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　 ６ 日現在

機関番号：１２１０１
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００１７７

研究課題名（和文）アクセス情報も秘匿するキーワード検索可能暗号

研究課題名（英文）Access pattern hiding searchable symmetric encryption scheme

研究代表者
黒澤　馨（Kurosawa, Kaoru）

茨城大学・理工学研究科（工学野）・教授

研究者番号：６０１５３４０９

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）：キーワード検索可能暗号では、ユーザは検索キーワードを秘密にしたまま、それを含むファイルを取り出したい。Private information retrieval (PIR)では、ユーザはインデックスiを秘密にしたまま、データベースX = (x_1, . . . , x_n)からx_iを取り出したい。本研究では、まず、任意のPIR方式とカッコーハッシュを組み合わせると、ユーザはキーワード集合を記憶しておくことなく、アクセス情報も秘匿できるキーワード検索可能暗号を構成できることを示した。次に、b重誤り訂正Lサーバ PIR 方式に対し、計算量がLの3乗のオーダーで済む効率のよい復号法を開発した。

研究成果の学術的意義や社会的意義
クライアントは、暗号化したファイルの集合をサーバに格納しておき、検索キーワードを秘密にしたままそのキーワードを含むファイルを取り出したい。このように、情報セキュリティと利便性という相反する２つの目的を両立させる暗号方式をキーワード検索可能暗号方式という。本研究では、まず、カッコーハッシュとprivate information retrieval(PIR)を組み合わせると、ユーザはキーワード集合を記憶しておくことなく、アクセス情報も秘匿できるキーワード検索可能暗号を構成できることを示した。次に、b重誤り訂正Lサーバ PIR 方式に対し計算量がLの3乗のオーダーで済む効率のよい復号法を開発した。

研究成果の概要（英文）：In the model of searchable symmetric encryption schemes, the user wants to obtain the files which includes the keyword keeping the keyword and files secret. In the model of private information retrieval (PIR), a server S holds a database x = (x1, . . . , xn) ∈{0, 1}n, and a user holds a secret index i_0. The user should be able to retrieve x_{i_0} without revealing no information on i_0. In this research, it is shown that we can construct a searchable symmetric encryption scheme which can hide even the access pattern from the server by combining any PIR scheme with cuckoo hashing, where the user does not need to keep the set of keywords. Further in the information theoretic setting, an efficient decoding algorithm is shown for a b error correcting L server PIR scheme. It runs in time O(L .

研究分野：現代暗号理論

キーワード：暗号　キーワード検索　アクセス情報

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

(1) クラウドサービスは近年著しく発展しているが、その一方で情報漏洩事故も多数報告されている。また、スノーデン氏による暴露も記憶に新しい。このような状況において、以下のような機能を有する暗号方式（図１）は多くの応用可能性を有すると考えられている。

格納フェーズにおいて、クライアントはサーバに共通鍵暗号で暗号化したファイルの集合を格納する。検索フェーズにおいて、クライアントは検索キーワードを秘密にしたまま、そのキーワードを含むファイルを取り出す。このように、情報セキュリティと利便性という相反する２つの目的を両立させる暗号方式を、キーワード検索可能暗号方式という。

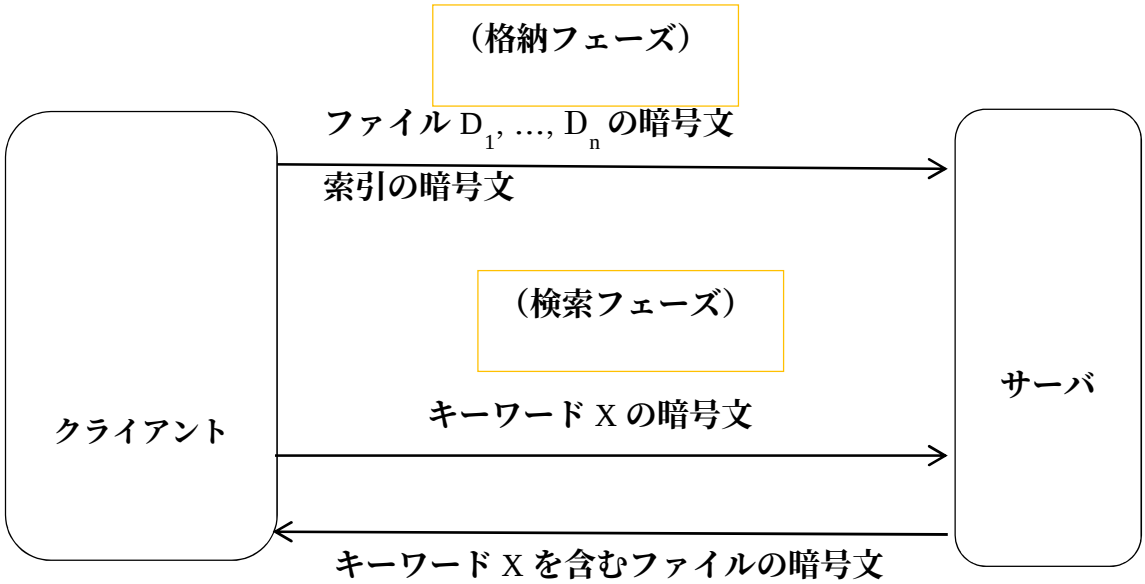

図１．キーワード検索可能暗号方式

最初のキーワード検索可能暗号方式は、2000 年に Song, Wagner, Perrig によって提案された。その後、ファイルの更新や追加を可能とする動的方式に関する研究、複数キーワードの AND 検索や OR 検索を可能とする方式に関する研究など、様々な側面にわたって活発に研究が行われてきた。

(2) 研究代表者は、秘匿性のみならず、ファイルの改ざん、削除、すり替えなど、サーバの能動的な不正をも防ぐ（信頼性）キーワード検索可能暗号方式を世界で初めて構成した。また、秘匿性と信頼性の両方を満たすことと、（いかなる環境下でも安全性が成り立つという）UC 安全性という非常に強い安全性が等価であることを証明した。さらに、UC 安全性を満たし、かつファイルの更新や追加を可能とする動的キーワード検索可能暗号方式を構成するとともに、AND 検索なのか OR 検索なのかも秘匿できる複数キーワード検索可能暗号方式を構成した。

２．研究の目的

検索フェーズにおいては、以下のようなアクセスパターン情報（表１）がサーバに漏れてしまう。まず、検索キーワード X に対しサーバがファイルの暗号文 C1, C3, C5 を返したとすると、添字の集合(1,3,5)がサーバに漏れているということになる。このような情報をデータパターンと呼ぶ。また、クライアントが同じキーワードを２回質問したといった情報が漏

れる。これを検索パターンと呼ぶ。これら２種類のアクセスパターン情報は最小漏洩情報とも呼ばれ、避けることができないと信じられてきた。

一方、サーバがキーワードの統計的情報など何らかの補助情報を知っていたとすると、アクセスパターン情報からだけでも検索キーワードを特定できてしまうということも知られている。

単にアクセスパターン情報を漏らさないだけなら、oblivious RAM というテクニックを使うと一応実現することができる。ここで、oblivious RAM とは、ランダム・アクセス・メモリ(RAM)への読み書きのアクセスパターンを秘匿する方法である。しかしこの方法は、1回の検索に log n ラウンドの通信と O(log n)の通信量を必要とし、非常に効率が悪い（n はデータ数）。

表１．アクセスパターン情報

データパターン	キーワード X を含むファイルの添字の集合が(1,3,5)であるという情報
検索パターン	同じキーワードを２回質問した、といった情報

本研究では、アクセスパターン情報すら極力秘匿し、かつ効率の良いキーワード検索可能暗号方式を構成することを目的とする。（単なる）キーワード検索方式に比べ、（単なる）RAM ははるかに basic な primitive であり、両者は等価でない。したがって、oblivious RAM を使うキーワード検索可能暗号方式より、もっと効率良くアクセスパターン情報の漏洩を防ぐことができるはずである。このような視点に基づき、以下のような研究を行う。

(1) データパターンを極力秘匿するような効率の良いキーワード検索可能暗号方式を開発する。
(2) 検索パターンを極力秘匿するような効率の良いキーワード検索可能暗号方式を開発する。
(3) さらに、それらをサーバの能動的な不正も検証可能な方式、および複数キーワードの AND/OR 検索も可能な方式に拡張する。

３．研究の方法

本研究では、アクセスパターン情報すら極力秘匿し、かつ効率の良いキーワード検索可能暗号方式を構成する。そのため、以下の計画、方法に基づいて研究を遂行する。

(1) アクセスパターン情報を利用した不正サーバの具体的な攻撃法を調査する。実際的な目標としては、そのような実害の起こらない程度に情報漏洩が抑えられればよい。
(2) （アクセスパターン情報の秘匿に適した）ファイルの暗号文、および索引の暗号文をサーバに格納するための新たなデータ構造を開発する。
(3) 上記に基づき、 (非効率な oblivious RAM を使用しない) キーワード暗号化検索のための新たなアルゴリズムを開発する。

４．研究成果

(1) キーワード検索可能暗号方式の安全性は、秘匿性、検証可能性、UC 安全性(universally composeble 安全性、汎用結合安全性)の３つに大別することができる。サーバがファイル、キーワード、索引について何もわからないとき、秘匿性を満たすという。サーバが偽りの検索結果を返したかどうかをクライアントが検出できるとき、検証可能性を満たすという。ど

んな複雑なシステムに組み込まれたとしても安全性が維持されるとき、UC 安全性を満たすという。研究代表者は、既に、秘匿性、検証可能性の両者を満たすことと UC 安全性を満たすことが等価であることを証明している。

また、キーワードの集合を辞書と呼ぶこととする。（たとえば、辞書={Austin, Boston, NY}。）また、クライアントが辞書を覚えておく必要がある方式を辞書あり方式、そうでない方式を辞書無し方式と呼ぶ。

さて、辞書無し方式において、クライアントが辞書に無いキーワード（たとえば、LA）でキーワード検索可能暗号方式の検索フェーズを走らせたとする。すると、サーバは、「ヒットするファイル無し」と回答することになる。このとき、本当にヒットするファイルが無いのか、本当は有るのにサーバがウソをついているのか、クライアントは区別がつかない。

本研究では、まず、この問題を解決できる方式を開発した。さらに、より一般的に、秘匿性のみを満たす任意の方式を、辞書無しで UC 安全性を満たす方式に変換する方法を示した。

(2) Private Information Retrieval (PIR)のモデルにおいては、sender は n ビットのデータベース($x_1,\cdots,x_n$)を持っている。Receiver はi_0を秘密にしたまま、x_{i_0}を取り出したい。自明は方法は、sender が($x_1,\cdots,x_n$)全体を receiver に送ることである。これより少ない通信量で実現したい。ある計算量的仮定の下で、通信量が$O((\log n)^2)$で済む PIR 方式が知られている。

検索フェーズが以下の 2 つのサブプロトコルから構成されるキーワード検索可能暗号方式をを考える。まず、クライアントは、検索キーワードを含むファイルのインデックスの集合を得る。次に、クライアントは、それらのインデックスを有するファイルの暗号文を入手する。

本研究では、任意の PIR 方式を基に、検索パターンを秘匿できる辞書無しキーワード検索可能暗号方式を構成できることを示した。これは、1 番目のサブプロトコルに PIR を組み込むことにより得られる。さらに、2 番目のサブプロトコルにも同様に PIR を組み込むと、データパターンも秘匿できる。この方法は、(1)の構成を拡張して得られている。

(3) 最後に、計算量的な仮定をしない情報理論的 PIR について、以下の結果を得た。情報理論的 PIR おいては、通信量を n ビット未満にすることはできないことが証明されている。一方、サーバを複数にし、各サーバは n ビットのデータベース($x_1,\cdots,x_n$)のコピーを持つとすると、通信量を n ビット未満にすることができることが知られている。

(k,ℓ) robust PIR 方式においては、ℓ台中 k 台のサーバが応答すれば、クライアントはx_{i_0}を取り出すことができる。Woodruff and Yekhanin は、通信量が$O(n^{1/(2k-1)}\times k\ell\log\ell)$で済む(k,ℓ) robust PIR 方式を示した。b 重誤り訂正ℓサーバ PIR 方式においては、ℓ台中 b 台のサーバが誤った応答を返してたとしても、クライアントは正しくx_{i_0}を取り出すことができる。Beimel and Stahl は、$\ell\geq k+2b$なら、(k,ℓ) robust PIR 方式を b 重誤り訂正ℓサーバ PIR 方式として使うことができることを示した。しかし、彼らの復号法は、効率が非常に悪い。以上を要約すると、$\ell\geq k+2b$の場合、通信量が$O(n^{1/(2k-1)}\times k\ell\log\ell)$で済む b 重誤り訂正ℓサーバ PIR 方式が存在するが、その復号法の効率は非常に悪い、ということになる。

本研究では、上記の b 重誤り訂正ℓサーバ PIR 方式に対し、効率の良い復号法を示した。その計算量は、$O(\ell^3)$である。本復号法は、リードソロモン符号に対する Berlekamp-Weltch 復号法を拡張することにより得られる。

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3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 Wakaha Ogata and Kaoru Kurosawa	４．巻 102-A (1)
２．論文標題 No-Dictionary Searchable Symmetric Encryption	５．発行年 2019年
３．雑誌名 IEICE Transactions (1)	６．最初と最後の頁 114-124
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.114	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 Wakaha Ogata, Kaoru Kurosawa	４．巻 LNCS 10322
２．論文標題 Efficient No-dictionary Verifiable Searchable Symmetric Encryption	５．発行年 2017年
３．雑誌名 Financial Cryptography 2017, LNCS 10322, Springer	６．最初と最後の頁 498-516
掲載論文のDOI（デジタルオブジェクト識別子） 1007/978-3-319-70972-7_28	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 Kaoru Kurosawa	４．巻 LNCS 11922
２．論文標題 How to Correct Errors in Multi-server PIR	５．発行年 2019年
３．雑誌名 ASIACRYPT 2019 (2)	６．最初と最後の頁 564-574
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-34621-8_20	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1件（うち招待講演　1件／うち国際学会　0件）

１．発表者名 黒澤馨
２．発表標題 辞書なし検索可能暗号について
３．学会等名 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）（招待講演）
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