様式Ｆ－１９

科学研究費助成事業（学術研究助成基金助成金）研究成果報告書

平成２５年５月 23 日現在

機関番号：１７１０２
研究種目：挑戦的萌芽研究
研究期間：2011～2012
課題番号：23650008
研究課題名（和文）計算量的に独立な一方向性関数の構成と暗号プロトコルへの応用に関する研究
研究課題名（英文） A study on construction of computationally independent one-way functions and their application to cryptographic protocols
研究代表者
櫻井 幸一（SAKURAI KOUICHI）
九州大学・システム情報科学研究院・教授
研究者番号：60264066

研究成果の概要（和文）：
主要課題であった計算量的な独立な関数の対に関して、具体的関数を離散対数の困難性のもとで構成する事に成功した。独立性の証明には、平方 Diffie-Hellmann 問題の困難性が通常の DH 問題のそれと同等であることを利用する。この結果は 2013 年の暗号と情報セキュリティシンポジウムで発表した。この成果を、複数の海外の研究者に紹介した。特にシンガポール国立大学での講演の際に、客員教授として滞在していた Yunlei ZHAO(復旦大学,中国)からは、彼自身の暗号プロトコル研究の一部に、類似の概念に相当する関数を利用していること、さらに関数の堅固性(non-malleable)という視点からもっと一般的な形での定式化をすすめられた。Yunlei ZHAO の 2013 年後半の半年の招聘期間中に､彼と共同でプロトコルの堅固性に注目し、暗号鍵交換方式における安全性との関係を論じた。この共同研究の一部は、Yunlei ZHAO が、2013 年との暗号と情報セキュリティ シンポジウムで発表した。

研究成果の概要（英文）：
We succeed to construct an explicit pair of computationally independent one-way functions from the hardness of the discrete logarithm problem. Our proof argument is based on the square Deffie-Hellmann problem. This main result is presented in Symposium of Cryptography and Information Security 2013 . Also we get a joint researcher, Prof. Yunlei ZHAO (Fudan Univ. China) who was visiting in Singapore Management Univ. when Kouichi SAKURAI has visited the security lab. His suggestion is some relationship between non-malleability of functions and our notion of computationally independent one-way functions. Prof. Yunlei ZHAO has visited Kyushu Univ. from Sept 2012 for 6 months thanks to NICT's inviting program of foreign researcher to Japan, and we perform joint research on this topic including cryptographic key exchange protocols, a partial result of which is presented also in Symposium of Cryptography and Information Security 2013.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
交付決定額	2,800,000	840,000	3,640,000

研究分野： 情報学分野
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：暗号理論、一方向性関数、疑似乱数生成、計算理論、Diffie-Hellmann 問題、暗号プロトコル、堅固性、安全性評価

１．研究開始当初の背景

1.1 学術的背景

一方向性関数は、代表的な暗号原理として暗号理論で研究されてきた。また一方向性関数の存在は、”NP vs P”問題との関係で計算量理論の重要な基礎分野としても確立され、数多くの研究論文が発表されている。暗号理論の主流としては、単一種の一方向性関数に基盤を置き、公開鍵暗号などすべての暗号原理を、この一方向性関数から導くなり、差分を解析するものである。

これに対して、研究代表者は、２０年前に、異なる２つの一方向関数に独立性の概念を導入した：

『*最近、interactive な証明系や大規模なネットワーク通信を考える上で、複数の一方向性函数を併用するプロトコルが数多く提案されているが、なりすましや秘密情報が漏れてしまうケースも少なくない。そうした理由の１つに、２つの一方向性函数 f,g を考えた時、この２つのペア{f,g}はもはや一方向性函数ではなくなるということが考えられる。こうしたことを踏まえて、ここでは一方向性函数のペアに対して「計算量的に独立」という概念を定義してその性質を調べ、また暗号認証プロトコルへの応用を考える。*』[櫻井-井上“一方向性函数に関する２、３の考察”1989 年暗号と情報セキュリテイシンポジウム]

しかしこの時点では、具体的に関数の存在証明までには至らず、その構成は、未解決問題として残ったままであった。これに対して研究代表者は、特殊ではあるが暗号ではよく利用される数論的構造を利用することで、本構成の糸口をつかんだ。ここに、２０年間保留にしてきた自身の独創的研究課題を掘り下げることになった。

1.2 関連研究

独立性を議論した関連研究としては、暗号原理の一つであるビット委託プロトコルにおいて、相互独立性の概念とその実現が、2001 年になってやっと MIT の暗号グループにより発表された[Mutually Independent Commitments” by Liskov, Lysyanskaya, Micali,Rezyin,and Smith,ASIACRYPT 2001]。ビット委託は、一方向性関数と密接に関係する暗号原理であるが、関数単体ではなく一方向性関数を利用したプロトコルであることに注意する。Liskov らは、２者間で双方がビット委託する際の公平性から、この概念に到達している。

また、暗号システムへ一方向性ハッシュ関数の族を応用する方式が提案されている[D. Naor, M. Naor, and J. Lotspiech, “Revocation and tracing schemes for stateless receivers,” Proc. CRYPTO2001]。ここでも、関数族の非相関を暗に仮定しているものの、関数の満たすべき厳密な性質までには言及していない。関数の性質次第ではシステムの安全性に影響するが、こうした問題点を指摘した論文すらまだ発表されていない。

２．研究の目的

暗号理論で基本的な役割を果たす一方向性関数の組に対する独立性と、これを満たす関数の具体的構成と応用を展開する。これにより、複数の暗号関数を利用する既存の暗号プロトコルの安全性を再評価すると同時に、新たに構成した関数を適用し安全性と通信効率とを向上させる。さらに、計算量的に独立な一方向性関数が原理としてどの程度強い暗号論的仮定なのか、構造論手法を用いて明らかにする。

何をどこまで明らかにしようとするのか

(1)２０年間、未解決のままであった具体的関数を、数論的仮定のもとで構成する。

(2)一方向性関数の独立性と、MIT グループによるビット委託の相互独立性との関係を明らかにする。

(3)計算量的独立な一方向関数が暗号原理として、どの程度強い仮定なのか、構造論的暗号理論の手法を用いて解析する。

学術的な特色及び予想される結果と意義

ヒューリスチックな議論のもとで、複数の一方向性関数族を利用した応用システムも提案されているが、我々の提案する独立性の概念を適用することで、こうした既存の提案システムの安全性を再評価し、期待する安全性達成のため、用いる暗号関数の条件を精密化することが可能となる。今回は、特殊な数論的仮定(Diffie-Hellmann 問題)を用いて、独立な一方向性関数の構成を試みるが、逆に、こうした数論的問題を内在的に特徴付ける性質の導出も期待でき、暗号と計算論の融合領域において、新たな研究分野の開拓にも貢献できる。

３．研究の方法

3.1 基礎研究かつ理論的検討が主なため、研究代表者が単独で２年間遂行した。初年度は関数の構成と性質の特徴解析を行った。

数論的仮定のもとで、具体的関数を、離散対数問題の上に構築する。

[Intractable Problems in Cryptography Neal Koblitz and AledMenezes Cryptology ePrint Archive: Report 2010/290]の６章では、平方 Diffie-Hellmann 問題の困難性が通常の DH 問題のそれと同等であることを示している。(squareDH = DH)

この命題とここでの証明技法は、探し求めていた計算量的に独立な関数の構成に有効である見込みが大であること予想して、研究を始めた。

積極的に海外の研究機関を訪問し、部分的な結果でも紹介に努めた。その中で、シンガポール国立大学での講演の際に、客員教授として滞在していた Yunlei ZHAO(復旦大学, 中

国)が、類似の問題意識をもっており、H24 年後半は、NICT の海外研究者招聘プログラムの支援を受けて、共同研究を実施した。

3.2 斬新なアイディアやチャレンジ性

独立な一方向性関数の組の概念は、研究代表者が、２０年前にその重要性を認識し提起した。

さらに、その後２０年以上、誰も研究していないという意味では独創的であり、類似のビット委託に関して MIT 暗号グループが１０年前に研究しているという意味で、影響力も含めて有意義である。この MIT の相互独立なビット委託の研究も、その後は途絶えていることに注意する。

3.3 新しい原理の発展や斬新な着想や方法論の提案、成功した場合の卓越した成果

暗号理論も、この２０年間で大進歩した。計算理論的に困難な数論問題の解析もすすみ、楕円曲線型離散対数問題やペアリングなど新しい道具も進化している。特に Diffie-Hellman 問題に今回は注目し、特殊ではあるが、多くの研究者が導入しているある種の数論的仮定をつかえば、我々が求める計算量的に独立な関数の構成が可能であることがわかってきた。（本申請時の 2010 年１０月時点では、有力な候補となる構成がほぼわかってきた。）

一方向性関数をもちいた暗号システムは数多く提案され、安全性も証明されたものが多いが基本的には単一の一方向性関数に基づくものである。一方向性関数のみを仮定した基本システムは、その汎用性から適用範囲は広いが、通信効率が課題となる。このため、公開鍵暗号原理や、さらには実装可能な RSA 暗号に

より強い仮定を設けても、効率改善をはかる設計が行なわれている。ゼロ知識証明を利用した暗号プロトコルの効率改善のために、複数の一方向性関数を導入した研究

[K.Koyama,”Direct Direct demonstration of the power to break public-key cryptosystems”, Proc. Auscrypto’90]もあるが、関数に関する強い仮定を残したままで、理論的な存在証明や性質までは深く議論されない現状にある。本研究の関数の構成が実現した場合には、こうした現在の暗号システムの課題を一挙に解決することが期待できる。

今回、Diffie-Hellmann 問題の困難性を利用して、独立関数の構成と証明が成功したとする。この結果は、逆に、Diffie-Helmann 問題の内在的な性質の１つを、この関数の独立性の概念が反映している、とも解釈できる。このアイデアを発展させ、離散対数の特殊な構造に特化した Diffie-Hellmann 問題を、数論的性質によらずに定義することをこころみる。現在まで、Diffie-Hellman 問題は、数多く暗号理論の基盤になっているが、未だにだれも、自然な拡張に成功していないことに注意する。

3.4 副産物：独立な一方向性関数が存在しないクラスを明らかにすることも、それ自身興味がある。法 N が共通な RSA 関数族 $RSA_E(x)=x^E \bmod N$ では、存在しないことは RSA の基本性質の１つであるが、この問題を共通法の一変数多項式、あるいは多変数多項式に拡張することも興味深い。とくに、多変数多項式暗号系は現在、ポスト量子暗号として活発に研究されている[J.Ding and B.Y.Yang, “Multivariate Public Key Cryptography” in Post Quantum Cryptography edited by D. J. Burnstain et.al 2009.]。多変数多項式系で独立な一方向性が発見できれば、新たな暗号系の構築に利用できる。逆に、独立でない多変数多項式系のクラスが明らかにできれば、安全でないパラメータの特徴付けに応用できる。

４．研究成果

4.1 主要課題であった計算量的な独立な関数の対に関して、具体的関数を離散対数の困難性のもとで構成する事に成功した。独立性の証明には、平方Diffie-Hellmann問題の困難性が通常のDH問題のそれと同等であることを利用する。この結果は、2013年との暗号と情報セキュリティシンポジウムで発表した。

4.2　主定理

定義（一方向性関数）多項式時間計算可能な関数f(x)が一方向性とは、f(x)からｘを計算することが多項式時間では困難な場合である。

注：多項式時間は、一般には確率的多項式時間で扱う。

定義（計算量的に独立）２つの１方向性関数の組(f(x),g(x))が計算量的に独立であるとは、次の２つを満足することである：

性質A:　(f(x), g(x))の関数が１方向性である.性質B: f(x)からg(x)の計算が多項式時間では困難、かつg(x)からf(x)の計算が多項式時間では困難。

[事例]共通法RSA関数の3つの例を考える：

$RSA_2(x)=x^2 \bmod N$,
$RSA_3(x)=x^3 \bmod N$,
$RSA_4(x)=x^4$ mond N

この３つの内のどの２つをとっても、我々の定義する計算量に独立ではないことに注意する。(RSA_2 と RSA_3 とから、$x=RSA_3(x)/RSA_2(x)$ が計算可能となる。 RSA_4 は、$(RSA_2)^2 \bmod N$ として計算可能である。)。

この性質は、 法 N が共通な RSA 関数族

$RSA_E(x)=x^E \bmod N$ でも成り立つ。関数ごとに異なる法を利用すれば独立性を保証できるとも思える. しかし、Hastad により、多くの場合やはり独立性が満たされないことが知られている [J.Håstad: Solving Simultaneous Modular Equations of Low Degree. SIAM J. Comput. 17(2)1988]。これは、RSA 系の一方向性関数では、独立な関数族がないであろう、という否定的証拠となる。この Hastad の結果は、独立性の定義の性質 A に関するもので、我々が要求する性質はさらに性質 B も加わることに注意する。性質 A と B とを両方満足することの理論的証明が困難という課題がここにある。実際には、離散対数と素因数分解など、異なる数論的仮定に基づく多くの一方向性関数は独立であると予想される。また、実用的暗号アルゴリズム DES と代表的なハッシュ関数 SHA なども、独立であろうと期待されるが、理論的な証明まで含めた研究は皆無である。

我々は、本研究で次の主定理を得た：
定理：２つの離散対数関数を考える: f(x)=g^x mod p, g(x)= g^{x^2}mod p. 離散対数の計算困難性の下で、この２つの関数の組は、計算量的に独立である。

証明には、[Intractable Problems in Cryptography Neal Koblitz and AledMenezes Cryptology ePrint Archive: Report 2010/290]の６章で議論されている、平方 Diffie-Hellmann 問題の困難性が通常の DH 問題のそれと同等であることを用いる (squareDH = DH)。したがって、定理に必要な仮定は、離散対数問題の計算困難性よりも、もう少し強い Diffie-Hellmann 問題の困難性であることに注意する。

4.3 この成果を、複数の海外の研究者に紹介した。特にシンガポール国立大学での講演の際に、客員教授として滞在していたYunlei ZHAO(復担大学, 中国)からは、彼自身の暗号プロトコル研究の一部に、類似の概念に相当する関数を利用していること、さらに関数の堅固性(non-malleable)という視点からもっと一般的な形での定式化をすすめられた。Yunlei ZHAOの2012年後半の半年の招聘期間に、彼と共同でプロトコルの堅固性に注目し、暗号鍵交換方式における安全性との関係を論じた。この共同研究の一部は、Yunlei ZHAOが、2013年の暗号と情報セキュリティシンポジウムで発表した。

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 4 件）
1. 北原基貴, 西出隆志, 櫻井幸一, ″認証機能を埋め込んだ公開鍵暗号の提案”, 暗号と情報セキュリティシンポジウム (SCIS),CDROM,pp.8-8,SCIS,2012(査 読 無)
2. 北原基貴, 西出隆志, 櫻井幸一,″署名データを組み込んだRSA公開鍵生成法の提案”,情報処理学会, 九州支部, 火の国情報シンポジウム,CDROM,pp.8-8, 2012(査読無)
3. 田中哲士,西出隆志,櫻井幸一,″GPU による並列化を用いた多変数二次多項式の高速代入計算”,電子情報通信学会 総合大会,CDROM,pp.1-1,2012(査読無)
4. 北原　基貴,櫻井　幸一″離散対数と素因数分解問題とに基づく ID ベース暗号の構築と安全性に関する考察”, 2013 年暗号と情報セキュリティシンポジウム,京都,1 月 22～25 日,2013

〔学会発表〕（計　2 件）
1. 櫻井 幸一,″計算量的に独立な関数族のいくつかの性質に関する考察”,2013 年暗号と情報セキュリティシンポジウム, 京都,1 月 22～25 日,2013
2. Shengli Liu, Kouichi Sakurai, Moti Yung, Fangguo Zhang and Yunlei Zhao, ″ Revisiting HMQV and Its Variants”, 2013 年暗号と情報セキュリティシンポジウム, 京都,1 月 22～25 日,2013

〔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://itslab.csce.kyushu-u.ac.jp/index-j.html

６．研究組織
(1)研究代表者
櫻井 幸一　(SAKURAI　KOUICHI)
九州大学・システム情報科学研究院・教授
研究者番号：60264066

(2)研究分担者
なし

(3)連携研究者
なし