様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月 ３０ 日現在

機関番号：１２６１２
研究種目：基盤研究(C)（一般）
研究期間：2018～2022
課題番号：１８Ｋ１１２９３

研究課題名（和文）長期間運用に耐えうる共通鍵暗号による秘匿検索暗号

研究課題名（英文）Searchable Symmetric Encryption for a Long Term Use

研究代表者
太田　和夫（Ohta, Kazuo）

電気通信大学・大学院情報理工学研究科・特任教授

研究者番号：８０３３３４９１

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：検索可能暗号はクラウドに暗号化したデータを預託して、キーワードによってデータを暗号化したまま検索を実行する技術である。本研究では、共通鍵暗号ベースの検索方式について文書とキーワードの対の集まりの世代更新機能について検討する。
　単一ユーザ型で任意のタイミングでキーワードファイルをサーバに登録可能な動的検索可能暗号について特許出願した。
　一方、代表的論文を精査し、SSE-1では予期しない条件で検索を行った場合に無限ループが発生する場合があり、SSE-2では厳密に定義した安全性定義では許容されない情報が漏洩することを指摘した。指摘したこれらの問題を解決する方式と特許出願した方式を統合して論文にした。

研究成果の学術的意義や社会的意義
検索可能暗号(SSE)はクラウドに機微な情報を預託しつつ検索可能とするプライバシ保証技術である。共通鍵暗号ベースの検索方式が高速で暗号化と検索が可能なので早期に普及すると想定して研究とした。
申請時に文書の集まりとキーワードの集まりの世代更新機能を課題としたが、任意のタイミングでファイル・キーワードをサーバに登録可能な動的方式(DSSE)が研究の主流となり、その流れに従い研究成果を特許取得した。世代更新の課題は解決できた。
　DSSEの有力方式について安全性証明の欠陥を指摘し、その方式を基にDSSE方式を提案して国際会議で発表した。また、SSEの代表的論文の問題を指摘し解決する方式を論文にした。

研究成果の概要（英文）：Searchable encryption is a technology that entrusts encrypted database to the cloud and performs keyword searches while the data is encrypted without leaking the private information. In this research, we examine the update functionality of the database where pairs of documents and keywords are kept securely and efficiently using symmetric key encryption.
A patent application has been filed for a single-user type dynamic searchable encryption (DSSE) that can update the database in the server at anytime.
On the other hand, after scrutinizing representative paper (Currtmola et al. 2003), we pointed out that infinite loops may occur in SSE-1 when searches are performed under unexpected conditions, and that a subtle information that is not allowed by an improved security definition is leaked in SSE-2. So we formulated a strong forward security. The method for solving the point-outed problems and the DSSE method for which the patent application was filed have been integrated into a full paper.

研究分野：情報セキュリティ

キーワード：検索可能暗号　動的検索可能暗号　(強)フォワード安全性　バックワード安全性

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

秘匿検索暗号(SSE) はクラウドに暗号化したデータを預託して、キーワードによってデータを暗号化したまま検索を実行することを可能にする技術である。預託データに関するクラウドへの情報漏洩を回避不可能なもののみに限定しつつ、キーワード検索を可能とするプライバシー保持できる重要な暗号技術の 1 つである(図 1)。最近では、既存のクラウド上で秘匿検索暗号によるファイルの暗号化やキーワード検索を実現する製品も登場するなど、実用化に向けた動きが活発化している。

２．研究の目的

本研究では、共通鍵暗号ベースの検索方式が高速で暗号化と検索が可能なので早期に普及すると想定し、当該技術を用いて長期間にわたってサービスを継続することを目的として、暗号化データベースの維持管理として文書の集まりとキーワードの集まりの世代更新機能と、複数ユーザへの拡張性を保証できるデータベース蓄積・検索機能の実現方法について検討する。併せて、機能拡張に伴う安全性を再定義して、提案方式の効率向上と安全性証明を行う。

３．研究の方法

計画時：基本型では一人のユーザが登録と検索を行うが、複数ユーザ型では複数のユーザが同一の暗号化データベースに対して登録と検索を行えるようにしたい。第一期に単一ユーザ型でのベータベース更新手続き技術を確立し、第二期に複数ユーザ型のデータベース構築法を検討する。第三期にはそれらの統合技術について検討して、最後に安全性証明を与える。

遂行結果：基本型での研究を遂行するなかで更新要求時に随時暗号化データベースを更新可能な方式の研究が主流となりつつあることを察知した。第二期の研究テーマ（複数ユーザ型 SSE）を、任意のタイミングでファイル・キーワードをサーバに登録可能な動的検索可能暗号(Dynamic SSE: DSSE) の文献調査と方式提案に変更して、第三期に実装実験と安全性評価を行った。

具体的には以下のとおり。

まず、図 1 に SSE の概要図を，図 2 に DSSE で可能となる追加及び削除といった更新処理の概要図を示す。

1 年目は、単一ユーザ型でデータベース更新手続き技術を確立することを目標にして研究を行った。特に任意のタイミングでファイル・キーワードをサーバに登録可能な動的検索可能暗号 (Dynamic SSE: DSSE) について検討を行い、特許出願した(代表的な研究成果：特許)。単一ユーザに限定した場合の DSSE を実現できたので、計画時に設定した、基本的な利用形態での世代更新機能の課題は解決できた。

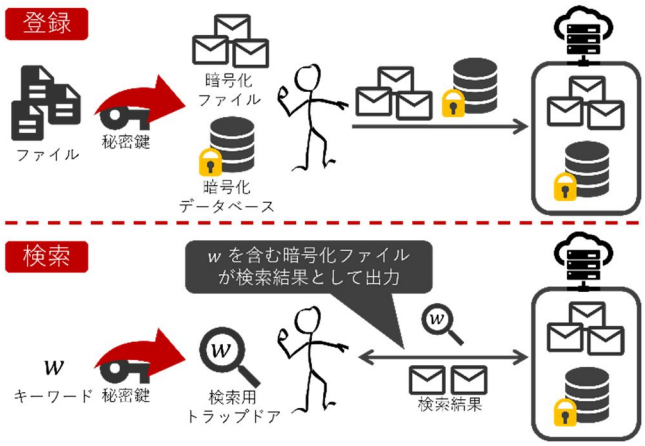

図 1：SSE の概要図

2 年目は、理論的に既存の DSSE では
扱いが不明確だった漏洩情報について厳密な定式化を行うことで「強フォワード安全性」と呼ぶ安全性概念を定式化した。 海外の研究所などを訪問して、安全性概念の重要性をアピールしたものの、残念ながら国際学会での採録には至らなかった。

3 年目は研究方針を変更して基本に返り、SSE の安全性を初めて定式化して安全性証明を与え

た代表的論文(Curtmola et al. 2003 年)を理論面および実装面の問題がないか精査した。

4 年目は、3 年目の成果と 1 年目に得られた DSSE 方式（実装評価を含む）とを統合して本プロジェクトの成果として取りまとめて論文を作成して投稿した。また、DSSE の調査を通じて有力な方式について安全性証明の欠陥を指摘し、その方式を基に DSSE 方式を提案して国際会議（CODASPY2022）で発表した(代表的な研究成果：文献 1)。

5 年目は、上記の査読結果をうけて論文を修正して、IEICE 論文として出版した（代表的な研究成果：文献 2)。

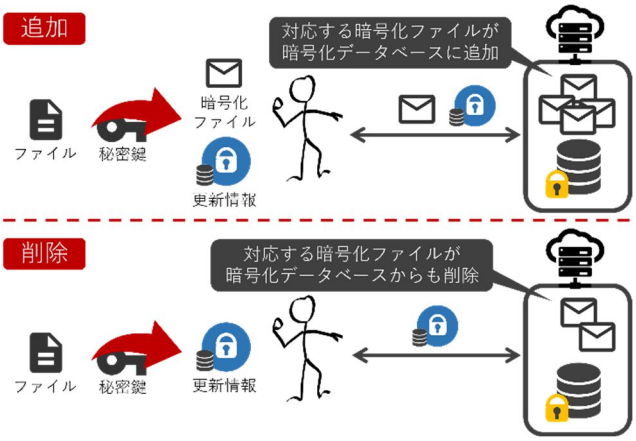

図 2：DSSE における更新処理（追加・削除）

4．研究成果

以下では、最終成果である IEICE 論文の成果について説明する。Curtmola 論文では SSE-1 及び SSE-2 と呼ばれる SSE 方式が提案されていたが、SSE-1 では予期しない条件で検索を行った場合に無限ループが発生する場合があり、SSE-2 では論文の本文から読み取れる安全性への要求条件と安全性定義に齟齬があり、また論文で記載されている手順は動作しないことを発見した(注)。これらの問題の解決法を 1 年目に得られた DSSE 方式と統合して IEICE 論文を出版した。

4.1 SSE-2 におけるダミー追加処理の改良と DSSE への拡張

SSE-2 では、ファイルを暗号化し、暗号化データベースに登録する際、余分な情報、特に各ファイルが何種類のキーワードを含むかに関する情報が漏洩しないように、ダミー用のエントリも併せて登録している。

	正規エントリ					ダミーエントリ				
	f_1	f_2	f_3	$\cdots$	f_n	f_1	f_2	f_3	$\cdots$	f_n
w_1	✓		✓	$\cdots$			✓		$\cdots$	✓
w_2	✓	✓		$\cdots$	✓			✓	$\cdots$	
w_3		✓		$\cdots$		✓		✓	$\cdots$	✓
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$w_{\lvert\Lambda\rvert}$	✓			$\cdots$	✓		✓	✓	$\cdots$	

図 3：ダミーの横方向への追加

具体的には、SSE-2 及びその後続研究では、図 3 に示すような、暗号化データベース作成用のルックアップテーブルを横に伸ばす形でダミーを作成していた。こうすることで、各ファイル $f_1, \ldots, f_n$ が必ずすべてのキーワード $w_1, \ldots, w_{|\Lambda|}$ に関するエントリをもち、実際にそのファイルがキーワードを含むなら正規エントリ、そうでないならばダミーエントリをもつ。結果として、各ファイルのエントリ数が必ず一定になるため、余分な情報、特に各ファイルが何種類のキーワードを含むかについての情報が漏れない。

しかしながら、この方式には、(1)ダミー数が必要以上に多く、特に登録され得るキーワードの数だけダミーを作成するため膨大な数なる、(2)DSSE に拡張するためには、図 3 のルックアップテーブルの正規エントリ部とダミーエントリ部の両方をそれぞれ横方向に拡張する必要があり、ファイルの追加処理が煩雑になる等の弊害が生じる、といった課題があることを発見した。

そこで、本研究では、ルックアップテーブルを縦に拡張するアプローチを取ることで、それらの問題を解決した（図 4 参照）。具体的には、ダミーの追加個数をファイルごとに設定し、そのファイルが理論上含みうるキーワード数分だけダミーを生成することで、必要最小限のダミー数に抑えることに成功した。例えば、図 4 のファイル f_1 が理論上含みうるキーワード数（max_1 ）と実際のキーワード数（$|\mathcal{W}_1|$）の差の分だけダミーを作ればよい。また、DSSE への拡張の際には図 4 のルックアップテーブルを横方向に拡張するだけで済むため、簡潔な処理で DSSE に拡張することに成功した。

		f_1	$\cdots$	f_i	$\cdots$	f_n
正規エントリ	w_1	✓	$\cdots$	✓	$\cdots$	
	w_2	✓	$\cdots$		$\cdots$	✓
	w_3		$\cdots$	✓	$\cdots$	
	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\ddots$	$\vdots$
	$w_{\lvert\Lambda\rvert}$	✓	$\cdots$		$\cdots$	✓
ダミーエントリ	1	✓	$\cdots$	✓	$\cdots$	✓
	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
	$\mathsf{max}_n - \lvert\mathcal{W}_n\rvert$	✓	$\cdots$	✓	$\cdots$	✓
	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	
	$\mathsf{max}_1 - \lvert\mathcal{W}_1\rvert$	✓	$\cdots$	✓	$\cdots$	
	$\vdots$		$\cdots$	$\vdots$	$\ddots$	
	$\mathsf{max}_i - \lvert\mathcal{W}_i\rvert$		$\cdots$	✓	$\cdots$	

図 4：ダミーの縦方向への追加

表 1 にも示す通り、DSSE 提案方式は実用的にも優れており、結果として特許を取得した。

表 1：Enron データセットを用いた場合のダミー数

パラメータ	最大のファイル	最小のファイル	平均
ファイル f_{id} のサイズ (bytes)	2,011,957	398	4,445
最大エントリ数 $\mathsf{max}_{\mathsf{id}}$	251,495 (= max)	58	343.7
実際のエントリ数 $\lvert\mathcal{W}_{\mathsf{id}}\rvert$	59,148	12	77.1
SSE-2 のダミー数 ($\mathsf{max} - \lvert\mathcal{W}_{\mathsf{id}}\rvert$)	192,347	251,483	251,417.9
提案方式のダミー数 ($\mathsf{max}_{\mathsf{id}} - \lvert\mathcal{W}_{\mathsf{id}}\rvert$)	192,347	46	266.6

(注)： 同様の問題は既存研究で指摘され動作手順が提案されていたが、本文から読み取れる安全性が「強安全性」であることを発見しその実現法を示したことが、本研究のオリジナリティである。

4.2　SSE-1 の無限ループ解決方法

SSE-1 では検索の際、サーバはユーザから受け取った検索キーワードに対応する結果を一括して得るために、一連の結果を Table と Array を使って紐づける。

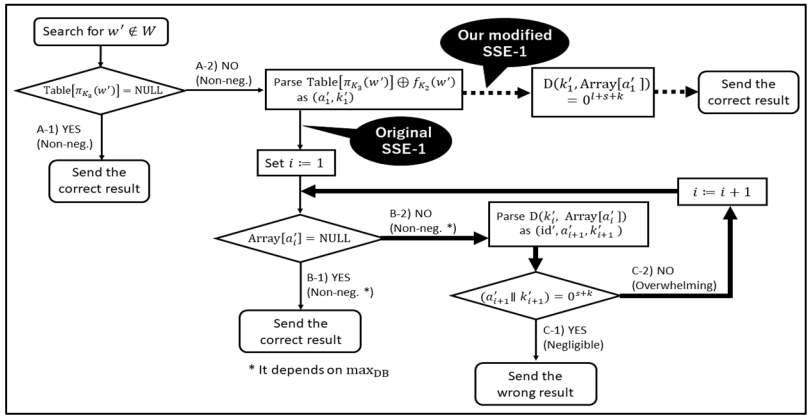

図 5：SSE-1 におけるループ発生条件とその解決方法

しかし，未使用のキーワードを検索すると、Array 内でそのキーワードに関係のないエントリを誤った鍵で復号する。この事象が発生すると、サーバは暗号化データベースの「紐づけ」をたぐる操作を(偶然に終了条件を満たすまで)繰り返す（図 5，Original SSE-1）。

本研究では、ループ発生時の条件を分析して Array 内に検索結果が空集合であることを表すエントリを追加し、未使用キーワードの検索時に必ずそのエントリを参照するように Table を変更することでこの問題を解決した（図 5，Our Modified SSE-1）。

代表的な研究成果

文献 1:
Y. Watanabe, K. Ohara, M. Iwamoto, and K. Ohta
Efficient Dynamic Searchable Encryption with Forward Privacy under the Decent Leakage
Proc. of ACM CODASPY 2022

文献 2:
Y. Watanabe, T. Nakai, K. Ohara, T. Nojima, Y. Liu, M. Iwamoto, and K. Ohta
How to Make a Secure Index for Searchable Symmetric Encryption, Revisited
IEICE Transactions on Fundamentals Vol. E105-A(12) 2022　pp. 1559-1579

特許
名称：動的検索可能暗号処理システム及び動的検索可能暗号処理方法
発明者：渡邉洋平、岩本貢、太田和夫
産業財産権の種類：出願番号　特願 2019-111977　（2019/06/17）
登録番号　特許第 7276767 号　（2023/05/10）

５．主な発表論文等

〔雑誌論文〕　計17件（うち査読付論文　16件／うち国際共著　1件／うちオープンアクセス　6件）

１．著者名 Y. Watanabe, T. Nakai, K. Ohara, T. Nojima, Y. Liu, M. Iwamoto, and K. Ohta	４．巻 E105-A(12)
２．論文標題 How to Make a Secure Index for Searchable Symmetric Encryption, Revisited	５．発行年 2022年
３．雑誌名 IEICE Transactions on Fundamentals	６．最初と最後の頁 1559-1579
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2021EAP1163	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Komano Yuichi、Iwamoto Mitsugu、Ohta Kazuo、Sakiyama Kazuo	４．巻 LNCS 13809
２．論文標題 Lightweight Authentication Using Noisy Key Derived from?Physically Unclonable Function	５．発行年 2023年
３．雑誌名 Proc. SecITC 2022, Lecture Notes in Computer Science, Springer	６．最初と最後の頁 203～221
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-32636-3_12	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Y. Watanabe, K. Ohara, M. Iwamoto, and K. Ohta	４．巻 -
２．論文標題 Efficient Dynamic Searchable Encryption with Forward Privacy under the Decent Leakage	５．発行年 2022年
３．雑誌名 ACM CODASPY 2022	６．最初と最後の頁 312-323
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3508398.3511521	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 K. Emura, R. Ito, S. Kanamori, R. Nojima, and Y. Watanabe	４．巻 -
２．論文標題 State-free End-to-End Encrypted Storage and Chat Systems based on Searchable Encryption	５．発行年 2022年
３．雑誌名 ICEIS 2022	６．最初と最後の頁 312-323
掲載論文のDOI（デジタルオブジェクト識別子） 10.5220/0011045200003179	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Takeshi Nakai, Satoshi Shirouchi, Yuuki Tokushige, Mitsugu Iwamoto & Kazuo Oht	4．巻 ー
2．論文標題 Secure Computation for Threshold Functions with Physical Cards: Power of Private Permutations	5．発行年 2022年
3．雑誌名 New Generation Computing	6．最初と最後の頁 ー
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00354-022-00153-7	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Takeshi Nakai, Yuto Misawa, Yuuki Tokushige, Mitsugu Iwamoto & Kazuo Ohta	4．巻 39
2．論文標題 How to Solve Millionaires’ Problem with Two Kinds of Cards	5．発行年 2021年
3．雑誌名 New Generation Computing	6．最初と最後の頁 73-96
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00354-020-00118-8	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Atsushi Takayasu and Yohei Watanabe	4．巻 849
2．論文標題 Revocable Identity-based Encryption with Bounded Decryption Key Exposure Resistance: Lattice-based Construction and More	5．発行年 2021年
3．雑誌名 Theoretical Computer Science	6．最初と最後の頁 64-98
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2020.10.010	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Kohei Matsuda, Sho Tada, Makoto Nagata, Yuichi Komano, Yang Li, Takeshi Sugawara, Mitsugu Iwamoto, Kazuo Ohta, Kazuo Sakiyama, and Noriyuki Miura	4．巻 59
2．論文標題 An IC-level countermeasure against laser fault injection attack by information leakage sensing based on laser-induced opto-electric bulk current density	5．発行年 2020年
3．雑誌名 Japanese Journal of Applied Physics	6．最初と最後の頁 02-1-02-12
掲載論文のDOI（デジタルオブジェクト識別子） 10.7567/1347-4065/ab65d3	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Takeshi Nakai, Yuto Misawa, Yuuki Tokushige, Mitsugu Iwamoto, and Kazuo Ohta	４．巻 -
２．論文標題 How to Solve Millionaires' Problem with Two Kinds of Cards	５．発行年 2021年
３．雑誌名 New Generation Computing	６．最初と最後の頁 73-96
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00354-020-00118-8	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Kaoru Takemure, Yusuke Sakai, Bagus Santoso, Goichiro Hanaoka, and Kazuo Ohta	４．巻 LNCS12505
２．論文標題 Achieving Pairing-Free Aggregate Signatures using Pre-Communication between Signers	５．発行年 2020年
３．雑誌名 Proc. of ProvSec 2020	６．最初と最後の頁 65-84
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-62576-4_4	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Tomoki Uemura, Yohei Watanabe, Yang Li, Noriyuki Miura, Mitsugu Iwamoto, Kazuo Sakiyama, and Kazuo Ohta	４．巻 -
２．論文標題 A Key Recovery Algorithm Using Random Key Leakage from AES Key Schedule	５．発行年 2020年
３．雑誌名 Proc. of ISITA 2020	６．最初と最後の頁 382-386
掲載論文のDOI（デジタルオブジェクト識別子） 10.34385/proc.65.C01-10	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Yoshiki Abe, Mitsugu Iwamoto, and Kazuo Ohta	４．巻 -
２．論文標題 How to Detect Malicious Behaviors in a Card-Based Majority Voting Protocol with Three Inputs	５．発行年 2020年
３．雑誌名 Proc. of ISITA 2020	６．最初と最後の頁 377?381
掲載論文のDOI（デジタルオブジェクト識別子） 10.34385/proc.65.C01-9	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 渡邉 洋平	4．巻 65(9)
2．論文標題 検索可能暗号：データベースシステムの安全な運用に向けて	5．発行年 2020年
3．雑誌名 ケミカルエンジニヤリング	6．最初と最後の頁 552-560
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Y. Abe, M. Iwamoto, and K. Ohta	4．巻 LNCS11891
2．論文標題 Efficient Private PEZ Protocols for Symmetric Functions	5．発行年 2019年
3．雑誌名 Proc. Theory of Cryptography Conference (TCC2019)	6．最初と最後の頁 372-392
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-36030-6_15	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 K. Ohara, Y. Watanabe, M. Iwamoto, and K. Ohta	4．巻 E102.A
2．論文標題 Multi-Party Computation for Modular Exponentiation Based on Replicated Secret Sharing	5．発行年 2019年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1079-1090
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1079	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 K. Ohara, K. Emura, G. Hanaoka, A. Ishida, K. Ohta, and Y. Sakai	4．巻 E102.A
2．論文標題 Shortening the Libert-Peters-Yung Revocable Group Signature Scheme by Using the Random Oracle Methodology	5．発行年 2019年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1101-1117
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1101	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Yohei Watanabe, Yoshihisa Kuroki, Shinnosuke Suzuki, Yuta Koga, Mitsugu Iwamoto, Kazuo Ohta	4．巻 -
2．論文標題 Card-Based Majority Voting Protocols with Three Inputs Using Three Cards	5．発行年 2018年
3．雑誌名 Proc. International Symposium on Information Theory and Its Applications (ISITA2018)	6．最初と最後の頁 218-222
掲載論文のDOI（デジタルオブジェクト識別子） 10.23919/ISITA.2018.8664324	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計21件（うち招待講演　4件／うち国際学会　3件）

1．発表者名 植村 友紀，渡邉 洋平，李 陽，三浦 典之，岩本 貢，崎山 一男，太田 和夫
2．発表標題 AES鍵スケジュールからの固定ビット数漏洩を用いた鍵復元アルゴリズムの性能評価
3．学会等名 暗号と情報セキュリティシンポジウム（SCIS2021）
4．発表年 2021年

1．発表者名 渡邉 洋平，大原 一真，岩本 貢，太田 和夫
2．発表標題 より少ない漏洩の下で安全な動的検索可能暗号への変換手法
3．学会等名 コンピュータセキュリティシンポジウム（CSS）
4．発表年 2020年

1．発表者名 根岸 奎人，渡邉 洋平，岩本 貢
2．発表標題 視覚復号型秘密分散法における任意の改ざんを検知する手法
3．学会等名 暗号と情報セキュリティシンポジウム（SCIS2021）
4．発表年 2021年

１．発表者名
初貝 恭祐，安部 芳紀，中井 雄士，品川 和雅，渡邉 洋平，岩本 貢

２．発表標題
時間ドロボー問題に対する健全性誤りのない物理的ゼロ知識証明

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2021）

４．発表年
2021年

１．発表者名
中井 雄士，徳重 佑樹，岩本 貢，太田 和夫

２．発表標題
秘匿置換を用いたカードベースしきい値関数プロトコル

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2021）

４．発表年
2021年

１．発表者名
安部 芳紀，岩本 貢，太田 和夫

２．発表標題
対称関数を効率的に計算するPrivate PEZ プロトコル（from TCC 2019）

３．学会等名
電子情報通信学会ISEC研究会（招待講演）

４．発表年
2020年

１．発表者名
植村友紀，李陽，三浦典之，岩本貢，崎山一男，太田和夫

２．発表標題
鍵のランダムな漏洩に対するAES鍵スケジュール復元アルゴリズム

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
竹牟禮薫，坂井祐介，Bagus Santoso，花岡悟一郎，太田和夫

２．発表標題
事前通信モデルにおけるペアリングを用いない集約署名

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
品川和雅，三浦典之，岩本貢，崎山一男，太田和夫

２．発表標題
気泡検出器を用いたゼロ知識非破壊検査

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
安部芳紀，岩本貢，太田和夫

２．発表標題
任意の始集合を持つ関数を計算するprivate PEZプロトコル

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
渡邉洋平

２．発表標題
フォワード安全かつ検索時通信量が最適な動的検索可能暗号

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
安部芳紀，岩本貢，太田和夫

２．発表標題
任意の関数を計算するprivate PEZプロトコルの改善

３．学会等名
コンピューターセキュリティシンポジウム（CSS）2019

４．発表年
2019年

１．発表者名
渡邉洋平，大原一真，岩本貢，太田和夫

２．発表標題
(強)フォワード安全な動的検索可能暗号の効率的な構成

３．学会等名
コンピューターセキュリティシンポジウム（CSS）2019

４．発表年
2019年

１．発表者名
Kazuo Ohta

２．発表標題
Strong Forward Privacy for Dynamic Searchable Encryption

３．学会等名
Seminar at Google - Searchable Encryption Talk（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Kazuo Ohta

２．発表標題
Card-based Majority Voting Protocols with Three Inputs Using Three Cards

３．学会等名
the International Secure Multi-party Computation Forum（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Yoshiki Abe, Mitsugu Iwamoto, Kazuo Ohta

２．発表標題
How to improve the private PEZ protocol for general functions

３．学会等名
The 14th International Workshop on Security (IWSEC2019), poster session（国際学会）

４．発表年
2019年

１．発表者名
太田和夫

２．発表標題
現代暗号研究の事始め ～ 1つのケーススタディ ～

３．学会等名
情報理論・情報セキュリティ・ワイドバンドシステム合同研究会（招待講演）

４．発表年
2019年

１．発表者名
渡邉洋平，岩本貢，太田 和夫

２．発表標題
効率的でフォワード安全な動的検索可能暗号

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

１．発表者名
平野 貴人，川合 豊，小関 義博，岩本 貢，太田 和夫

２．発表標題
共通鍵型マルチユーザ検索可能暗号の検索機能拡張

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

１．発表者名
Wenjia Wang, Yoshiki Abe, Mitsugu Iwamoto, and Kazuo Ohta,

２．発表標題
Three-Party Private Set Operation Protocols Using Polynomials and OPPRF

３．学会等名
暗号と情報セキュリティシンポジウム (SCIS2019)

４．発表年
2019年

１．発表者名
Bagus Santoso and Kazuo Ohta.

２．発表標題
Another Look at One-More Discrete Logarithm Problem in Generic Model

３．学会等名
暗号と情報セキュリティシンポジウム (SCIS2019)

４．発表年
2019年

〔図書〕　計4件

１．著者名	４．発行年
Michael Sipser (著/文), 田中 圭介 (監修 | 翻訳), 藤岡 淳 (監修 | 翻訳), 阿部 正幸 (翻訳), 植田 広樹 (翻訳), 太田 和夫 (翻訳), 田中 圭介 (翻訳), 藤岡 淳 (翻訳), 渡辺 治 (翻訳)	2023年
２．出版社	５．総ページ数
共立出版	272
３．書名	
計算理論の基礎　[原著第3版] 1.オートマトンと言語	

１．著者名	４．発行年
Michael Sipser (著/文), 田中 圭介 (監修 | 翻訳), 藤岡 淳 (監修 | 翻訳), 阿部 正幸 (翻訳), 植田 広樹 (翻訳), 太田 和夫 (翻訳), 田中 圭介 (翻訳), 藤岡 淳 (翻訳), 渡辺 治 (翻訳)	2023年
２．出版社	５．総ページ数
共立出版	208
３．書名	
計算理論の基礎　[原著第3版] 2.計算可能性の理論	

１．著者名 Michael Sipser (著/文), 田中 圭介 (監修 | 翻訳), 藤岡 淳 (監修 | 翻訳), 阿部 正幸 (翻訳), 植田 広樹 (翻訳), 太田 和夫 (翻訳), 田中 圭介 (翻訳), 藤岡 淳 (翻訳), 渡辺 治 (翻訳)	４．発行年 2023年
２．出版社 共立出版	５．総ページ数 288
３．書名 計算理論の基礎　[原著第3版] 3.複雑さの理論	

１．著者名 太田 和夫, 岩本 貢, 渡邉 洋平 (取材協力)	４．発行年 2021年
２．出版社 Newton Press	５．総ページ数 28
３．書名 ニュートン別冊　数学の世界 現代編 増補第2版, 暗号 個人情報を守る数学	

〔出願〕　計0件

〔取得〕　計1件

産業財産権の名称 動的検索可能暗号処理システム及び動的検索可能暗号処理方法	発明者 渡邉洋平, 岩本貢, 太田和夫	権利者 情報通信研究機構, 電気通信大学
産業財産権の種類、番号 特許、特許第7276767号	取得年 2023年	国内・外国の別 国内

〔その他〕

―

６．研究組織

	氏名 (ローマ字氏名) (研究者番号)	所属研究機関・部局・職 (機関番号)	備考
研究分担者	岩本　貢 (Iwamoto Mitsugu) (50377016)	電気通信大学・大学院情報理工学研究科・教授 (12612)	
研究分担者	渡邉　洋平 (Watanabe Yohei) (40792263)	電気通信大学・大学院情報理工学研究科・助教 (12612)	

６．研究組織（つづき）

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	中井　雄士 (Nakai Takeshi) (00926389)	豊橋技術科学大学・工学研究科・助教 (13904)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関