様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成　25年　5月　30日現在

機関番号：８２６２６
研究種目：若手研究（B）
研究期間：2010～2012
課題番号：２２７００００２０
研究課題名（和文）完全準同型ファンクショナル暗号の実現に向けた挑戦的研究

研究課題名（英文）Research towards Constructing Homomorphic Functional Encryption

研究代表者
アッタラパドゥン　ナッタポン（ATTRAPADUNG　NUTTAPONG）
独立行政法人産業技術総合研究所・セキュアシステム研究部門・主任研究員
研究者番号：４０５１５３００

研究成果の概要（和文）：本研究は、クラウドコンピューティングにおけるセキュリティソリューションとなる暗号方式を提案する。これまでに、クラウド上のデータベース管理と、クラウド上のデータ処理時のセキュリティが主な課題であるが、クラウドプロバイダーの信頼性を仮定せず、かつ、プライベートクラウドを利用しない状況での解決方法はまだ提案されていなかった。本研究はこのような状況においても安全なシステムを考案する。具体的な成果は、効率のよいかつ高度なアクセス制御機能を持つ暗号方式としてコンパクトな「関数型暗号」の提案および、データが正しく処理される際にデータの真正性が保持される仕組みである「準同型電子署名」の提案である。

研究成果の概要（英文）：In this research, we provide some cryptographic solutions for the security in cloud computing environments. The problem for cloud security can be related to two main applications: cloud database and cloud computing. However, previously there is no security solution that is independent of the reliability of the cloud provider and the use of private cloud. In this research, we propose two secure mechanisms in such situation. First, for cloud database applications, we propose efficient encryption schemes that allow fine-grained access control mechanism over encrypted data, namely compact functional encryption schemes. Second, for cloud computing applications, we propose efficient digital signature schemes that allow authenticity-preservation on authenticated data via cloud computation, namely homomorphic signature schemes.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010年度	1,000,000	300,000	1,300,000
2011年度	1,000,000	300,000	1,300,000
2012年度	800,000	240,000	1,040,000
年度			
年度			
総　計	2,800,000	840,000	3,640,000

研究分野：情報学
科研費の分科・細目：情報基盤・情報セキュリティ
キーワード：暗号、クラウドセキュリティ、関数型暗号、準同型電子署名

１．研究開始当初の背景

近年 IT 業界におけるコンピューティング環境として、従来型からクラウドコンピューティングへのパラダイムシフトが注目を集めている。クラウドコンピューティングの利点は主に、データの一元管理とデータへのユビキタスアクセスが実現できること及び、クライエント側のハードウェアやソフトウェア導入・更新・管理コストの削減、である。しかし、データとその処理のアウトソーシングにより、情報流出の危険性が伴う可能性は従来よりずっと高く、クラウドコンピューティングにおけるセキュリティ問題の解決は緊急の課題である。具体的に、クラウド上のデータベース管理と、クラウド上のデータ処理時のプライバシーが主な課題である。

２．研究の目的

上述の要求を解決するには、高度なアクセス制御機能をもつ暗号方式および、クラウドでデータ処理を行うため、暗号化されたデータを復号せずに機密性を維持したまま処理ができる暗号方式が必要となる。本研究の目的はこのような方式を提案することである。図１はクラウドセキュリティの概念を表す。図１では、横軸はセキュリティ要求の種類：機密性（Confidentiality）、または真正性（Integrity）であり、縦軸はクラウドのアプリケーションの種類：データベースストレージ（Cloud storage）またはデータの計算（Cloud computing）である。本研究はデータベースストレージの時の機密性（Confidentiality for cloud storage）およびデータ計算の時の真正性（Integrity for cloud computing）に着目する。

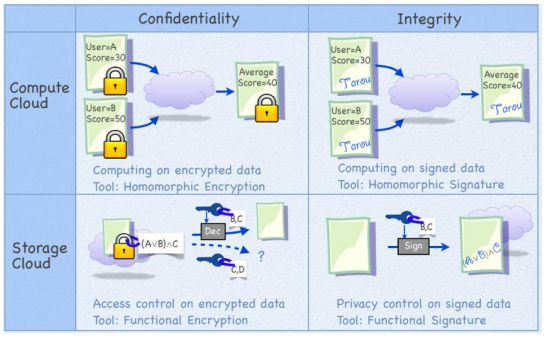

図１：クラウドセキュリティの要求とアプリケーション

３．研究の方法

本研究の方法は二つの項目に分ける。一つ目は高度なアクセス制御機能をもつ暗号方式に関する研究であり、二つ目は暗号化されたデータを復号せずに機密性を維持したまま処理ができる暗号方式に関する研究である。それぞれの方式について、モデルと安全性の定義を行い、方式を設計し、理論的に安全性証明を行い、さらに実用性を高めるために最適化をする。

高度なアクセス制御機能をもつ暗号方式として、「関数型暗号」（または、ファンクショナル暗号）のモデルと安全性について定義を行い、暗号方式の構成法を提案する。関数型暗号は、公開鍵暗号や ID ベース暗号、属性ベース暗号の一般化である。関数型暗号は述語（真理関数）R による定義である。R に関する関数型暗号では、秘密鍵と暗号文にそれぞれ属性パラメータ X と Y が対応付けられており、R(X,Y) = 1（「真」を意味する値）が成立するときのみ復号が可能となる。応用先によって R を適切に定義すれば、要求されるアクセス制御機能が実現できる。具体的な例として、R に論理式充足テスト述語を用いる。例えば、送信者が“人事部の全員”および“C 課の課長と主任”に送りたいときに、それに相当する論理式 V=「人事部」or（「C 課」and（「課長」or「主任」））を生成した上で、関数型暗号で暗号化する。すると、例えば C 課２９歳主任の Mr. Z は条件式 V を満たす属性を持つため、暗号文を復号でき、一方 D 課５０歳課長の Mr. Q は条件式 V を満たす属性を持たないため、暗号文の復号が不可能である。この例を図２で表す。このような関数型暗号のモデルを定義する。次に、安全性モデルでは、暗号理論のスタンダードモデルにより定義する。（詳細は論文に参考）。安全性の特徴は、攻撃者が秘密鍵を掻き集めて結託攻撃を行ったとしても対応できる点にある。

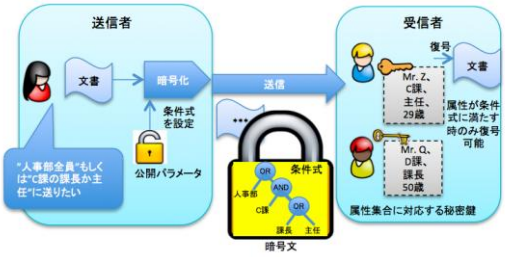

図２：関数型暗号の利用例

暗号化されたデータを復号せずに機密性を維持したまま処理ができる暗号方式に関する研究では、準同型暗号と呼ばれるものである。本研究は、クラウド内のデータの真正性を着目し、真正性が保証されたデータがク

ラウドアウトソーシングによる処理されても、処理されたあとのデータについての真正性も保証可能にする認証技術を提案する。この技術は、準同型電子署名と呼ばれる。

準同型電子署名の仕組みは以下のようである。元のデータ $X_1, \cdots, X_n$ に対し、電子署名 $Sig_1, \cdots, Sig_n$ があるとする。この電子署名はそれぞれのデータの真正性を保証するものである。すると、関数 f で計算したあとのデータ、つまり $Y=f(X_1, \cdots, X_n)$ についても元々の電子署名から新たな電子署名 Sig が生成でき、この電子署名 Sig が Y の真正性を保証するものになる。この仕組みは図３で表す。

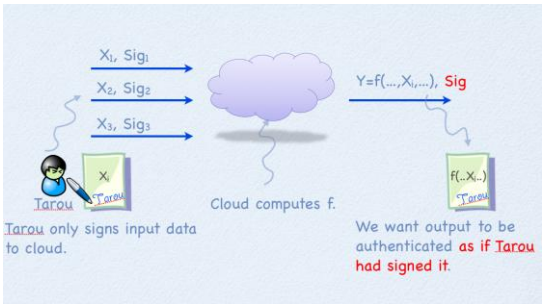

図３：準同型電子署名の仕組み

４．研究成果

関数型暗号に関する研究の主な成果は、モデルと安全性について定義を行い、強い安全性をもつ関数型暗号方式を提案した。具体的には、楕円曲線上の「ペアリング」を用いて方式を設計し、強い安全性モデルである Adaptive security で安全性証明を考案した。基本的な成果は論文⑥で発表した。さらに、それを拡張し、広いクラスの高機能暗号を統一し取り扱い可能な関数型暗号方式の構成法を提案した。この成果は、論文④で発表した。次に、実用性の高い関数型暗号に関する研究である。成果の内容としては関数型暗号方式の一つの例である属性ベース暗号の効率の良い方式の構成法を提案した。この方式の特徴は関数型暗号の高機能性を落とすことなく、方式の暗号文サイズが小さくすることが可能となった。これにより提案の暗号方式を効率よく実現することが可能となる。この成果は論文⑤で発表を行った。この方式はアクセス制御可能な有料放送などが応用例となるキーポリシータイプという種類の属性ベース暗号である。さらに、そのデュアルタイプとなる暗号文ポリシータイプという属性ベース暗号の効率の良い方式も提案した。このタイプの応用例はアクセス制御可能なパブリッククラウドなどである。この方式の特徴も上述の提案方式と同様に、関数型暗号の高機能性を落とすことなく、方式の暗号文サイズが小さくすることが可能となった。属性ベース暗号の研究分野において、本研究の提案方式が現在暗号文サイズと復号の計算量に関しては最も効率の良い方式である。この結果は論文③で Theoretical Computer Science(2012) という権威のる国際論文誌に採録された。

準同型電子署名に関する研究の成果は、モデルと安全性について定義を行い、強い安全性をもつ準同型電子署名方式を提案した。この技術も前者の技術と同様に楕円曲線上の「ペアリング」を用いて方式を設計し、強い安全性モデルで安全性証明を考案した。基本的な成果は論文②で発表した。さらに、計算（関数 f）のクラスを線形関数クラスまたはサブストリング関数クラスに限定することで、効率のよい準同型電子署名を提案した。この成果は論文①で発表した。

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　6 件）

①. Nuttapong Attrapadung, Benoît Libert, Thomas Peters. “Efficient Completely Context-Hiding Quotable and Linearly Homomorphic Signatures,” In Lecture Notes in Computer Science, Vol. 7778, pp. 386-404, Springer, 2013.03. DOI:10.1007/978-3-642-36362-7_24

②. Nuttapong Attrapadung, Benoît Libert, Thomas Peters. “Computing on Authenticated Data: New Privacy Definitions and Constructions,” In Lecture Notes in Computer Science, Vol. 7658, pp. 367-385, Springer, 2012.12. DOI:10.1007/978-3-642-34961-4_23

③. Nuttapong Attrapadung, Javier Herranz, Fabien Laguillaumie, Benoît Libert, Elie de Panafieu, Carla Ràfols. “Attribute-Based Encryption Schemes with Constant-Size Ciphertexts,” In Theoretical Computer Science, Vol. 422, pp. 15-38, Elsevier, 2012.03. DOI:10.1016/j.tcs.2011.12.004

④. Nuttapong Attrapadung, Benoît Libert. “Functional Encryption for Public-Attribute Inner Product,” In Journal of Mathematical Cryptology, Vol. 5, No. 2, pp. 115-158, 2011.10. DOI:10.1515/jmc.2011.009

⑤. Nuttapong Attrapadung, Benoît Libert,

Elie de Panafieu. “Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts,” In Lecture Notes in Computer Science, Vol. 6571, pp. 90-108, Springer, 2011.03. DOI:10.1007/978-3-642-19379-8_6

⑥. Nuttapong Attrapadung, Benoît Libert. “Functional Encryption for Inner Product: Achieving Constant-Size Ciphertexts with Adaptive Security or Support for Negation,” In Lecture Notes in Computer Science, Vol. 6056, pp. 384-402, Springer, 2010.05. DOI:10.1007/978-3-642-13013-7_23

〔学会発表〕(計 4件)

①. Nuttapong Attrapadung, Benoît Libert, Thomas Peters. “Efficient Completely Context-Hiding Quotable and Linearly Homomorphic Signatures,” Public Key Cryptography－PKC 2013, 2013.03, Nara, Japan

②. Nuttapong Attrapadung, Benoît Libert, Thomas Peters. “Computing on Authenticated Data: New Privacy Definitions and Constructions,” Advances in Cryptology - ASIACRYPT 2012, 2012.12, Beijing, China.

③. Nuttapong Attrapadung, Benoît Libert, Elie de Panafieu. “Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts,” Public Key Cryptography - PKC 2011, 2011.03, Sicilia, Italy.

④. Nuttapong Attrapadung, Benoît Libert. “Functional Encryption for Inner Product: Achieving Constant-Size Ciphertexts with Adaptive Security or Support for Negation,” Public Key Cryptography - PKC 2010, 2010.05, Paris, France.

６．研究組織

(1)研究代表者

ナッタポン　アッタラパドゥン
(Nuttapong Attrapadung)
独立行政法人産業技術総合研究所・セキュアシステム研究部門・主任研究員
研究者番号：40515300