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　元 年　 ５ 月　 ８ 日現在

機関番号：１５４０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１８７

研究課題名（和文）クラウドコンピューティングにおける高機能暗号の安全性向上および効率化

研究課題名（英文）High-functional cryptosystems with more security and efficiency in cloud computing

研究代表者
中西　透（Nakanishi, Toru）

広島大学・工学研究科・教授

研究者番号：５０３０４３３２

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：クラウドコンピューティングでは，サーバ管理者による情報漏洩がありうるため，従来の暗号技術より高度な機能をもつ高機能暗号の研究が盛んに行なわれている．しかし，そのような高機能暗号の一つである検索可能暗号では，サーバが検索されるキーワードを推測できてしまうという安全性の問題がある．また，サーバでの暗号状態計算を検証する方式が提案されているが，大量の公開パラメータを必要とする問題がある．本研究では，キーワード推測を防止した検索可能暗号を提案する．また，公開パラメータサイズを大きく軽減した暗号状態計算検証方式を提案し，レピュテーションシステムへ応用する．

研究成果の学術的意義や社会的意義
本研究の学術的意義は、従来の方式では実現できていなかった，クラウド環境における検索可能暗号の新しい安全性の実現，および暗号状態計算検証における公開パラメータサイズの削減である．さらに，方式提案だけではなく，安全性保証とともに，プライバシー保護技術への応用や実装も意義があるといえる．本研究により，安全性と効率性を両立したクラウドコンピュティングの実現が可能となると考える．

研究成果の概要（英文）：In cloud computing, a server can reveal some information, and thus high-functional cryptosystems have been intensively researched, which has higher functions than conventional cryptosystems. However, in searchable encryptions of high-functional cryptosystems, there is a security problem that a server can guess searched keywords. On the other hand, a verification scheme to check encrypted computations has been proposed, but it needs lots of public parameters. In this research, we propose a searchable encryption secure against the keyword-guessing attack. Additionally, we propose a verification scheme for encrypted computations where public parameters are greatly reduced, and apply it to reputation systems.

研究分野：情報セキュリティ

キーワード：高機能暗号　プライバシー保護

様　式　C－１９、F－１９－１、Z－１９、CK－１９（共通）

１．研究開始当初の背景

モバイル端末の普及により，データをサーバ上に保存してサービスをオンラインで利用するクラウドコンピューティングの利用が進んでいる．クラウド環境では，外部のクラウドサーバにコンテンツデータが保存されるが，不正アクセスによる情報漏洩を防ぐために暗号化が必要となる．現在，クラウドサーバ側で暗号化・アクセス制御が行なわれているが，サーバの管理者によるデータの覗き見の可能性がある．また，海外のクラウドサーバでは国家レベルでの検閲の可能性もある．このような問題への対策は，送信者・受信者の二者間の通信を想定した従来の暗号技術では不十分であり，より高機能な暗号技術の開発が求められている．

クラウド環境に適した高機能暗号として，検索可能暗号が盛んに研究されている．通常の暗号と異なり，検索可能暗号では，ユーザは秘密鍵から各検索キーワードに対応した検索秘密鍵を生成する．暗号文は，キーワードの検索暗号文から成る．ユーザが検索したいキーワードの検索秘密鍵をクラウドサーバに渡し，サーバは検索暗号文のキーワードと検索秘密鍵のキーワードが等しいかどうかのみチェックすることができる．これにより，クラウドサーバへ暗号化したコンテンツを保存しておき，サーバがキーワードやコンテンツを把握することなく，ユーザがキーワード検索を行なうことができ，必要なデータのみをダウンロードできるようになる．しかし，従来提案されている検索可能暗号では，サーバが検索されるキーワードを辞書攻撃することにより推測できてしまうため，安全性に問題がある．

また，クラウドサーバに保存した大量のデータに対して，暗号化したま加算演算を行なう暗号状態計算の研究がされている．これにより，サーバには各データを秘匿したまま，計算を委託することができる．この暗号状態計算では，サーバが正しく暗号文演算を行なっていない場合，正しくない計算結果となってしまうため，暗号状態計算の正当性検証が必要となる．そこで，暗号状態計算の正当性を検証可能な準同型署名方式が提案されている．しかし，この従来方式では，大量の公開パラメータを必要としてしまうため，その実用性に問題がある．

２．研究の目的

本研究では，キーワード推測攻撃を防止した検索可能暗号を新たに提案して，その安全性を示す．また，従来方式を改良することにより，公開パラメータサイズを大きく軽減した暗号状態計算検証方式を提案する．そして，PC 上で構築した方式をプロトタイプ実装し，実環境での実用性を示す．さらに，暗号状態計算の応用として，プライバシーを保護したレピュテーションベースの匿名認証についても検討する．

３．研究の方法

(1) 検索可能暗号における安全性の向上

従来の公開鍵ベース検索可能暗号の基本構成は以下となる．キーワード w の暗号文はペア $(A,B)=(g^r, e(H(w),PK)^r)$ として計算される．ここで，g は公開された定数パラメータ，r は暗号文作成のための乱数，$PK=g^x$ は秘密鍵 x に対する公開鍵，H はハッシュ関数，e はペアリングである．一方，キーワード w' の検索秘密鍵 C は，秘密鍵 x を用いて，$C=H(w')^x$ として計算される．このとき，キーワードの等価性チェックは，$e(C,A)=B$ が成立するかのチェックとなる．これは，ペアリングの双線形性により，左辺が $e(H(w')^x, g^r)=e(H(w'),PK)^r$ となり，$w=w'$ であるときかつそのときのみ，チェックの検証式が成立するためである．しかし，公開鍵 PK はすべての参加者が利用できるため，クラウドサーバも，任意のキーワード w に対して検索暗号文を生成可能である．このため，キーワードが乱数でない状況では，キーワードの辞書を用いて，すべてのキーワードの暗号文を生成し，等価性チェックを行なうことにより，検索秘密鍵のキーワード w' を推測できてしまう．

そこで本研究では，検索秘密鍵を作成するユーザが，暗号化を行なうことができるユーザを限定できる方式を提案する．従来の基本構成において，$B=e(H(w),PK)^r$ によりキーワードと検索可能ユーザの公開鍵 PK がバインドされている．この $H(w)$はハッシュ関数によりキーワードに係らず乱数を出力するが，キーワードがランダムでないため，キーワードの総当たり攻撃が可能となっている．そこで，乱数 K に対して $H(K|w)$のように計算することを考える．ここで，この K は指定された暗号化ユーザしか作れないようにする．複数の復号ユーザを指定できる暗号として放送型暗号がある．この放送型暗号の暗号文 D を検索可能暗号の公開鍵として設定することを考える．放送型暗号では，指定された復号ユーザのみが復号して，ランダムなセッション鍵 K_{Brod} を導出できる．この K_{Brod} を従来の検索暗号方式での K の代わりに用いることを考える．すると，検索暗号文暗号文は $(A,B)=(g^r, e(H(K_{Brod}|w),PK)^r)$として計算されることになる．一方，放送型暗号では，暗号文 D を生成する者も K_{Brod} を導出できるため，検索秘密鍵を $C=H(K_{Brod}|w')^x$ と設定できる．このとき，キーワード同一性のチェックは，従来構成と同様に $e(C,A)=B$ でよい．この放送型暗号を用いた拡張により，放送型暗号 D を復号できる者しか K_{Brod} を導出できないために，検索暗号文(A,B)は指定されたユーザしか作成できなくなっている．こうして，クラウドサーバも作成できず，従来構成での安全性の問題点が解決される．

(2) 暗号状態計算における正当性検証の効率化

従来の暗号状態計算の検証方法は以下の通りである．準同型性をもつ署名を用いる場合，$Sig(E(M_1+M_2+\cdots+M_n))=Sig(E(M_1))Sig(E(M_2))\cdots Sig(E(M_n))$となるが，同一署名の加算を繰り返すことにより，任意の非負整数 $w_1,w_2,\cdots,w_n$ に対して $Sig(E(M_1^{w1}+M_2^{w2}+\cdots+M_n^{wn}))=Sig(E(M_1))^{w1}Sig(E(M_2))^{w2}\cdots Sig(E(M_n))^{wn}$ となるため，この署名だけでは単純には加算結果であるかの検証ができない．このため，この署名では複数のメッセージに署名できることを利用して，各暗号文 $E(M_i)$ の署名を $Sig(E(M_1),g,1,\cdots,1),Sig(E(M_2),1,g,1,\cdots 1),\cdots,Sig(E(M_n),1,\cdots 1,g)$ として計算する．すると，これらの署名同士を演算すると，$Sig(E(M_1^{w1}+M_2^{w2}+\cdots+M_n^{wn}),g^{w1},g^{w2},\cdots,g^{wn})$となるため，平文メッセージ部の $w_1,w_2,\cdots w_n$ がすべて１であることを検証することにより，$E(M_1+M_2+\cdots+M_n)$の署名であることが確認できる．しかし，この署名方式の公開パラメータ数は署名できるメッセージの個数(n)に比例するため，n が大きい場合に問題となる．

そこで本研究では，１つの g の代りに，複数のパラメータ $g_1,g_2,\cdots,g_k$ を用いることを考える．そして，暗号文の署名を $Sig(E(M_1),g_1,1,\cdots,1),Sig(E(M_2),g_2,1,\cdots 1),\cdots,Sig(E(M_k),g_k,1,\cdots 1),Sig(E(M_{k+1}),1,g_1,1,\cdots,1),\cdots,Sig(E(M_n),1,\cdots 1,g_k)$として計算する．この場合，これらの署名同士を演算すると，$Sig(E(M_1^{w1}+M_2^{w2}+\cdots+M_n^{wn}),g_1^{w1}g_2^{w2}\cdots,g_1^{wk+1}g_2^{wk+2}\cdots,\cdots)$となるため，従来方式と同様に平文メッセージ部の $w_1,w_2,\cdots w_n$ がすべて１であることを検証することにより，$E(M_1+M_2+\cdots+M_n)$の署名であることが確認できる．この提案方式では，検証用のベクトルの１要素が，$g_1,g_2,\cdots,g_k$で表現できるため，ベクトルのサイズを n/k に削減できる．こうして，署名方式の公開パラメータサイズが n/k に軽減できる．一方，追加でパラメータ $g_1,g_2,\cdots,g_k$ が追加されることから，両者の個数をバランス化するために，$k=\sqrt{n}$ とすることにより，全体のパラメータ数を $2\sqrt{n}$ にすることができ，効率化される．

また本研究では，提案した暗号状態計算検証法の有用性を確認するために，ユーザのピューテション(評判)を匿名で検証できるシステムへの応用を行なうとともに，レピューテションベースの匿名認証も検討する．

４．研究成果

(1) 検索可能暗号における安全性の向上

3.(1) の着想に基づき，暗号化ユーザを限定した検索可能暗号である Designated-Senders PEKS(Public-key Encryption with Keyword Search)を構築した．アルゴリズムの構築では，Eurocrypt2004 で Boneh らにより提案された，ペアリングベースの公開鍵検索暗号 PEKS をベースとして，着想に基づき拡張を行なっている．また，放送型暗号も，Crypto2005 で提案されたペアリングベースの方式(BGW)を利用している．3.(1) で示したように，指定されたユーザのみがキーワード暗号化を行なえるため，サーバによる辞書を用いたキーワード推測攻撃が防止されている．

提案方式の効率については，暗号化において放送型暗号(A,B)の復号が追加されるが，BGW 放送型暗号方式のために暗号化ユーザ数に依存せず効率的に行なえる．提案方式の検索秘密鍵生成およびキーワード等価性チェックの処理は，ベースの PEKS 方式と同様のため，高速に処理可能である．一方，暗号化ユーザは，事前に検索可能ユーザから公開鍵を取得する必要があり，暗号化ユーザ集合が変化する度に取得しなければならない．このことは，従来方式からのデメリットであるが，クラウドベースでの検索アプリケーションを想定する場合，暗号化ユーザ集合が変化する際にクラウドサーバに公開鍵を登録し，暗号化ユーザはキーワード暗号文を送信する際にクラウドサーバにアクセスするため，その際に新しい公開鍵を取得するようにすれば問題ないと考えられる．

また，提案方式の安全性を保証するため，PEKS での安全性定義を基にして，Designated-Senders PEKS の安全性定義を行なった．従来の PEKS では，暗号文の強秘匿性(二つのキーワードからランダムに一つを選び，その暗号文を敵アルゴリズムに与えたとき，どちらであるかを有意に判定できない安全性)が定義されるが，これに加えて，検索秘密鍵の秘匿性を新たに定義した．これは，検索ユーザに指定されていない敵アルゴリズムに対して，二つのキーワードからランダムに一つを選び，そのキーワードに対応した検索秘密鍵を与えられても，どちらであるか有意に判定できない安全性である．この安全性を満たす場合，敵アルゴリズムと想定されるサーバは，検索キーワードを推測できないため，本研究で想定する辞書による攻撃を防止できる．そして，この Designated-Senders PEKS の安全性定義を提案方式が満たすことを，従来の PEKS および BGW 方式でも用いている標準的な数学的仮定を基に定式的に証明した．これにより，提案方式の安全性が保証されている．

さらに，提案方式の拡張として，放送型暗号の代わりに属性ベース暗号を用いた方式も提案した．属性ベース暗号とは，所属・職種のようなユーザの属性を用いて，その属性をもつ者のみが復号可能な暗号である．さらに，属性の論理式も指定できる．放送型暗号では，個別のユーザ ID から暗号化ユーザグループを指定する必要がありユーザ管理に負担を要するが，属性ベース暗号を用いる場合，属性のみで指定できるため，ユーザ管理の負担が軽減できる．

(2) 暗号状態計算における正当性検証の効率化

提案方式のアプリケーションとして，ユーザのレピュテーションをサーバ(管理者)に対して秘匿しつつ集計でき，他ユーザに余計な情報を漏らすことなくゼロ知識証明できる評価システムを構築し，提案した．提案方式では，多数のユーザのサーバが参加する．ある被評価ユーザ A は，他のユーザとサービス内でのインタラクションを行なった結果として評価され，評価点が n 人の他ユーザから暗号化されてサーバに与えられる．サーバは，それらに証明書を付与して保証し，準同型暗号により評価点の総計の暗号文 1 つに集約して被評価ユーザ A に渡す．この際，従来提案されている準同型署名を用いることにより，証明書も 1 つの証明書に集約できる．ユーザ A が他ユーザに自身のレピュテーションを示す場合，評価点の総計の暗号文と集約された証明書をゼロ知識証明することにより，自身の信頼度を余計な情報(ID など)を漏らすことなく匿名認証することができる．これにより，プライバシーを侵害することなく各ユーザの信頼度を評価することができ，安全かつプライバシーが保証されたサービスが実現できる．この際，暗号文および証明書を集約できることから，ユーザ数 n に依存したコストがかからないため，効率的である．

しかし，上記したように，従来の準同型署名を用いた手法では，加算結果の保証を行なうために検査用の長さ n のベクトルを付与する必要があり，用いる公開パラメータ数が n に比例してしまう．そこで，3.(2)の着想に基づいてベクトルサイズを $k=\sqrt{n}$ にすることにより，公開パラメータ数を $2\sqrt{n}$ になるように提案評価システムの拡張を行なった．これによる計算時間の増加はなく，効率的に公開パラメータ数の削減ができている．

提案システムでは，各評価ユーザが，不正な評価値(指定される評価値以外の値)の暗号文を送信する可能性がある．そこで，暗号文中の評価点が指定された範囲内にあることを証明するゼロ知識証明プロトコルを追加した．これにより，評価ユーザによる不正送信を防止できる．

さらに，提案システムを PC(CPU:Core i5-4460,Memory:7.8GB)上でプロトタイプ実装した．準同型署名を用いているため，評価ユーザ数 100 の場合でも 250ms 程度でゼロ知識証明できることが確認できている．一方，公開パラメータサイズも 5KB 程度と効率的である．

プライバシーを保護した提案評価システムに関連して，レピュテーションに基づいた匿名認証についての検討も行なった．ユーザ認証により不正アクセスは防止できるが，通常の ID を用いた認証では，サーバ側で ID の紐づけによる利用履歴が取得できることから，その不正な情報流出・漏洩が問題となっている．そこで，ID を秘匿したまま正当なユーザかの確認を行なえる匿名認証が研究されており，提案した評価システムも，匿名で認証しつつユーザの信頼性を他ユーザのレピュテーションにより評価できる，匿名認証となっている．匿名認証では，ユーザ失効を匿名性を維持しながら効率的に実現する必要があり，本研究では，失効可能匿名認証方式を検討した．また，匿名のままユーザの属性を認証する必要もあるため，匿名属性認証の検討も行なった．さらに，ユーザのレピュテーションに基づいてユーザ失効を行なう必要もあるため，レピュテーションベースの失効可能匿名認証の検討も行なった．

５．主な発表論文等

〔学会発表〕（計 9 件）

① 上野山 大貴，中西 透, “線型準同型署名を用いた管理者に対して秘匿性を持つ評価システムの改善,” 情報処理学会 CSEC 研究会, 2018 年 12 月.

② 上野山 大貴，中西 透, “線型準同型署名を用いた管理者に対して秘匿性を持つ評価システム,” 電子情報通信学会 ISEC 研究会, 2017 年 12 月.

③ 齋藤 尭範，中西 透, “サーバによるキーワード推測攻撃に対して安全な検索可能公開鍵暗号の安全性検討と拡張,” 電子情報通信学会 ISEC 研究会, 2017 年 12 月.

④ Takanori Saito, Toru Nakanishi, “Designated-Senders Public-Key Searchable Encryption Secure against Keyword Guessing Attacks,” 4th International Workshop on Information and Communication Security (WICS'17), 2017 年 11 月.

⑤ 齋藤 尭範，中西 透, “サーバによるキーワード推測攻撃に対して安全な検索可能公開鍵暗号の提案,” コンピュータセキュリティシンポジウム 2016 (CSS2016), 2016 年 10 月.

６．研究組織

(1)研究分担者

なし

(2)研究協力者

研究協力者氏名：野上 保之

ローマ字氏名： (NOGAMI, Yasuyuki)