様式 C-7-2

自己評価報告書

平成 23 年 4 月 27 日現在

機関番号：22604
研究種目：基盤研究（C）
研究期間：2008　～ 2011
課題番号：20540125
研究課題名（和文）代数学的アルゴリズムの計算量的困難性に関する研究とその公開鍵暗号への応用
研究課題名（英文）A Study of the Hardness of Algebraic Algorithms and Its Applications to Public-Key Cryptography
研究代表者
内山　成憲（UCHIYAMA SHIGENORI）
首都大学東京・大学院理工学研究科・准教授
研究者番号：40433172

研究分野：数物系科学
科研費の分科・細目：数学・数学一般（含確率論・統計数学）
キーワード：アルゴリズム、暗号・認証、量子コンピュータ

１．研究計画の概要

1970 年代の公開鍵暗号の概念の提案以来、数多くの実用的な公開鍵暗号方式が提案され、それらは IT 社会とも呼ばれる現代社会では欠かすことのできない重要な技術となっている。一方、その安全性を支える代表的な数学的問題は量子計算機と呼ばれる計算機が実用的になった将来には、効率よく解かれてしまうことが知られている。有名な RSA 暗号や Rabin 暗号の安全性は素因数分解問題に、ElGamal 暗号の安全性は有限体（又は、有限体上の楕円曲線）上の離散対数問題の計算量的困難さにそれぞれ基づいている。これらの整数論的問題は、現在のところ十分大きなサイズであれば、既存の計算機の性能をもってしても現実的な時間では解くことは非常に難しいと考えられている。一方、量子計算機と呼ばれる次世代の計算機が実現された暁には、これらの整数論的な問題は、1994 年に Shor により提案された量子計算機に基づくアルゴリズムを用い効率良く解かれることが示されている。現在の計算機の進歩の歴史や、上記の整数論的問題に基づく公開鍵暗号が現代社会の根幹を支える重要技術の１つとなっている事を考えると、近い将来量子計算機が実現された際に、社会に与える影響の大きさを少しでも軽減するためにも、今からその対策を進めておくことは十分に意義があると考えられる。本研究では、量子計算機を用いた攻撃に対して耐性を持つ公開鍵暗号の提案を目標とし、既存の方式やそれが基づく数学的問題の解析を行うものである。大きくわけて以下の２段階で行う。

（１）代数学的な問題に対するアルゴリズムの解析及び改良：格子に関連する問題や組み合わせ論に関する問題等、量子計算機を用いても解くことが困難と考えられる問題、特に他の今まで扱われることのなかった代数学的な問題も視野に入れ実装も含めた解析を行う。

（２）上記の問題に基づく新しい落とし戸つき一方向性関数の構成：実用的な公開鍵暗号のしかけとなる一方向性関数の候補としては上記の数論的な問題しかないと言っても過言ではなく他の代数学的なアルゴリズムの解析に基づき、新しい一方向性関数の構成を試みる。

２．研究の進捗状況

これまで、量子計算機に関して耐性があると期待される方式の安全性解析及び関連する代数学的アルゴリズムの解析を行ってきた。主な結果を以下に述べる。多変数暗号と呼ばれる公開鍵暗号の一方式であり、高速なデジタル署名方式である 1IC 方式と呼ばれるものに対して、最も一般的な条件の下で実用的な攻撃アルゴリズムを提案し、実装実験により提案手法が効率的であることを示した。1IC への攻撃法は Fouque 等によって既に提案されてはいたが、彼等はパラメータ 1 が奇数の場合のみ詳しく扱っていた。我々の提案方式は彼等のものとは異なり、1 が偶数奇数の双方に有効である。次に、格子における最短ベクトルを求める問題の困難性に基づくナップザック暗号の安全性評価について解析を進め、Sampling Reduction と呼ばれるアルゴリズムの改良法の提案およびその実装を行った。パラメータサイズが大きくなると実装そのものが困難となるため比較的小さなサイズのもにしか扱えなかったが、ある条件下では提案手法が高速であることを実装実験により確認した。Shamir によって提案されていた双有理置換を用いた署名方式

の非可換版が、2008 年に橋本等によって提案されていたが、これに対して、いくつかのシステムパラメータが小さな場合に効率的に動く攻撃法を提案し、実装によりその効果を確かめた。2009 年に Gentry によって格子を用いた世界初の完全な準同型暗号が提案されたが、パラメータ生成等を含めて実装に関して詳細には述べられていなかったため、具体的なパラメータ生成法を提案し、比較的小さなサイズのものではあるが実装によりその効果を確かめた。最後に、楕円曲線上のペアリングの計算に関して、Elliptic Net と呼ばれる数列を用いた新しい計算法が 2007 年に Stange によって提案されていたが、これに対するある高速化に対して解析を行い、実装によりその効果を確かめた。また、それらを用いて現在知られている効率のよいペアリングである Ate ペアリングとその変形ペアリングを書き換える詳しい公式を提案し、実装によりその効果を確かめた。また、既存のペアリング計算手法である Miller のアルゴリズムに関して、正規化と呼ばれる操作を施す必要性について詳しい解析を行い、現在知られている BN 曲線等のペアリングに適した楕円曲線を用いる限りは、必ずしも正規化は必要ないことを数学的に証明した。その他、代数曲面暗号と呼ばれる暗号方式へのリダクション攻撃と呼ばれる攻撃法の一般化を提案した。

３．現在までの達成度

②おおむね順調に進展している。

量子計算機に対して耐性があると期待されている方式の解析や解析が十分でないと考えられる代数学的な問題やアルゴリズムの解析には十分に時間をかける必要があり、それを主に行ってきたが、安全だと期待されていた署名方式等への効率的な攻撃法の提案等も成功しており、現状ではおおむね順調に進展していると考えられる。

４．今後の研究の推進方策

今まで行ってきたいくつかの代数学的アルゴリズムの解析や暗号方式の解析に基づき具体的な問題の定式化やそれに基づく落とし戸つき一方向性関数の構成に取り組む。

５． 代表的な研究成果

（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 4 件）

① Naoki Ogura, Go Yamamoto, Tetsutaro Kobayashi, Shigenori Uchiyama, A Key Generation Algorithm for Gentry’s Lattice Based Homomorphic Encryption Scheme, Proc. of IWSEC2010, LNCS6434, 70-83, 2010, 査読有
② Naoki Ogura, Shigenori Uchiyama, Cryptanalysis of the Birational Permutation Signatue Scheme over a Non-commutative Ring, JSIAM Letters, Vol.2, 85-88, 2010, 査読有
③ Naoki Ogura, Shigenori Uchiyama, On Patarin’s Attack against the 1IC Scheme, IEICE Trans. Fundamentals, Vol.E93-A, No.1, 33-41, 2010, 査読有
④ 小椋直樹, 内山成憲, 中村憲, SFLASH署名方式への攻撃法の実装について, 日本応用数理学会論文誌, Vol.19, No.4, 433-445, 2009, 査読有

〔学会発表〕（計 5 件）

① 小椋直樹, 三原千穂, 秋山浩一郎, 三宅秀亨, 内山成憲, 代数曲面暗号に対するFaugereらの攻撃法の理論的考察, 2011 年暗号と情報セキュリティシンポジウム, 2011 年 1 月 27 日, リーガロイヤルホテル小倉
② 小椋直樹, 内山成憲, 金山直樹, 岡本栄司, 正規化されたMiller関数を用いたペアリング計算についての注意, 2011 年暗号と情報セキュリティシンポジウム, 2011 年 1 月 27 日, リーガロイヤルホテル小倉
③ 小椋直樹, 金山直樹, 内山成憲, 岡本栄司, Elliptic Net を用いた Ate ペアリングとその変形, 日本応用数理学会 2010 年度年会, 2010 年 9 月 8 日, 明治大学
④ 小椋直樹, 内山成憲, 非可換双有理置換を用いた署名方式の安全性について, 日本応用数理学会 2009 年度年会, 2009 年 9 月 30 日, 大阪大学豊中キャンパス
⑤ 小椋直樹, 内山成憲, 1IC 方式への Fouque 等の攻撃法について, 2009 年暗号と情報セキュリティシンポジウム, 2009 年 1 月 21 日, 大津プリンスホテル

〔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〕