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　 ５ 月　 ９ 日現在

機関番号：１５３０１
研究種目：基盤研究(B)（一般）
研究期間：2013～2015
課題番号：２５２８００４７

研究課題名（和文）楕円ペアリング暗号に対する共役有理点ノルムを用いた分散並列攻撃法の開発と実証実験

研究課題名（英文）Security Evaluation for Elliptic Curve Pairing-based Cryptography with Conjugate Rational Points by Distributed and Parallelized Experiments

研究代表者

野上　保之（Nogami, Yasuyuki）

岡山大学・自然科学研究科・准教授

研究者番号：６０３１４６５５

交付決定額（研究期間全体）：（直接経費）　　10,900,000円

研究成果の概要（和文）：本研究では、楕円ペアリング暗号に対する安全性評価を行うために、rho法を中心とする様々な攻撃手法とそのための改良を行い、実験を行った。具体的には、ランダムウォークを効果的に行うための乱数の生成法を検討し、攻撃を効率よく並列化するための手法を検討した。また、楕円曲線に関する種々の計算の効率化と、rho法自身の性能を評価するために多数の点を生成し、それらをすべて記憶した場合の攻撃評価も行った。その結果として、88ビットの楕円ペアリング暗号であれば4台の計算機で3時間弱で攻撃を完了することを確認した。現在、114ビットの場合の攻撃を継続中である。

研究成果の概要（英文）：In order to evaluate the security of elliptic curve pairing-based cryptography, this research has considered several attacking method, particularly rho method with some improvements and experiments. In detail, this research discussed a random number generator for efficiently carrying out random walks of rational points and then discussed an efficient distributed parallel attacks. Then, this paper also developed some efficient arithmetic operations on elliptic curve and evaluated some other approaches that kept all of generated random rational points for the attack in contrast to rho method. As a result, this research could show that 88 bit pairing-based cryptography could be broken with about three hours computation by 4 PCs. This research still keeps on attacking 114 bit pairing-based cryptography.

研究分野：情報セキュリティ

キーワード：ペアリング暗号　乱数検定　攻撃・安全性評価　並列処理　データ解析

１．研究開始当初の背景

インターネットを中心とする高度 ICT 社会において、電子的な個人認証を簡便に実現し、様々なセキュリティ活用サービスを構築する、その礎となる公開鍵暗号方式として RSA 暗号や楕円曲線暗号が広く用いられてきた。これらの暗号方式は、その提案以来、多様な解読法・攻撃を退け、十分にその安全性が認められた上で実用に供している。にもかかわらず、個人情報漏えい問題が後を絶たない。そのようなことから、総務省が示している UNS（Ubiquitous Network Security）戦略では、次世代の認証技術という位置づけで、個人の情報を介することなく電子認証を実現する「匿名認証技術」の実用化に向けたロードマップが示されている。本研究開発で取り扱う楕円ペアリング暗号は、その実現に必須かつ安全性の肝となる重要な要素技術であり、我々の研究グループでも、標準化動向をにらみながら、世界最高速のペアリング暗号を実現する技術を提案してきた。しかし一方で、ペアリング暗号の高速化・効率化のための世界的な潮流が、まさに楕円ペアリング暗号の解読（脆弱性）にも大きく寄与することを指摘してきている。

２．研究の目的

本研究では、楕円ペアリング暗号に対し、様々な高速化手法を駆使して、かつ大学の計算機資源を活用した大規模な分散並列処理により緻密に実装して、RSA 暗号や楕円曲線暗号の安全性評価のような、十分な解読攻撃を施すことで、その安全性を評価する。

３．研究の方法

① 楕円ペアリング暗号での ECDLP に対する Rho 法をベースとした攻撃法の提案

一般に、埋め込み次数と呼ぶペアリングパラメータは 2 から 20 程度の整数である。そのような幾つかのよく知られる楕円ペアリング曲線に対して、効率のよい衝突型の攻撃手法を提案する。具体的には、近年の効率のよいペアリング暗号が、楕円曲線上の有理点が成すある特殊な加法群を用いていることに着目し、その特長がペアリング暗号の効率化のみならず、衝突型の攻撃手法にもその効率化に寄与することを理論的・具体的に示してきている。その上で、これをさらに効率化する方法として、Frobenius 写像に基づく共役有理点集合に対し、効率よくかつ偽衝突なくリスト化する手法を検討し、楕円曲線上の有理点がなす加法群における ECDLP を解くというアプローチをとった。その効率のよいリスト化、リストからの効率のよい衝突発見（偽衝突なし）に対して本研究開発では、複雑な計算を必要とすることなく簡便に与えられ、共役な有理点に対してのみ同じ値をとり、かつ有理点の情報を効率よく圧縮できるノルムを活用することを考える。

② 攻撃を効率化するためのランダム点生成法の提案とその乱数性に関する統計的評価

効率的なランダムウォークの方法として、一つのランダムな有理点の生成に要する計算操作が、楕円加算１回分ほどで済むものが提案されている。本研究においても、処理効率としてこれに匹敵するよう、今回考えている共役な有理点集合に対し、これに活用する Frobenius 写像やノルムと対応して、効率よくランダム点を生成する手法とその並列化を検討する。とくに並列化に関しては、複数の計算機を用いた並列攻撃に適用できるよう工夫し、具体的なアルゴリズムとして実装・実験を行う。一方で、ランダムウォーク法で重要となるのが辿る有理点のランダム性であり、提案するランダムウォークについて乱数性の評価・検証を行う。整数乱数の生成に対するアプローチとして、カオス写像の一つであるロジスティック写像を考える。これまでの研究では十分でなかった「ランダムウォークに対する乱数性の検証」には、代表的な乱数検定である NIST 検定など用いる。

③ 効率のよい攻撃の並列化手法と衝突点解析法の実現

ランダムウォーク法に関する研究により、多数の異なる初期値を生成することにより、Rho 法をベースとした攻撃手法は、並列に動作させることが可能となる。通常、初期値の生成そのものを並列化することは簡単ではないため、この処理は前処理として実施する。得られた初期値に対して、Rho 法をベースとした攻撃手法はスレッドを用いた並列処理により、短時間で多数の有理点を調査する。ここでは高性能な計算機を用い、1 ノードで 32 程度の並列処理を想定する。続く衝突点解析は単純に実装すると、計算済みの有理点を記憶するために広大なメモリ空間を必要とするため、上述のノルムを用いて記憶するデータの量を削減する。ノルムの衝突解析は、基数木を用いた木構造のデータを用いることにより、データ量に対して対数のオーダーの処理で効率的に実現できる。この基数木に関連する処理もスレッドを用いた並列処理により、高速化する。

④ 多数の計算機を用いた大規模な分散並列攻撃実験

有理点空間を分割してそれぞれを 1 台の DNS サーバで管理させ、各 DNS サーバでは動的登録（dynamic update）機能を用いて攻撃データの登録を行う。その際、既に存在しているデータを更新することになれば、衝突点が見つかったことになる。ただし、1 台の DNS サーバで管理するデータは膨大（数十 TB）になるため、メインメモリ上にデータを置くよう

な通常の DNS サーバの仕組みでは扱うことができない。そこで DLZ(Dynamic Loadable Zone)機能を活用し、大規模なデータを扱えるように工夫する。

４．研究成果

① 本研究では、ペアリング曲線の中でも曲線のパラメータを組織的に決定することができるためよく使用される、BN 曲線を対象とした。攻撃手法としては、rho 法を用いた。rho 法は楕円加算と呼ばれる有理点同士の加算を繰り返すことによって攻撃する。楕円加算はモンゴメリトリックと呼ばれる既存手法で効率化し、効率化した後の楕円加算において、その主な計算時間を占めるのは素体上乗算である。素体上乗算を効率的に計算するアルゴリズムとしてモンゴメリ乗算を用いた。本研究では、128bit 以下の整数におけるモンゴメリ乗算に対象を絞り、その時の効率のよい実装手法について検討した。具体的には、128bit 整数上での通常のモンゴメリ乗算と Separated Operand Scanning Method のコストを比較し、その効率性について考察した。また、BN 曲線上 1 の群構造を利用した改良やモンゴメリトリックといった既存手法と本稿での提案手法を組み合わせた場合、どの程度の ECDLP を解けるのかという実装実験を行った。実験には 1 台の計算機のみを用いるのではなく、複数台の計算機を用いた並列解読システムを実装した。並列計算システムはクライアント－サーバモデルを採用し、効率的な実装を行った。具体的には、Solid State Drive(SSD)と Hard Disk Drive(HDD) の両方を用いた効率の良いサーバを構成した。性能評価の結果、鍵長が 88bit の ECDLP を 4 台の計算機を用いることで、約 2 時間 35 分で解読できた。その上で、岡山大学と北九州市立大学の計算機資源を活用し約 2000 コアで１ヵ月の並列攻撃を約１ヵ月行い、平均的な攻撃成功までの約 1/4 を終えている。今後も攻撃実験を継続する予定である。

② 並列処理を用いた衝突攻撃実験に適した乱数系列について検討を行ってきた。ここで乱数生成に関して必要な条件は、並列に生成される各乱数が重複無く、偏り無く生成されることと考え、2 通りのアプローチから乱数生成を行った。一つは、長い周期の系列を生成可能で初期値鋭敏性を備え、計算量の少ないロジスティック写像を用いた乱数系列について評価を行った。具体的には、この写像を固定ビット長の演算で実装して得られる乱数について系列長や統計的な性質について解析し、ビット長に対して長い周期の系列を生成する条件を確認するなど多くの成果が得られた。また、今回実際の攻撃においてロジスティック写像を用いた乱数生成を実装したが、ロジスティック写像を用いることによる優位性は得られていない。もう一つのアプローチは、優れた統計的な性質を持つ m-系列と k 乗剰余を組み合わせて構成される系列について様々な解析を行い、こちらも多くの成果が得られている。今後、実装する上でこれらの系列が優位に働くパラメータの選定も課題として残っている。

③ 衝突攻撃実験は、多数の有理点を保存する単純な衝突攻撃手法と、他の研究者にもよく採用されている少数の有理点を保存する rho 法型の手法に対して、並列処理を用いた実装をし、64 コアのサーバ PC での性能評価実験を行った。単純な衝突攻撃では有理点群の構造を利用した効率化手法が有効に働き、512GB の主記憶があれば、鍵長 74 ビットを 2 週間程度で解けることが分かったが、rho 法型の手法は 20 倍程度高速な結果となった。rho 法型の手法に対して有効な有理点群の構造を探求し、rho 法型の手法を改善することが課題である。

④ 多数の計算機を用いた大規模な分散並列攻撃実験では、動的登録（DNS update）機能を用いて攻撃データの登録および衝突検出を行う方法を確立した。この方法では、数値データを 16 進文字列（4 ビット/文字）ではなく、エンコード方法の工夫により 6 ビット/文字で表現することで、効率化を行っている。また、1 つの更新メッセージに多数（25 程度以上）の攻撃データを含めるとオーバヘッドが減少し、攻撃時間を短縮できることも確認した。なお、DLZ（Dynamic Loadable Zone）の活用については、rho 法における特徴点を用いた衝突判定法の適用により、当初の予定より十分少ないデータ量しか扱わないこと、およびゾーン分割により DNS サーバ自身も分散可能であることから実施を見送った。

５．主な発表論文等

〔雑誌論文〕（計　3件）

① Y. Nogami, K. Tada, and S. Uehara, A geometric sequence binarized with Legendre symbol over odd characteristic field and its properties, IEICE Transaction, vol. E97, pp. 2336-2342, 2014.

② Y. Nogami and T. H. Austin, Associative Rational Points for Improving Random Walks with Collision-based Attack on Elliptic Curve Discrete Logarithm Problem, International Journal of Computer and Information Technology, vol. 4, issue 4, 2015.

③ 荒木,宮崎,上原,礒崎, 整数上のロジスティック写像におけるビット毎の出現頻度に関する考察, 日本応用数理学会論文誌,vol.25, no.3, pp. 191-206, 2015.

〔学会発表〕（計４３件）

① Y. Nogami, K. Tada, S. Uehara, A Binarization of Geometric Sequences with Legendre Symbol and Its Autocorrelation, IWSDA'13, 2013.

② T. Miyazaki, C. Miyazaki, S. Uehara, S. Araki, A Study on the Lyapunov Exponents of Sequences Generated by the Logistic Map over Integers, IWSDA'13, 2013.

③ 三好,山井,野上, BN 曲線上の ECDLP に対する Rho 法の DNS を用いた衝突検出の性能評価, 暗号と情報セキュリティシンポジウム, 2014.

④ Y. Kono, Y. Nogami, T. Kusaka, Experimental Evaluation of the Efficiency of Associative Rational Points for Random Walks on ECDLP, ISCIT2014, 2014.

⑤ C. Miyazaki, T. Miyazaki, S. Uehara, S. Araki, Relations between evaluations of NIST tests and Lyapunov exponents of sequences generated by the Logistic map over integers, ISITA2014, 2014.

⑥ 手邊, 野上, 上原, 奇標数体上の原始多項式とべき乗剰余性に基づいた多値系列の生成, 第 37 回情報理論とその応用シンポジウム, 2014.

⑦ 三好, 野上, 日下, 山井, 70 台程度の計算機を並列に用いた 94bit の ECDLP の解読, 暗号と情報セキュリティシンポジウム, 2015.

⑧ H. Ino, Y. Nogami, N. Begum, S. Uehara, R. Morelos-Zaragoza, K.Tsuchiya, Examining the Linear Complexity of Multi-value Sequence generated by Power Residue Symbol, ICISS2015, 2015.

⑨ H. Ino, Y. Nogami, N. Begum, S. Uehara, R. Morelos-Zaragoza, K. Tsuchiya, A Consideration on Crosscorrelation of a kind of Trace Sequence over Finite Field, WICS Poster, CANDAR'15, 2015.

⑩ 宮崎,荒木,上原,野上, 素体上のロジスティック写像の生成系列におけるビット抽出方法と乱数性, 暗号と情報セキュリティシンポジウム, 2016.

⑪ 三好,山井,野上, 楕円曲線暗号解読における Dynamic DNS を用いた解読成功判定, 情報処理学会インターネットと運用技術研究会研究報告,2016.

⑫ 三好,野上,日下,山井, BN 曲線上の楕円離散対数問題の解読におけるモンゴメリ乗算の最適化, 暗号と情報セキュリティシンポジウム, 2016.

〔その他〕
ホームページ：
http://www.ec.okayama-u.ac.jp/~sws/nogami/Works/Kibanb2013.html

６．研究組織

(1)研究代表者
野上　保之（Nogami、 Yasuyuki）
岡山大学・大学院自然科学研究科・准教授
研究者番号：６０３１４６５５

(2)研究分担者
上原　聡（Uehara、 Satoshi）
北九州市立大学・国際環境工学部・教授
研究者番号：９０２１３３８９

日下　卓也（Kusaka、 Takuya）
岡山大学・大学院自然科学研究科・講師
研究者番号：００３３６９１８

山井　成良（Yamai、 Nariyoshi）
東京農工大学・工学研究院・教授
研究者番号：９０２１０３１９