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：８２６３６
研究種目：基盤研究(C)
研究期間：2011～2013
課題番号：２３５０００３１

研究課題名（和文）長期利用可能な新しい暗号技術の研究開発

研究課題名（英文）R&D of New Cryptographic Technologies with Long-Term Usability

研究代表者
王　立華（Wang, Lihua）

独立行政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：００４４７２２８

交付決定額（研究期間全体）：（直接経費）　　3,900,000円、（間接経費）　　1,170,000円

研究成果の概要（和文）：従来の公開鍵暗号システムは量子計算機の発展に伴い安全性が揺らぎつつあるため、Lattice暗号と非可換暗号の研究によって、量子攻撃に耐えられる新しい暗号の構築を目指している。一方、クラウドコンピューティングというネットワーク環境が発展するにつれて、利便性が要求されると同時に、安全面やプライバシー保護への需要も高まってくる。

そこで、この需要に応じる代理再暗号(PRE)や準同型暗号など暗号プリミティブとLattice、Braidなど非可換代数構造のプラットフォームを結合して、量子攻撃に耐えられ、クラウドなど新な応用環境に適応する長期利用可能な新しい暗号方式を設計することが本課題の目的とする。

研究成果の概要（英文）：The development of quantum computation casts serious threats to the security of most existing public-key cryptosystems. Cryptosystems that are secure against quantum attacks and can be run on traditional computers are desirable and known as post-quantum cryptosystems. On the other hand, public cloud storage service provides several benefits, including availability (being able to access data from anywhere) and reliability, at a relatively low cost. An adoptable cloud storage service should aim to achieve the best of both worlds by providing the security of a private cloud and the functionality of a public cloud.
We investigated cryptographic technologies with long-term usability on the following two issues: Post-Quantum Cryptography (Lattice-based cryptography and non-commutative cryptography) and Practical Cryptography for Cloud Security (proxy re-encryption, threshold encryption, secret sharing scheme, and position authentication using homomorphic encryption, etc.).

研究分野：総合領域

科研費の分科・細目：情報学・情報学基礎

キーワード：暗号系

１．研究開始当初の背景

(1) 現在、広く使われている暗号システムは次の２種類である：ひとつは整数分解難題(IFP)仮説に基づいているもの(例えば RSA 暗号システム)。もう一つは、離散対数計算難題仮説に基づいているもの(例えば ElGamal 暗号システム、米国のデジタル署名標準(DSS)、楕円曲線暗号システム(ECC)、ペアリングベース(Pairing-based)暗号システム)。しかし、これらの暗号システムはすべて、量子計算機時代においては安全ではなくなる。1994 年、Shor は大整数分解と離散対数計算の効率良い量子アルゴリズムを提案した。2003 年、Shor の離散対数問題の量子アルゴリズムは楕円曲線上に適応可能になった。これらのアルゴリズムが実行可能になった場合は、現在使われている多数の暗号システムは安全ではなくなる。また、一方では、量子計算機が普及していない現在も、計算機の能力は進化し続けているので、次世代の情報の安全性とプライバシー保護にあっては、常に安全性を維持しなければならない問題が存在する。併せて、暗号技術の運用では新しい暗号システムへ移行するまでに一定期間の猶予を持つ必要がある。そのため、長期に渡る安全性確保のため、量子アルゴリズム攻撃に対しても安全な暗号システム(Post Quantum)を構築する必要がある。

(2)　暗号技術の応用環境の変化によって、新しい暗号のプリミティブについての研究が求められている。例えば、ユーザーの利便性向上を目指すクラウドコンピューティング環境などである。クラウド環境において、ユーザーは、全てのデータをクラウドの中にあるサーバーに保存することによって、データ管理が楽に行えるようになる。しかし、ユーザー側からはクラウドサービスの構造については未知であり、サーバーと管理者を信頼することが難しい。従って、よりユーザーに対する利便性や信頼性を高めるためには、データを暗号化してから保存するという基本対策の他、「許可された複数のユーザー間で暗号化データを共有すること(各自の鍵を使用)」や「暗号化データを復号せずに必要な計算処理ができること」など新しいセキュリティ機能の実現が求められている。これについては、既存の暗号システムでは対応しきれない。そのため、これらを満たす新しい暗号のプリミティブの研究が求められており、近年、注目を集める代理再暗号(PRE)、準同型暗号技術などはこの課題を解決することができると考えられている。

２．研究の目的

従来の公開鍵暗号システムは量子計算機発展に伴い安全性が揺らぎつつあるため、研究代表者は Lattice と Braid を代表とする非可換暗号の研究によって、量子攻撃に耐えられる新しい暗号の構築を目指している。一方、クラウドコンピューティングというネットワーク環境が発展するにつれて、利便性が要求されると同時に、安全面やプライバシー保護への要求も高まってくる。そこで、研究代表者はこの要求に応じる代理再暗号(PRE)や準同型暗号など暗号のプリミティブと Lattice、Braid など非可換代数構造のプラットフォームを結合して、量子攻撃に耐え、クラウドなど新たな応用環境に適応する長期の利用が可能な新しい暗号方式を設計することを本課題の目的とした。

３．研究の方法

(1) 計画・目標：
ポスト量子暗号とクラウド環境で実用的な暗号について二つの課題に分けて年度計画をセッティングし、計画的に研究を遂行した。
課題１．Lattice や Braid 群など非可換代数構造に基づいて、ポスト量子暗号方式について研究
課題２．IBE や PRE、準同型暗号について理論的な研究から、新しい安全性を実現するプロトコルの設計、さらに効率性と評価手法の研究
さらに、これまでの成果を踏まえて、実用性に富んだ PRE や準同型暗号など暗号のプリミティブと Lattice、Braid など非可換代数構造のプラットフォームを結合して、量子攻撃に耐え、新たな応用環境に適応する長期の利用が可能な新しい暗号方式の設計を本課題の研究目標とした。上記の二つの課題に向けて、具体的に下記の様に研究を行った。

<table>
<tr><th></th><th>23 年度</th><th>24 年度</th><th>25 年度</th><th></th></tr>
<tr><td rowspan="4">課題１</td><td colspan="3">既存の Lattice 暗号・非可換暗号を研究調査</td><td rowspan="4">成果発表
今後の展開を検討</td></tr>
<tr><td colspan="2">暗号方式の設計と評価手法を探索</td><td></td></tr>
<tr><td colspan="2">安全性向上を目指す、長期利用が可能な暗号方式を設計</td><td></td></tr>
<tr><td colspan="3">ポスト量子暗号方式設計・分析に関する協力者：Wang，Cao，Aono，Boyen，Phong</td></tr>
<tr><td rowspan="4">課題２</td><td colspan="2">応用から要望調査</td><td></td><td rowspan="3">提案方式を実装</td></tr>
<tr><td colspan="3">利便性向上を目指す暗号方式を設計</td></tr>
<tr><td colspan="2">提案方式の応用調査と実装の準備</td><td></td></tr>
<tr><td colspan="3">クラウド環境で実用的な暗号に関して協力者：Mambo，Shao，Wang，Tanaka，Waseda，Nojima，Moriai</td></tr>
<tr><td rowspan="2">結合</td><td colspan="3">耐量子攻撃、かつクラウド環境に適応する長期の利用が可能な暗号方式の設計</td><td>成果・展開</td></tr>
<tr><td colspan="3">Lattice ベース PRE 暗号方式設計・分析に関する協力者：Phong，Aono，Boyen</td></tr>
</table>

(2) 理論研究：
① Lattice 暗号の研究
Lattice 暗号の研究は Ajtai、Hoffstein ら、Regev、Gentry など専門家達の貢献によって、大きく進展し、数多くの Lattice 方式が相次ぎ提案された。例えば、効率がよい NTRU、完全準同型暗号や(H)IBE など。しかし、Lattice に基づく認証暗号や代理暗号に関する研究はまだ少ない。既存の研究を調査し、Lattice に基づいて、プライバシー保護の安全性を満たす PRE 方式を設計し、安全性証明技術について理論的な研究を行った。
② 非可換暗号の研究
Braid や Inner automorphism 群など非可換代数構造に基く暗号は非可換暗号と呼ばれている。Braid 暗号システムは誕生以来長さや線形表現に基づいた攻撃などを受けているが、核心の難題仮説、すなわち、Conjugacy Search Problem(CSP)はまだ破られていない。研究代表者は Inscrypt2010 で一般的な非可換代数構造に基づいて、安全性が CSP の困難性仮説に帰着する暗号方式の構築手法を発表し、二つの実装が可能な例を挙げた（特殊の Matrix Monoid と super summit set (SSS) 中の Braid）が、実用性と安全性の実証は欠如する。さらに安全性要件を分析し、暗号に適応できる他の非可換代数構造と実用的なシステムの構築手法を探索した。
③ 準同型暗号技術の研究
準同型暗号技術の特徴にしたがって、同じ鍵で暗号化されたデータを暗号化されたまま計算することが可能である。理論的には、準同型暗号システムは、CCA2 安全性を満たすことが不可能である。以前の準同型暗号システムは、しばしば、CPA 安全性しか証明されていなかった。Lipmma の最新の研究成果（Inscrypt2010）によると、いくつかの準同型暗号システムは CCA1 安全性が証明されている。これは準同型暗号研究にとって"良い"ニュースである。一方、Lattice 暗号の研究と共に進展する完全準同型暗号技術も近年注目されている。そこで、適切にパラメータを設定することによって、NTRU 暗号システムは完全準同型属性を持つ可能性や、RSA 暗号システムは代数準同型になる可能性を探索した。さらに、電波の届く時刻の延長から位置情報を推測する位置情報認証するシステムに加法準同型暗号を導入することによって、より安全性が強化された位置情報認証システムの設計などを試みた。
④ 代理再暗号化(PRE)技術の研究
PRE とクラウドコンピューティングモデルは非常に関連性がある。しかし、現在の PRE 方式には、欠陥があり、新しいネットワーク応用環境によって要求されている安全性をすべて提供することができない。特に、結託攻撃に関して安全モデルと方式の欠如である。研究代表者は上記の要件を意識した ID ベース PRE については初歩的な成果を得たが、機能上の改善や、実運用視点では計算コストの改善に取り組む必要がある。そこで、Lattice に基づいて、暗号文の拡張がしない単方向かつマルチホップの CCA セキュアな PRE や Pairing に基づいて、耐結託攻撃の PRE などの提案を試みた。
⑤ Threshold 暗号や秘密分散に関する研究
当初計画に含まれなかった内容であるが、Threshold secret sharing scheme と public key encryption(TSSS と TPKE)は分散システムにおいて重要な暗号技術である。さらに、鍵の再分割が可能な TPKE 方式を活用することによって、選択暗号文攻撃 CCA に対してセキュアな PRE 方式の一般構造が可能になる(CT-RSA2012)。既存研究の安全性は事前に攻撃者を固定するような静的な結託攻撃しか考えられなかったケースを改善する提案や効率性を改善する提案を試みた。

(3) 提案したシステムの実現性を検証：
PRE に関する提案方式の応用について、検討調査し、機密のレベルに応じて処理が可能な暗号化ファイル共有（デモ）システムを実装し、システムの実現性を検証した。

(4) 研究調査：
文献調査からスタートし、学会参加によって最新情報収集と研究交流や、メールベースと当面研究打ち合わせなどの手段で当分野の研究協力者と共同研究によって、計画を遂行した。

４．研究成果

下記成果(1)～(2)と(6)は課題１ポスト量子暗号、(3)～(6)は課題２クラウド環境で実用的な暗号の関連成果である。その中(6)は課題１と課題２を結合した成果である。

(1) **Lattice 暗号**：LWE に基づいて、量子攻撃に耐える効率的な認証暗号(Signcryption)方式を提案した。既存の Lattice ベース認証暗号方式と比べ、本研究主な貢献は初めて standard model 安全性を満たす方式を提案した。成果はインパクトファクタ 1.38 である論文誌 Mathematical Problems in Engineering に掲載された【5．雑誌論文⑦参照】。
(2) **非可換暗号**：Inner automorphism 群に基づいて耐量子攻撃の Chameleon ハッシュ関数と one-time signature 方式を提案した。特別の非可換代数構造下の Conjugacy Search Problem (CSP)関連仮定に基づいて標準モデルの CPA/CCA 安全性を満たす DHIES 方式を提案し、論文誌 Fundamental Informaticae と Security Comm．Networks に掲載された【5．雑誌論文⑥⑩と学会発表②参照】。
(3) **位置情報認証方式**：クラウド環境においては、ユーザー認証やアクセス制御にこれまで以上の安全性が要求され、位置情

報や時刻など物理的な情報を組み合わせる手法も検討されている。このように位置情報を利用する場面が多々出現している状況であるが、位置の詐称をネットワークプロトコルで見破ることは難しいという欠点もある。そこで位置情報そのものの正当性を示す認証方式が必要である。本研究では準天頂衛星及び地上放送の電磁波を利用した位置情報認証システムに加法準同型暗号を導入し、位置情報の詐称や改ざんなど中間者攻撃を防ぐ位置情報認証システムの設計を行った。成果は国内学会 SITA2011 で発表し、論文誌 IEICE で掲載された【5. 雑誌論文⑤と学会発表④参照】。

(4) **Threshold 暗号方式**：本研究では、標準モデルの下で高い安全性を満たしつつ、効率が良い方式の設計と評価を行った。具体的に、Hashed Diffie-Hellman 仮定で、静的な結託攻撃に対して選択暗号文攻撃(CCA)安全な効率が良い TPKE 方式、および素数 Order のペアリングに基づいて、弱い動的結託選択暗号文攻撃に(CCA-like)対して安全な TSSS 方式を初めて設計し、成果は The computer Journal と International J. of Distributed sensor network に採録された【5. 雑誌論文③④⑧と学会発表③参照】。特に、SCIS2014 で Hashed Diffie-Hellman に基づいて提案された方式を拡張したら鍵の再分割が可能になるという発表があったため、今後、効率的な PRE の一般化構造への展開が可能である。

(5) **プロキシ暗号**: まず、代理人に委託した権限を無効化させることが可能な Certificate ベース代理復号方式 standard model 下で IND-CCA 安全性を証明した。次は、代理復号と代理再暗号の二つの機能付き、IND-CPA/CCA に対して安全なプロキシ暗号方式（IBPdr）を提案した。IBPdr を用いて、機密のレベルに応じた処理が可能な暗号化データストレージシステムを実装した。本システムの応用例として非常時にも対応が可能な医療情報共有システムを挙げられる。さらにセキュアな自動車情報共有システムの実装などへの展開が可能である。本システムについて、国内学会 SCIS2014 で発表した。理論的な成果はインパクトファクタ 3.6 以上である論文誌 Information Sciences、および論文誌 IEICE で掲載された【5. 雑誌論文①⑨と学会発表①参照】。

(6) **Key-Private PRE:** LWE に基づいて、攻撃者が再暗号化鍵を持つ場合でも、この鍵に関わるユーザーが推測できないプロキシ再暗号化方式を設計した。量子攻撃に耐え、クラウドなど新たな応用環境に適応する長期利用が可能な暗号方式となる。成果は暗号界で歴史がある国際会議 Indocrypt2013 で発表し、LNCS プロシーディングで掲載された【5. 雑誌論文②参照】。

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 10 件）

① Lihua Wang, Jun Shao, Zhenfu Cao, Masahiro Mambo, Akihiro Yamamura, and Licheng Wang, "Certificate-Based Proxy Decryption Systems with Revocability in the Standard Model," Information Science, 査読有, 247:188-201 (2013) http://dx.doi.org/10.1016/j.ins.2013.06.026

② Yoshinori Aono, Xavier Boyen, Le Trieu Phong, Lihua Wang, "Key-Private Proxy Re-encryption under LWE," INDOCRYPT 2013, Springer-Verlag, Berlin, 査読有, LNCS 8250: 1-18 (2013) DOI:10.1007/978-3-319-03515-4_1

③ Yuanju Gan, Lihua Wang, Licheng Wang, Ping Pan and Yixian Yang, "Efficient Construction of CCA-Secure Threshold PKE Based on Hashed Diffie-Hellman Assumption," The computer Journal, 査読有, 56(10):1249-1257 (2013) DOI:10.1093/comjnl/bxs167

④ Yuanju Gan, Lihua Wang, Licheng Wang, Ping Pan, and Yixian Yang, “Efficient Threshold PKE with Full Security Based on Dual Pairing Vector Spaces”, International Journal of Communication Systems, 査読有(2013) DOI: 10.1002/dac.259

⑤ 田中 秀磨、王 立華、市川 隆一、岩間 司、小山 泰弘、“準同型暗号技術による位置情報認証 ”IEICE、査読有、J96-D(8): 1913-1924 (2013)

⑥ Ping Pan, Licheng Wang, Yuanju Gan, and Yixian Yang, Lihua Wang, "Chameleon Hash Functions and One- Time Signature Schemes from Inner Automorphism Groups," Fundamental Informaticae, 査読有, 126: 103-119 (2013) DOI: 10.3233/FI-2013-873

⑦ Jianhua Yan, Licheng Wang, Lihua Wang, Yixian Yang, Wenbin Yao, “Efficient Lattice-Based Signcryption in Standard Model”, Mathematical Problems in Engineering, 査読有 (2013) http://dx.doi.org/10.1155/2013/702539/

⑧ Yuanju Gan, Lihua Wang, Licheng Wang,

Ping Pan and Yixian Yang, "Publicly Verifiable Secret Sharing Scheme with Provable SecurityAgainst Chosen Secret Attacks," International Journal of Distributed Sensor Networks, 査読有 (2013)
http://dx.doi.org/10.1155/2013/902462

⑨ Lihua Wang, Licheng Wang, Masahiro Mambo, and Eiji Okamoto, "Identity-Based Proxy Cryptosystems with Revocability and Hierarchical Confidentialities," IEICE Transaction on Fundamentals, 査読有, E95-A(1): 70-88 (2012)
DOI: 10.1587/transfun.E95.A.70

⑩ Ping Pan, Lihua Wang, Licheng Wang, Lixiang Li, and Yixian Yang, "CSP-DHIES: A New Public-Key Encryption Scheme From Matrix Conjugation," Security and Communication Networks, 査読有, 5(7): 809-822 (2012)
DOI:10.1002/sec.376

〔学会発表〕(計4件)

① 王 立華、早稲田 篤志、野島 良、盛合 志帆、"PRINCESS:プロキシ再暗号化技術を活用したセキュアなストレージシステム"、査読無、2014年暗号と情報セキュリティシンポジウム SCIS2014、Jan.21-24、2014. 鹿児島県鹿児島市城山観光ホテル

② 王 立華、"Study on CSP-based Cryptography、" 代数系および計算機科学基礎研究集会、(口頭発表のみ) 査読無、Feb. 20-22、2012. 京都府京都市京都大学数理解析研究所

③ Yuanju Gan, Lihua Wang, Ping Pan, Licheng Wang, and Yixian Yang, "A CCA Secure Threshold KEM Scheme," 査読無, 2012 年暗号と情報セキュリティシンポジウム SCIS2012、Jan.30-Feb.2, 2012. 石川県金沢市金沢エクセルホテル東急

④ 王 立華、田中 秀磨、市川 隆一、岩間 司、小山 泰弘、"電波を使った位置情報認証"、第 34 回情報理論とその応用シンポジウム SITA2011、査読無、pp. 234-239、Nov.29-Dec.2、2011.岩手県岩手郡鶯宿ホテル森の風鶯宿

〔その他〕
ホームページ等
http://www2/nsri/fund/wang/kakenhi/index.html
http://www.nict.go.jp/nsri/fund/papers.html

６．研究組織
(1)研究代表者
王 立華 (WANG, Lihua)
独立行政法人 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：00447228

(2) 研究協力者：
・Licheng Wang (WANG, Licheng)
中国北京郵電大学・State Key Laboratory of Networking and Switching Technology・准教授
・Zhenfu Cao (CAO, Zhenfu)
中国上海交通大学・Department of Computer Science and Engineering・教授
・満保雅浩 (MAMBO, Masahiro)
金沢大学・理工研究域電子情報学系・教授
研究者番号：60251972
・Jun Shao (SHAO, Jun)
中国 Zhejiang Gongshang University・School of Computer and Information Engineering・准教授
・青野良範 (AONO, Yoshinori)
独立行政法人 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・研究員
研究者番号：50611125
・Xavier Boyen (BOYEN, Xavier)
Queensland University of Technology・准教授
・Le Trieu Phong (LE, Trieu Phong)
独立行政法人 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・研究員
研究者番号：40583191
・田中秀磨 (TANAKA, Hidema)
防衛大学校・情報工学科・准教授
研究者番号：30328570
・早稲田篤志 (WASEDA,Atsushi)
独立行政法人 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・研究員
研究者番号：10455454
・野島良 (NOJIMA, Ryo)
独立行政法人 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：40446597
・盛合志帆 (MORIAI, Shiho)
独立行政法人 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・室長
研究者番号：80636192