量子コンピュータの出現に対抗し得る公開鍵暗号の研究（081603008）

Research on Post-Quantum Cryptography

研究代表者

辻井重男　中央大学研究開発機構

Shigeo Tsujii　Research and Development Initiative, Chuo University

研究分担者

笠原正雄†　五太子政史†　小林邦勝†　境隆一†

只木孝太郎†　富田悦次†　林彬†　藤田亮†　村上恭通†

Masao Kasahara†　Masahito Gotaishi†　Kunikatsu Kobayashi†　Ryuichi Sakai†

Kohtaro Tadaki†　Etsuji Tomita†　Akira Hayashi†　Ryo Fujita†　Yasuyuki Murakami†

†中央大学研究開発機構

†Research and Development Initiative, Chuo University

研究期間　平成 20 年度～平成 22 年度

概要

本研究開発では、量子コンピュータが実用化された暁においても、現用あるいは新世代ネットワークで、安心・安全に秘匿通信やディジタル署名が行えることを目的として、暗号方式のみを置き換えれば済むような安全性の高い公開鍵暗号方式について研究開発を進めた。具体的には、多変数公開鍵暗号、ナップザック公開鍵暗号、及び、誤り訂正符号応用公開鍵暗号を研究開発の対象とし、本研究開発では、これら 3 種類の公開鍵暗号方式の各々について研究を深めると共に、それらの各論を総合し体系付ける立場からの研究を行った。

Abstract

This research project has been aimed at developing still secure encryption and digital signature schemes on the actually-used network or the new generation network, even though quantum computers are put in practical use, in such a way that the actually-used schemes only have to be replaced by our new schemes to accomplish the security against quantum computers. In particular, we have developed multivariate public key cryptosystems, knapsack-type public key cryptosystems, and code-based public key cryptosystems. We have deepened each of the researches on the three schemes, and moreover have integrated the theories of the three schemes to systematize them.

１．まえがき

現在、電子政府や電子商取引を始めとする広い分野において、電子署名や共通鍵暗号の鍵配送に利用されている公開鍵暗号は、RSA 暗号、及び楕円暗号である。RSA 暗号はその安全性を素因数分解の困難性に、楕円暗号は離散対数問題の困難性にそれぞれ依拠している。他方、量子コンピュータに関する研究が鋭意進められているが、それが実用化された場合、素因数分解問題も離散対数問題も、多項式時間という現実的時間（例えば数時間から数百日）で解かれてしまうことが明らかにされている。量子コンピュータの実現がいつになるか、予想は難しいが、一般に、技術の進歩は大方の予想に反して急速に展開することも少なくないので、今から、その出現に備えておかねばならない。

本研究開発は、このような暗号アルゴリズムの長期的な、あるいは不意の危殆化に備えて、量子コンピュータの出現に対抗し得る公開鍵暗号の構成法を確立することを目的としている。

２．研究内容及び成果

具体的には、多変数公開鍵暗号、ナップザック公開鍵暗号、そして誤り訂正符号応用公開鍵暗号の 3 種類の公開鍵暗号方式について研究開発を行った。研究開発の過程では、各方式の研究を深める過程で生まれたアイデアを、研究グループ全員で共有し、討議を重ね、相乗効果を得て、効率よく研究開発を推進した。特に、本研究開発の研究代表者・分担者全員は、会合（ゼミ）やメール等で、常時、情報交換を重ね、また実験データを転送し合い、緊密に連絡をとりながら研究開発を進めた。そして、本研究開発メンバーによる合同研究会を、年 5 回から 6 回、計 16 回開催して、互いに成果を持ち寄り、議論を深めた。

以下、多変数公開鍵暗号、ナップザック公開鍵暗号、誤り訂正符号応用公開鍵暗号、NP 完全型暗号方式に関する総合的考察の順に、具体的成果について説明する。

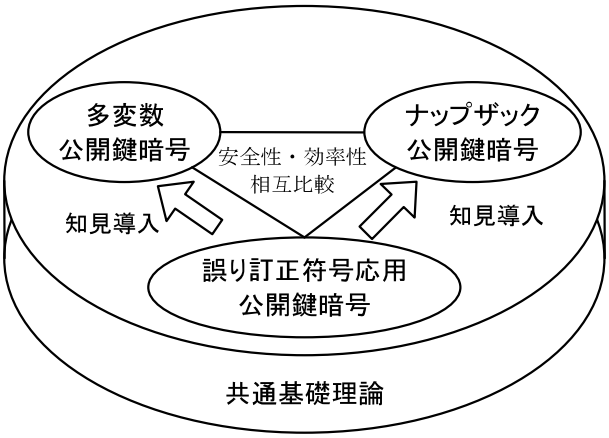

図　本研究開発の概要

２．１．多変数公開鍵暗号

多様な多変数公開鍵暗号を強化する汎用的概念装置である持駒方式について、これまでの方式をより効率化する

方法に関する研究を進め、PPS方式の提案に至っている。この新方式について、報道発表を行ない、新聞掲載されている。線形持駒行列方式については、効率的な鍵生成アルゴリズムの開発や、計算機実験に基づかない、厳密な理論を展開した。

安全性評価手法としては、グレブナ基底について、より効率的な計算法を提案し、その有効性を確認した。また、この種の攻撃に対する耐性等の立場から、公開鍵多項式にランダム性を導入し、これを向上するための方法を追及した。特に、ランク攻撃については、厳密解析を行うなど、数多くの検討を行った。そして、これら安全性に関する知見を基に、安全性の高いディジタル署名である、強化型STS署名方式、役割交代型署名方式の開発に至っている。

２．２．ナップザック公開鍵暗号

非線形性の導入や、誤り訂正符号、巡回符号、中国人の剰余定理、そして、一般のナップザック問題や、いままで使われることのなかった組み合わせ問題の応用等、多種多様な手法を取り入れることにより、新規性の大きい、より安全なナップザック公開鍵暗号方式の構成を行った。これらの方式の安全性に関しては、計算機実験による広範な調査等を行うことにより、多くの新たな知見を得ている。これまでに提案している行列型の方式については、安全性解析を完成させ、解読困難性を理論的に示すことができた。さらなる新方式の提案にあたっては、計３件の特許出願を行っている。

安全性評価手法としては、解析手法の確立を目指し、従来からある Shamir の攻撃法、並びに LLL アルゴリズムを用いる攻撃法のそれぞれについて、暗号に適した攻撃手法の解析を行った。

２．３．誤り訂正符号応用公開鍵暗号

誤り訂正符号応用公開鍵暗号は、多変数公開鍵暗号、或いはナップザック公開鍵暗号と、奥深い所で繋がっており、その結び付きについての考察は、様々な可能性を与え得る、という新しい視点に基づいて、研究開発を進めた。そして、これを追求した結果、これらの暗号方式のそれぞれが有する弱点を互いに補強し合う、新しい暗号方式を開発した。特に、平文・暗号文対応が、真に１対多となる方式を実現し、線形多変数公開鍵暗号において、新しい分野を開拓した。また、効率的な組み合わせ手法を探究した結果、確率的構造を導入することに成功し、注目すべき成果を得た。

２．４．NP 完全型暗号方式に関する総合的考察

NP 完全問題のより効率的な解法の研究は、本研究開発で開発を行う NP 完全型暗号方式の安全性向上に直結する。そのため、典型的な NP 完全問題であり、かつ多くの重要な応用を持つ、最大クリーク問題を中心に取り上げ、この問題がアルゴリズムの革新により、どれほど効率化されるのかを、実験的、理論的に明らかにした。特に、アルゴリズムの各部分の効果について詳細な理論的、或いは実験的解析を行い、アルゴリズムの高速性が由来する要因を特定した。そして、それを最大クリーク抽出アルゴリズム一般の高速化の基本技術として位置付け、他の研究グループが異なった手法に基づいてアルゴリズムを開発する場合においても、その効率化に容易に転用出来る形に発展させ、更に、多変数公開鍵暗号の攻撃アルゴリズムの高速化の基本技術として確立した。具体的には、先ず、逐次詳細化した理論的解析結果を、一般グラフの上において与えた。従来の理論解析の殆どは、特殊グラフの上でしかなされておらず、他の NP 完全問題との関係付けが困難であった。これに対して、一般グラフ上における本結果は、大きな意義を持つ進展である。

３．むすび

本研究開発は、実用的な量子コンピュータが現れる将来にその有効性が発揮される技術であるが、現在のネットワークでも、また NGN などの新世代ネットワーク上でも、そのまま活用できる技術である。RSA 暗号や楕円暗号に基づく現在の公開鍵基盤に対し脅威となるほどの大規模な量子コンピュータの実用化は、20 年以上先とも言われているが、仮に 10 年先に量子コンピュータが出現したとしても、或いは、現在のコンピュータ環境の下で、素因数分解や離散対数問題を効率的に解くアルゴリズムが万一発見されて、RSA 暗号や楕円暗号が使用不可能となったとしても、本研究開発で得られた成果は、暗号の危殆化を防いで、情報ネットワークの安全性を保護し、人・モノ・金・文書などの真正性を保証する公開鍵暗号方式の実用化に対して有用な知見と手法を提供するものである。このように、本研究開発で最終的に得られた成果は、関連分野、及び社会経済に大きな波及効果を与えるものである。

【誌上発表リスト】

[1] Shigeo Tsujii, Masahito Gotaishi, Kohtaro Tadaki, and Ryo Fujita: “Proposal of a signature scheme based on STS trapdoor,” Proc. PQCrypto 2010, Lecture Notes in Computer Science, Springer-Verlag, Vol.6061, pp.201-217, May 25-28, 2010, Darmstadt, Germany.

[2] Tomohiro Shintani and Ryuichi Sakai: “Cryptanalysis on 2 dimensional subset-sum public key cryptosystem,” Proc. ICIS 2009, ACM International Conference Proceeding Series, ACM, Vol.403, pp.1466-1469, November 24-26, 2009, Seoul, Korea.

[3] Yasuyuki Murakami, Takeshi Nasako, and Masao Kasahara: “A new trapdoor in knapsack public-key cryptosystem with two sequences as the public key,” Proc. ICCIT2008, Vol.2, pp.357-362, November 11-13, 2008, Busan, Korea.

【申請特許リスト】

[1] 辻井重男, 小林邦勝, 笠原正雄:「複数のナップザックを用いる公開鍵暗号方式による暗号システム、鍵生成装置、暗号化装置、復号装置、データ交換方法およびプログラム」, 提出日 2009.12.16, 特願 2009-285093.

[2] 林彬:「鍵生成装置、およびその装置を利用可能な暗号化装置ならびに復号装置」, 提出日 2009.7.31, 特願 2009-179664.

[3] 林彬:「暗号鍵生成装置、およびその装置を利用可能な暗号化装置ならびに復号装置」, 提出日 2009.4.23, 特願 2009-105254.

【受賞リスト】

[1] Theoretical Computer Science Top Cited Article 2005-2010　受賞、受賞対象　Etsuji Tomita, Akira Tanaka, Haruhisa Takahashi: “The worst-case time complexity for generating all maximal cliques and computational experiments,” (Invited paper for the special issue on COCOON 2004), Theoretical Computer Science, 363, pp.28-42 (2006).
http://www.uec.ac.jp/news/prize/20100906-2.html

【報道発表リスト】

[1]「量子コンピュータでも解けない次世代の暗号方式」, セキュリティ産業新聞, 2009 年 7 月 10 日号,
http://www.secu354.co.jp/contents/cyumoku/09/cyumoku-090710-2-09.htm

【本研究開発課題を掲載したホームページ】

http://www2.chuo-u.ac.jp/kikoh/scope/chuo-crypt-scope-index.html