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２４年　５月１８日現在

機関番号：１１３０１
研究種目：基盤研究(C)
研究期間：２００９～２０１１
課題番号：２１５００００２
研究課題名（和文）量子計算による攻撃に対して安全な暗号化関数の構築

研究課題名（英文）Constructing encryption functions secure against quantum computing

研究代表者
静谷　啓樹　（SHIZUYA HIROKI）
東北大学・教育情報基盤センター・教授
研究者番号：５０１９６３８３

研究成果の概要（和文）：
現在のセキュリティ基盤に使用されている暗号系は、量子計算機によってそのほとんどが破綻する危険がある。本研究は、量子計算のこの潜在的な能力が現実になる前に、破綻を回避するための理論基盤と対抗策を構築しようというものである。その対抗策とは、現在の暗号系の安全性の根拠となっている問題と別のより困難な問題を融合させて、量子計算機といえども困難な領域に問題を移動させることが基本となっている。本研究ではこれを「リフティング」と呼んでいる。本研究により、リフトされるべき問題の範囲とその計算量理論的性質、リフトに使われるより難しい問題との関係などが明らかにされた。

研究成果の概要（英文）：
Quantum computers are potentially powerful enough to break any existing cryptographic schemes that are used to keep information and information systems safe and secure. Therefore we attempt to establish a theoretical background to construct a countermeasure against quantum computing. Our main idea is to strengthen the difficulty of a cryptographic primitive by combining it with other harder problem, so that the strengthened primitive can be placed beyond the reach of quantum computers. We call this technique “lifting”. In this research project, we have shown the lower bound of cryptographic primitives to be lifted, their complexity-theoretic properties, and the relationships among the problems used for lifting.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
平成 21 年度	500,000	150,000	650,000
平成 22 年度	300,000	90,000	390,000
平成 23 年度	300,000	90,000	390,000
年度			
年度			
総　計	1,100,000	330,000	1,430,000

研究分野：　総合領域
科研費の分科・細目：　情報学・情報基礎
キーワード：　暗号化関数、量子計算機、素因数分解問題、離散対数問題、NPMV 完全、NP 完全

１．研究開始当初の背景

暗号技術は、共通鍵系、公開鍵系、及びそれらの混成系に概ね分類される。このうち公開鍵系は単なる秘密通信だけでなく、ディジタル署名や個人認証などの機能を利用して、電子政府、電子マネー、電子決済、公開鍵基

盤など、重要な社会・経済基盤が組み上げられている。それらの安全性を担保しているのは、素因数分解問題や離散対数問題、及びそれらの派生問題を現実的時間内に解くことの難しさである。逆に言えば、この二つの問題を解く効率的なアルゴリズムが発見されれば、現代の社会・経済基盤は即座に破綻する。

1994年に公表されたショア（P. W. Shor）のアルゴリズムは、量子計算機上でこれら二つの問題を効率的に解くものである。すなわち、量子計算機が本格的に実用化されれば、現在の公開鍵系技術の殆どが破綻することを意味している。なお、ショアのアルゴリズムを実際に量子計算機上にインプリメントし、合成数15を3と5に分解できたとの報告があるが(L.M.K. Vandersypen et al, Nature, 2001)、まだ現実的脅威ではない。

量子計算機の本格的実用化が何年後かについては研究者によって様々な意見があり、大きな幅がある。しかしながら、破綻のシナリオが現に存在する以上は、何らかのブレークスルーによる本格的実用化の突発的繰上げに備え、現行の公開鍵系技術に関して対策を講じ、破綻を回避、もしくは最小限度のダメージに抑える技術を開発しておく必要がある。

２．研究の目的

本研究ではこのような背景に基づいて、現在の公開鍵系技術の枠組みを大幅に変えることなく、量子計算機の実用化という事態を迎えても、最小限度のダメージで破綻を回避できる新しい手法を構築することを目的としている。

具体的には、素因数分解問題(IF)と離散対数問題(DL)という現在の公開鍵技術の根幹をなす二つの問題に対して、それぞれに別の問題(Q)を自然に融合させ、難しさを持ち上げること（本研究では「リフティング」(lifting)と呼ぶ）によって新しい問題を構成し、それに基づいて新しい暗号化関数を導出する。その際、問題Qは量子計算機で効率的に解かれるとは知られていない問題を選ぶことが重要である。これにより量子計算機によってIFやDLの難しさが崩れてもQの困難さは依然として残り、完全な破綻は回避できる。

本研究は、そのようなリフティング技術及びそれを支える理論の構築を目的としている。

３．研究の方法

リフティングの概念と基本形は研究代表者らの先行研究（Hasegawa, Hatanaka, Isobe, Shizuya, IEICE Trans. Fundamentals, 2008）で示されており、この手法を現実の問題に適用できるよう鍛え上げれば本研究の目標に達する。そのためには、手法の各構成要素について基礎的な事実を解明して蓄積する必要があり、本研究期間を通じて、基本的には次の二つのアプローチにより研究を進めた。

(1)リフトされる側の性質の解明

素因数分解問題(IF)や離散対数問題(DL)を別の（量子計算機では容易に解かれないと考えられる)問題Qでリフトするにあたって、IFやDLに帰着する派生問題、定義する有限群の違いに応じたDLのバリエーションなどについて、それらの複雑さの位置づけをNPやNPMVのクラスの中で特徴づける。この作業は、暗号への応用の観点から持ち上げるべき問題の範囲を特定するとともに、リフティング前後の比較により、その効果を計算量のクラスの言葉で表現するために必要である。

(2)リフトする側とされる側の性質の解明

IFやDLなどリフトされる側の問題と、リフトする側の問題Qとの間に明確な帰着関係が存在するならば、帰着が見つかっていない別のQ’ でリフトするよりは、攻撃の手がかりが多いという意味で安全性が弱まるのは明らかである。互いに多項式時間帰着しそうもない問題のペアを見つけることは、それゆえ重要である。

４．研究成果

本研究で得た成果の概要を前節に記載の二つのアプローチに沿って述べる。

(1)リフトされる側の性質の解明

①公開鍵系の安全性は、何らかの問題の難しさを仮定することで成立している。そのような仮定の中で最も強い仮定（したがって、ひどく難しいとまでは示されていない問題を現実的に困難と見なす立場の仮定）の一つとして、擬自由群仮定が知られている。これは直観的に言えば、ある群を対象にしたとき、その群が計算量的な意味で自由群の性質も同等に備えているという仮定である。これが成り立てば、例えば自由群の上で解のない方程式は、対象となる群の上でも（解はあるかもしれないが）事実上、計算量的に解けないと方程式となる。RSA 型合成数を法として構成される剰余類環の乗法群について、もしその群に擬自由群仮定が成立すれば、RSA 暗号など素因数分解問題(IF)に付随するほとんどの暗号系は安全になるため、リフトされる側の問題の範囲としては下限的な位置づけとなる。本研究では、擬自由群の概念に関して従来、複数の研究者が独立に定義してきたものを再吟味し、それらの定義の包含関係（同等性も含む）を証明することで、統一的な擬自由群の姿を初めて明らかにした。

②離散対数問題(DL)に帰着する派生問題である Diffie-Hellman 問題(DH)に関して、DHを解くのは現実的に困難であるとする立場を「DH 仮定」と呼ぶ。擬自由群について DH

仮定が成立するかどうか、すなわち DH 問題を定義する群が擬自由群ならば DH 問題は困難であるかどうかは未解決問題であったが、わずかに弱い形の問題設定で検討することで、それを肯定的に解決した。
③DL のバリエーションとして、代数的トーラス上の離散対数問題(TDL)がある。TDL は暗号系におけるメッセージ効率の観点から重要な応用を持っているが、その問題の難しさについては、計算量理論の観点から厳密には解明されていなかった。本研究では、底の位数の証明が付いた（すなわち群の位数の素因数分解が与えられているという状況での）有限体上の離散対数問題が TDL に帰着することを証明し、TDL の難しさが一般的な DL の難しさで下から支えられていることを明らかにした。またこの結果は素因数分解問題(IF)が簡単に解けるならば、DL と TDL の難しさが等価であることも意味している。
④リフティングの結果として定義域がクラス co-NP にも属することとなった関数 f の複雑さに関する二つの新しい特徴づけが得られた。すなわち、$f \in$ FewPFg ならば、f の計算はある NP∩co-NP の言語に帰着すること、ならびに任意の $f \in$NPMVg について、f の計算が NP∩co-NP の言語に帰着するならば NP = co-NP となることを示した。 二つ目の主張は、NP≠co-NP である限り NPMVg の関数の中には、その計算が NP∩co-NP を超える難しさで特徴づけられるものが存在することを意味している。一方で、暗号系に応用しやすい問題は、受理・拒絶の両方の証拠が得られるという意味で NP∩co-NP で特徴づけられるものが多い（確率的クラスに拡張した場合は AM∩co-AM)。これらの事実と量子計算機で容易に解かれる範囲と重ね合わせることにより、量子計算による攻撃に耐えうる暗号化関数の存在限界の目安が得られる。
(2) リフトする側とされる側の性質の解明
①リフトする側の問題とリフトされる側の問題のペアに明確な帰着関係があっては、リフティング後に共倒れになる可能性があることから、互いに帰着しそうもないペアが存在するならば、それをリフティングに使うことを目指して検討を行った。その結果、ある特定の帰着計算モデルのもとで「帰着しない関数のペア」が存在することを具体的に指摘した。これは、もし帰着したとすると、起こりえないと信じられている事態を招くという意味で、「帰着しない」という現実を導く手法である。具体的に「帰着しない」と証明したのは、IF に関連する関数（強 RSA 問題と呼ばれる問題を計算する関数）と DL に関連する関数（判定版の DH 問題を計算する関数）である。この両問題に関してこのような形で分離に成功したのは 2 例目である（1 例目も研究代表者らによる)。
②リフティングの結果として生成された問題を既存の枠組みで認証などに応用するのではなく、リフティングという手法を直接的に活かせる新たな枠組みとして「少知識証明」(Little Knowledge Proof System)なる対話証明的な概念の提案と検討を始めた。具体的には、従来の統計的ゼロ知識証明や完全ゼロ知識証明をもつ言語のクラスを超えたもので特徴づけられる問題に対しても、ゼロ知識証明と類似のプロトコルで、ただし知識の漏れを許容する形で証明ができるようにすることを目指している。リフティングのペアを適切に選ぶことにより、量子計算機の実用化によっても破綻しないと期待される問題が構成されるが、それを含むと考えられる新たな認証系の一構成が示された。

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３件）［査読有り］
(1) Shingo Hasegawa, Shuji Isobe, Hiroki Shizuya, “On the Pseudo-Freeness and the CDH Assumption,” International Journal of Information Security, 8, 347-355, 2009.
(2) Shuji Isobe, Eisuke Koizumi, Yuji Nishigaki, Hiroki Shizuya, “On the Complexity of Computing Discrete Logarithms over Algebraic Tori,” Lecture Notes in Computer Science, 5888, 433-442, 2009.
(3)静谷啓樹, “情報セキュリティ教育の輪郭線,” 情報リテラシー研究論叢, 1, 72-83, 2012.

〔学会発表〕（計７件）
(1)長谷川真吾, “言語認識の複雑さと関数計算の複雑さの関係,” 電子情報通信学会情報セキュリティ研究会, 2010 年 7 月 2 日, 弘前大学.
(2)福光正幸, “SLP を用いた帰着に基づく暗号学的仮定の分離,” 電子情報通信学会 2011 年暗号と情報セキュリティシンポジウム, 2011 年 1 月 25 日, 北九州市リーガロイヤルホテル小倉.
(3)Shingo Hasegawa, “On the Relationship between Recognizing Languages and Computing Functions,” 電子情報通信学会 2011 年暗号と情報セキュリティシンポジウム, 2011 年 1 月 25 日, 北九州市リーガロイヤルホテル小倉.
(4)許智元, “多価関数における自己帰着と many-one 型帰着について,” 電子情報通信学会情報セキュリティ研究会, 2011 年 3 月 4 日, 大阪大学.
(5)福光正幸, “SLP に基づく強 RSA 仮定と DDH 仮定の分離,” 電子情報通信学会情報セキュリティ研究会, 2011 年 11 月 15 日, 大阪

電気通信大学.
(6)岩崎淳也, “情報の漏れを許容する知識の対話証明,”電子情報通信学会情報セキュリティ研究会, 2011 年 11 月 15 日, 大阪電気通信大学.
(7)高橋大樹,“環準同型性を持つ公開鍵暗号の一構成,” 電子情報通信学会 2012 年暗号と情報セキュリティシポジウム, 2012 年 2 月 1 日, 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
http://www.isl.is.tohoku.ac.jp/~shizuya/

６．研究組織
(1)研究代表者
静谷 啓樹（SHIZUYA HIROKI）
東北大学・教育情報基盤センター・教授
研究者番号：５０１９６３８３

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：