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　２ 年　 ６ 月 ２８ 日現在

機関番号：２７３０１
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００１８９

研究課題名（和文）検索可能暗号の秘密鍵更新メカニズムの解析と設計と評価

研究課題名（英文）Key Updatable Searchable Encryption: Concept, Scheme and Evaluation

研究代表者
松崎　なつめ（Matsuzaki, Natsume）

長崎県立大学・情報システム学部・教授

研究者番号：１０７８１８９１

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：検索可能暗号は，クラウドに預託した暗号文から暗号化したクエリを用いて暗号化したまま所望の情報を検索可能とする暗号である．2000年から研究が開始されて以降，高機能暗号の中でも実用化に近い技術として盛んに研究されている．本研究では，検索可能暗号のIoT環境での実用化を想定し，モバイル機器からの鍵漏洩（鍵紛失や盗難）に対策するため，モバイル機器内の秘密鍵を更新可能な検索可能暗号を，コンセプト，要件と方式を研究し，実装と安全性の面で評価する．3年間の研究期間において，国内外研究会／シンポジウム（査読なし）を計9件，国際会議1件（＋現在投稿中1件），国際ジャーナル1件の成果を上げた．

研究成果の学術的意義や社会的意義
例えばスマートフォンの位置情報などをクラウドに預託し，後日預託した中から特定の情報を検索する場合を想定する．預託する情報の多くは，個人のプライバシを含むため，暗号化したままクラウドにて検索する「検索可能暗号」が有用となる．本研究では，IoT環境での実用化を想定し，クライアントデバイス（上記例では，スマートフォン）内の暗号鍵が漏洩したり紛失した場合の対策として，デバイス内の秘密鍵を更新可能な「鍵更新機能付き検索可能暗号」を初めて開発した．

研究成果の概要（英文）：Searchable encryption enables a client to search over encrypted data in a server using a specific keyword, while keeping the keyword secret. Since the research started in 2000, it has been actively researched as a technology close to practical use in advanced cryptography using cloud technology. In this research, we first develop "key updatable searchable encryption" that can update the private key in the mobile device to prevent the key leakage (caused by loss of theft of the device) in the IoT environment. We study a concept, schemes and evaluate them in terms of implementation and safety. During the three-year research period, we achieved the results of 9 papers without peer review, 1 paper with peer review of international conference (and additionally 1 paper currently submitted), and 1 paper of international journal.

研究分野：暗号技術

キーワード：検索可能暗号　鍵更新機能　IoT　鍵漏洩対策

１．研究開始当初の背景

(1) 検索可能暗号

検索可能暗号は，クラウドに預託したインデックス付きの暗号文から，暗号化したクエリを用いて所望の情報を暗号化したまま検索可能とする暗号であり，高機能暗号の中でも実用化に近い技術として盛んに研究されている．検索可能暗号は，2000 年に Song, Wagner, Perrig によって提案され，インデックスの暗号化とクエリの暗号化に共通の鍵を用いる共通鍵系（Searchable Symmetric Encryption : SSE）と，異なる鍵を用いる公開鍵系（Public Key Encryption with Keyword Search : PEKS）に分類される．SSE の代表的な方法は，2006 年に Cultmola らにより提案された．その後，インデックスの追加を可能とする方式，類似検索が可能な方式，ドキュメントやクエリの秘匿性に関する安全性証明やクラウドの不正を監視可能な方式など，様々な側面にわたって活発に研究がされている．また，PEKS は，ID ベース暗号の応用の位置づけで 2004 年 Boneh らが双線形ペアリングを用いた方式を提案した．PEKS は SSE に比べ，ID ベース暗号の安全性証明に関する研究実績を適用可能である一方，暗号化や検索の処理時間等，実用面で課題がある．

(2) IoT 環境

検索可能暗号では，クライアント側で保有する鍵を用いて，暗号文を作成し，またクエリの暗号化を行う．従来の研究では，このクライアント側の鍵が安全に保管されているとの前提のもと，主にクラウドの攻撃に対して安全な方式が検討されてきた．今後，検索可能暗号の IoT 機器での適用を考えると，加えてクライアントからの鍵漏洩対策が必要となる． なぜならば，スマートフォンなどのように IoT 機器が持ち運び可能な機器である場合には，機器の盗難や紛失による鍵の漏洩の危険があるからである．また，コスト的な制約により IoT 機器内の鍵の耐タンパー実装を突破される危険もある．本研究では，検索可能暗号におけるクライアント側の鍵漏洩対策に着目する．

(3)鍵管理

鍵管理とは，鍵漏洩対策を含む，暗号に用いる鍵の生成から更新，廃棄までを設計・運用することにより，暗号システムの安全性を維持する方式であり，暗号研究をさらに実用化に向けて深化するには必須の研究領域である．暗号方式における鍵管理の研究は，米国国立標準技術研究所（NIST）による SP800-57 など，方式やその運用の標準化がすすめられすでに成熟しているが，検索可能暗号をはじめとする高機能暗号においては未着手であった．

本研究では，検索可能暗号における鍵管理，特にクライアントからの鍵漏洩対策の１つとして，鍵の更新に着目する．鍵を定期的／不定期に更新し，漏洩の可能性のある以前の鍵は削除することにより，暗号システムの安全維持を実現する．

２．研究の目的

本研究の目的は次のとおりである．鍵更新機能付き検索可能暗号は，筆者の知る限り初めてのコンセプトであり要件，方式，評価までを以下の通り研究して提供する．

(1) 具体的な UseCase を考慮し，鍵更新機能付き検索可能暗号における課題を明確化する
(2) 鍵更新時におけるセキュリティ要件とシステム要件を明確化する
(3) 公開鍵系と共通鍵系それぞれで具体的な方式を提示する
(4) 安全性の定義を行い，提案した方式の安全性を評価する
(5) IoT 機器を想定し，例えばラズベリーパイで実装して評価する
(6) (3)で提示した方法に関し，(4)(5)で安全性と実装性の評価をしたうえで，(1)(2)の課題と要件と照らし合わせ，全体を取りまとめたうえで，残課題と将来拡張について検討する．

３．研究の方法

(1) 研究体制

研究は研究代表の松崎（全体推進，方式設計，評価），研究分担者の穴田氏（方式設計，安全性評価）と金岡氏（方式設計，実装評価）の 3 人で議論し，分担して進めた．

(2) 研究スケジュール

◆ 2017 年度：
・鍵更新機能付き検索可能暗号のモデル，コンセプトと課題を明確化
・公開鍵系の鍵更新機能付き検索可能暗号（KU-PEKS）の課題解決アプローチの検討，安全性の定義，具体的方式について提案

◆ 2018 年度
・2017 年に引き続き，KU-PEKS の具体的方式の評価
・共通鍵系の鍵更新機能付き検索可能暗号（KU-SSE）の課題解決アプローチの検討

◆ 2019 年度
・KU-SSE の安全性の定義，具体的方式，評価

４．研究成果

(1) 成果要約

本研究では，検索可能暗号の IoT 環境での実用化を想定し，モバイル機器からの鍵漏洩（鍵紛失や盗難）に対策するため，モバイル機器内の秘密鍵を更新できる検索可能暗号を，そのコンセプトから方式を研究し，実装と安全性の面で評価する．3 年間の研究期間において，国内外研究会／シンポジウム（査読なし）を計 9 件，国際会議 1 件（＋現在投稿中 1 件），国際ジャーナル 1 件の成果を上げた．

(2) 検索可能暗号の秘密鍵更新メカニズムのコンセプト，要件の提示

鍵更新機能付き検索可能暗号においては，クライアント側の鍵更新に伴ってクラウドに暗号文を預託した時に用いた鍵バージョンと，その後のクエリに用いる鍵バージョンの整合性が課題となる．

本研究では，上記鍵バージョンでの整合性に関し，実用性に即し，次の２つの要件(a)(b)を設定している．なお，これら要件の前提としては，クライアント側の鍵更新のたびに，クラウド側の膨大な数の暗号文をすべて最新バージョンの鍵に対応した暗号文に作り直すことは困難であると仮定している．その理由は，暗号文の容量が膨大であることに加え，暗号文を書き換えることは，クラウド側のデータ保存方法を制約することになるためである．

(a) 古い鍵で暗号化した暗号文は，新しい鍵で暗号化したクエリで検索可能

この要件は，クライアント鍵を更新するときに， 古いクライアント鍵をクライアントから削除することを推奨／許容するためである．古いクライアント鍵は漏洩の可能性があるため，安全性のためクライアントから削除することが推奨される．

また，セキュア実装領域が制約される IoT 機器に実装される場合，記憶容量を節約するため古い鍵を削除してもよいとするのが妥当である．このため，新しい鍵だけを用いて，古い鍵で暗号化した暗号文を対象に検索できることが必要である．

(b) 新しい鍵で暗号化した暗号文は，古い鍵で暗号化したクエリで検索不可

この要件は，クライアント鍵を更新するときに，漏洩の可能性がある古いクライアント鍵を使えなくする（無効化する）ためである．古いクライアント鍵は，もしその鍵が漏洩したとしても，同じバージョンの鍵を用いた古い暗号文を検索可能となる．次善策として，本要件では，少なくとも新しい鍵で暗号化した暗号文は，漏洩の可能性のある古い鍵で暗号化したクエリを用いて検索不可とする．

本研究では，上記要件に従い，実用上妥当な安全性を定義したうえで，安全性を確保して上記整合性を合わせるための，変換部の追加を検討する．

また，鍵更新機能付き検索可能暗号は，基にする検索可能暗号の分類に従って，鍵更新機能付き共通鍵系 SSE（KU-SSE)と公開鍵系 PEKS（KU-PEKS）に分類され，以下の(3)(4)において，それぞれの研究成果を示す．

(3) 公開鍵系の鍵更新機能付き検索可能暗号（KU-PEKS）の開発

KU-PEKS のコンセプト，要件と安全性の定義を行い，２つのモデル（公開鍵更新モデル，鍵隔離モデル）のそれぞれにおいて具体的な方式の提案と安全性の証明と，IoT での実装を想定しラズベリーパイ上での処理時間の評価を行った．KU-PEKS での方式は，鍵バージョンを整合するための変換部は，暗号文側に備える．

２つのモデルのうち，公開鍵更新モデルは，クライアント側の秘密鍵の更新に伴い，対応する公開鍵も更新して公開する必要がある一方，シンプルな構成になる．公開鍵更新モデルは，一般的な公開鍵暗号と検索可能暗号を組み合わせて構成される．また 鍵

隔離モデルは，クライアント側の秘密鍵を更新しても対応する公開鍵を不変にするため，新しい公開鍵の公開や古い公開鍵の無効化を含む運用コストが削減でき，実用に近いモデルとなる．鍵隔離モデルは，一般的な鍵隔離暗号と鍵隔離型検索可能暗号を組み合わせて構成される．後者は前者に比べ実装規模が大きくなる一方，上記述べた通り，運用コストを削減できる． 研究の成果は， 国内外研究会／シンポジウム（査読なし）を 6 件，国際会議 1 件，国際ジャーナル 1 件である．

(4) 共通鍵系の鍵更新機能付き検索可能暗号（KU-SSE）の開発

KU-SSE のコンセプト，要件と安全性の定義を行い，既存の 3 種類の SSE 方式（(1) ヘルパー鍵を用いて暗号化クエリを変換する方法 (2) 共通鍵系隠れベクトル暗号を用いる方法 (3) 乱数関数を用いる方法）をそれぞれ拡張して，KU-SSE の具体的な方式の提案と安全性の証明，ラズベリーパイ上での処理時間の評価を行った．KU-PEKS の方式が，一般的な PEKS 等を組み合わせて一律的に構成できるのに比べ，KU-SSE は，個々の SSE の方式に依存した方法で構成している．研究の成果は， 国内外研究会／シンポジウム（査読なし）を 3 件，国際会議投稿中 1 件である．

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Hiroaki Anada, Akira Kanaoka, Natsume Matsuzaki and Yohei Watanabe	４．巻 10946
２．論文標題 Information Security and Privacy	５．発行年 2018年
３．雑誌名 23rd Australasian Conference, ACISP 2018, Wollongong, NSW, Australia, July 11-13, 2018, Proceedings(Springer)	６．最初と最後の頁 341-359
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-93638-3	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 Hiroaki Anada, Akira Kanaoka, Natsume Matsuzaki & Yohei Watanabe	４．巻 19
２．論文標題 Key-updatable public-key encryption with keyword search (Or: How to realize PEKS with efficient key updates for IoT environments)	５．発行年 2020年
３．雑誌名 International Journal of Information Security	６．最初と最後の頁 15-38
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/s10207-019-00441-2	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 －

〔学会発表〕　計9件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 松崎なつめ，穴田啓晃
２．発表標題 鍵更新機能付き共通鍵型検索可能暗号の一実現方式
３．学会等名 電子情報通信学会ISEC研究会
４．発表年 2019年

１．発表者名 松崎なつめ，穴田啓晃，金岡晃
２．発表標題 鍵更新機能付き共通鍵型検索可能暗号の一実現　～委譲可能擬似乱数関数を用いた実現方式～
３．学会等名 暗号と情報セキュリティシンポジウム　SCIS2020
４．発表年 2020年

１．発表者名
Hiroaki Anada, Akira Kanaoka, Natsume Matsuzaki and Yohei Watanabe

２．発表標題
Key-updatable Public-key Encryption with Keyword Search : An Efficient Construction

３．学会等名
Poster session on IWSEC 2018 (Information Workshop on Security)（国際学会）

４．発表年
2018年

１．発表者名
松崎 なつめ, 穴田 啓晃, 金岡 晃, 渡邉 洋平

２．発表標題
鍵更新機能付き検索可能暗号：効率化に向けた一工夫

３．学会等名
CSS2018 (Computer Security Symposium)

４．発表年
2018年

１．発表者名
松崎 なつめ, 穴田 啓晃

２．発表標題
鍵更新機能付き共通鍵型検索可能暗号に向けて

３．学会等名
SCIS2019 (Symposium on Cryptography and Information Security)

４．発表年
2019年

１．発表者名
松崎なつめ, 穴田啓晃, 渡邉洋平

２．発表標題
鍵更新可能な検索可能暗号の一提案　～検索可能代理人再暗号化の適用について～

３．学会等名
電子情報通信学会　情報セキュリティ研究会　ISEC2017-1

４．発表年
2017年

１．発表者名 松崎なつめ，穴田啓晃，渡邉洋平
２．発表標題 鍵更新機能付き検索可能暗号：公開鍵更新モデルによる実現
３．学会等名 コンピュータセキュリティシンポジウムCSS2017
４．発表年 2017年

１．発表者名 渡邉洋平，穴田啓晃，松崎なつめ
２．発表標題 鍵更新機能付き検索可能暗号：鍵隔離モデルによる実現
３．学会等名 コンピュータセキュリティシンポジウムCSS2017
４．発表年 2017年

１．発表者名 松崎なつめ，穴田啓晃，金岡晃，渡邉洋平
２．発表標題 鍵更新機能付き検索可能暗号の一般的構成
３．学会等名 暗号と情報セキュリティシンポジウムSCIS2018
４．発表年 2018年

〔図書〕　計0件

〔産業財産権〕

〔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	穴田　啓晃 (Anada Hiroaki) (40727202)	長崎県立大学・情報システム学部・教授 (27301)	

６．研究組織（つづき）

	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	金岡　晃 (Kanaoka Akira) (00455924)	東邦大学・理学部・准教授 (32661)	