科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　２５　日現在

機関番号：　８２６２６
研究種目：　挑戦的萌芽研究
研究期間：　2011～2013
課題番号：　２３６５６２５７

研究課題名（和文）問題ある平文の暗号化を不可能とする暗号方式の実現に関する研究

研究課題名（英文）Study on Public Key Encryption with Restricted Plaintext Space

研究代表者
花岡　悟一郎（Hanaoka, Goichiro）

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・研究グループ長

研究者番号：３０４１５７３１

交付決定額（研究期間全体）：（直接経費）　　2,900,000円、（間接経費）　　870,000円

研究成果の概要（和文）：本研究においては、近年の緊迫した世界情勢を鑑み、高度に安全であると同時にテロリスト等による悪用を許すことのない情報通信ネットワークの確立を大きな目的とする。本研究においては、平文空間を制限可能な公開鍵暗号の設計、安全性評価、実装を行った。また、そのための基盤的理論の構築を行った。これらの成果は、国際会議や国際査読誌などで発表を行っている。

研究成果の概要（英文）：The main motivation of this work is to provide a technology which yields confidentiality of communication but prevents those by malicious users, e.g. terrorists. In this work, as a candidate of such a technology, we study public key encryption with restricted plaintext space. Specifically, we construct a concrete scheme, evaluate its security, and implement it. We also study its fundamental theory. These results were preseted in international conferences and journals.

研究分野：　手元にデータがありません

科研費の分科・細目：　手元にデータがありません

キーワード：　暗号理論

１．研究開始当初の背景

現在まで長期にわたり、イラクやパレスチナなどの中東地域をはじめ、世界各地で緊迫した情勢が続いており、またそれら以外の地域においてもテロリズムの脅威にさらされている。一方、最新の暗号技術により実現される安全性は、すでに極めて高度な水準に達しており、なおかつ、非常に簡便な利用が可能となっている。そのため、これらの技術は、上記のような軍事活動にも積極的な活用がなされていると考えられている。このような世界情勢を考慮し、スパイやテロリストによる活動を制限すべく、紛争地域やテロリズムの脅威にさらされている諸国では、暗号技術の利用の制限が検討されている。たとえば、カナダ Research in Motion 社のスマートフォン BlackBerry では、暗号化された通信データに関し、その内容を当局が十分に監視することができないため、国家安全保障上の観点から、アラブ首長国連邦、インド、サウジアラビアなどでは、通信サービスの規制の検討がなされている。同様に、米国でも、暗号化された利用者の通信内容を、事業者がいつでも自由に復元できる機能（所謂、Key Escrow 機能）を付け加えるよう、インターネットサービス事業者などに対して要請することが米国連邦捜査局により検討されている。このような状況は、善意の利用者による暗号技術の正当な活用を激しく妨げるものであり、ネットワーク社会の発展に関する深刻な阻害要因となる。

２．研究の目的

本研究においては、上記のような緊迫した世界情勢を鑑み、善意の利用者による暗号技術の正当な活用を妨げることなく、国家の安全を脅かす悪意ある利用を防ぐための暗号技術について研究を行うことで、善意ある利用者の誰もが制約を受けることなく最先端暗号技術の恩恵を享受でき、なおかつ、その悪用を決して許すことのないネットワーク社会の確立に貢献することを目的とする。具体的には、特に、ある特定の平文を暗号化することが不可能であるような暗号方式の設計および実装を行う。そのような暗号方式を用いることで、犯罪に関わる特定のキーワード（たとえば、「爆弾テロ + 実行」等）を含む一切の平文の暗号化の禁止がなされ、したがって、善意の利用者の正当な利用を妨げる恐れが著しく軽減される。しかしながら、このような機能をもつ暗号方式はこれまでに全く知られておらず、それを実現することは、国際的に深刻な社会問題の解決に対して顕著な貢献するだけでなく、学術的にも極めて意義深く、暗号理論分野全体を大きく発展させるものである。

３．研究の方法

本研究期間においては、キーワード検索可能暗号と呼ばれる技術に対し、非自明かつ大幅な改良を加えることで、上述の機能をもつ暗号方式を設計し、実装による実用性の検討を行う。なお、キーワード検索可能暗号においては、送信者に悪意の無いことを想定したモデルとなっており、目的となる暗号方式と明確に異なっている。したがって、その単純な拡張だけでは目的の達成は極めて困難である。したがって、本研究においては、単に方式の設計を行うのみにとどまらず、その基盤となる理論的整備を行うものとする。特に、公開鍵暗号に対し、機能の付加や安全性の高度化を行う際、本質的に求められる要件を明らかにすることで、目的とする上記技術の実現がそもそも実現可能であるか、さらに、実現可能であるとしてどのような構成の方針が有望であるかについての示唆を与えるものとする。

４．研究成果

上述の通り、本研究においては、近年の緊迫した世界情勢を鑑み、高度に安全であると同時にテロリスト等による悪用を許すことのない情報通信ネットワークの確立を大きな目的とする。特に、そのようなネットワーク社会において真に要求される全く新たな暗号技術の実現を目指す。現在、多くの研究者による活発な研究開発により、最新の暗号技術によって提供される安全性は極めて高度なレベルに達していると考えられる。その一方で、そのような技術は、テロリスト等が犯罪行為を行う際の情報伝達にも非常に有用な技術となっている。この事態を根本的に解決する技術の創出が本研究の目標となる。三年計画の初年度である平成 23 年度においては、公開鍵暗号全般、特に、キーワード検索可能暗号などの周辺分野について研究動向を調査し、得られた知見を元に提案方式のプロトタイプの設計を行った。具体的には、まず、実用的な公開鍵暗号を設計するための一般的手法を整理し、それに関する新たな方法論の提案を行った。さらに、それにより得られた知見を用いて、最終目標とする上記技術のプロトタイプとして、平文空間に関して動的な制限を加えることが可能な公開鍵暗号方式の設計を行った。これらの成果は、国際英文誌 IEICE Trans. on Fundamentals および国際会議 IWSEC 2011（Springer-Verlag 社 Lecture Notes in Computer Science に収録）に採録されている。研究計画においては、当初は平成 23 年度にはプロトタイプの実装実験までを予定していたが、実際にはプロトタイプの構成が理論的にも非常に高度なものとなったことから、実装よりも理論解析を中心に研究を進めることとなった。特に、厳密な数学的安全性評価を行い、妥当な安全性定義の上で、同方式が証明可能安全性を持つことを示した。

平成 24 年度においては、前年度において設計および安全性評価を行った、平文空間に関して動的な制限を加えることが可能な公開鍵暗号方式について、その問題点を検討し、それを克服するための基盤的理論の構築と、要素技術の設計を行った。本年度は、特に、検索可能暗号、関数暗号、ゼロ知識証明について研究を行い、これらの技術の拡張に基づく、本研究の目的を達成するための方針を明らかにした。これらの成果により、暗号理論分野全体において最も権威ある国際会議である CRYPTO 2012 や、同様に、公開鍵暗号分野において最も権威ある国際会議のひとつである PKC 2012, 2013 において、合計 7 件もの成果を発表している。これらの成果はいずれも、Springer-Verlag 社の Lecture Notes in Computer Science シリーズとしても出版がなされている。

平成 25 年度においては、前年度までに設計と安全性評価を行った平文空間に関して動的な制限を加えることが可能な公開鍵暗号方式の設計について、実装の可能性について検討を行った。特に、楕円エルガマル暗号において平文空間を 0,1 のみに制限した方式について実装を行い、極めて高速に機能することを明らかにしている。また、この手法がある種のアプリケーションにおいて非常に有用な機能を提供することも示している。これらの成果については今後国際会議等での発表を検討している。これらの成果の他、上述の目標を達成する別の手段として、公開鍵暗号における復号結果の正当性の証明方法や、属性ベース暗号によるアクセス制御についても検討を行った。これらの成果は、国際査読誌 International Journal of Information Security や国際会議 PKC 2014 に採録されている。

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 11 件）

Shota Yamada, Nuttapong Attrapadung, Goichiro Hanaoka, Noboru Kunihiro: “A Framework and Compact Constructions for Non-monotonic Attribute-Based Encryption.” Lecture Notes in Computer Science, Vol. 8383, pp. 275-292, 2014, 査読有. DOI: 10.1007/978-3-642-54631-0_16

Keita Emura, Goichiro Hanaoka, Yusuke Sakai, Jacob C. N. Schuldt: “Group signature implies public-key encryption with non-interactive opening.” Int. J. Inf. Sec. Vol. 13(1), pp. 51-62, 2014, 査読有. DOI: 10.1007/s10207-013-0204-y

Takahiro Matsuda, Goichiro Hanaoka: “Key Encapsulation Mechanisms from Extractable Hash Proof Systems, Revisited.” Lecture Notes in Computer Science, Vol. 7778, pp. 332-351, 2013, 査読有. DOI: 10.1007/978-3-642-36362-7_21

Keita Emura, Goichiro Hanaoka, Go Ohtake, Takahiro Matsuda, Shota Yamada: “Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption.” Lecture Notes in Computer Science, Vol. 7778, pp. 32-50, 2013, 査読有. DOI: 10.1007/978-3-642-36362-7_3

Goichiro Hanaoka, Takahiro Matsuda, Jacob C. N. Schuldt: “On the Impossibility of Constructing Efficient Key Encapsulation and Programmable Hash Functions in Prime Order Groups.” Lecture Notes in Computer Science, Vol. 7417, pp. 812-831, 2012, 査読有. DOI: 10.1007/978-3-642-32009-5_47

Shota Yamada, Goichiro Hanaoka, Noboru Kunihiro: “Space Efficient Signature Schemes from the RSA Assumption.” Lecuture Notes in Computer Science, Vol. 7293, pp. 102-119, 2012, 査読有. DOI: 10.1007/978-3-642-30057-8_7

Shota Yamada, Nuttapong Attrapadung, Bagus Santoso, Jacob C. N. Schuldt, Goichiro Hanaoka, Noboru Kunihiro: “Verifiable Predicate Encryption and Applications to CCA Security and Anonymous Predicate Authentication.” Lecture Notes in Computer Science, Vol. 7293, pp. 243-261, 2012, 査読有. DOI: 10.1007/978-3-642-30057-8_15

Takahiro Matsuda, Goichiro Hanaoka, Kanta Matsuura: “Relations between Constrained and Bounded Chosen Ciphertext Security for Key Encapsulation Mechanisms.” Lecture Notes in Computer Science, Vol. 7293, pp. 576-594, 2012, 査読有. DOI: 10.1007/978-3-642-30057-8_34

Yusuke Sakai, Jacob C. N. Schuldt, Keita Emura, Goichiro Hanaoka, Kazuo Ohta: “On the Security of Dynamic Group Signatures: Preventing Signature Hijacking.” Lecture Notes in Computer Science, Vol. 7293, pp. 715-732, 査読有. DOI: 10.1007/978-3-642-30057-8_42

Yusuke Sakai, Goichiro Hanaoka, Kaoru Kurosawa, Kazuo Ohta: “How to Shorten a Ciphertext of Reproducible Key Encapsulation Mechanisms in the Random Oracle Model.” IEICE Trans. Fundamentals

Vol. 94-EA(6), pp. 1293-1305, 2011, 査読有. DOI: 10.1587/transfun.E94.A.1293

Yusuke Sakai, Keita Emura, Goichiro Hanaoka, Yutaka Kawai, Kazumasa Omote: “Towards Restricting Plaintext Space in Public Key Encryption.” Lecture Notes in Computer Science, Vol. 7038, pp. 193-209, 2011, 査読有. DOI: 10.1007/978-3-642-25141-2_13

〔学会発表〕（計 9 件）

Shota Yamada, Nuttapong Attrapadung, Goichiro Hanaoka, Noboru Kunihiro: “A Framework and Compact Constructions for Non-monotonic Attribute-Based Encryption.” 17th International Conference on Practice and Theory in Public Key Cryptography (PKC 2014), 2014年3月26日～2014年3月28日, Buenos Aires, Argentina.

Takahiro Matsuda, Goichiro Hanaoka: “Key Encapsulation Mechanisms from Extractable Hash Proof Systems, Revisited.” 16th International Conference on Practice and Theory in Public Key Cryptography (PKC 2013), 2013年2月26日～2012年3月1日, 奈良.

Keita Emura, Goichiro Hanaoka, Go Ohtake, Takahiro Matsuda, Shota Yamada: “Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption.” 16th International Conference on Practice and Theory in Public Key Cryptography (PKC 2013), 2013年2月26日～2012年3月1日, 奈良.

Goichiro Hanaoka, Takahiro Matsuda, Jacob C. N. Schuldt: “On the Impossibility of Constructing Efficient Key Encapsulation and Programmable Hash Functions in Prime Order Groups.” 32nd Annual Cryptology Conference (CRYPTO 2012), 2012年8月19日～2012年8月23日, Santa Barbara, CA, USA.

Shota Yamada, Goichiro Hanaoka, Noboru Kunihiro: “Space Efficient Signature Schemes from the RSA Assumption.” 15th International Conference on Practice and Theory in Public Key Cryptography (PKC 2012), 2012年5月21日～2012年5月23日, Darmstadt, Germany.

Shota Yamada, Nuttapong Attrapadung, Bagus Santoso, Jacob C. N. Schuldt, Goichiro Hanaoka, Noboru Kunihiro: “Verifiable Predicate Encryption and Applications to CCA Security and Anonymous Predicate Authentication.” 15th International Conference on Practice and Theory in Public Key Cryptography (PKC 2012), 2012年5月21日～2012年5月23日, Darmstadt, Germany.

Takahiro Matsuda, Goichiro Hanaoka, Kanta Matsuura: “Relations between Constrained and Bounded Chosen Ciphertext Security for Key Encapsulation Mechanisms.” 15th International Conference on Practice and Theory in Public Key Cryptography (PKC 2012), 2012年5月21日～2012年5月23日, Darmstadt, Germany.

Yusuke Sakai, Jacob C. N. Schuldt, Keita Emura, Goichiro Hanaoka, Kazuo Ohta: “On the Security of Dynamic Group Signatures: Preventing Signature Hijacking.” 15th International Conference on Practice and Theory in Public Key Cryptography (PKC 2012), 2012年5月21日～2012年5月23日, Darmstadt, Germany.

坂井 祐介, ヤコブ・シュルツ, 江村 恵太, 花岡 悟一郎, 太田 和夫: "グループ署名の安全性について" 2012 年 暗号と情報セキュリティシンポジウム. (2012/2/2). 石川県, 金沢エクセルホテル東急.

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

特になし

６．研究組織

(1)研究代表者

花岡 悟一郎（HANAOKA, Goichiro）
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・研究グループ長
研究者番号：30415731

(2)研究分担者

アフエルト レナルド
（AFFELDT, Reynald）
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： 40415641

アッタラパドン 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

縫田 光司（NUIDA, Koji）
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： 20435762

(3)連携研究者

（　　）

研究者番号：