様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　６　月　１７　日現在

機関番号：　８２６３６
研究種目：　若手研究(B)
研究期間：　2012～2015
課題番号：　２４７００００９

研究課題名（和文）クラウド環境におけるセキュリティを確保する新たな暗号方式の提案

研究課題名（英文）A cryptographic scheme maintaining security for cloud environments

研究代表者
江村　恵太（Emura, Keita）

国立研究開発法人情報通信研究機構・ネットワークセキュリティ研究所セキュリティ基盤研究室・主任研究員

研究者番号：３０５９７０１８

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：クラウド環境下におけるセキュリティの確保に応用可能な暗号技術として準同型暗号が注目されている。しかしながら公開鍵暗号として求められるCCA安全性は、準同型暗号では理論的に実現不可能である。本研究では、アプリケーションに影響を与えない範囲で適切に準同型暗号の機能を制限することで、理想的な安全性を実現する準同型暗号方式「鍵付き準同型暗号」を提案した。本成果は公開鍵暗号における権威ある国際会議の1つであるPKC2013に採録されるとともに、国内における最大のセキュリティに関する会議である暗号と情報セキュリティシンポジウム（SCIS）2012においてイノベーション論文賞を受賞した。

研究成果の概要（英文）：It is widely recognized that homomorphic encryption never achieves security against adaptive chosen-ciphertext attack (CCA security). We propose a homomorphic encryption scheme with CCA security by adequately modifying the model of homomorphic encryption which we call keyed-homomorphic encryption. Our result was accepted to PKC 2013 which is a well-known international workshop in the public key encryption area, and was awarded the SCIS Innovation Paper Award from IEICE in 2012.

研究分野：　公開鍵暗号

キーワード：　鍵付き準同型暗号　適応的暗号文選択攻撃

１．研究開始当初の背景

準同型暗号とは、データ M1 とデータ M2 の暗号文 C1、C2 が与えられた場合、暗号文を復号することなく C1,C2 のみから M3=f(M1,M2) の暗号文を作成できる暗号方式である。関数 f としては加算や乗算などが考えられ、例えば個々のデータの値を明らかにすることなくその合計値を計算するなどの秘匿計算 (例えば電子投票など) に用いることができる。近年では、f として任意の関数が実現可能な完全準同型暗号方式が提案され、暗号界のみならず産業界から大きな反響を呼んだ。その理由として、準同型暗号がクラウド環境下におけるセキュリティの確保に応用可能な技術として注目されていることが挙げられる(例えばデータベースに保管された暗号化データを復号することなく暗号文のまま更新できる)。準同型暗号の安全性を向上することはすなわち、クラウド型アプリケーションの普及に多大なる影響を与え、情報化社会に与える効果は計り知れない。

２．研究の目的

準同型暗号がクラウド環境下におけるセキュリティの確保に応用可能な技術として注目されている一方で「暗号文を加工して別の暗号文が計算できる」という性質は、安全性の視点からは「暗号文が偽造可能」と言っているのに等しい。そのため公開鍵暗号として求められる「攻撃者に最大限優位な環境を与えたとしても、データに関する情報は 1 ビットたりとも漏えいしない」という安全性 (以下 CCA 安全性) は準同型暗号では理論的に実現不可能である。例えば入札などで M の暗号文 C に対し、M (=100 万円など) は分からなくても、M’=M+1 (101 万円) に対する暗号文 C’が作成できれば、入札値を改ざん可能となる。すなわち準同型暗号というフレームワーク自体が理想的な安全性と決して両立し得ない。ここで準同型暗号が CCA 安全性をみたす術はない本質的な原因は「任意のユーザが準同型性を利用可能」であるという性質であることに注意されたい。そこでこの性質が現実的に必須であるのか？について考察する。例として、(クラウド環境で想定される準同型暗号の最も一般的なアプリケーションである) データベースに保管された暗号化データを復号することなく更新するシステムを考える。もし任意のユーザが暗号文を更新可能であれば、いつ/どのように/誰が/暗号文を修正したのかを正確に把握することは極めて困難であるといえる。現実的に、パブリッククラウドなどリソースの割り当てを動的に行う環境下においては、出先のデータベースで予期しない修正を施される危険性を排除することは難しく、またプライベートクラウドのように閉じた環境下であったとしても、データベースにアクセス可能な全てのユーザが暗号文を修正可能であることは、他人のデータを改ざんするなどの問題を引き起こす可能性を排除できない。

以上より、「任意のユーザが準同型性を利用可能」であるという性質は理想的な安全性の実現を阻害しているばかりか、予期せぬ変更に対応できないという問題を生むことが判明した。そこでこの問題を解決する根本的な方式として、「準同型性を利用可能なユーザを限定する」準同型暗号を考える。このような暗号を構成するために、本研究の目標を暗号文の復号はできないが準同型性を作用可能な秘密鍵 (準同型作用鍵) HK を生成する技術を創出することと設定し、この暗号プリミティブを「鍵付き準同型暗号」と名付ける。鍵付き準同型暗号では (C1,C2,HK)から f(M1,M2) の暗号文 C3 を作成できるが、C1,C2 から M1、M2、f(M1,M2)に関する情報は一切漏えいしない。通常の公開鍵暗号と同様に DK を用いることで、C3 から f(M1,M2) を得ることができる。準同型性の利用には HK が必要なことから攻撃者は暗号文を加工できず、そのため復号結果に関する情報が一切漏れないことを保証する安全性を定義することができる。HK を所持しないユーザ視点からは理想的な安全性を持つ公開鍵暗号そのものであることから、鍵付き準同型暗号は「準同型暗号の有用性はそのままにその安全性を飛躍的に向上させた」方式であり、かつその安全性はこれまでの準同型暗号のフレームワークでは理論的に達成不可能であることにも注目されたい。

３．研究の方法

一般的に「セキュリティは高ければ高いほど良い」という風潮があり、そのためか暗号理論では「如何に強いセキュリティを実現するか？」という観点で主に研究が進められている。そのため現状の暗号技術では「全ての情報を秘匿することで， 安全ではあるがサービス向上や悪用防止に有用な情報をも同時に秘匿」もしくは「サービス向上や悪用防止ために、安全性をないがしろにする」の両極端な方策のどちらかを受け入れざるを得ない。後者を受け入れることは社会的に受け入れ難く、そのため学術的には安全性をより高める方向へと研究が進められている。そのため、例えば準同型暗号に関して言えば、強い安全性を有するがために準同型性など有用な特性をも無くしているか、もしくは準同型性という機能と引き換えに安全性を犠牲にしているかの両極端な方式しか知られていないのが現実である。そのため準同型性作用のみを許しつつ復号は許さない制御技術を創出するには既存技術を組み合わせでは到底成し得ないといえる。

そこで準同型暗号が理想的な安全性をみたす術はない本質的な原因は「任意のユーザが準同型性を利用可能」であるという性質であることに着目する。この問題を解決する根本的な方式として、「準同型性を利用可能なユーザを限定する」準同型暗号を考える。まず「データごとに暗号文を復号できる/できないを切り分け可能な技術」に関する研究を行い、そこで得た知見を元にさらに暗号文の復号ができないデータに対して準同型性を作用可能とする技術を創出することで、準同型性を利用可能なユーザを適切に制御する公開鍵暗号を提案する。

次に実際のクラウド環境で要請される安全性を鍵付き準同型暗号にフィードバックする.鍵付き準同型暗号では暗号文を更新可能なユーザが適切に制限されており、例えば出先のデータベースで予期しない修正を施されるといった危険性を排除することが可能である。すなわちデータベース管理者に HK を預託、データ更新時には管理者が本人確認のための認証を行った後データを更新するというシステムが考えられる。さらにコンテンツ配信者に HK を預託、暗号化されたデータに対し配信者のみがある情報（不正コピー防止用の電子透かしや正当な配信者が配布したデータであることを示す証明書など）を埋め込むシステムなどの悪用防止策としての応用や、暗号化データの集計を委託することで、集計コストの分散及びあるエリアごとの集計が可能になるなどの応用が考えられる。このように復号鍵 DK と準同型作用鍵 HK を分離したことで HK を預託することが可能になる一方、預託した HK の漏洩が問題となる。前述したとおり、鍵付き準同型暗号においては、HK を持たない攻撃者視点からは鍵付き準同型暗号は理想的な安全性を有する一方で、HK を持つ（内部）攻撃者視点からは、通常の準同型暗号における安全性の域を出ない。そこで第二の方策として、鍵付き準同型暗号に準同型作用鍵 HK の漏洩耐性を付与することで、より現実的なアプリケーションの構築の構成要素として耐えうる暗号プリミティブとして鍵付き準同型暗号を確立する。より具体的には、HK を取得可能な攻撃者に対し最大限優位な情報を与えるモデルにおいて、暗号文からデータに関する情報を得ることができない方式を提案する。攻撃者に与える情報は HK がいつ漏洩するのかによってその優位性が異なり、HK の漏洩タイミングごとに決定される。すなわち、「常に」準同型性を利用可能な既存準同型暗号では決して達成し得ない安全性をモデル化していると言える。

４．研究成果

準同型性用の秘密鍵を定義することで、準同型演算が可能なユーザを制限するとともに、準同型演算鍵を所持しないユーザに対しては CCA 安全性を保証する「鍵付き準同型暗号」を提案した。具体的には、ハッシュ証明システム（Hash Proof System、HPS）を利用した鍵付き準同型暗号の一般的構成法を与え、乗法準同型を持つ方式（DDH ベース)、加法準同型を持つ方式（DCR ベース）を構成した。本成果は公開鍵暗号における権威ある国際会議の１つである PKC2013 に採録されるとともに、国内における最大のセキュリティに関する会議である暗号と情報セキュリティシンポジウム（SCIS) 2012 においてイノベーション論文賞を受賞した。

公開鍵暗号の発展形として、任意の値が公開鍵として使用可能な ID ベース暗号が知られている。そこで鍵付き準同型性を ID ベース暗号に拡張した暗号方式「鍵付き準同型 ID ベース暗号」を提案した。同じ ID に対して作成された暗号文に対し、準同型作用鍵を用いることで準同型演算（乗法）を行うことができ、準同型作用鍵を持たないユーザに対しては CCA 安全性を保証する。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　0　件）

〔学会発表〕（計　3　件）

1．江村恵太，花岡悟一郎，松田隆宏，縫田光司，山田翔太：鍵付き準同型 ID ベース暗号，暗号と情報セキュリティシンポジウム (SCIS)，3E4-3，2015 年 1 月 22 日，リーガロイヤルホテル小倉（福岡県北九州市）

2．Keita Emura，Goichiro Hanaoka，Go Ohtake，Takahiro Matsuda，Shota Yamada：Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption. Public Key Cryptography，32-50，2013 年 3 月 1 日，新公会堂（奈良県奈良市）

3．江村恵太，花岡悟一郎，松田隆宏，大竹剛，山田翔太：適応的選択暗号文攻撃者に対し安全な準同型暗号，暗号と情報セキュリティシンポジウム（SCIS)，2A1-6，2012 年 1月31日，金沢エクセルホテル東急（石川県金沢市）

〔図書〕（計　0　件）

〔産業財産権〕
○出願状況（計　0　件）

○取得状況（計　0　件）

〔その他〕
ホームページ等

６．研究組織

(1)研究代表者

江村 恵太　　（EMURA, Keita）

国立研究開発法人情報通信研究機構ネットワークセキュリティ研究所セキュリティ基盤研究室 主任研究員

研究者番号：30597018

(2)研究分担者

（　　）

研究者番号：

(3)連携研究者

（　　）

研究者番号：