h_1(key) = 5$ and $h_2(key) = 3$. Then the server retrieves

$$\langle \alpha_1, \beta_1, \gamma_1\rangle = T_1(5) = \langle null, F_k(1\|5), null\rangle,$$
$$\langle \alpha_2, \beta_2, \gamma_2\rangle = T_2(3) = \langle key_4, F_k(2\|3\|key_4), F_k(3\|key_4\|C_1, C_3, C_7)\rangle.$$

Because $key \notin \{\alpha_1, \alpha_2\}$, the server returns $C^* = \emptyset$ and $\mathsf{Proof} = (\alpha_1, \beta_1, \alpha_2, \beta_2) = (null, F_k(1\|5), key_4, F_k(2\|3\|key_4))$.

Table 1 Example.

keyword w_j	$C(w_j)$	$h_1(key_j)$	$h_2(key_j)$
w_1	C_1, C_4, C_5, C_8	6	1
w_2	C_2	2	4
w_3	C_1, C_4	6	4
w_4	C_1, C_3, C_7	6	3
w_5	C_2, C_6	7	8
w_6	C_5, C_8	7	6
w_7	C_1	2	8

Table 2 Cuckoo hash tables (T_1, T_2).

i	$T_1(i)$
1	$\langle$ null , $F_k(1\|1)$, null $\rangle$
2	$\langle key_7,\ F_k(1\|2\|key_7),\ F_k(3\|key_7\|C_1)\rangle$
3	$\langle$ null , $F_k(1\|3)$, null $\rangle$
4	$\langle$ null , $F_k(1\|4)$, null $\rangle$
5	$\langle$ null , $F_k(1\|5)$, null $\rangle$
6	$\langle key_3,\ F_k(1\|6\|key_3),\ F_k(3\|key_3\|C_1, C_4)\rangle$
7	$\langle key_6,\ F_k(1\|7\|key_6),\ F_k(3\|key_6\|C_5, C_8)\rangle$
8	$\langle$ null , $F_k(1\|8)$, null $\rangle$

i	$T_2(i)$
1	$\langle key_1,\ F_k(2\|1\|key_1),\ F_k(3\|key_1\|C_1, C_4, C_5, C_8)\rangle$
2	$\langle$ null , $F_k(2\|2)$, null $\rangle$
3	$\langle key_4,\ F_k(2\|3\|key_4),\ F_k(3\|key_4\|C_1, C_3, C_7)\rangle$
4	$\langle key_2,\ F_k(2\|4\|key_2),\ F_k(3\|key_2\|C_2)\rangle$
5	$\langle$ null , $F_k(2\|5)$, null $\rangle$
6	$\langle$ null , $F_k(2\|6)$, null $\rangle$
7	$\langle$ null , $F_k(2\|7)$, null $\rangle$
8	$\langle key_5,\ F_k(2\|8\|key_5),\ F_k(3\|key_5\|(C_2, C_6))\rangle$

3. The client verifies if $key \notin \{\alpha_1, \alpha_2\}$, $\beta_1 = F_k(1\|h_1(key)\|\alpha_1)$, and $\beta_2 = F_k(2\|h_2(key)\|\alpha_2)$.

4.3 Efficiency

The efficiency of our transformed scheme $\mathtt{vSSE}_1$ is estimated as follows:

- In the store phase, $|\mathcal{W}|$ keys are stored in two tables, where each table has size $m = |\mathcal{W}| + 1$. Therefore, the client takes the expected time $O(|\mathcal{W}|) + time(\mathtt{Setup}_0)$ to run $\mathtt{Setup}_1$ from Eq. (3).
- In the search phase, the search time for $w \in \mathcal{W}$ is almost the same as that of the original scheme.
- The server takes only $O(1)$ time to prove that $w \notin \mathcal{W}$ because the search time is constant in cuckoo hashing.

To prove that $w \notin \mathcal{W}$, in the method of [35], the server takes $O(N \log N|\mathcal{W}|)$ time. In the concrete method (Algorithm 1+2) in [6], it takes $O(\log|\mathcal{W}|) + time(\mathtt{Search}_0)$.

4.4 Security

Theorem 1: If the underlying scheme $\mathtt{SSE}_0$ has $L = (L_1, L_2)$-privacy and F is a pseudorandom function, then our scheme $\mathtt{vSSE}_1$ has $L' = (L'_1, L'_2)$-privacy such that

$$L'_1(\mathcal{D}, \mathcal{W}) = L_1(\mathcal{D}, \mathcal{W}) \cup \{|\mathcal{W}|\},$$
$$L'_2(\mathcal{D}, \mathcal{W}, \mathbf{w}, w_i) = L_2(\mathcal{D}, \mathcal{W}, \mathbf{w}, w_i) \cup \{\mathtt{SPattern}(\mathbf{w}, w_i), [w_i \in \mathcal{W}]\}. \quad (4)$$

In the all existing SSE schemes, $|\mathcal{W}| \in L_1(\mathcal{D}, \mathcal{W})$ and $\{\mathtt{SPattern}(\mathbf{w}, w_i), [w_i \in \mathcal{W}]\} \subseteq L_2(\mathcal{D}, \mathcal{W}, \mathbf{w}, w_i)$. (There may be some exceptions which use oblivious RAM. But such SSE schemes are inefficient.) So, the client's privacy in our vSSE scheme has the same level as that of the underlying SSE scheme.

(Proof) Let $\mathbf{S}_0$ be a simulator of the underlining SSE scheme which has (L_1, L_2)-privacy. We construct a simulator $\mathbf{S}$ of our vSSE scheme which achieves (L'_1, L'_2)-privacy as follows.

(Store phase) In $\mathbf{Game}_{sim}$, $\mathbf{S}$ takes $L'_1(\mathcal{D}, \mathcal{W}) = L_1(\mathcal{D}, \mathcal{W}) \cup \{|\mathcal{W}|\}$ as an input. $\mathbf{S}$ runs $\mathbf{S}_0(L_1(\mathcal{D}, \mathcal{W}))$ and gets its output $(\mathcal{I}_0, C)$. Next $\mathbf{S}$ constructs T_1 and T_2 as follows. Note that the size of each T_1, T_2 is $m = |\mathcal{W}| + 1$.

- Choose $key'_1, \ldots, key'_{|\mathcal{W}|}$ randomly, where key'_i is the simulated value of $key_j = F_K(0\|w_j)$ such that $\{key'_1, \ldots, key'_{|\mathcal{W}|}\} = \{key_1, \ldots, key_{|\mathcal{W}|}\}$.
- Construct the cuckoo hash tables (T'_1, T'_2) which store $(key'_{\pi(1)}, \ldots, key'_{\pi(|\mathcal{W}|)})$, where π is a random permutation. Let h_1, h_2 be the two hash functions which are used to construct (T'_1, T'_2).
- For $a = 1, 2$ and $i = 1, \ldots, |\mathcal{W}| + 1$, if $T'_a(i) = key'_j$ for some j, then choose two random strings r and r', and $T_a(i) \leftarrow \langle key'_j, r, r'\rangle$. Otherwise, choose a random string r and $T_a(i) \leftarrow \langle null, r, null\rangle$.

$\mathbf{S}$ sends $(\mathcal{I}_0, T_1, T_2, h_1, h_2)$ and C to the challenger. Let $cntr \leftarrow 1$, where $cntr$ will denote the number of distinct keywords which the client has queried.

(Search phase) In the ith search phase, $\mathbf{S}$ takes $L'_2(\mathcal{D}, \mathcal{W}, \mathbf{w}, w^*) = L_2(\mathcal{D}, \mathcal{W}, \mathbf{w}, w^*) \cup \{\mathtt{SPattern}(\mathbf{w}, w^*), [w^* \in \mathcal{W}]\}$ as an input. $\mathbf{S}$ first obtains $t_0(w^*)$ by running $\mathbf{S}_0(L_2(\mathcal{D}, \mathcal{W}, \mathbf{w}, w^*))$, and sets

$$key^*_i \leftarrow \begin{cases} key'_{cntr} & \text{if } sp_j = 0 \text{ for all } j \text{ and } w^* \in \mathcal{W}, \\ key^*_j & \text{if } sp_j = 1 \text{ for some } j, \\ \text{random} & \text{otherwise.} \end{cases}$$

$$cntr \leftarrow \begin{cases} cntr + 1 & \text{if } sp_j = 0 \text{ for all } j \text{ and } w^* \in \mathcal{W}, \\ cntr & \text{otherwise.} \end{cases}$$

$\mathbf{S}$ outputs $(key^*_i, t_0(w^*))$ as a simulated trapdoor.

We will prove that there is no adversary $\mathbf{A}$ who can efficiently distinguish between $\mathbf{Game}_{real}$ and $\mathbf{Game}_{sim}$. We consider a game sequence $(\mathbf{Game}_{real}, \mathbf{Game}_{mid}, \mathbf{Game}_{sim})$. $\mathbf{Game}_{mid}$ is the same as $\mathbf{Game}_{real}$ except that all values of $F_k(\cdot)$ are replaced with random strings. For $i \in \{real, mid, sim\}$, define

$$P_i = \Pr[\ \mathbf{A} \text{ outputs } b = 1 \text{ in } \mathbf{Game}_i].$$

Then $|P_{real} - P_{mid}|$ is negligible because F is a pseudorandom function. We can also see that $|P_{mid} - P_{sim}|$ is negligible from the (L_1, L_2)-privacy of the underlying SSE scheme. Consequently, $|P_{real} - P_{sim}|$ is negligible. □

Theorem 2: Our vSSE scheme $\mathtt{vSSE}_1$ satisfies strong reliability if F is a pseudorandom function.

(Proof) We look at the pseudorandom function F as a MAC.

Suppose that there exists an adversary $\mathbf{B} = (\mathbf{B}_1, \mathbf{B}_2)$ who can break the strong reliability of our vSSE scheme, and $\mathbf{B}$ runs the search phase q times. Let $(\tilde{C}^*_i, \widetilde{\mathsf{Proof}}_i)$ be $\mathbf{B}_2$'s response to $t(w_i) = (key_i, t_0(w_i))$ in the ith search phase, and let

$$(C(w_i), \mathsf{Proof}_i) = \mathtt{Search}_1(\mathcal{I}, C, t(w_i)).$$

From the definition, $\mathbf{B}$ strongly wins if there exists $i \in \{1, \ldots, q\}$ such that

$$(\tilde{C}^*_i, \widetilde{\mathsf{Proof}}_i) \neq (C(w_i), \mathsf{Proof}_i) \quad \text{and}$$
$$\mathtt{Dec}_1(K, (key_i, t_0(w_i)), \tilde{C}^*_i, \widetilde{\mathsf{Proof}}_i) \neq \perp. \quad (5)$$

By using $\mathbf{B}$, we will construct a forger $\mathbf{F}$ against the MAC, where $\mathbf{F}$ has oracle access to F_k.

First, $\mathbf{F}$ randomly chooses $J \in \{1, \ldots, q\}$. Then, $\mathbf{F}$ runs $\mathbf{B}$ by playing the role of the challenger $\mathbf{C}$ (see Fig. 3) until the $(J-1)$th search phase. During this simulation, when $\mathbf{C}$ needs to compute $F_k(x)$ for some x, $\mathbf{F}$ queries x to its oracle F_k.

In the Jth search phase, there are three cases:

(1) $\widetilde{\mathsf{Proof}}_J = \tilde{\gamma}$.

In this case, $\mathbf{F}$ outputs $m' = (3\|key_J\|\tilde{C}^*_J)$ and $tag' = \tilde{\gamma}$

as a forgery of the MAC F.

(2) $\mathsf{Proof}_J = \gamma$ and $\widetilde{\mathsf{Proof}}_J = (\tilde{\alpha}_1, \tilde{\beta}_1, \tilde{\alpha}_2, \tilde{\beta}_2)$.
Since $\mathsf{Proof}_J = \gamma$, there exists $a \in \{1, 2\}$ such that $T_a(h_a(key_J)) = \langle key_J, F_k(a\|h_a(key_J)\|key_J), \ldots\rangle$. For this a, $\mathbf{F}$ outputs $m' = (a\|h_a(key_J)\|\tilde{\alpha}_a)$ and $tag' = \tilde{\beta}_a$ as a forgery.

(3) $\mathsf{Proof}_J = (\alpha_1, \beta_1, \alpha_2, \beta_2)$ and $\widetilde{\mathsf{Proof}}_J = (\tilde{\alpha}_1, \tilde{\beta}_1, \tilde{\alpha}_2, \tilde{\beta}_2)$.
If there exists $a \in \{1, 2\}$ s.t. $(\alpha_a, \beta_a) \neq (\tilde{\alpha}_a, \tilde{\beta}_a)$, then, $\mathbf{F}$ outputs $m' = (a\|h_a(key_J)\|\tilde{\alpha}_a)$ and $tag' = \tilde{\beta}_a$ as a forgery. Otherwise $\mathbf{F}$ outputs "fail."

Now $\mathbf{F}$ succeeds in forgery if $\mathbf{B}$ strongly wins and $\mathbf{F}$ correctly predicts i which satisfies Eq. (5), i.e., Eq. (5) holds in $i = J$. Since $\mathbf{F}$ predicts J correctly with probability $1/q$, we obtain that

$$\Pr[\mathbf{F} \text{ succeeds in forgery}] \geq \Pr[\mathbf{B} \text{ strongly wins in } \mathbf{Game}_{reli}] \times \frac{1}{q}.$$

□

We prove the UC-security of $\mathtt{vSSE}_1$ in Appendix.

5. Search-Pattern Hiding

As mentioned before, the existing no-dictionary SSE schemes leak search pattern. Namely, they have (L_1, L_2)-privacy (Def. 1) such that L_2 includes search pattern.

In this section, we show a no-dictionary search-pattern hiding SSE scheme such that the encrypted index table is only a few times larger than $\mathcal{I}_0$ which is defined in Sect. 1.2.

We consider a model such that the search phase consists of two subprotocols. In the first subprotocol, the client obtains

$$\mathcal{ID}(w) = \{i \mid D_i \text{ contains } w \text{ as a keyword}\}$$

for the search word w. In the second subprotocol, he obtains

$$C(w) = \{C_i \mid i \in \mathcal{ID}(w)\}.$$

We focus on the first subprotocol, in which the search pattern should be hidden. The definition of privacy is the same as Def. 1.

If we use PIR in the second subprotocol in addition, we can hide even the access pattern.

5.1 PIR

PIR is a two party protocol between a sender and a receiver such as follows. The sender has a database $\mathcal{M} = (m_1, \ldots, m_N)$. The receiver wants to obtain m_{idx} without revealing the index idx. A trivial solution is that the sender sends the entire $\mathcal{M}$ to the receiver. In PIR, this must be realized with less amount of communication. There exists a PIR scheme such that the communication overhead is $O((\log N)^2)$ [29], [32].

A PIR scheme consists of four algorithms $(\mathtt{Gen}_{PIR}, \mathtt{Query}_{PIR}, \mathtt{Ans}_{PIR}, \mathtt{Dec}_{PIR})$, where the first two are PPT algorithms and the last two are PT algorithms.

- $(pk, sk) \leftarrow \mathtt{Gen}_{PIR}(1^\lambda)$: The receiver runs this algorithm, and sends pk to the sender. He keeps sk secret.
- $Q^{idx} \leftarrow \mathtt{Query}_{PIR}(sk, idx)$: The receiver runs this algorithm when he wants to obtain m_{idx}, and sends Q^{idx} to the sender.
- $rsp \leftarrow \mathtt{Ans}_{PIR}(pk, \mathcal{M}, Q^{idx})$: The sender runs this algorithm, and sends rsp back to the receiver.
- $res \leftarrow \mathtt{Dec}_{PIR}(sk, rsp)$: The receiver runs this algorithm, and obtains $res = m_{idx}$.

The sender should learn no information on idx from (pk, Q^{idx}).

More formally, a PIR scheme has to satisfy the following property; For any idx and idx', (pk, Q^{idx}) and $(pk, Q^{idx'})$ are computationally indistinguishable.

5.2 No-Dictionary Search-Pattern Hiding

We show our no-dictionary SSE scheme, $\mathtt{SSE}_2$, which can hide even the search pattern. For each $w_j \in \mathcal{W}$, let $\mathcal{ID}(w_j) = \{id_1, \ldots, id_{k_j}\}$.

$\mathtt{SSE}_2 = (\mathtt{Setup}_2, \mathtt{Trpdr}_2, \mathtt{Search}_2, \mathtt{Dec}_2)$

- $\mathtt{Setup}_2$:

1. Generate two PIR key pairs $(sk_1, pk_1), (sk_2, pk_2)$.
2. Choose a key K' of a symmetric encryption scheme $(\mathtt{Enc}, \mathtt{Dec})$ randomly.
3. For each $D_i \in \mathcal{D}$, compute $C_i \leftarrow \mathtt{Enc}_{K'}(D_i)$ and set $C = (C_1, \ldots, C_N)$.
4. Compute $\mathcal{ID}'(w_j) \leftarrow \mathtt{Enc}_{K'}(id_1\| \cdots \|id_{k_j}\|00 \cdots 00)$ for all $w_j \in \mathcal{W}$, where 0s are padded so that $|\mathcal{ID}'(w_1)| = |\mathcal{ID}'(w_2)| = \cdots = |\mathcal{ID}'(w_{|\mathcal{W}|})|$.
5. Choose a key k of pseudo-random function F randomly, and compute $key_j \leftarrow F_k(w_j)$ for all $w_j \in \mathcal{W}$.
6. Construct cuckoo hash tables (T_1, T_2) that stores $\langle key_j, \mathcal{ID}'(w_j)\rangle$. Note that
$$T_1(h_1(key_j)) = \langle key_j, \mathcal{ID}'(w_j)\rangle$$
or
$$T_2(h_2(key_j)) = \langle key_j, \mathcal{ID}'(w_j)\rangle$$
holds.
7. Output $((K', sk_1, sk_2, k), (T_1, T_2, pk_1, pk_2), C)$.

The client sends (T_1, T_2, pk_1, pk_2) and C to the server, and keeps (K', sk_1, sk_2, k) secret.

- $\mathtt{Trpdr}_2$:

1. Compute $key \leftarrow F_k(w)$.
2. Compute $Q_b \leftarrow \mathtt{Query}_{PIR}(sk_b, h_b(key))$ for $b = 1, 2$.
3. Output $t(w) = (Q_1, Q_2)$

The client sends $t(w) = (Q_1, Q_2)$ to the server, where w is a search word.

- $\mathtt{Search}_2$:

1. Compute $rsp_b \leftarrow \mathtt{Ans}_{PIR}(pk_b, T_b, Q_b)$ for $b = 1, 2$.
2. Output (rsp_1, rsp_2).

The server returns (rsp_1, rsp_2) to the client.

- $\mathtt{Dec}_2$:

1. Compute $res_b \leftarrow \mathtt{Dec}_{PIR}(sk_b, rsp_b)$ for $b = 1, 2$.
2. If $res_1 = \langle F_k(w), \mathcal{ID}'_1 \rangle$, then decrypt $\mathcal{ID}'_1$ and obtain $\mathcal{ID}(w)$.
3. If $res_2 = \langle F_k(w), \mathcal{ID}'_2 \rangle$, then decrypt $\mathcal{ID}'_2$ and obtain $\mathcal{ID}(w)$.
4. Otherwise output $\mathcal{ID}(w) = \emptyset$, which means that "$w \notin \mathcal{W}$."

The client obtains $\mathcal{ID}(w)$ even if $w \notin \mathcal{W}$.

If $w = w_j$, the trapdoor $t(w) = (Q_1, Q_2)$ is a pair of queries to retrieve $T_1(h_1(key_j))$ and $T_2(h_2(key_j))$. Therefore, either of res_1 and res_2 is equal to $\langle key_j, \mathcal{ID}'(w_j) \rangle$ from the property of cuckoo hashing and PIR.

We can use arbitrary encoding methods to represent $\mathcal{ID}(w)$. For example, $\mathcal{ID}(w) = \{2, 4, 5\}$ can be encrypted as $\mathcal{ID}'(w) = \mathtt{Enc}_{K'}(010110\cdots)$. In this case, padding is unnecessary because the length of plaintext is constant. This encoding is more efficient when hit rate is relatively large.

The following theorem shows that $\mathtt{vSSE}_2$ does not leak the search pattern.

Theorem 3: Define

$$L''_1(\mathcal{D}, \mathcal{W}) = (|\mathcal{W}|, |D_1|, \ldots, |D_N|, L_{max}),$$
$$L''_2(\mathcal{D}, \mathcal{W}, \mathbf{w}, w_i) = (),$$

where

$$L_{max} = \max_{w_i \in \mathcal{W}} |\mathcal{ID}(w_i)|.$$

If

- $(\mathtt{Gen}_{PIR}, \mathtt{Query}_{PIR}, \mathtt{Ans}_{PIR}, \mathtt{Dec}_{PIR})$ is a secure PIR scheme,
- F is a pseudorandom function, and
- $(\mathtt{Enc}, \mathtt{Dec})$ is an IND-CPA secure symmetric encryption scheme,

then our scheme $\mathtt{SSE}_2$ has $L = (L''_1, L''_2)$-privacy.

(Proof) We construct a simulator $\mathbf{S}_2$ which achieves (L''_1, L''_2)-privacy as follows.

(Store phase)

On input $L''_1(\mathcal{D}, \mathcal{W}) = (|\mathcal{W}|, |D_1|, \ldots, |D_N|, L_{max})$, $\mathbf{S}_2$ computes $(T'_1, T'_2, pk'_1, pk'_2)$ and C' as follows.

1. As in $\mathtt{Setup}_2$, generate two PIR key pairs (sk'_1, pk'_1), (sk'_2, pk'_2), and choose K'.
2. For each $i \in \{1, \ldots, N\}$, compute $C'_i \leftarrow \mathtt{Enc}_{K'}(0^{|D_i|})$ and set $C' = (C'_1, \ldots, C'_N)$.
3. Compute $\mathcal{ID}''_j \leftarrow \mathtt{Enc}_{K'}(0^{L_{max}})$ for all $j \in \{1, \ldots, |\mathcal{W}|\}$.
4. Choose a random string key'_j for all $j \in \{1, \ldots, |\mathcal{W}|\}$ as the simulated value of $F_k(w_j)$.
5. Construct cuckoo hash tables (T'_1, T'_2) that stores $\langle key'_j, \mathcal{ID}''_j \rangle$.

$\mathbf{S}_2$ sends $(T'_1, T'_2, pk'_1, pk'_2)$ and C' as the simulated values of (T_1, T_2, pk_1, pk_2) and C to the challenger.

(Search phase)

$\mathbf{S}_2$ outputs $t'(w) = (Q'_1, Q'_2)$, where

$$Q'_b \leftarrow \mathtt{Query}_{\mathrm{PIR}}(sk_b, 1).$$

We will prove that there is no adversary who can efficiently distinguish between $\mathbf{Game}_{real}$ and $\mathbf{Game}_{sim}$. We consider a game sequence $(\mathbf{Game}_{real}, \mathbf{Game}_1, \mathbf{Game}_2, \mathbf{Game}_{sim})$.

$\mathbf{Game}_1$ is the same as $\mathbf{Game}_{real}$ except that all queries Q_b in search phases are replaced with $Q'_b \leftarrow \mathtt{Query}_{\mathrm{PIR}}(sk_b, 1)$. From the security of PIR, $\mathbf{Game}_{real}$ and $\mathbf{Game}_1$ are indistinguishable.

$\mathbf{Game}_2$ is the same as $\mathbf{Game}_1$ except that all values of $F_k(w_j)$ are replaced with random strings key'_j as in $\mathbf{Game}_{sim}$. From the pseudorandomness of F, $\mathbf{Game}_1$ and $\mathbf{Game}_2$ are indistinguishable.

The difference between $\mathbf{Game}_2$ and $\mathbf{Game}_{sim}$ is that

- In $\mathbf{Game}_2$, $C_i = \mathtt{Enc}_{K'}(D_i)$ and $\mathcal{ID}'(w_j) = \mathtt{Enc}_{K'}(\mathcal{ID}(w_j))$, where $\mathcal{ID}(w_j)$ are padded so that $|\mathcal{ID}(w_j)| = L_{max}$.
- In $\mathbf{Game}_{sim}$, $C'_i = \mathtt{Enc}_{K'}(0^{|D_i|})$ and $\mathcal{ID}''(w_j) = \mathtt{Enc}_{K'}(0^{L_{max}})$.

Therefore, $\mathbf{Game}_1$ and $\mathbf{Game}_2$ are indistinguishable from IND-CPA security of $(\mathtt{Enc}, \mathtt{Dec})$.

Consequantly, $|P_{real} - P_{mid}|$ is negligibly small. □

The above theorem shows that $\mathtt{SSE}_2$ leaks no information in the search phase. However, if a user downloads the hit files $C_i \in C(w)$ without using PIR, the server may learn some information about the search result. In such a case, total leakage becomes $L''_2(\mathcal{D}, \mathcal{W}, \mathbf{w}, w) = \mathcal{ID}(w)$.

In general, efficiency must be sacrificed to obtain search-pattern hiding with/without dictionary.

- The search process needs two round-trip communication to complete keyword search process.
- In general, PIR is built by using asymmetric technique. So, the scheme needs high computation/communication cost.

5.3 How to Add Reliability

By using the same idea as in Sect. 4, we can add the reliability to the above scheme. The client generates cuckoo hash tables (T_1, T_2) such that

$$T_1(h_1(key_j)) = \langle key_j, \mathcal{ID}'(w_j), F_k(1 \| h_1(key_j) \| key_j \| \mathcal{ID}'(w_j)) \rangle$$

or

$$T_2(h_2(key_j) = \langle key_j, \mathcal{ID}'(w_j), F_k(2\|h_2(key_j)\|key_j\|\mathcal{ID}'(w_j))\rangle$$

holds, where $key_j = F_k(0\|w_j)$. Then the client checks the validity of the answer from the server in the same way as in Sect. 4.

6. Conclusion

In this paper, we studied two cases in which construction of efficient no-dictionary SSE schemes is not trivial, and showed that the cuckoo hashing technique can be used to solve the problem in both cases.

First, we proposed a generic transformation from any passively secure SSE scheme to a no-dictionary verifiable SSE scheme. The efficiency of the transformed scheme is almost the same as the underlying SSE scheme.

We next presented a no-dictionary search-pattern hiding SSE scheme that has a compact encrypted index table. In addition, we showed that our no-dictionary search-pattern hiding scheme can be modified to a verifiable scheme with small cost.

References

[1] L. Ballard, S. Kamara, and F. Monrose, "Achieving efficient conjunctive keyword searches over encrypted data," 7th International Conference on Information and Communication Security (ICICS 2005), pp.414–426, 2005.
[2] N. Baric and B. Pfitzmann, "Collision-free accumulators and fail-stop signature schemes without trees," EUROCRYPT 1997, LNCS, vol.1233, pp.480–494, 1997.
[3] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A concrete security treatment of symmetric encryption," FOCS 1997, pp.394–403, 1997.
[4] M. Bellare, R. Guerin, and P. Rogaway, "XOR MACs: New methods for message authentication using finite pseudorandom functions," CRYPTO 1995, LNCS, vol.963, pp.15–28, 1995.
[5] S. Bellovin and W. Cheswick, "Privacy-enhanced searches using encrypted bloom filters," Technical Report 2004/022, IACR ePrint Cryptography Archive, https://eprint.iacr.org/2004/022, 2004.
[6] R. Bost, P.-A. Fouque, and D. Pointcheval, "Verifiable dynamic symmetric searchable encryption: Optimality and forward security," Technical Report 2016/62, IACR ePrint Cryptography Archive, https://eprint.iacr.org/2016/062, 2016.
[7] J.W. Byun, D.H. Lee, and J. Lim, "Efficient conjunctive keyword search on encrypted data storage system," EuroPKI, LNCS, vol.4043, pp.184–196, 2006.
[8] J. Camenisch and A. Lysyanskaya, "Dynamic accumulators and application to efficient revocation of anonymous credentials," CRYPTO 2002, LNCS, vol.2442, pp.61–76, 2002.
[9] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," FOCS 2001, pp.136–145, 2001.
[10] R. Canetti, "Universally composable signatures, certification and authentication," Technical Report 2003/239, IACR ePrint Cryptography Archive, https://eprint.iacr.org/2003/239, 2003.
[11] Full version of [9]: Technical Report 2000/067, IACR ePrint Cryptography Archive, https://eprint.iacr.org/2000/067, last revised 16 July 2013.
[12] D. Cash, S. Jarecki, C.S. Jutla, H. Krawczyk, M. Rosu, and M. Steiner, "Highly-scalable searchable symmetric encryption with support for Boolean queries," CRYPTO 2013, Part I, LNCS, vol.8042, pp.353–373, 2013.
[13] D. Cash, J. Jaeger, S. Jarecki, C.S. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, "Dynamic searchable encryption in very-large databases: Data structures and implementation," Symposium on Network and Distributed Systems Security (NDSS 2014), 2014.
[14] D. Cash and S. Tessaro, "The locality of searchable symmetric encryption," EUROCRYPT 2014, LNCS, vol.8441, pp.351–368, 2014.
[15] Y. Chang, M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," Applied Cryptography and Network Security (ACNS 2005), LNCS, vol.3531, pp.442–455, 2005.
[16] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," ACM Conference on Computer and Communications Security 2006, pp.79–88, 2006.
[17] Full version of [16]: Technical Report 2006/210, IACR ePrint Cryptography Archive, https://eprint.iacr.org/2006/210, 2006.
[18] S. Garg, P. Mohassel, and C. Papamanthou, "TWORAM: Efficient oblivious RAM in two rounds with applications to searchable encryption," CRYPTO 2016, Part III, LNCS, vol.9816, pp.563–592, 2016.
[19] E.-J. Goh, "Secure indexes," Technical Report 2003/216, IACR ePrint Cryptography Archive, https://eprint.iacr.org/2003/216, 2003.
[20] P. Golle, J. Staddon, B.R. Waters, "Secure Conjunctive Keyword Search over Encrypted Data," Applied Cryptography and Network Security (ACNS 2004), LNCS, vol.3089, pp.31–45, 2004.
[21] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," Financial Cryptography and Data Security (FC 2013), LNCS, vol.7859, pp.258–274, 2013.
[22] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," ACM Conference on Computer and Communications Security 2012, pp.965–976, 2012.
[23] K. Kurosawa, "Garbled searchable symmetric encryption," Financial Cryptography and Data Security (FC 2014), LNCS, vol.8437, pp.234–251, 2014.
[24] K. Kurosawa and Y. Ohtaki, "UC-secure searchable symmetric encryption," Financial Cryptography and Data Security (FC 2012), LNCS, vol.8437, pp.285–298, 2012.
[25] K. Kurosawa and Y. Ohtaki, "How to update documents verifiably in searchable symmetric encryption," Cryptology and Network Security (CANS 2013), LNCS, vol.8257, pp.309–328, 2013.
[26] The final version of [24]. Technical Report 2015/251, IACR ePrint Cryptography Archive, https://eprint.iacr.org/2015/251, 2015.
[27] K. Kurosawa, K. Sasaki, K. Ohta, and K. Yoneyama, "UC-secure dynamic searchable symmetric encryption scheme," Advances in Information and Computer Security (IWSEC 2016), LNCS, vol.9836, pp.73–90, 2016.
[28] R. Kutzelnigg, "Bipartite random graphs and cuckoo hashing," Fourth Colloquium on Mathematics and Computer Science Algorithms, Trees, Combinatorics and Probabilities, DMTCS Proceedings, pp.403–406, 2006.
[29] H. Lipmaa, "An oblivious transfer protocol with log-squared communication," Information Security (ISC 2005), LNCS, vol.3650, pp.314–328, 2005.
[30] M. Naveed, M. Prabhakaran, and C. Gunter, "Dynamic searchable encryption via blind storage," IEEE Symposium on Security and Privacy 2014, pp.639–654, 2014.
[31] W. Ogata and K. Kurosawa, "Efficient no-dictionary verifiable searchable symmetric encryption," Financial Cryptography and Data Security (FC 2017), LNCS, vol.10322, pp.498–516, 2017.
[32] R. Ostrovsky and W.E. Skeith, III, "A survey of single-database private information retrieval: Techniques and applications," Public Key Cryptography 2007, LNCS, vol.4450, pp.393–411, 2007.
[33] R. Pagh and F.F. Rodler, "Cuckoo hashing," J. Algorithms, vol.51, no.2, pp.122–144, 2004.
[34] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," IEEE Symposium on Security and Privacy 2000, pp.44–55, 2000.
[35] S. Taketani and W. Ogata, "Improvement of UC secure searchable symmetric encryption scheme," The 10th International Workshop on

Security (IWSEC 2015), LNCS, vol.9241, pp.135–152, 2015.
[36] P. Wang, H. Wang, and J. Pieprzyk, "Keyword field-free conjunctive keyword searches on encrypted data and extension for dynamic group," Cryptology and Network Security (CANS 2008), LNCS, vol.5339, pp.178–195, 2008.

Appendix: UC-Security for No-Dictionary vSSE

If a protocol is secure in the universally composable (UC) security framework, its security is maintained even if the protocol is combined with other protocols [9]–[11]. The UC security is defined based on *ideal functionality* $\mathcal{F}$. Kurosawa and Ohtaki introduced an ideal functionality of vSSE [24], [26]. Taketani and Ogata [35] generalized it in order to handle the general leakage functions $L = (L_1, L_2)$ as shown in Fig. A· 1.

In the no-dictionary verifiable SSE setting, the real world is described as follows. We assume a real adversary, $\mathbf{A}^{\mathrm{uc}}$, can control the server arbitrarily, and the client is always honest. For simplicity, we ignore session id.

In the store phase, an environment, $\mathbf{Z}$, chooses $(\mathcal{D}, \mathcal{W})$ and sends them to the client. The client computes $(K, \mathcal{I}, C) \leftarrow \mathtt{Enc}(1^\lambda, K, \mathcal{D}, \mathcal{W}, \{(w, \mathcal{D}(w)) \mid w \in \mathcal{W}\})$, and sends $(\mathcal{I}, C)$ to the server. The client stores $K^\dagger$ and the server stores $(\mathcal{I}, C)$. In the search phase, $\mathbf{Z}$ chooses a word $w \in \{0,1\}^*$ and sends it to the client. The client computes $t(w) \leftarrow \mathtt{Trpdr}(K, w)$ and sends it to the server. The server, who may be controlled by real adversary $\mathbf{A}^{\mathrm{uc}}$, returns $(\tilde{C}^*, \widetilde{\mathsf{Proof}})$ to the client. The client computes $\tilde{\mathcal{D}}(w) \leftarrow \mathtt{Dec}(K, t(w), \tilde{C}^*, \widetilde{\mathsf{Proof}})$ and sends $\tilde{\mathcal{D}}(w)$ to $\mathbf{Z}$. Note that $\tilde{\mathcal{D}}(w)$ can be $\perp$. After repeating several searches, $\mathbf{Z}$ outputs a bit b.

On the other hand, the ideal world is described as follows: In the store phase, $\mathbf{Z}$ sends $(\mathcal{D}, \mathcal{W})$ to the dummy client. The dummy client sends $(\mathbf{store}, \mathcal{D}, \mathcal{W})$ to functionality $\mathcal{F}^L_{vSSE}$ (see Fig. A· 1). In the search phase, $\mathbf{Z}$ sends w to the dummy client. The dummy client sends $(\mathbf{search}, w)$ to $\mathcal{F}^L_{vSSE}$, and receives $\mathcal{D}(w)$ or $\perp$ (according to ideal adversary $\mathbf{S}^{\mathrm{uc}}$'s decision), which is relayed to $\mathbf{Z}$. At last, $\mathbf{Z}$ outputs a bit b

In both worlds, $\mathbf{Z}$ can communicate with $\mathbf{A}^{\mathrm{uc}}$ (in the real world) or $\mathbf{S}^{\mathrm{uc}}$ (in the ideal world) in an arbitrary way.

Store: Upon receiving the input $(\mathbf{store}, sid, D_1, \ldots, D_N, \mathcal{W})$ from the dummy client, verify that this is the first input from the client with $(\mathbf{store}, sid)$.
If it is, then store $\mathcal{D} = \{D_1, \ldots, D_N\}$, and send $L_1(\mathcal{D}, \mathcal{W})$ to $\mathbf{S}^{\mathrm{uc}}$. Otherwise, ignore this input.
Search: Upon receiving $(\mathbf{search}, sid, w)$ from the client, send $L_2(\mathcal{D}, \mathcal{W}, \mathbf{w}, w)$ to $\mathbf{S}^{\mathrm{uc}}$. Note that in a no-dictionary vSSE scheme, the client may send $w \notin \mathcal{W}$. If $\mathbf{S}^{\mathrm{uc}}$ returns `accept`, then send $\mathcal{D}(w)$ to the client. If $\mathbf{S}^{\mathrm{uc}}$ returns `reject`, then send $\perp$ to the client.

Fig. A· 1 Ideal functionality $\mathcal{F}^L_{vSSE}$.

†He may forget $\mathcal{D}, \mathcal{W}, C, \mathcal{I}$.

UC-security of no-dictionary vSSE scheme is defined as follows.

Definition 4 (UC-security with leakage L): We say that a given no-dictionary vSSE scheme has universally composable (UC) security with leakage L against non-adaptive adversaries, if for any PPT real adversary $\mathbf{A}^{\mathrm{uc}}$, there exists a PPT ideal adversary (simulator) $\mathbf{S}^{\mathrm{uc}}$, and for any PPT environment $\mathbf{Z}$,

$$|\Pr[\mathbf{Z} \text{ outputs 1 in the real world}] - \Pr[\mathbf{Z} \text{ outputs 1 in the ideal world}]|$$

is negligible.

We can show the following theorem.

Theorem 4: If a no-dictionary vSSE scheme satisfies L-privacy and strong reliability for some L, it has UC security with leakage L against non-adaptive adversaries.

(Proof) Assume that the scheme satisfies L-privacy and strong reliability.

We consider four games $\mathbf{Game}_0, \ldots, \mathbf{Game}_3$. Let

$$p_i = \Pr[\mathbf{Z} \text{ outputs 1 in } \mathbf{Game}_i]$$

for a fixed $\mathbf{A}^{\mathrm{uc}}$. $\mathbf{Game}_0$ is equivalent to the real world in the definition of UC security. So,

$$p_0 = \Pr[\mathbf{Z} \text{ outputs 1 in the real world}].$$

$\mathbf{Game}_1$ is different from $\mathbf{Game}_0$ in the following points.

- In the store phase, the client records $(\mathcal{D}, \mathcal{W}, \mathcal{I})$ as well as the key K.
- In the search phase, if $\mathbf{A}^{\mathrm{uc}}$ instructs the server to return $(\tilde{C}^*, \widetilde{\mathsf{Proof}})$ such that $(\tilde{C}^*, \widetilde{\mathsf{Proof}}) \neq (C^*, \mathsf{Proof}) \leftarrow \mathtt{Search}(\mathcal{I}, C, t(w))$, then the server returns `reject` to the client. Otherwise the server returns `accept`.
- If the client receives `accept` from the server, he sends $\mathcal{D}(w)$ to $\mathbf{Z}$. Otherwise, he sends $\perp$ to $\mathbf{Z}$.

$\mathbf{Game}_1$ is the same as $\mathbf{Game}_0$ until $\mathbf{A}^{\mathrm{uc}}$ instructs the server to return $(\tilde{C}^*, \widetilde{\mathsf{Proof}})$ such that

$$\mathtt{Dec}(K, t(w), \tilde{C}^*, \widetilde{\mathsf{Proof}}) \neq \perp \quad \text{and} \quad (\tilde{C}^*, \widetilde{\mathsf{Proof}}) \neq (C^*, \mathsf{Proof}).$$

The above condition is the (strongly) winning condition of $\mathbf{B}$ in $\mathbf{Game}_{reli}$. So, we can obtain

$$|p_0 - p_1| \leq \max_{\mathbf{B}} \Pr[\mathbf{B} \text{ strongly wins in } \mathbf{Game}_{reli}].$$

From the assumption, $|p_0 - p_1|$ is negligibly small.

In $\mathbf{Game}_2$, we split the client into two entities, client1 and client2, as follows: (See Fig. A· 2(a).)

- Both client1 and client2 receive all input from $\mathbf{Z}$.
- In the store phase, only client2 sends $(\mathcal{I}, C)$ to the server.
- In the search phase, only client2 sends $t(w)$ to the server. Then, only client1 receives `accept`/`reject` from the

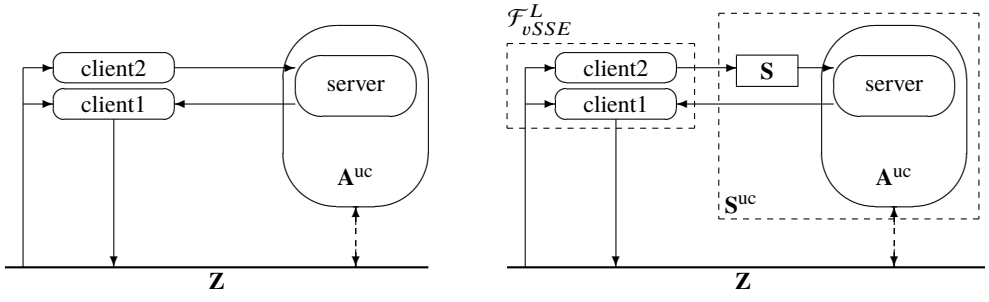


Fig. A · 2 (a) $\mathbf{Game}_2$, (b) $\mathbf{Game}_3$.

server, and sends $\mathcal{D}(w)/\perp$ to $\mathbf{Z}$.

This change is conceptual only. Therefore $p_2 = p_1$.

Now, we look at ($\mathbf{Z}$, client1, server, $\mathbf{A}^{\mathrm{uc}}$) and client2 as an adversary $\mathbf{A}$ and a challenger $\mathbf{C}$ in the real game of privacy, respectively. Then, from the assumption, there exists a simulator $\mathbf{S}$ such that Eq. (2) is negligible.

In $\mathbf{Game}_3$, client2 plays the role of the challenger in the simulation game of privacy; he sends $L_1(\mathcal{D}, \mathcal{W})$ or $L_2(\mathcal{D}, \mathcal{W}, \mathbf{w}, w)$ to the simulator $\mathbf{S}$, and then $\mathbf{S}$ sends its outputs (the simulated message) to the server. (See Fig. A· 2(b).) Again, we look at ($\mathbf{Z}$, client1, server, $\mathbf{A}^{\mathrm{uc}}$) as $\mathbf{A}$. Then $\mathbf{Game}_3$ is the simulation game and $\mathbf{Game}_2$ is the real game. Therefore

$$|p_3 - p_2| \leq |\Pr[\mathbf{A} \text{ outputs 1 in } \mathbf{Game}_{real}] - \Pr[\mathbf{A} \text{ outputs 1 in } \mathbf{Game}_{sim}^{L}]|,$$

and it is negligible from the assumption.

In $\mathbf{Game}_3$, (client1, client2) behaves exactly the same way as $\mathcal{F}_{vSSE}^{L}$ in the ideal world. So, considering ($\mathbf{S}$, server, $\mathbf{A}^{\mathrm{uc}}$) as a simulator $\mathbf{S}^{\mathrm{uc}}$, we obtain

$$p_3 = \Pr[\mathbf{Z} \text{ outputs 1 in the ideal world}]$$

for this simulator. Consequently, we can say that for any $\mathbf{A}^{\mathrm{uc}}$ there exists $\mathbf{S}^{\mathrm{uc}}$ such that $|p_0 - p_3| = |\Pr[\mathbf{Z} \text{ outputs 1 in the real world}] - \Pr[\mathbf{Z} \text{ outputs 1 in the ideal world}]|$ is negligible. □

Corollary 1: If $\mathtt{SSE}_0$ has $L = (L_1, L_2)$-privacy and F is a pseudorandom function, the vSSE scheme $\mathtt{vSSE}_1$ obtained from $\mathtt{SSE}_0$ using the transformation in Sect. 4 is UC-secure with leakage $L' = (L'_1, L'_2)$ where L and L' are given in Theorem 1.

Wakaha Ogata received the B.S., M.E. and D.E. degrees in electrical and electronic engineering in 1989, 1991 and 1994, respectively, from Tokyo Institute of Technology. From 1995 to 2000, she was an Assistant Professor at Himeji Institute of Technology. Since 2000 she has been working for Tokyo Institute of Technology, and now she is a Professor from 2013. Her current interests are cryptography and information security.

Kaoru Kurosawa received the B.E. and Dr. Eng. degrees in electrical engineering in 1976 and 1981, respectively, from Tokyo Institute of Technology. From 1997 to 2001, he was a Professor in Tokyo Institute of Technology. He is currently a Professor in the Department of Computer and Information Sciences at Ibaraki University. His current research interest is cryptography. He was Program Chair for Asiacrypt 2007, PKC 2013 and some other conferences. Dr. Kurosawa is a member of IEEE, ACM, IACR, IEICE. He received the excellent paper award of IEICE in 1981, the young engineer award of IEICE in 1986, Telecom System Scientific Award of Telecommnucations Avdancement Foundation in 2006 and Achievement Award of IEICE in 2007.

Journal of Signal Processing, Vol.22, No.4, pp.165-168, July 2018

SELECTED PAPER AT NCSP'18

Experimental Evaluation of Hybrid PWM/DPAM Dimming Control Method for Digital Color Shift Keying Using RGB-LED Array

Yusuke Matsuda[1], Yusuke Kozawa[2] and Yohtaro Umeda[3]

[1,3] Tokyo University of Science
2641 Yamazaki, Noda, Chiba 278–8510, Japan
E-mail: [3]ytrm_tkb@rs.noda.tus.ac.jp

[2] Ibaraki University
4–12–1 Nakanarusawa, Hitachi, Ibaraki 316–8511, Japan
E-mail: kozawa@ieee.org

Abstract

In this work, we focus on digital color shift keying (DCSK), which is one of the modulation schemes of visible light communication (VLC). DCSK is an extended version of IEEE 802.15.7 color shift keying (CSK) that transmits data through the intensity ratios of red, green, and blue. Digitally controlled LED drivers of DCSK can also reduce the nonlinearity effect caused by the shift of the intensity amplitude. DCSK supports lighting functions such as flicker mitigation, target color control, and dimming control. For the dimming control method of DCSK, two schemes have been considered. One is pulse width modulation (PWM), which changes the duty cycle of optical transmit signals, and the other is digital pulse amplitude modulation (DPAM), which changes the number of red, green, and blue LEDs (RGB-LEDs) being used. In a previous analysis, a hybrid scheme of PWM and DPAM was proposed that could achieve both a wider dimming range than DPAM and a higher spectral efficiency than PWM. Unlike in theoretical analysis, with actual LED drivers, the dimming level (DL) obtained by PWM, DPAM, and hybrid PWM/DPAM may cause errors due to individual differences in the dimming method and LED drive current. In this work, we experimentally evaluate the accuracy of DL and the symbol error rate (SER) of DCSK with PWM, DPAM, and hybrid PWM/DPAM.

1. Introduction

Visible light communication (VLC) is a wireless communication system that provides both communication and lighting functions [1][2]. To apply VLC to an illumination source, a VLC modulation method must consider the effects of the modulated light signal that humans perceive as well as support flicker mitigation, dimming control, color temperature control, a high color rendering index (CRI), and so on. IEEE 802.15 Task Group 7 proposed three VLC modulation methods for flicker mitigation and dimming support: on-off keying (OOK), variable pulse position modulation (VPPM), and color shift keying (CSK) [3][4]. The CSK system is particularly promising because it can increase the data speed by combining the outputs of red, green, and blue in RGB-LED (*i.e.*, trichromatic LED (TLED)). In CSK, M signal points are mapped inside the RGB constellation triangle on the CIE xy chromaticity diagram [5] and are presented by the intensity ratio of red, green, and blue. When the individual intensities of red, green, and blue in a TLED are P_R, P_G, and P_B, respectively, the total intensity is constant (i.e., $P_R + P_G + P_B = const.$) for flicker mitigation. CSK can also utilize the original frequency response of the LED of MHz order, while the frequency response of the blue LED with phosphor is limited to just MHz order due to the phosphor [6][7]. However, CSK systems suffer from LED nonlinearity effects when adjusting to the desired optical intensity due to the change in the current driving with a digital-to-analog converter (DAC). This analog-controlled LED causes nonlinearities of the current to voltage (I-V) characteristics and intensity to current (Φ-I) characteristics of the LED [8]. Moreover, an analog-controlled LED also causes an undesired color shift, which is the peak wavelength shift caused by changing the drive current of the LED. As a solution to these problems, Monteiro and Hranilovic proposed a linear variable current driver including predistortion to linearize the LED output intensity [9]. This variable current driver allows the desired drive current I to flow into an LED linearly due to the open collector nature of an OP AMP. However, these architectures increase the system complexity and they cannot prevent the problem of an undesired color shift. Digital CSK (DCSK) has also been considered as a means of overcoming the drawbacks of CSK [10]-[12]. In DCSK, the desired optical intensity is represented by digitally controlled LEDs in multiple RGB-LEDs (*i.e.*, an RGB-LED array). This can reduce the system complexity and minimize the effect of LED nonlinearity.

In this work, we focus on a dimming control method for DCSK with RGB-LEDs. Generally, two dimming control schemes have been considered for CSK [13]: pulse width modulation (PWM) and pulse amplitude modulation (PAM). PWM dims by changing the duty cycle of optical transmit signals, while PAM generally dims by adjusting the drive current of the LED, which increases the system complexity,

as mentioned earlier. Therefore, for DCSK, digitally controlled PAM (DPAM) is proposed, which dims by changing the number of RGB-LEDs being used in an RGB-LED array. In a previous study, a hybrid scheme of PWM and DPAM was proposed [14] that could achieve both a wider dimming range than DPAM and a higher spectral efficiency than PWM. Unlike in theoretical analysis, with actual LED drivers, the dimming level (DL) obtained by PWM, DPAM, and hybrid PWM/DPAM may cause errors due to individual differences in the dimming method and LED drive current. In this work, we experimentally evaluate the accuracy of DL and the symbol error rate (SER) of DCSK with PWM, DPAM, and hybrid PWM/DPAM.

2. System Setup

2.1 PWM dimming control method

PWM is generally used for the dimming control in VLC. This method dims the light intensity in VLC by changing the pulse width. In a DCSK system, the duty cycle of optical transmission signals is related to the brightness of the lighting. We define the number of dimming stages of PWM, N'_{max}, as

$$N'_{max} = \frac{T_s}{T_c} \tag{1}$$

where T_s is the symbol duration of the original DCSK and T_c is the chip duration for PWM dimming control. Then, the PWM DL, ε_{PWM}, is represented as

$$\varepsilon_{PWM} = \frac{N_{PWM}}{N'_{max}} \times 100\% \quad (N_{PWM} = 1, 2, \cdots, N'_{max}) \tag{2}$$

where N_{PWM} is the PWM signal duration.

DCSK with PWM can represent a wider dimming range by decreasing the chip duration, T_c; however, the spectral efficiency of DCSK with PWM is less than that of the original DCSK.

2.2 DPAM dimming control method

The PAM dimming control method generally dims by adjusting the drive current of LEDs. However, analog current control causes a color shift problem, and we also have to linearize the LED nonlinearity effects.

As a possible solution to these problems, DPAM is considered [14]. DPAM represents the DLs by changing the number of active RGB-LEDs in the RGB-LED array. Therefore, the number of dimming stages is limited by the number of RGB-LEDs in the RGB-LED array. When we define the number of RGB-LEDs for the original DCSK as N_{min} and the number of RGB-LEDs in the RGB-LED array as N_{RGB}, the number of dimming stages of DPAM can be written as

$$N_{max} = \left\lfloor \frac{N_{RGB}}{N_{min}} \right\rfloor \tag{3}$$

where $\lfloor \cdot \rfloor$ is the floor function. Then, the DPAM DL, ε_{DPAM}, is represented as

$$\varepsilon_{DPAM} = \frac{N_{DPAM}}{N_{max}} \times 100\% \quad (N_{DPAM} = 1, 2, \cdots, N_{max}) \tag{4}$$

The spectral efficiency of DCSK with DPAM is the same as that of the original DCSK. However, the number of RGB-LEDs in the RGB-LED array is limited, so the number of dimming stages of DCSK with DPAM is less than that of DCSK with PWM.

2.3 Hybrid PWM/DPAM dimming control method for DCSK

A hybrid PWM/DPAM system was proposed in a previous study [14]. This system combines PWM and DPAM to enable a wider dimming range than DPAM and a higher spectral efficiency than PWM by selecting the optimum combination.

The number of dimming stages of hybrid PWM/DPAM, N, can be written as

$$N = N'_{max} \times N_{max} \tag{5}$$

Then, the DL, ε, is represented as

$$\varepsilon = \frac{N_{PWM}}{N'_{max}} \times \frac{N_{DPAM}}{N_{max}} \times 100\% \tag{6}$$

However, the hybrid PWM/DPAM system cannot actually represent N DLs because they include overlapped patterns such as $(\varepsilon_{DPAM}, \varepsilon_{PWM}) = (100\%, 33\%) = (33\%, 100\%)$, which theoretically result in $\varepsilon = 33\%$.

Figure 1 shows an example of the transmit signal pattern model of a 4-ary DCSK with the hybrid PWM/DPAM dimming control method using nine RGB-LEDs. When $N_{min} = 3$, DPAM can represent three dimming stages. By combining PWM with three dimming stages, the hybrid PWM/DPAM can represent nine dimming stages including overlapped DLs.

2.4 Experimental setup

The experimental setup of DCSK is shown in figure 2. Transmission data is generated from a field-programmable gate array (FPGA : Xilinx virtex-6). We programmed a pseudorandom binary sequence (PRBS) generator, DCSK modulator, and hybrid PWM/DPAM dimming controller into the FPGA. The generated DCSK signal is applied to an LED driver, and the signal data are converted into an optical signal

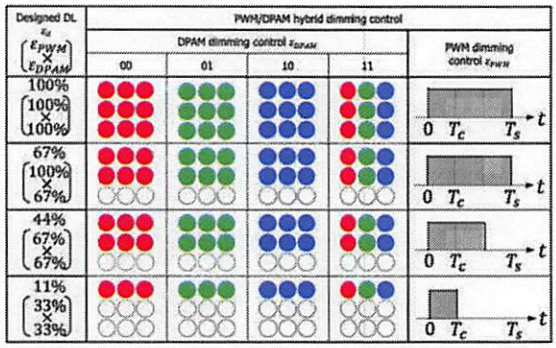


Figure 1: Transmit signal pattern model of 4-ary DCSK with hybrid PWM/DPAM dimming control using nine RGB-LEDs

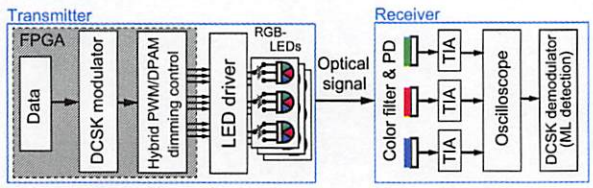


Figure 2: Experimental setup of 4-ary DCSK using nine RGB-LEDs with hybrid PWM/DPAM dimming control

by the LEDs (OptoSupply [15]: bullet-type color LEDs). At the receiver side, three p-i-n PDs (Hamamatsu S6775 [16], spectral response range: 320–1100 nm, effective photosensitive area: 26.4 mm^2) with color band-pass filters (MidOpt BP series [17]) followed by transimpedance amplifiers (TIAs) (Analog devices AD8015, bandwidth: 240 MHz [18]) convert the received current signal into a voltage signal color by color, which is then recorded by an oscilloscope (keysight MSO6104A [19], max sample rate: 4 GSa/s) and demodulated by maximum likelihood (ML) detection using MATLAB. The DLs are measured by an illuminance spectrometer (TOPCON IM-1000 [20]).

The geometry of the DCSK system is shown in figure 3. The distance between the transmitter and receiver, D, is varied from 20 cm to 55 cm and the optical clock rate of DCSK is set to 1 MHz (2 Mbps). We considered three DLs for ε_{PWM} and ε_{DPAM}, as follows:

$$\begin{aligned}\varepsilon_{PWM} &= \frac{T_c}{T_s} \times N_{PWM} \times 100\% \\ &= \left(\frac{33}{100} \times 100\%, \frac{67}{100} \times 100\%, \frac{100}{100} \times 100\%\right) \\ \varepsilon_{DPAM} &= \frac{N_{min}}{N_{RGB}} \times N_{DPAM} \times 100\% \\ &= \left(\frac{3}{9} \times 100\%, \frac{6}{9} \times 100\%, \frac{9}{9} \times 100\%\right)\end{aligned}$$

so N is 9 ($N = N_{PWM} \times N_{DPAM}$) including overlapped

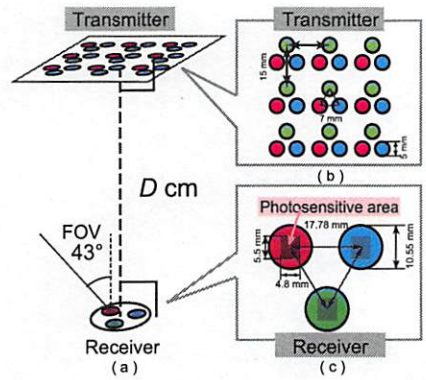


Figure 3: (a) Geometry of transmitter and receiver of the DCSK system, (b) Transmitter layout with nine RGB-LEDs, (c) Receiver layout with color filters and PDs

Table 1: Experimental conditions

FPGA evaluation kit	Xilinx ML605
LED (Red)	OptoSupply OS5RKA5111A[15]
LED (Green)	OptoSupply OSG58A5111A
LED (Blue)	OptoSupply OSB56A5111A
PD	Hamamatsu S6775[16]
Color filter (Red)	MidOpt BP635[17]
Color filter (Green)	MidOpt BP525
Color filter (Blue)	MidOpt BP470
TIA	Analog devices AD8015
Illuminance spectrometer	TOPCON IM-1000[20]
Oscilloscope	Keysight MSO6104A[19]
Irradiance of each LED (D = 20cm)	approx. 25 mW/m^2
Modulation scheme	4-ary DCSK
Optical clock rate	1 MHz (2 Mbps)
Distance between transmitter and receiver D	20 – 55 cm

DLs. The transmit signal pattern is the same as in figure 1.

The experimental conditions are listed in table 1. The irradiance of each LED is set to approximately 25 mW/m^2 for flicker mitigation. The optical clock rate is set to 1 MHz (2 Mbps).

3. Results

The dimming accuracy of each DL is shown in table 2. The designed DL, ε_d, is written as

$$\varepsilon_d = \varepsilon_{PWM} \times \varepsilon_{DPAM} \tag{7}$$

The measured DL, ε_m, is normalized by the maximum irradiance, which is measured at $\varepsilon_d = 100\%$. The relative error, e, is written as

$$e = \frac{\varepsilon_m - \varepsilon_d}{\varepsilon_d} \times 100[\%] \tag{8}$$

Table 2: Dimming accuracy of each DL

Designed dimming level ε_d[%] ($\varepsilon_{PWM} \times \varepsilon_{DPAM}$)	Measured dimming level ε_m[%]	Relative error e [%]
100.0 (100.0 × 100.0)	100.0	-
66.7 (100.0 × 66.7)	68.2	2.25
67.0 (67.0 × 100.0)	66.1	-1.34
44.7 (67.0 × 66.7)	45.1	0.89
33.3 (100.0 × 33.3)	34.1	2.40
33.0 (33.0 × 100.0)	33.2	0.61
22.2 (67.0 × 33.3)	22.7	2.25
22.0 (33.0 × 66.7)	22.5	2.27
11.0 (33.0 × 33.3)	11.6	5.45

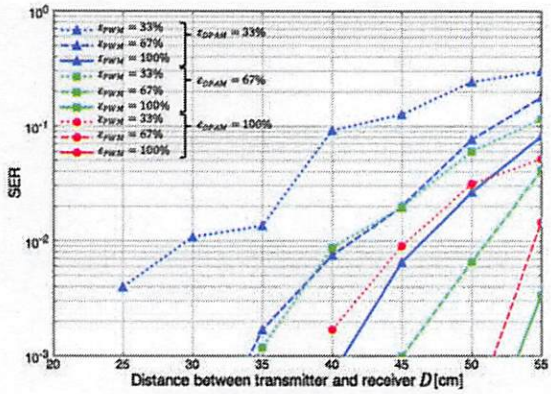


Figure 4: SER versus distance between transmitter and receiver D

From table 2, PWM achieves high DL accuracies compared with those of DPAM. For example, when ε_d is about 67%, PWM can achieve a relative error of -1.34, while the relative error of DPAM is 2.25. Similarly, when ε_d is about 33%, PWM can achive a relative error of 0.61, while the relative error of DPAM is 2.40. This is because multiple RGB-LEDs in DPAM increase the effect of individual differences in the LED drive current. Z 9110:2011 of JIS (Japanese industrial standards) defines that the minimum difference in illuminance which can be perceived is about 1.5 times [21]. The practical tolerance of the relative error is therefore about 50%.

Figure 4 shows the SER versus the distance between the transmitter and receiver, D. When ε_d is high, the SER decreases because the optical power is proportional to ε_m.

4. Conclusions

We experimentally evaluated the dimming accuracy and SER of DCSK with hybrid PWM/DPAM dimming control. When there were several combinations representing the same DL, the PWM scheme had greater dimming accuracy than the DPAM scheme due to the individual differences among RGB-LEDs. Moreover, the SER increased when the measured DL ε_m was high because the optical power of the received signal increased.

Acknowledgments

This research was supported by JSPS KAKENHI Grants 15K21397 and 17K18143.

References

[1] Y. Tanaka, S. Haruyama and M. Nakagawa: Wireless optical transmissions with white colored LED for wireless home links., Proc. IEEE PIMRC, Vol. 2, pp. 1325-1329, 2000.

[2] T. Komine and M. Nakagawa: Fundamental analysis for visible-light communication system using LED lights, IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, pp. 100-107, 2004.

[3] IEEE Standard for Local and Metropolitan Area NetworksPart 15.7: Short-Range Wireless Optical Communication Using Visible Light, IEEE Standard 802.15.7, 2011.

[4] S. Rajagopal, R. D. Roberts and S.-K. Lim: IEEE 802.15. 7 visible light communication: Modulation schemes and dimming support, IEEE Communications Magazine, Vol. 50, No. 3, pp. 72–82, 2012.

[5] CIE, "Commission Internationale de l'Eclairage Proc.," 1931.

[6] D. C. O' Brien, G. Faulkner, H. L. Minh, O. Bouchet, M. EI Tabach, M. Wolf, J. W. Walewski, S. Randel, S. Nerreter, M. Franke, K.-D. Langer, J. Grubor, and T. Kamalakis: Home access networks using optical wireless transmission, Proc. IEEE PIMRC, pp. 1–5, 2008.

[7] J. Grubor, O. C. Gaete Jamett, J. W. Walewski and K.-d.Langer: High-speed wireless indoor communication via visible light, ITG Fachbericht, Vol. 198, pp. 203–208, 2007.

[8] N. Murata, Y. Kozawa and Y. Umeda: Digital color shift keying with multicolor LED array, IEEE Photonics Journal, Vol. 8, No. 4, pp. 1–13, 2016.

[9] E. Monteiro and S. Hranilovic: Design and implementation of color-shift keying for visible light communications, IEEE/OSA Journal of Lightwave Technology, Vol. 32, No. 10, pp. 2053–2060, 2014.

[10] H. Shimamoto, Y. Kozawa and Y. Umeda: An experimental evaluation on EVM performance for 4-CSK (color shift keying) using visible light with multiple full-color LEDs, Proc. IEEE Radio and Wireless Symposium (RWS), pp. 206-208, Jan. 2015.

[11] N. Murata, H. Shimamoto, Y. Kozawa and Y. Umeda: Performance evaluation of digital colour shift keying for visible light communications, Proc. IEEE International Conference on Communication Workshop (ICCW), pp. 1374–1379, June 2015.

[12] M. S. Islim and H. Haas: Modulation Techniques for Li-Fi, ZTE Commun., Vol. 14, No. 2, pp. 29–40, Apr. 2016.

[13] J. Y. Sung, C. W. Chow and C. H. Yeh: Dimming-discrete-multi-tone (DMT) for simultaneous color control and high speed visible light communication, Opt. Exp., Vol. 22, No. 7, pp. 7538–7543, Mar. 2014.

[14] J. Okumura, Y. Kozawa, Y. Umeda and H. Habuchi: Hybrid PWM/DPAM dimming control for digital color shift keying using RGB-LED array, IEEE Journal on Selected Areas in Communications., Vol. 36, No. 1, pp. 45-52, 2017.

[15] Optosupply Electronics, May 2018. [Online]. Available: http://www.peace-corp.co.jp/data/opto

[16] Hamamatsu Photonics K.K. "S6775" May 2018. [Online]. Available: http://www.hamamatsu.com/jp/en/product/category/3100/4001/4103/S6775/index.html

[17] Midwest Optical Systems, Inc. May 2018. [Online]. Available: http://midopt.com/filters/bandpass/

[18] A. Burton, C. Amiot, H. L. Minh and Z. Ghassemlooy: Design of an integrated optical receiver for mobile visible light communications, PGNet, 2011.

[19] Keysight, MSO6104A, May 2018. [Online]. Available: http://www.keysight.com/en/pdx-x202252-pn-MSO6104A/mixed-signal-oscilloscope-1-ghz-4-analog-plus-16-digital-channels?pm=spt&nid=-32537.1150417&cc=US&lc=eng

[20] TOPCON "IM-1000," May 2018. [Online]. Available: http://www.topcon-techNo.co.jp/en/products/op_meas/im-1000.html

[21] General rules of recommended lighting levels, JIS Z 9110, 2011.

ATLANTIS PRESS
Journal of Robotics, Networking and Artificial Life, Vol. 5, No. 2 (September 2018) 135-138

A Training Method for the Speech Controlled Environmental Control System Based on Candidate Word Discriminations

Taro Shibanoki[*], Masaki Watanabe[*], Go Nakamura[†], Takaaki Chin[†], Toshio Tsuji[‡]
[*]*Ibaraki University, 4-12-1, Nakanarusawacho, Hitachi, 316-8511, Japan*
[†]*Hyogo Rehabilitation Center, 1070 Akebonocho, Nishi-Ku, Kobe,651-2181, Japan*
[‡]*Hiroshima University, 1-4-1, Kagamiyama, Higashi-Hiroshima,739-8527, Japan*
e-mail: taro.shibanoki.ts@vc.ibaraki.ac.jp, 14t4070a@vc.ibaraki.ac.jp, g_nakamura@assistech.hwc.or.jp, chin@assistech.hwc.or.jp, tsuji@bsys.hiroshima-u.ac.jp
http://bs.cis.ibaraki.ac.jp

Abstract

This paper proposes a concept of a training system for the speech controlled environmental control system: Bio-Remote based on candidate word discriminations. The proposed system can provide three-types of voice signal training: (1) volume, (2) tempo/timing and (3) candidate word which are important for accurate speech recognition based on false recognition results. During the training, such three kinds of features are extracted from measured voice signals and visually and auditory fed back to the user in real time. This allows the user to train speech abilities even if false recognition results are extracted because of slurred speech. The efficacy of the proposed system was demonstrated through training experiments for slurred speech conducted with healthy participants. The results showed that the proposed system was capable for the training of speech abilities.

Keywords: speech training, environment control system (ECS), speech recognition, candidate word, learning-type look-up table.

1. Introduction

The number of disabled people in Japan continues to increase annually and stands at 1.76 million. The population of severely disabled people in particular was around 760,000, and such patients associated with a speech disability reached 81,000 [1].

Against such a background, many speech-controlled environmental control systems (ECSs) have been developed [2], [3]. However, it is difficult for patients with dysarthria to use such systems, since the models used in these systems considers standard adults' speech. Although some studies have investigated the use of speaker-dependent models to support the learning of individual users' voices [4], and the authors' research group also proposed the voice signal-based manipulation method for ECS based on candidate word discrimination [5], fluctuating speech makes discrimination difficult.

The speech training system can support the recovery of as much of a user's speech as possible, and it has been widely discussed as motivation and long-term experiences for users [6], [7]. However, it can be difficult to fully recover verbal functioning because of individual differences and degrees of disability.

This paper proposed a training system for a speech-controlled environmental control system based on candidate word discrimination that can acquire the skill of fixed speech. After the training, the user's intention can be accurately discriminated, even if the user cannot fully recover his/her verbal functioning.

2. Speech Training System Based on Candidate Word Discrimination

Figure 1 shows the structure of the proposed speech training system based on candidate word discrimination. The proposed system provides training for patients with dysarthria to speak the same way every time, even with slurred speech. This training can be applied to control the training of a voice-controlled environmental control system [5] with slurred speech.

The proposed speech training system consists of a PC with a feedback display, audio processor, and microphone. During the speech training, the display

provides the extracted features of voice signals and current status of the users' abilities to improve their speech skills. The details of the system are described in the following subsections.

2.1. *Voice signal processing*

The structure of the voice signal processing is shown in Fig. 1. First, the amplitude and timing information of voice signals are extracted, and discrimination results are then obtained using the candidate words/phenomes $\boldsymbol{W}_h$/$\boldsymbol{M}_h$ and the log-likelihoods $T(\boldsymbol{W}_h)$ with the candidate word discrimination method [5].

2.1.1. *Extraction of voice signal features*

Voice signals are recorded using a microphone and sampled at 16 [kHz]. The amplitude information $v(t)$ of the measured voice signals with full-wave rectification and low-pass filtering (cut-off frequency: 1 [Hz]) is obtained based on the gains of the amplifier and microphone input levels.

Feature vector $\boldsymbol{X}$ used for speech recognition is then defined as the low-frequency components of Mel-frequency cepstrum coefficients (MFCCs) for each frame, and the output probabilities $P(\boldsymbol{X}|\boldsymbol{W})$ of a feature vector $\boldsymbol{X}$ from word $\boldsymbol{W} = \{w_1, w_2, \ldots, w_K\}$ (w_k: word, K: number of words) are calculated using an N-gram model and phoneme-hidden Markov model (phoneme HMM) dividing the words $\boldsymbol{W}$ into phonemes $m = \{m_1, m_2, \ldots, m_J\}$ (m_j: phoneme, J: number of phonemes) and matching phoneme HMM to $\boldsymbol{X}$. Subsequently, the top H words $\boldsymbol{W}_h$ ($h = 1, 2, \ldots, H$) with the maximum log-likelihood, their phonemes $\boldsymbol{M}_h$, and log-likelihoods $T(\boldsymbol{W}_h)$ are extracted using Julius [8].

2.1.2. *Intention estimation using candidate word discrimination*

The user's intention is discriminated using the learning-type look-up table (LUT) [5]. The user is instructed to utter C words (corresponding to the control commands of domestic appliances) multiple times, and top V words ${}^{c}W_v$ with their maximum log-likelihood and their phonemes ${}^{c}M_v$ and log-likelihood $T({}^{c}W_v)$ in H extracted words are corresponded to each discrimination class ($c = 1, 2, \ldots, C$; $v = 1, 2, \ldots, V$; $V < H$) in the learning stage. In the discrimination stage, a new set of H words are extracted, and the phenomes ${}^{(D)}M_u$ ($u = 1, 2, \ldots, U$; $U < H$) of top U words with their maximum log-likelihood are compared

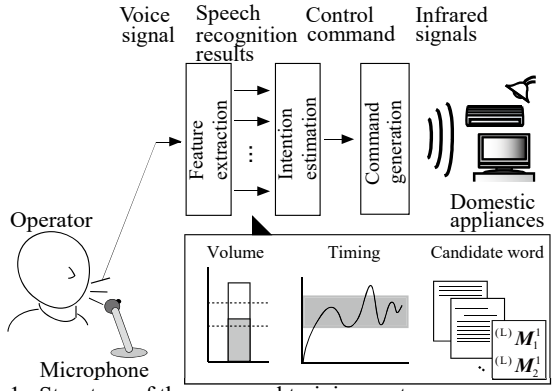
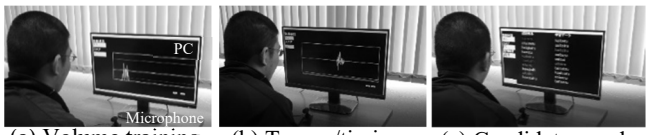


Fig. 1. Structure of the proposed training system



(a) Volume training (b) Tempo/timing training (c) Candidate word speech training

Fig. 2. Scenes from the training

to phoneme ${}^{(L)}M^{c}_i$ ($i = 1, 2, \ldots, I_c$; I_c: number of learning data for class c) of each discrimination class memorized in the learning-type LUT. The coincidence $s^{c}_{u,i}$ between ${}^{(D)}M_u$ and ${}^{(L)}M^{c}_i$ is then calculated, and a class with a maximum value of r^{c} representing the average of all $s^{c}_{u,i}$values (the number of coincident phonemes) is then taken as the discrimination result. To disambiguate discrimination, the difference between log-likelihoods $T({}^{(D)}W_u)$ and $T({}^{(L)}W^{c}_i)$ is used to determine the result when the same values for some classes are obtained.

2.2. *Speech training for candidate word discrimination method*

For speech therapy, the treatment of articulation, prosody and pitch range, speech rate, vocal volume, or resonance is important [6]. The proposed speech training is therefore composed of three stages (see Fig. 2), as explained in the following subsections.

Before the training, to make the learning data sets used in each training, the trainee is instructed to utter C words T times, and the maximum/minimum and average volumes of each word are determined. The durations of $C \times T$ words $[{}^{\text{start}}D^{c}_t, {}^{\text{end}}D^{c}_t]$ used in the timing/tempo control training are also determined using Julius [8].

2.2.1. *Volume control training*

In this training, the trainee practices adjusting the vocal volume level. During the training, the amplitude information extracted from a measured voice signal is presented on the display with the desired values (predetermined maximum/minimum and average). The trainee controls his/her voice signal so the extracted amplitude information follows the average value and falls within the min./max. range. The training result is evaluated using the following equation.

$$S_t = \begin{cases} 100 - (V_{\mathrm{ave}} - v(\mathrm{t})) & (V_{\min} \le v(\mathrm{t}) \le V_{\max}) \\ 0 & (V_{\min} > v(\mathrm{t}), v(\mathrm{t}) > V_{\max}) \end{cases}. \quad (1)$$

The closer the amplitude information is to the average, the higher the score, and if it exceeds the min./max. values, the score becomes zero. The average of the S_t value of speech duration is output at the end of each trial.

2.2.2. *Tempo/timing control training*

For accurate discrimination using the candidate word discrimination method, it is also important to control the timing and time from the start to the end of speech. In this training, the trainee controls the tempo/timing of his/her speech. During the training, the stored voice signals of each word are randomly shown in the display. The trainee is instructed to regulate his/her speech duration and timing according to the pre-specified timing shown in waveforms. The system evaluates the ratio of extracted speech duration to pre-specified duration in this training.

2.2.3. *Candidate word speech training*

Candidate word speech training is conducted so the trainee speaks approximately the same way every time. The candidate phonemes for each discrimination word and extracted trainee's phonemes are shown in the display during this training. The trainee practices to control his/her speech so similar candidate phonemes are extracted. The score of this training is defined as a ratio of the number of complete/ambiguous coincidence in candidate and extracted phonemes:

$$S_h = \begin{cases} (100 - S_{\mathrm{th}})/D_{\mathrm{cmp}} & (L({}^{(L)}M_i^c, M_h) = 0) \\ (100 - S_{\mathrm{th}})/D_{\mathrm{amb}} & (0 < L({}^{(L)}M_i^c, M_h) \le L_{\mathrm{th}}), \\ 0 & (L_{\mathrm{th}} < L({}^{(L)}M_i^c, M_h) \end{cases} \quad (2)$$

where $L(\cdot)$ represents Levenshtein distance.

3. Training Experiments

3.1. *Method*

To verify the efficacy of the proposed training system, training experiments were performed with three healthy males (subjects A–C, 22.3 $\pm$ 1.15 [year]). In the experiments, participants were instructed to speak with their tongue touching the maxillary central to simulate slurred speech. The parameters used in the experiments were set as C = 7, T = 10, H = 10, V = 10, U = 5, D = 10, $L_{\mathrm{th}} = 1$, D_{cmp} = 10, D_{amb} = 500, and S_{th}=50. The other parameters, K, J, and I_c, were adjusted based on the input voice signal durations and learning procedure results. Ten sessions of each training stage were performed in the training experiments, and discrimination experiments were also performed before and after training to verify the effectiveness of the proposed training method. In the discrimination experiments, participants were asked to utter each word three times without feedback.

3.2. *Results and discussion*

Figure 3 shows examples of experimental results. From this figure, the training scores are stable as the number of sessions increased, and the average discrimination rates before and after training have relatively high accuracy. Although participants simulated slurred speech, they could utter each word the same way from the beginning of the training.

Therefore, other training experiments were performed so the participants could mimic other participants' speech. In the experiments performed, Sub. A trained using Subs. B and C's learning data sets. These experimental results are shown in Fig. 4, and it is confirmed that Sub. A cannot follow other participants' speech during 10 training sessions. An additional 10 training sessions were therefore performed with words, the score of which was below 40. In the latter 10 sessions, each score was gradually increased as the number of training sessions increased. The average discrimination rates before and after 20 training sessions were 61.90 $\pm$ 48.56 [%] and 80.95 $\pm$ 39.27 [%], respectively, and the significant difference before and after training was confirmed at a level of 1 [%]. These outcomes indicated that the proposed training system was capable of speech training.

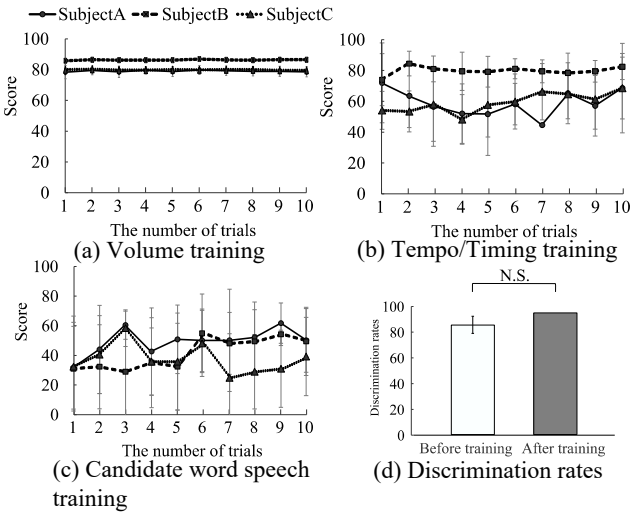


Fig. 3. Experimental results

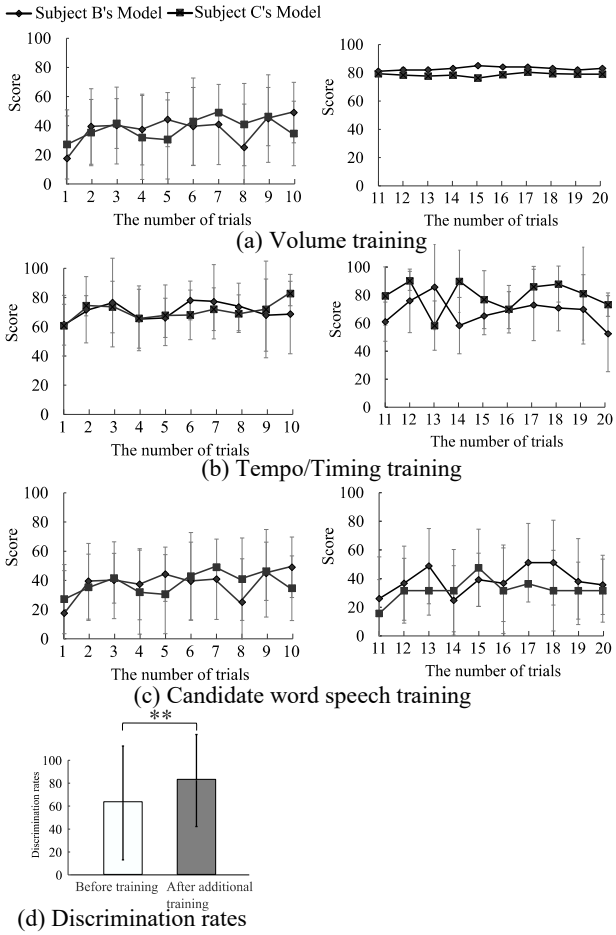


Fig. 4. Experimental results using the other subjects' learning data sets (Sub. A).

4. Conclusion

This paper proposes a speech training system for the voice signal controlled ECS based on candidate word discriminations. The proposed training system provides three types of speech training that are important to speak in the same way every time. In the training experiments, it could be confirmed that the trainees' speech skills were gradually improved through training using the proposed system.

In future work, the authors plan to perform training experiments for patients with dysarthria and establish an online tuning method of training levels for each stage.

Acknowledgements

This work was partially supported by JSPS/MEXT KAKENHI Grant Numbers 17K12723 and 26330226.

References

1. Ministry of Health, Labour and Welfare, "Ministry of Health, Labour and Welfare Fact-Finding Investigation of Fisically Disabled," *http://www8.cao.go.jp/shougai/whitepaper/h25hakusho/zenbun/furoku_08.html* (accessed December 2017).
2. Glamo Inc., iRemocon Wi-Fi, *http://i-remocon.com/aboutiremoconwifi/* (accessed December 2017).
   Nature Inc., Nature Remo, *http://nature.global/* (accessed December 2017).
3. M. S. Hawley, P. Enderby, P. Green, S. Cunningham, S. Brownsell, J. Carmichael, M. Parker, A. Hatzis, P. O. Neill and R. Palmer, A Speech-controlled Environmental Control System for People with Severe Dysarthria, *Medical Engineering & Physics*, **29** (5), 2007, pp. 586-593.
4. T. Shibanoki, G. Nakamura, K. Shima, T. Chin and T. Tsuji, Operation Assistance for the Bio-Remote Environmental Control System Using a Bayesian Network-based Prediction Model, *Proceedings of 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Milan, Italy, 2015, pp. 1160-1163.
5. J. Mühlhaus, H. Frieg, K. Bilda,and U. Ritterfeld, Game-Based Speech Rehabilitation for People with Parkinson's Disease, *UAHCI 2017, Part III, LNCS10279* (M. Antona and C. Stephanidis Eds), 2017, pp. 76-85.
6. J. Tamplin, A Pilot Study into the Effect of Vocal Exercises and Singing on Dysarthric Speech, *Neurorehabilitation*, **23,** 2008, pp. 207-216.
7. Large vocabulary Continuous Speech Recognition Engine, Julius, *http://julius.sourceforge.jp/index.php* (accessed December 2017).

3. プロジェクト業績

【特許】

1) 米山一樹，吉田麗生，小林鉄太郎，川原祐人，冨士仁，"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"，国際出願，PCT/JP2018/17124
2) 外岡秀行，室伏拓実，須佐綾太，伊藤達男，"路面状態検知装置"，国内出願，2018-158827
3) 藤芳明生，“検索システム、検索方法、及び検索プログラム”，国内出願，2018-159778
4) 米山一樹，岡野裕樹、吉田麗生，小林鉄太郎，"通信システム、サーバ装置、通信端末、通信方法、及びプログラム"，国内出願，2018/179336
5) 羽渕裕真，金森勝美，イット ワンシット，”無線制御装置、無線通信装置および無線通信システム”,国内出願，2018-093910

【学術誌論文】

1) 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”, Journal of Robotics, Networking and Artificial Life, Vol. 5, No. 2 (September 2018), pp. 135-138, 2018.
2) Kanako Komiya, Minoru Sasaki, Hiroyuki Shinnou, Manabu Okumura, “Domain Adaptation using Word Embeddings for Word Sense Disambiguation”, 自然言語処理, Vol.25, No.4 (September 2018), pp.463-480.
3) Kanako Komiya, Masaya Suzuki, Tomoya Iwakura, Minoru Sasaki, Hiroyuki Shinnou, “Comparison of Methods to Annotate Named Entity Corpora”, ACM Transactions on Asian and Low-Resource Language Information Processing (TALLIP), Volume 17 Issue 4, (August 2018) Article No. 34.
4) Kazuki Yoneyama, Reo Yoshida, Yuto Kawahara, Tetsutaro Kobayashi, Hitoshi Fuji, Tomohide Yamamoto, "Exposure-Resilient Identity-Based Dynamic Multi-Cast Key Distribution", IEICE Trans. on Fundamentals, vol.E101.A, No.6, pp.929-944, Jun. 2018.
5) Shota Suto, Toshiya Watanabe, Susumu Shibusawa and Masaru Kamada: Multi-touch tabletop system using infrared image recognition for user position identification, *Sensors*, Special issue - Advances in Infrared Imaging: Sensing, Exploitation and Applications, Vol. 18, No.5, 1559 (18 pages) , May 2018.
6) Daiki Ito, Michitoshi Niibori and Masaru Kamada: Real-time web-cast system by multihop WebRTC communications, International Journal of Grid and Utility Computing, Vol.9, No.4, pp.345-356, Sep. 2018.
7) Keisuke Osawa, Hiromasa Habuchi, and Yusuke Kozawa : "Theoretical Analysis on Bit Error Rate of Visible-Light Variable N-parallel Code-Shift-Keying", IEICE Transaction on Fundamentals, Vol.E101-A, No.12, pp.2352-2358, (2018-12)
8) Yusuke Matsuda, Yusuke Kozawa and Yohtaro Umeda: "Experimental Evaluation of Hybrid

PWM/DPAM Dimming Control Method for Digital Color Shift Keying Using RGB-LED Array", Journal of Signal Processing, Vol. 22, No. 4, pp. 165-168, July 2018.

9) 樽林雄飛, 外岡秀行: "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, Vol. 38, No. 2, pp. 137-148, April 2018.
10) Wakaha Ogata, Kaoru Kurosawa: No-Dictionary Searchable Symmetric Encryption. IEICE Transactions 102-A(1): 114-124 (2019)

【国際会議論文】

1) Akinaga Ueda, Hayato Tada, Kaoru Kurosawa: (Short Paper) How to Solve DLOG Problem with Auxiliary Input. IWSEC 2018: 104-113
2) Hayato Tada, Akinaga Ueda, Kaoru Kurosawa: How to Prove KDM Security of BHHO. IWSEC 2018: 281-296
3) Taro Shibanoki, Yuki Koizumi, Bi Adriel Jr. Yozan and Toshio Tsuji, “Selection of Motor Imagries for Brain–Computer Interfaces Based on Partial Kullback–Leibler Information Measure”, The Second Annual IEEE Life Sciences Conference (LSC), Montreal, Canada, 28-30 October, 2018 (accepted).
4) Kazuya Hashimoto, Taro Shibanoki, Go Nakamura, Takaaki Chin and Toshio Tsuji, “A Dual-arm Cooperation Training System for Myoelectric Prosthetic Hand Control”, The Second Annual IEEE Life Sciences Conference (LSC), Montreal, Canada, 28-30 October, 2018 (accepted).
5) Hiroyuki Shinnou, Xinyu Zhao and Kanako Komiya, “Domain Adaptation Using a Combination of Multiple Embeddings”, PACLIC 2018, Hong Kong, China, 1-3 December, 2018.
6) Masaya Suzuki, Kanako Komiya, Minoru Sasaki and Hiroyuki Shinnou, “Fine-tuning for Named Entity Recognition Using Part-of-Speech Tagging”, PACLIC 2018, Hong Kong, China, 1-3 December, 2018.
7) Jing Bai, Hiroyuki Shinnou and Kanako Komiya, “Domain Adaptation for Sentiment Analysis using Keywords in the Target Domain as the Learning Weight”, PACLIC 2018, Hong Kong, China, 1-3 December, 2018.
8) Aya Tanabe, Kanako Komiya, Masayuki Asahara, Minoru Sasaki and Hiroyuki Shinnou, “Detecting Unknown Word Senses in Contemporary Japanese Dictionary from Corpus of Historical Japanese”, JADH 2018, Tokyo, Japan, 9-11 September, 2018.
9) Kanako Komiya, Hiroyuki Shinnou, “Investigating Effective Parameters for Fine-tuning of Word Embeddings Using Only a Small Corpus”, DeepLo 2018, Workshop of ACL 2018, pp. 60-67, Melbourne Australia, 19 July, 2018.
10) Rui Suzuki, Kanako Komiya, Masayuki Asahara, Minoru Sasaki and Hiroyuki Shinnou, “All-words Word Sense Disambiguation Using Concept Embeddings”, LREC 2018, pp.1006-1011, Miyazaki Japan, 9-11 May, 2018.
11) Cheng Shi, Kazuki Yoneyama, "Verification of LINE Encryption Version 1.0 using ProVerif", International Workshop on Security (IWSEC 2018), LNCS11409, pp.158-173, Sep. 2018.
12) Atsushi Fujioka, Kazuki Yoneyama , "Single Private-Key Generator Security Implies Multiple Private-Key Generators Security", International Conference on Provable Security (ProvSec 2018), LNCS11192, pp.56-74, Oct. 2018.
13) Shintaro Terada, Kazuki Yoneyama, "Improved Verifiable Delegated Private Set Intersection", International Symposium on Information Theory and its Applications (ISITA 2018), pp.552-556, Oct. 2018.
14) Yuma Kanai, Kazuki Yoneyama, "On Hiding Access Timings in ORAM", International

Symposium on Information Theory and its Applications (ISITA 2018), pp.548-551, Oct. 2018.
15) Atsushi Fujioka, Katsuyuki Takashima, Shintaro Terada, Kazuki Yoneyama, "Supersingular Isogeny Diffie-Hellman Authenticated Key Exchange", International Conference on Information Security and Cryptology (ICISC 2018), LNCS11396, pp.177-195, Nov. 2018.
16) Shotaro Naiki, Masaki Kohana, Shusuke Okamoto and Masaru Kamada: A graphical front-end interface for React.js. In: L. Barolli et al. (eds.), Advances in Network-based Information Systems (Proceedings of the 21st International Conference on Network-based Information Systems, NBiS-2018), Lecture Notes on Data Engineering and Communications Technologies 22, Springer, pp.887-896, Sep. 2018.
17) Shinya Kinoshita, Michitoshi Niibori and Masaru Kamada: An attendance management system capable of mapping participants onto the seat map. In: L. Barolli et al. (eds.), Advances in Network-based Information Systems (Proceedings of the 21st International Conference on Network-based Information Systems, NBiS-2018), Lecture Notes on Data Engineering and Communications Technologies 22, Springer, pp.897-902, Sep. 2018.
18) Yasuhiro Ohtaki: An image source checker for educational presentation materials In: L. Barolli et al. (eds.), Advances in Network-based Information Systems (Proceedings of the 21st International Conference on Network-based Information Systems, NBiS-2018), Lecture Notes on Data Engineering and Communications Technologies 22, Springer, pp.903-912, Sep. 2018.
19) Minoru Sasaki: Multi-Domain Word Embeddings for Semantic Relation Analysis among Domains. Fourth Asia Pacific Corpus Linguistics Conference (APCLC2018), Sep. 2018 (Accepted).
20) Minoru Sasaki: Word Embeddings of Monosemous Words in Dictionary for Word Sense Disambiguation. The Twelfth International Conference on Advances in Semantic Processing (SEMAPRO2018), Nov. 2018 (Accepted).
21) Yasutomo Kimura, Minoru Sasaki: Stance Classification Using Political Parties in Tokyo Metropolitan Assembly Minutes. The Seventh International Conference on Data Analytics (DATA ANALYTICS 2018), Nov. 2018 (Accepted).
22) Mamoru Fujiyoshi, Akio Fujiyoshi, Hiroshi Tanaka and Toru Ishida, Universal Design Tactile Graphics Production System BPLOT4 for Blind Teachers and Blind Staffs to Produce Tactile Graphics and Ink Print Graphics of High Quality, 16th International Conference on Computers Helping People with Special Needs (ICCHP 2018), LNCS 10897, pp.167-176, July 2018
23) Masaki Kohana, Hiroki Sakaji, Akio Kobayashi, A Parallel Calculation Method on Web Browser for Contents Categorization, The 32th International Conference on Advanced Information Networking and Applications Workshop (WAINA-2018), pp. 40-44, May 2018
24) Masaki Kohana, Shusuke Okamoto, A Location-Based Web Browser Network for Virtual Worlds, In: L. Barolli et al. (eds.), Advances in Network-based Information Systems (Proceedings of the 21st International Conference on Network-based Information Systems, NBiS-2018), Lecture Notes on Data Engineering and Communications Technologies 22, Springer, pp. 929-936, Sep 2018
25) atsuya Ohyanagi, Tomoyuki Ishida, Noriki Uchida, Yoshitaka Shibata, and Hiromasa Habuchi: "Proposal of a Disaster Support Expert System Using Accumulated Empirical Data", The 12th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2018), July 2018
26) Yutaka Imaizumi, Hiromasa Habuchi, and Koichiro Hashiura : "Improved Packet Success Rate on MC-CDMA based On-demand WSN System with MPOMS", IEEE Vehicular Technology Society Asia Pacific Wireless Communications Symposium (APWCS 2018), Aug. 2018

27) Hikari Iiduka, Hiromasa Habuchi, and Yusuke Kozawa : "Proposal of VN-CSK System having Positioning Function", IEEE Vehicular Technology Society Asia Pacific Wireless Communications Symposium (APWCS 2018), Aug. 2018
28) Tomofumi Haruna, Hiromasa Habuchi, and Yusuke Kozawa : "Theoretical Analysis of Optical-Wireless Code Shift Keying System using Extended Einarsson Code", IEEE Vehicular Technology Society Asia Pacific Wireless Communications Symposium (APWCS 2018), Aug. 2018
29) Yuto Asano, Hiromasa Habuchi, and Yusuke Kozawa : "Exact Bit Error Rate Analysis for Optical-Wireless Framed-DOOK System", IEEE 7th Global Conference of Consumer Electronics (GCCE 2018), Oct. 2018
30) Takashi Tokunaga, Hiromasa Habuchi, Yusuke Kozawa, and Ran Sun: "BER Performance Impaired by Transmission Time Offset Between Users in Optical Wireless CSK/ACDMA System Using DMPOMs", IEEE 7th Global Conference of Consumer Electronics (GCCE 2018), Oct. 2018
31) Yutaka Imaizumi, Hiromasa Habuchi, and Yusuke Kozawa : "Enhanced On-demand WSN in terms of MC-CDMA with MPOMS", IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS 2018), Ishigaki, pp.102-106, (2018-11-28)
32) Run Sun, Hiromasa Habuchi, and Yusuke Kozawa : "Proposal of Optical Wireless Turbo Coded System with Hybrid PPM-OOK Signalling", International Conference on Signal Processing and Communication Systems (ICSPCS 2018), Cairns, Australia, (2018-12-18)
33) Yuto Asano, Hiromasa Habuchi, and Yusuke Kozawa : "Frame Error Detection Performance of Optical-Wireless Advanced Framed-DOOK System", International Conference on Signal Processing and Communication Systems (ICSPCS 2018), Cairns, Australia, (2018-12-19)
34) Lu Yangzhicheng, Tomoyuki Ishida, Hiromasa Habuchi : "Proposal of a Furniture Layout Simulation System using Mixed Reality Technology", The 24th International Symposium on Artificial Life and Robotics pp.808-811, (2019-01-24)
35) Ryo Nakai, Tatsuya Ohyanagi, Tomoyuki Ishida, Hiromasa Habuchi : "Proposal of a Scalable Interactive Visualization Environment using Large Display in Emergency", The 24th International Symposium on Artificial Life and Robotics pp.812-815, (2019-01-24)
36) Hikari Iizuka, Ran Sun, Hiromasa Habuchi, and Yusuke Kozawa : "High Accuracy Positioning System on Indoor Optical Wireless VN-CSK System",RISP International Workshop on Nonlinear Circuits, Communication and Signal Processing (NCSP'19), (2019-03-05)
37) Yuta Asano, Hiromasa Habuchi, and Yusuke Kozawa : "Effective Frame Error Detecting Scheme for Optical-Wireless Advanced Framed-DOOK System",RISP International Workshop on Nonlinear Circuits, Communication and Signal Processing (NCSP'19), (2019-03-05)
38) Ryuichi Takahashi, Kazuma Nishida, Yoshiaki Fukazawa: "Recommendation of Web Service Selection Algorithm Based on Web Application Review", IEEE TENCON2018, Oct. 2018.
39) Ryuichi Takahashi, Kazuma Nishida, Yoshiaki Fukazawa:" Recommendation Method for Service Selection Algorithm Based on User Preference", CSAE2018, Oct. 2018.
40) Hideyuki Tonooka, Yudai Mizoguchi: "Release of the Satellite-based Lake and Reservoir Temperature Database in Japan (SatLARTD-J) Version 3", 17th World Lake Conference, Oct. 2018.
41) 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”, 17th Hawaii

International Conference on Education 2019 (HICE2019), Jan. 2019.

42) Ryota Kimoto, Yusuke Kozawa, Yohtaro Umeda, Hiromasa Habuchi: “Underwater Visible Light Simultaneous Wireless Information and Power Transfer using Inverse Pulse Position Modulation Scheme”, RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing 2019 (NCSP 2019), March 2019.

43) Kazuya Hashimoto, Taro Shibanoki, Go Nakamura, Takaaki Chin and Toshio Tsuji, “A Dual-arm Cooperation Training System for Myoelectric Prosthetic Hand Control”, The Second Annual IEEE Life Sciences Conference (LSC), 2pages, Montreal, Canada, 28-30 October, 2018.

44) Taro Shibanoki, Yuki Koizumi, Bi Adriel Jr. Yozan and Toshio Tsuji, “Selection of Motor Imagries for Brain–Computer Interfaces Based on Partial Kullback–Leibler Information Measure”, The Second Annual IEEE Life Sciences Conference (LSC), pp. 243-246, Montreal, Canada, 28-30 October, 2018.

45) Kazuma Nishida, Ryuichi Takahashi and Yoshiaki Fukazawa, “Fault-tolerant Topology Determination for IoT Network”, The 13th International Conference on Ubiquitous Information Management and Communication, Phuket, Thailand, 4-6 January, 2019.

46) Mitsumasa Ota, Ryuichi Takahashi and Yoshiaki Fukazawa, “FAULT-TOLERANT TOPOLOGY CONTROL FOR IOT NETWORKS USING VARIABLE K-CONNECTIVITY”, 9th International Conference on Internet Technologies & Society 2019, Hong Kong, China, 8-10 February, 2019.

47) Ryu Sakamoto, Ryuichi Takahashi and Yoshiaki Fukazawa, “STABILITY-BASED LIVE MIGRATION USING DYNAMIC MARGIN”, 9th International Conference on Internet Technologies & Society 2019, Hong Kong, China, 8-10 February, 2019.

48) Hiroki Sakaji, Akio Kobayashi, Masaki Kohana, Yasunao Takano, Kiyoshi Izumi, “Estimation of Tags using Various Data for Online Videos,” The 33rd International Conference on Advanced Information Networking and Applications, Matsue, Japan, 27-29 March, 2019

49) Yasunao Takano, Yusuke Iijima, Kou Kobayashi, Hiroki Sakaji, Masaki Kohana, Akio Kobayashi, “Improving Document Similarity Calculation using Cosine-Similarity Graphs,” The 33rd International Conference on Advanced Information Networking and Applications, Matsue, Japan, 27-29 March, 2019

50) Hideyuki Tonooka, Yudai Mizoguchi, Release of the Satellite-based Lake and Reservoir Temperature Database in Japan (SatLARTD-J) Version 3, Proc. of 17th World Lake Conference, pp. 1254-1256, October, 2018.

【招待講演】

1) 黒澤馨、「辞書無し検索可能暗号について」、情報理論とその応用シンポジウム、特別セッション（情報セキュリティ）、2018.12.21.
2) 黒澤馨、「検索可能暗号について」、総務省委託研究SCOPEプロジェクト（中央大学）主催シンポジウム、2019.2.23

【研究会等】

1) 佐々木 稔, 古宮 嘉那子, 新納 浩幸, 単語の分散表現を用いた領域における出現単語の特徴分析, 言語資源活用ワークショップ 2018, pp. 552-559, (2018,09,05).
2) 新納浩幸, 鈴木類, 古宮嘉那子, 双方向 LSTM による分類語彙表番号を語義とした all-words WSD, 言語資源活用ワークショップ 2018, pp. 192-202, (2018,09,04).
3) 田邊絢, 古宮嘉那子, 浅原正幸, 佐々木稔, 新納浩幸, 日本語歴史コーパスの現代語辞書における未知語義判定システム, 言語資源活用ワークショップ 2018, pp. 112-117,

(2018,09,04).

4) 柳沼 大輝, 古宮 嘉那子, 新納 浩幸, 分散表現のファインチューニングによる語義曖昧性解消の領域適応, 情報処理学会 研究報告自然言語処理（NLP）, 2018-NL-236, (2018,07,09).
5) 佐々木 稔, 短文に対する補助文脈を考慮した語義曖昧性解消, 電子情報通信学会 言語理解とコミュニケーション研究会テキストアナリティクス・シンポジウム, NLC2018-18, (2018,09,06).
6) 佐々木 稔, 木村 泰知, Gaussian LDA を用いた地方議会会議録のトピック分析, 言語処理学会第 25 回年次大会, (2019,03,14)
7) 木村 泰知, 佐々木 稔, 東京都議会の会派を用いた Stance classification の試み, 言語処理学会第 25 回年次大会, (2019,03,15)
8) 久野和敏, 小飼敬, 上田賀一:グラフデータベースを用いたモデル検査手法の提案, 情報処理学会研究報告, ソフトウェア工学(SE), 2018-SE-198(9) (2018,03,02)
9) 堀田大貴, 平山秀昭, 早瀬健夫, 田原康之, 大須賀昭彦:プロセスマイニングにおけるビジネスプロセスモデルの自動修正に対応したゴールモデルの修正手法, 信学技報, vol. 118, no. 116, AI2018-1, pp. 1-6, (2018,07,02).
10) 羽渕裕真, 金森勝美, イット ワンシット : "スパースな疑似雑音符号を用いる DS/CDMA", 電子情報通信学会ワイドバンド研究会, WBS2018-1, pp.1-5, (2018-05-17)
11) 春名智文, 羽渕裕真, 小澤佑介 : "光無線 CSK システムへの拡張 Einarsson 符号の適用性", 電子情報通信学会ワイドバンド研究会 WBS2018-8, pp.17-22, (2018-07-06)
12) 飯塚暉, 羽渕裕真, 小澤佑介 : "光無線 VN-CSK システムにおける測位性能の検討", 電子情報通信学会ワイドバンド研究会 WBS2018-9, pp.23-27, (2018-07-06)
13) 今泉豊, 大川智広, 羽渕裕真, 橋浦康一郎 : "変形擬直交 M 系列対を用いるオンデマンド型 WSN におけるパケット成功率向上法", 電子情報通信学会ワイドバンド研究会, WBS2018-11, pp.35-40, (2018-07-06)
14) 浅野裕太, 羽渕裕真, 小澤佑介 : "光無線フレーム化 DOOK システムにおける同期シンボルによる誤り検出法の検討", 電子情報通信学会ワイドバンド研究会, WBS2018-16, pp.59-63, (2018-07-06)
15) 徳永岳, 孫冉, 羽渕裕真, 小澤佑介 : "DMPOMs を用いる光無線 CSK システムにおける同期性能を考慮した誤り率性能", 電子情報通信学会ワイドバンド研究会, WBS2018-17, pp.65-70, (2018-07-06)
16) 羽渕裕真, 金森勝美, イット ワンシット : "拡張 Einarsson 符号に変形擬直交 M 系列を融合する CSK", 電子情報通信学会ソサイエティ大会, A-9-6, (2018-09-11)
17) イット ワンシット, 金森勝美, 羽渕裕真 : "UWB インパルス無線における符号分割多元接続方式の検討", 電子情報通信学会ソサイエティ大会, A-9-7, (2018-09-11)
18) 浅野裕太, 羽渕裕真, 小澤佑介 : "誤り検出可能な光無線フレーム化 DOOK システム", 革新的無線通信技術に関する横断型研究会 MIKA2018, 3-13, (2018-09-27)
19) 孫冉, 羽渕裕真, 小澤佑介 : "光無線通信におけるハイブリッド PPM-OOK ターボ符号システム", 革新的無線通信技術に関する横断型研究会 MIKA2018, 3-14, (2018-09-27)
20) 木元亮太, 小澤佑介, 楳田洋太郎, 羽渕裕真 : "光強度変復調法を用いた水中可視光ワイヤレス給電通信システムに関する基礎検討", 革新的無線通信技術に関する横断型研究会 MIKA2018, 3-17, (2018-09-27)
21) 陳力源, 羽渕裕真: "SIK を用いる多視覚秘密分散法によるマルチルートネットワーク", 革新的無線通信技術に関する横断型研究会 MIKA2018, 4-2, (2018-09-27)
22) 浅野裕太, 羽渕裕真, 小澤佑介:"拡張フレーム化 DOOK システムのためのフレーム誤り検出法の検討", 電子情報通信学会ワイドバンド研究会, WBS2018-30(ITS2018-

13,RCC2018-61),pp.17-21, (2018-12-06)

23) 木元亮太，小澤佑介，楳田洋太郎，羽渕裕真 ："反転パルス位置変調方式を用いた水中可視光ワイヤレス給電通信システムに関する基礎検討"，電子情報通信学会ワイドバンド研究会, WBS2018-32 (ITS2018-15, RCC2018-63), pp.29-34, (2018-12-06)
24) 孫冉，羽渕裕真，小澤佑介 ："ハイブリッド PPM-OOK 信号形式を用いる光無線パンクチャードターボ符号システムの検討"，電子情報通信学会ワイドバンド研究会,WBS2018-72 (ITS2018-55, RCC2018-103), pp.249-253, (2018-12-07)
25) 真中佳祐，陳力源，羽渕裕真，小澤佑介 ："VN-CSK 照明可視光通信における等重み(2,2)視覚復号型秘密分散法"，電子情報通信学会東京支部学生会研究発表会, (2019-03-02)，発表予定
26) 木口朋洋，孫冉，羽渕裕真，小澤佑介 ："光無線 PPM-OOK システムのためのフレーム同期法 "，電子情報通信学会東京支部学生会研究発表会, (2019-03-02)，発表予定
27) 鈴木暁大，羽渕裕真 ："フレーム ALOHA を用いる MPSC-PDMA 方式"，電子情報通信学会東京支部学生会研究発表会, (2019-03-02)，発表予定
28) 孫冉，羽渕裕真，小澤佑介 ："光無線通信ターボ符号システムにおける信号伝送形式の一検討"，電子情報通信学会 WBS/IT/ISEC 合同研究会, WBS2018- (IT2018- ,ISEC2018-), (2019-03-07)，発表予定
29) 今泉豊，羽渕裕真，橋浦康一郎 ："変形擬直交 M 系列対を用いる ROD-WSN におけるノード間干渉の影響"，電子情報通信学会総合大会, (2019-03-19)，発表予定
30) 小栗勇太，外岡秀行，鹿島臨海工業地帯周辺における ASTER/FRP 画像の解析，日本リモートセンシング学会第 65 回学術講演会論文集, (2018.11.28).
31) 劉 明智，外岡秀行, MODIS 画像を用いた中国の中小都市におけるヒートアイランドの時系列解析，日本リモートセンシング学会第 65 回学術講演会論文集, (2018.11.28).
32) 溝口裕大，外岡秀行，衛星湖沼水温データベース日本編（SatLARTD-J）を用いた水温－気温差の季節変動に基づく湖沼分類，日本リモートセンシング学会第 65 回学術講演会論文集, (2018.11.28).
33) 外岡秀行，酒井理人，粂田綾香，中右浩二, ALOS-2/CIRC 及び CALET/CIRC のラジオメトリック校正の状況，日本リモートセンシング学会第 65 回学術講演会論文集, (2018.11.27).
34) 小池優希，外岡秀行，サロマ湖における MODIS 画像の熱力学解析による氷厚推定と現地検証（2），日本リモートセンシング学会第 65 回学術講演会論文集, (2018.11.27).
35) 平井暁裕，外岡秀行，李 雲慶，周辺のハイパースペクトル画像を利用したマルチスペクトル鉱物分類における WorldView-3/SWIR の有効性，日本リモートセンシング学会第 65 回学術講演会論文集, (2018.11.27).
36) 佐久間史洋，菊池雅邦，朝木萌奈，外岡秀行，加藤創史，神山徹 ："ASTER TIR の深宇宙・月校正"，日本リモートセンシング学会第 64 回学術講演会論文集，pp. 185-186, (2018.5.18)
37) 溝口裕大，外岡秀行 ："衛星湖沼水温データベース日本編 (SatLARTD-J) の準リアルタイム更新"，日本リモートセンシング学会第 64 回学術講演会論文集, pp. 45-46, (2018.5.18)
38) 小池優希，外岡秀行 :"サロマ湖における MODIS 画像の熱力学解析による氷厚推定と現地検証"，日本リモートセンシング学会第 64 回学術講演会論文集, pp. 159-160, (2018.5.17)
39) 小栗勇太，外岡秀行 :"ASTER 画像を利用した MODIS 熱異常アルゴリズム（MOD14）の性能解析"，日本リモートセンシング学会第 64 回学術講演会論文集，pp. 157-158, (2018.5.17)
40) 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 (2)"，日本リモートセンシング学会第 64 回学術講演会論文集，pp. 127-128, (2018.5.17)

41) 柴田 敏弥, 米山 一樹, "UC 安全動的検索可能暗号の拡張とフォワード安全性について", 暗号と情報セキュリティシンポジウム (SCIS 2019), Jan. 2019.
42) 金井 佑篤, 米山 一樹, "複数のファイルアクセス可能な ORAM", 暗号と情報セキュリティシンポジウム (SCIS 2019), Jan. 2019.
43) 松井 政裕, 岡野 裕樹, 村上 啓造, 小林 鉄太郎, 米山 一樹, "グループ鍵交換プロトコルにおける長期秘密鍵漏洩後の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 (SCIS 2019), Jan. 2019.
44) 藤岡 淳, 高島 克幸, 米山 一樹, "同種写像を用いた1ラウンド認証グループ鍵共有", 暗号と情報セキュリティシンポジウム (SCIS 2019), Jan. 2019.
45) 寺田 槙太郎, 米山 一樹, "CSIDH に基づくパスワードベース認証鍵交換 ", 暗号と情報セキュリティシンポジウム (SCIS 2019), Jan. 2019.
46) 野口 凌雅, 花谷 嘉一, 米山 一樹, "ProVerif による HEMS におけるグループ鍵管理の検証", 暗号と情報セキュリティシンポジウム (SCIS 2019), Jan. 2019.
47) 師 成, 米山 一樹, "ProVerif によるスマートコントラクト決済委託プロトコルの公平性の検証", 暗号と情報セキュリティシンポジウム (SCIS 2019), Jan. 2019.
48) 勝野 凌介, 米山 一樹, "IC カードとリーダ/ライタ間の認証プロトコルにおける認証再利用と暗号理論的安全性モデルの関係", 電子情報通信学会情報セキュリティ研究会, Mar. 2019.
49) 白井 直輝, 米山 一樹, "検証可能委譲秘匿ビット比較演算", 電子情報通信学会情報セキュリティ研究会, Mar. 2019.
50) 日置千仁, 岡田信一郎, “効果的な反復学習を促す得点計算法の学習失敗への対策とその検証”, 情報処理学会 コンピュータと教育研究会 146 回研究発表会, 2018 年 10 月.
51) 石川大輔, 岡田信一郎, “SQL 実習支援システムへの効果的な反復学習を促す得点計算法の導入”, 2019 年電子情報通信学会総合大会, 2019 年 3 月.
52) 太田光雅, 高橋竜一, 深澤良彰, “IoT ネットワークにおける障害耐性の高いトポロジー生成”, 電子情報通信学会 知能ソフトウェア工学研究会 (SIG-KBSE), 2018 年 7 月.
53) 原口春海, “鉄筋製造業における生産スケジューリングに関する研究”, 日本機械学会生産システム部門研究発表講演会 2019, 2019 年 3 月（発表予定）
54) 荒井宏, 原口春海, “鉄筋製造業における切断作業の効率化に関する研究”, 日本機械学会生産システム部門研究発表講演会 2019, 2019 年 3 月（発表予定）
55) 黒澤馨、上田明長、松橋駿斗、阪上佑介, "複数の小さな離散対数問題を解くアルゴリズム", 暗号と情報セキュリティシンポジウム (SCIS 2019), Jan. 2019.019.
56) 冨田斗威、尾形わかは、黒澤馨、"標準的な仮定のもとで leakage resilient かつ CCA 安全な ID ベース KEM", 暗号と情報セキュリティシンポジウム (SCIS 2019), Jan. 2019.019.

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

２０１８年度報告書

発行日　　平成 31 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