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２５年４月１１日現在

機関番号：１７１０２
研究種目：挑戦的萌芽研究
研究期間：2010～2012
課題番号：22650014
研究課題名（和文）大規模解読実験による公開鍵暗号の安全性解析

研究課題名（英文）Security Analysis of Public-Key Cryptography by Large-Scale Experiments

研究代表者
高木　剛（TAKAGI TSUYOSHI）
九州大学・マス・フォア・インダストリ研究所・教授
研究者番号：60404802

研究成果の概要（和文）：次世代公開鍵暗号として研究開発が進んでいるペアリング暗号の安全性は、有限体上の離散対数問題の困難性を根拠としている。本研究課題では、ペアリング暗号の高速実装が可能となる有限体 GF(3^{6n})の離散対数問題を、関数体篩法の大規模な計算機解読実験により解析評価した。2012 年度には 252 CPU コアの PC クラスタを用い、解読世界記録となる 923 ビットの有限体 GF($3^{6\cdot97}$)上の離散対数問題の計算に成功し、想定される攻撃の計算能力限界をより正確に評価可能となった。

研究成果の概要（英文）：The security of pairing-based cryptography, which is one of next-generation public-key cryptography, is based on the difficulty of solving the discrete logarithm problem over finite fields. In this research we analyzed the discrete logarithm problem over finite field GF(3^{6n}) used for efficient implementation of pairing-based cryptography by large-scale experiments. In 2012 we successfully achieved the top-record of solving the discrete logarithms over finite field GF(3^{582}) of 923 bits using a PC cluster of 252 CPUs in about 153 days, and it enables us to precisely estimate the upper bound of computational ability of expected attackers.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２０１０年度	1,700,000	0	1,700,000
２０１１年度	600,000	180,000	780,000
２０１２年度	600,000	180,000	780,000
２０１３年度	0	0	0
２０１４年度	0	0	0
総　計	2,900,000	360,000	3,260,000

研究分野：計算機システム・ネットワーク
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・認証、公開鍵暗号、ペアリング暗号、離散対数問題、大規模実験

１．研究開始当初の背景

(1)従来の公開鍵暗号では実現が困難な暗号プロトコルが構成できるペアリング暗号が

注目を集めている。特に、標数 3 の有限体 $GF(3^n)$ 上の η_T ペアリングの高速算術方法に関する論文が多くの発表されている。

(2)有限体 $GF(3^n)$ 上のペアリングの安全性は離散対数問題の困難性を基にしている。離散対数問題に対する最も効率的な解法として関数体篩法が知られているが、小規模な計算実験が 2 件報告されているに留まり、$GF(3^n)$ 上のペアリングの安全性を解析評価するための実験データが不十分であった。

２．研究の目的

本研究課題では、大規模な計算機解読実験により公開鍵暗号(特にペアリング暗号)の安全性を解析評価する。ペアリング暗号の高速実装で重要となる有限体 $GF(3^n)$ 上の離散対数問題を取り扱い、以下の問題に取り組む。

① 離散対数問題の解読世界記録の鍵長サイズを超える解読の世界新記録を目指す。

② 有限体 $GF(3^n)$ 上のペアリングで使用する鍵長サイズ n の解読計算時間を解析する。

③ 他の公開鍵暗号の解読実験との比較を行い安全な鍵長サイズ n を解析評価する。

３．研究の方法

ペアリング暗号の安全性は、有限体上の離散対数問題の困難性を基にしている。離散対数問題を最も高速に計算するアルゴリズムとして数体篩法/関数体篩法があり、次の 3 段階に大別することができる。

(a)多項式選択ステップ
(b)関係探索ステップ
(c)線形代数ステップ

本研究では、上記の各ステップに関して有限 $GF(3^n)$ の特徴を考察した高速化を検討し、$GF(3^n)$ 上の離散対数問題の解読世界新記録を目指す。また、解読結果に基づき $GF(3^n)$ 上のペアリングの安全性を解析評価して、実用化されている RSA 暗号と同等の安全性を持つ鍵サイズを検討する。

４．研究成果

(1) 従来の公開鍵暗号では実現が困難な暗号プロトコルが構成できるペアリング暗号が注目を集めており、RFC 5091 などで国際標準化が進められている。ペアリング暗号の安全性は有限体上の離散対数問題の計算量的困難性を基にしており、本研究課題では大規模な計算機解読実験によりペアリング暗号の安全性を解析評価することを目標とした。有限体 $GF(3^{6\cdot 71})$ 上の離散対数問題(676 ビット)を 96 コアのクラスタ計算機により約１ヶ月で解読することに成功し、2010 年時点での解読世界記録を達成した。これらの成果により、ペアリング暗号を実用化する上で安全となる鍵長を見積もることが可能となった。本成果は、査読付き論文２編(国際会議 PKC2010、電子情報通信学会英文論文誌）で発表し、解説記事２編（情報処理学会誌、電子情報通信学会誌）として執筆した。

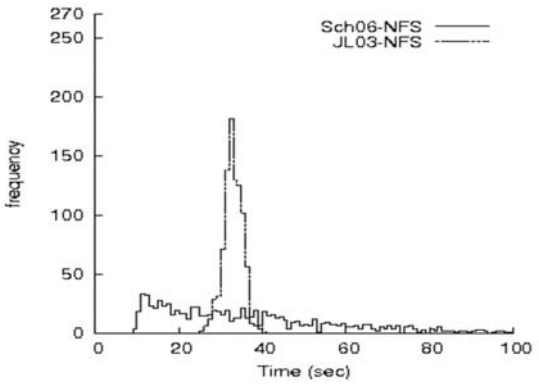

図 1. JL06 と Sch06 の計算時間分布

(2) 素体 GF(p)上の離散対数問題に対して漸近的に最速な解読法として数体篩法がある。素数 p に条件を付けない有限体 GF(p)に対する数体篩法として Joux-Lercier の数体篩法(JL03) が知られている。Schirokauer は、low hamming weight な素数 p に対して、p に条件を付けない有限体 GF(p)に対する数体篩法よりも計算量が小さい数体篩法を提案した(Sch10)。本研究課題は、259-bit 以下のいくつかの素数 p に対し JL03 及び Sch10 の比較実験を行った。Xeon E5440 を 2 機搭載した PC 1 台で実験を行い、gcc, pthread, GMP を利用した。Sch10 は JL03 に対して 146-bit (194-bit,259-bit)ではそれぞれ 4.3 倍 (8.5 倍, 18.1 倍) 高速で結果を得た。より大きい bit 長では実行時間の差がより大きくなるため、Sch10 が有利な low weight な素数 p を暗号システムで用いる場合は、Sch10 に対して安全な素数 p の bit 長を見積もる必要がある。本成果は国際会議 International Workshop on Coding and Cryptology (IWCC 2011)において発表した。

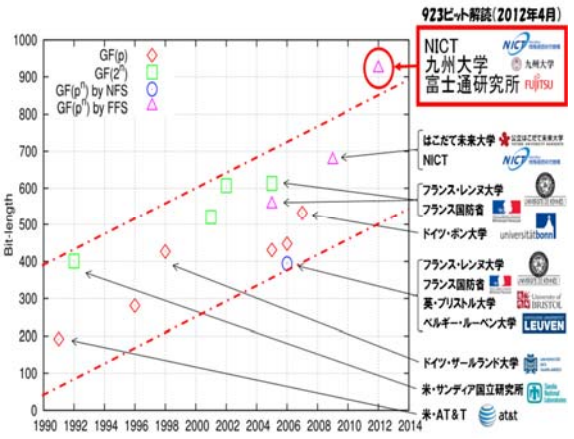

図 2. 離散対数問題の解読世界記録

(3)ペアリング暗号の高速実装で用いられた有限体 GF(3^6)の n 次拡大体上の離散対数問題の解読実験を行った。ペアリング暗号の性能評価のために多くの論文で実装評価されている拡大次数 n=97 (923 ビット) を考察し、関数体篩法を実装することにより大規模な解読実験を行った。関係式探索ステップでは、格子篩を 212CPU コアによる並列計算により実装し 153.1 日間で約 153×10^6 個の関係式を集めた。線形代数ステップは、151 ビットの素数を法とする行列サイズ 6 百万×6 百万の連立 1 次方程式を 252CPU コアの並列 Lanczos 法により 80 日間の計算が必要であった。個別離散対数ステップなどの計算を含め合計 148.2 日間で解読することに成功した(2012 年 4 月)。本研究課題の大規模実験により攻撃者の計算能力限界を正確に解析することが可能となり、拡大次数 n=509 の位数 3357 ビットの有限体 GF(3^{6n})は今後 20 年間安全に利用できる見積もりを得た。本成果は、査読付き論文として 2 編 (ISPEC 2012, Asiacrypt 2012) の発表を行った。

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 10 件）

① Takuya Hayashi, Takeshi Shimoyama, Naoyuki Shinohara, Tsuyoshi Takagi, Breaking Pairing-Based Cryptosystems using η_T Pairing over GF(3^{97}), 18th International Conference on the Theory and Application of Cryptology and Information Security, Asiacrypt 2012, 査読有, LNCS 7658, 2012, pp. 43-60.
DOI: 10.1007/978-3-642-34961-4_5

② 林卓也, 下山武司, 篠原直行, 高木剛, GF(3^n)上の η_T ペアリングを用いたペアリング暗号の安全性評価, 電子情報通信学会研究報告, 信学技報, 査読無, Vol.112, No.39, 2012, pp.1-5.

③ Naoyuki Shinohara, Takeshi Shimoyama, Takuya Hayashi, Tsuyoshi Takagi, Key Length Estimation of Pairing-Based Cryptosystems using η_T Pairing, 8th International Conference, ISPEC 2012, 査読有, LNCS 7232, 2012, pp.228-244.
DOI: 10.1007/978-3-642-29101-2_16

④ 坂本恭一, 林卓也, 高木剛, 数体篩法における Joux-Lercier の多項式選択法について, 2012 年暗号と情報セキュリティシンポジウム, SCIS2012, 査読無, 2B1-2, 2012, pp.27.

⑤ Takuya Hayashi, Naoyuki Shinohara, Lihua Wang, Shin'ichiro Matsuo, Masaaki Shirase, Tsuyoshi Takagi, Solving a 676-bit Discrete Logarithm Problem in GF(3^{6n}), IEICE Transaction, Fundamentals of Electronics, Communications and Computer Sciences : A, 査読有, Vol.E95-A, No.1, 2012, pp.204-212.
DOI: 10.1587/tranfun.E95.A.204

⑥ 林卓也, 高木剛, 離散対数問題に対する解読世界記録の推移, 電子情報通信学会誌, 査読無, 94 巻 11 号, 2011, pp.977-981.
http://ci.nii.ac.jp/naid/110008762196

⑦ Kenichiro Hayasaka, Tsuyoshi Takagi, An Experiment of Number Field Sieve over GF(p) of Low Hamming Weight Characteristic, International Workshop on Coding and Cryptology, IWCC 2011, 査読有, LNCS 6639, 2011, pp. 191-200.
DOI: 10.1007/978-3-642-20901-7_11

⑧ 林卓也, 高木剛, 離散対数問題解読世界記録更新への道 -676 ビットの解読-, 情報処理, 査読無, Vol.51, No.9, 2010, pp.1181-1188.
http://ci.nii.ac.jp/naid/110007700785

⑨ Takuya Hayashi, Naoyuki Shinohara, Lihua Wang, Shin'ichiro Matsuo, Masaaki Shirase, Tsuyoshi Takagi, Solving a 676-bit Discrete Logarithm

Problem in GF(3^{6n}), 13th International Conference on Practice and Theory in Public Key Cryptography, PKC 2010, 査読有, LNCS 6056, 2010, pp.351-367. DOI: 10.1007/978-3-642-13013-7_21

⑩ 早坂健一郎, 高木剛, 素体 GF(p)上の離散対数問題に対する数体篩法の比較実験, 情報処理学会コンピュータセキュリティシンポジウム, CSS2010, 査読無, 2B1-1, 2010, pp.489-494.

〔学会発表〕(計 4 件)

① 高木剛, 次世代公開鍵暗号 - ペアリング暗号 - , 統計科学研究会, 第 15 回情報・統計科学シンポジウム(BIC シンポジウム), 招待講演, 2010 年 12 月 3 日, 九州大学伊都キャンパス.

② 高木剛, 有限体上の離散対数問題の困難性, 2012 年電子情報通信学会総合大会, 招待講演,2012 年 3 月 22 日, 岡山大学.

③ Tsuyoshi Takagi, An Experiment of Number Field Sieve over GF(p) of Low Hamming Weight Characteristic, International Workshop on Coding and Cryptology, IWCC 2011, 招待講演, 2011 年 6 月 2 日, Qingdao Garden Hotel, 青島, 中国.

④ 高木剛, 次世代公開鍵暗号に関する研究の最前線, NICT 情報通信セキュリティシンポジウム 2013, 招待講演, 2013 年 2 月 14 日, 品川フロントビル.

〔その他〕

ホームページ
http://imi.kyushu-u.ac.jp/~takagi/

５．研究組織

(1) 研究代表者

高木　剛 (TAKAGI TSUYOSHI)
九州大学・ﾏｽ・ﾌｫｱ・ｲﾝﾀﾞｽﾄﾘ研究所・教授
研究者番号：60404802