様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　６　月　２９　日現在

機関番号：　８２６３６
研究種目：　基盤研究(C)（一般）
研究期間：　2012～2015
課題番号：　２４５００００１５

研究課題名（和文）新世代暗号の安全性を支える困難性仮定の正当性検証技術の開発

研究課題名（英文）Development of automatic analysis of hardnes assumptions for cryptosystems

研究代表者

吉田　真紀（Yoshida, Maki）

国立研究開発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アーキテクチャ研究室・主任研究員

研究者番号：５０３３５３８７

交付決定額（研究期間全体）：（直接経費）　　4,000,000円

研究成果の概要（和文）：情報セキュリティの基幹技術である暗号の安全性は，ある種の数学問題の求解が困難であること（困難性仮定）に支えられている．本研究の目的は，新世代の暗号に対して，その安全性を支える困難性仮定の正当性を検証する技術の開発である．まず困難性仮定を定式化し，正当性検証法を設計・実装した．そして，実際の困難性仮定への適用し，暗号設計者向けに検証ツールを開発した．

研究成果の概要（英文）：The security of many cryptosystems relies on the hardness assumption of certain computational problems, such as Diffie-Hellman problem and the factoring. The goal of this project is the development of an automatic analysis method that determines whether an attack exists or not and further derives all the possible attacks. We proposed a method focuses on a wide class of the problems on the existing hardness assumptions, and uses a computer algebra system. We further extend our method to analyze the security of cryptosystems.

研究分野：　情報セキュリティ

キーワード：　暗号　困難性仮定　正当性検証　Bilinear Group　Generic Model

１．研究開始当初の背景

情報セキュリティの基幹技術である暗号の安全性は，ある種の数学問題の困難性仮定に基づく．今世紀に入り，新しいセキュリティパラダイムを構成できる数学的構造として Bilinear Group(BG) が発明され，従来では実現が困難であった ID ベース暗号など新世代の暗号が活発に研究開発されている．新世代暗号の安全性を本当の意味で保証するためには，BG に関する困難性仮定の正当性を保証する必要がある．しかし，困難性証明は数学分野における代表的な未解決問題の１つ「P 対 NP 問題」と関係するため容易ではない．

現状，BG に関する困難性仮定の正当性を保証する唯一の方法は,Generic Model (GM) と呼ばれる計算モデルにおいて問題の困難性を証明することである．GM は問題が基とする数学的構造における演算を理想化（限定）した計算モデルであり，GM における困難性証明は一定レベル以上の国際会議や論文誌で必須となっている．

GM における困難性証明の主要な議論は，問題に対する一般的な解法（攻撃と呼ばれる）の非存在証明である．この証明は手間がかかるだけでなく，単純なミスにより攻撃の見逃しが生じやすい．実際に著名で権威ある国際会議の論文で導入された BG 上の問題の困難性証明の誤りが後に指摘されている．

２．研究の目的

本研究の目的は，新世代の暗号に対して，その安全性を支える困難性仮定の正当性を検証する技術の開発である．具体的には，BG 上で定義された問題の困難性仮定に対して，GM における攻撃の見逃し防止技術を開発し，それを基に正当性検証ツールを開発する．本研究の目的が達成されれば，新世代暗号に適した正当な困難性仮定を容易に定義でき，安全性向上に大きく寄与する．

３．研究の方法

本研究の目的を達成するために，以下の手順で実施する．

(1) 困難性仮定の定式化
(2) GM における正当性検証法の設計
(3) 設計した正当性検証法の実装と適用実験
(4) 暗号設計者向けに検証ツールの開発

本研究では，困難性仮定の正当性証明において誤りが含まれやすい攻撃有無判定・導出に焦点を絞ることで検証を可能とする．なお，検証分野における既存のいずれの手法も，対象とする数学的構造を抽象化して表現しており，数学的性質を完全に反映できない．そのため，攻撃の見逃しを防ぐことが困難であり，対象クラスを強く制限する必要が生じる．それに対して本研究では，数学的性質を組み込んでいる数式処理システムを利用することで，抽象化による攻撃見逃しを避け，対象クラスを実用レベルまで十分広くする．

４．研究成果

本研究の成果を示す．

(1) 困難性仮定の定式化

暗号分野の代表的な論文アーカイブ Cryptography ePrint Archive（ePrint と呼ぶ）と著名で最も難関な国際会議の論文を精査し，BG 上の困難性仮定（数十個）を抽出した．困難性仮定の定義では，困難と仮定する問題のインスタンスジェネレータ，問題を解こうとするアルゴリズムに与えられるオラクル，解の正しさを検証する決定性アルゴリズムを定義することとなる．問題のインスタンスジェネレータにパラメータが設定される場合は，問題のサイズがパラメータによって異なり，パラメータを大きくすると増大する．問題にオラクルが与えられる場合は対話性をもつという．問題に対する正しい解は必ずしも１つとは限らず，多数あり得る．本様式に着目し，3 つの属性（対話性，問題サイズの固定性，解の固有性）に基づき定式化した（表 1 参照）．一般に上位クラスの問題ほど記述が単純で，GM における困難性の証明も単純となる．本定式化により，暗号設計者が困難性仮定を定義する際に，いずれのクラスに含まれるか容易に判定できるようになる．さらに，多様な困難性仮定を統一的に扱うことが可能となった．

表１：困難性仮定の 3 つの属性と分類

対話性		問題サイズ		解の固有性		例
無	有	固定	増大	固有	多数	
x		x		x		DH, DL, DDH
x		x			x	HDL, SDH
x			x	x		k-BDHE, k-DDH MSE-DDH
x			x		x	l-SDH, k-linear
	x	x		x		GBDH, 1MDH, One-sided Gap DH
	x	x			x	LRSW, M-LRSW E-LRSW
	x		x	x		−
	x		x		x	−

(2) GM における正当性検証法の設計

属性の組み合わせに基づき困難性仮定を分類し，GM における正当性検証に不可欠な攻撃有無判定・導出を定式化した．そして，攻撃有無判定・導出が可能となるための十分条件を導出し，攻撃有無判定・導出法を設計した．なお，攻撃有無判定・導出は，連立方程式の立式・求解となる．攻撃が存在する場合の出力は，全ての攻撃を表現する一般的な

形式としており，解の式として与える．また，攻撃の見逃しがないことを GM の定義に基づき理論的に証明した．

(3) 正当性検証法の実装と適用実験

まず，各クラスの代表例となる困難性仮定に対して攻撃有無判定・導出法を数式処理システム Maple および Mathematica で実装し適用した．結果として，Maple では，いずれの困難性仮定についても攻撃が存在しないことを確認できた．一方，Mathematica では実行が止まらず計算量が爆発したと思われたため，以降は Maple を利用することとした．

(4) 暗号設計者向けに検証ツールの開発

困難性仮定の記述から正当性を検証する Maple プログラムを自動生成するシステムを開発した．本システムでは，検証結果を有効利用できるように，正当性の判定結果に加えて，攻撃の記述を出力するようにしている．なお，Maple プログラムは各問題で 30 行程度であった．実験環境を以下に示す．

Maple：14
CPU：Intel(R) Core(TM) 2 Duo 2.40GHz
メモリ：3.25GB
OS：Windows XP Professional Service Pack 3

問題サイズのパラメータの値と，オラクルへの問い合わせ回数は，本来はセキュリティパラメータの多項式とする必要がある．本研究では実行時間の都合上，近年のセキュリティパラメータ λ=160 の log 値として，それぞれ 7 まで適用した．困難性仮定の定式化において，ePrint および著名な国際会議の論文から抽出した困難性仮定のうち，対話性が無く，問題サイズが固定あるいは解が固有の困難性仮定はいずれも 1 秒以内で判定結果が出力された．一方，問題サイズが増大かつ解が多数ある困難性仮定は判定結果の出力に要する時間が長くなり，例えば k-BDHE は約一日を要した．また，判定できなかったパラメータがある問題は k-CAA，(n,t)-MSE-DDH，E-LRSW である．k-CAA については k=4, 6 の場合であり，方程式の根を含んだ形の解が出力された．これは，五次以上の代数方程式に解の公式が必ずしも存在しないためであり，方程式が Maple で解けなかったことを意味する．

ePrint は数多くの最新論文が逐次追加されているが，査読が無いため玉石混交となっている．そのため，検証により正当性の保証を与える意義は大きい．

(5) 新世代暗号への拡張

当初計画の最終年度（平成 26 年度）に海外の研究グループが同様の方式を本研究に先がけて国際会議（CRYPTO2014）で提案したため，計画を変更し，対象を困難性仮定から新世代暗号そのものに拡張することとし，期間を 1 年延長した．困難性仮定の正当性検証法から新世代暗号の安全性検証への拡張では，まず，困難性仮定の定式化における，困難と仮定する問題のインスタンスジェネレータ，問題を解こうとするアルゴリズムに与えられるオラクル，解の正しさを検証する決定性アルゴリズムを，それぞれ新世代暗号のインスタンスジェネレータ（すなわち，鍵生成，暗号化・復号あるいは署名・検証），攻撃者に与えられるオラクル，攻撃者の成功を検証する決定性アルゴリズムに対応付けた．そして，安全性検証法の設計では，困難性仮定の正当性検証法と同様に，攻撃の有無判定・導出を定式化し，手法を考案した実装と適用実験では，著名で権威ある国際会議で発表された方式について攻撃も発見し，修正方式も考案した．

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. Maki Yoshida and Toru Fujiwara, “Efficient Usage of Cover Free Family in Broadcast Encryption,” IEICE Transactions on Fundamentals, vol.E99-A, no.6, pp.1-8 (2016-06), 査読有.
DOI: 10.1587/transfun.E99.A.1216

②. Maki Yoshida and Toru Fujiwara, “On the Impossibility of d-Multiplicative Non-perfect Secret Sharing,” IEICE Transactions on Fundamentals, vol.E98-A, no.2, pp.58-64 (2015-02), 査読有.
DOI: 10.1587/transfun.E98.A.767

③. Itsuki Suzuki, Maki Yoshida, and Toru Fujiwara, “Generic Construction of GUC Secure Commitment in the KRK Model,” LNCS 7631, pp.244-260 (2012-11), 査読有.
DOI: 10.1007/978-3-642-34117-5_16

④. Maki Yoshida, Toru Fujiwara, and Marc Fossorier, “Optimum General Threshold Secret Sharing,” LNCS 7412, pp.187-204 (2012-08), 査読有.
DOI: 10.1007/978-3-642-32284-6_11

〔学会発表〕（計 9 件）

①. 櫻田英樹，米山一樹，吉田真紀，花谷嘉一，“形式検証に向けた QUIC の安全性定義の検討,”日本応用数理学会 2015 年度年会，数理的技法による情報セキュリティ(FAIS)，2015 年 9 月 11 日，金沢大学（石川県金沢市）.

②. Maki Yoshida, “Invited Talk: Trade-off between Resiliency and Efficiency of Cryptographic Protocols -- The Case of Information Theoretical Security --,” IEICE Technical Reports, vol.115, no.38, pp.69-74, May 22th 2015, The Kyoto International Community House (Sakyo-ku, Kyoto).

③. Hideki Sakurada, Kazuki Yoneyama, Yoshikazu Hanatani, and Maki Yoshida, “Toward Exact Assumptions for UC Commitments with Automated Verification,” The 2015 Symposium on Cryptography and Information Security, January 23th 2015, RIHGA Royal Hotel Kokura (Kitakyusyu, Fukuoka).

④. 吉田真紀, 水野修, “暗号プロトコル安全性検証の可視化に向けて,” 2015 年暗号と情報セキュリティシンポジウム, 2015 年 1 月 23 日, リーガロイヤルホテル小倉 (福岡県北九州市).

⑤. 吉田真紀, “暗号プロトコルの評価の理論と可視化,” Small-workshop on Communications between Academia and Industry for Security (招待講演), 九州大学西新プラザ (福岡県福岡市).

⑥. Hironobu Tozuka, Maki Yoshida, and Toru Fujiwara, “Salt-and-Pepper Image Watermarking System for IHC Evaluation Criteria,” Proceedings on the First International Workshop on Information Hiding and its Criteria for evaluation (IWIHC2014), pp.31-36, June 3th 2014, KYOTO GARDEN PALACE (Kamigyo-ku, Kyoto).

⑦. Seigo Ikeda, Maki Yoshida, and Toru Fujiwara, “Theoretical Performance Analysis of Hybrid Additive-Multiplicative Watermarking,” IEICE Technical Reports, vol.112, no.420, pp.77-82, January 30th 2013, Tohoku University (Sendai, Miyagi).

⑧. Seigo Ikeda, Maki Yoshida, and Toru Fujiwara, “New Hybrid Additive-Multiplicative Watermarking with Better Tradeoff between Image Quality and Detection Accuracy,” 2012 International Symposium on Information Theory and its Applications (ISITA2012), October 31th 2012, Hawaii (USA).

⑨. Seigo Ikeda, Maki Yoshida, and Toru Fujiwara, “Hybrid Additive-Multiplicative Watermarking for General Embedding Domains,” IEICE Technical Reports, vol.112, no.129, pp.9-16, July 19th 2012, Hokkaido University of Science (Sapporo, Hokkaido).

〔図書〕(計 1 件)

①. 鈴木斎輝, 吉田真紀, 汎用的結合可能な安全性, 日本応用数理学会監修/薩摩順吉・大石進一・杉原正顕 (編) 応用数理ハンドブック (2013).

６．研究組織

(1)研究代表者

吉田 真紀 (YOSHIDA, Maki)

国立研究開発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アーキテクチャ研究室・主任研究員

研究者番号：50335387