様式 C-19

科学研究費補助金研究成果報告書

平成　21 年　9 月　7 日現在

研究種目：基盤研究（B）
研究期間：2005～2008
課題番号：17300002
研究課題名（和文）　サイドチャネル攻撃に対して安全な公開鍵暗号に関する研究

研究課題名（英文）
Research on Public Key Cryptosystems Secure against Side Chanel Attack

研究代表者
宮地　充子　(Miyaji Atsuko)
北陸先端科学技術大学院大学・情報科学研究科・教授
研究者番号：10313701

研究成果の概要：
非接触型や接触型 IC カードの爆発的な普及に伴い，IC カードを利用した電子サービスが広がりつつある．IC カードのサービスでは高速性・小メモリ性を実現できる楕円曲線暗号が脚光を浴びているが,IC カード上のデータ処理はサイドチャネル攻撃による秘密鍵の解読が脅威となっている．近年，べき演算の途中で入力されるメモリ値の消費電力や，アドレス値の違いによる消費電力の違いの利用など,サイドチャネル攻撃は複雑かつ強力になる状況が続いている．
本研究はサイドチャネル攻撃に対して安全かつ効率的な楕円曲線暗号のスカラー倍算の generic model の構築を実現した．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００５年度	4,000,000	0	4,000,000
２００６年度	3,000,000	0	3,000,000
２００７年度	2,300,000	690,000	2,990,000
２００８年度	1,500,000	450,000	1,950,000
年度			
総　計	10,800,000	1,140,000	11,940,000

研究分野：総合領域
科研費の分科・細目：情報学
キーワード：セキュリティ，サイドチャンネル，公開鍵暗号，楕円曲線，安全性証明

１．研究開始当初の背景

近年，非接触型や接触型 IC カードの爆発的な普及に伴い,IC カードを利用した電子サービスが広がりつつある．これら電子サービスに不可欠な技術である暗号，本人認証，ディジタル署名を実現するのが公開鍵暗号である．公開鍵暗号は安全性の土台となる数学的問題により，大きく 3 つの方式がある．素因数分解問題，離散対数問題（DLP），楕円曲線上の離散対数問題（ECDLP）に基づく方式である．ECDLP に基づく楕円曲線暗号は他の公開鍵暗号と比較し，強力な解読がなく小さい鍵で同等の安全性を実現できる．このことから，IC カードでは高速性・小メモリ性を実現できる楕円曲線暗号が脚光を浴びている．しかし IC カード上のデータ処理は，サイドチャネル攻撃という消費電力量の観測による秘密鍵の解読を可能にした．サイドチャネル攻撃は安全性の土台である数学的問題の直接的解読ではなく，署名生成時などの情報（サイドチャネル情報）を入手し，その情報を利用して鍵を解読する．楕円曲線暗号の場

合，基本演算であるべき演算 kG 実行時の消費電力を測定し，k の値を推測する．べき演算とは，kG = G + ･･･ + G (G の k 回の和)の演算で，k が秘密鍵，G が既知のデータとなる．なお，他の公開鍵暗号の必須の基本演算もべき演算である．サイドチャネル攻撃は公開鍵暗号の主要部であるべき演算の実装方法に対する攻撃といえる．

当初サイドチャネル攻撃は，べき演算の構成要素である加算 G+G と 2 倍算 2G の二つの演算の電力消費量の違いを利用する攻撃で，単純な方法で回避可能であった．しかし，べき演算の途中で入力されるメモリ値の消費電力の違いや，アドレス値の違いによる消費電力の違いを利用するなど，サイドチャネル攻撃は複雑かつ強力になり，その度に新たな回避策が必要になるという状況が続いている．

２．研究の目的

近年，べき演算の途中で入力されるメモリ値の消費電力や，アドレス値の違いによる消費電力の違いの利用など，サイドチャネル攻撃は複雑かつ強力になる状況が続いている．本研究はサイドチャネル攻撃に対して安全かつ効率的なスカラー倍算の generic model の構築を目的とする．

3.研究の方法

本研究において以下の順で研究を行った．

(1)サイドチャネル攻撃の攻撃手法を解析する．

(2)(1)の解析を利用し，サイドチャネル攻撃に対して，安全なスカラー倍算のアルゴリズムを構築する．

(3)(2)のアルゴリズムを一般化し，予備計算テーブルの持ち方をフレキシブルに設定することで，サイドチャネル攻撃に対して安全，かつメモリサイズを汎用的に設定可能なスカラー倍算のアルゴリズムの構築．

4.研究成果

本研究の主要成果を以下に記載する．

(1) ランダム化初期点(RIP)を用いたスカラー倍算アルゴリズム BRIP, EBRIP は，全ての DPA 及び SPA に強力なアルゴリズムである．しかし，Address-bit DPA(ADPA) を考慮するとメモリが増加する問題があった．本研究ではこの問題点を解消し，小メモリ量で ADPA にも強力な方法を提案した．

(2) DDPA 対策の一つにスカラーの bit 表現をランダム化させる方法がある．既存の方法では，確率的にランダム化がされないビットが存在し，そのビットを利用した攻撃があった．本研究ではこの問題を解決し，全てのビットが確率的にランダム化される方法を提案した．

(3)ランダム化初期点(RIP)を用いたスカラー倍算アルゴリズムは DPA 及び SPA に強力でテーブルを利用するアルゴリズムであるが，利用可能なテーブルの大きさが限られており，汎用性がないという問題があった．本研究では，(１)の手法を適用し，任意のテーブルサイズにおいて効率的なアルゴリズムが構築可能な generic model を提案した．これにより全ての DPA, SPA に強力で，かつ汎用的なテーブル利用のアルゴリズム q を可能にした．

(4)上記(1)-(3)は加算連鎖の改良である．このため，楕円曲線暗号と同様に超楕円曲線暗号においても利用可能である．超楕円曲線暗号に関しては，楕円曲線暗号と比べ，サイドチャネル攻撃に耐性を持つアルゴリズムの研究が少なく，例えば，SPA に強力な加算公式なども提案されていなかった．本研究では，超楕円曲線において新たに識別不可能な加法方式を構築した．この加算公式により，サイドチャネル攻撃に強力な超楕円曲線暗号を実現した．

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　67 件）

1. K. Emura, A. Miyaji and K. Omote, “A Dynamic Attribute-Based Group Signature Scheme and its Application in an Anonymous Survey for the Collection of Attribute Statistics”, The Forth International Conference on Avail ability, Reliability and Security, 487-492. 2009. 査読有

2．A. Miyaji and M. Sukegawa, “New Correlations of RC4 PRGA Using Nonzero-Bit Differences”, ACISP 2009, Lecture Notes in Computer Science, 5594 (2009), Springer-Verlag, 134-152. 査読有

3. S. Hirasawa and A. Miyaji, “Elliptic curves with a pre-determined embedding degree”, The 2009 IEEE International Symposium on Information Theory, ISIT 2009, 2391-2395. 査読有

4. K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, “A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length”, The 5th

Information Security Practice and Experience Conference, ISPEC 2009, Lecture Notes in Computer Science, 5451 (2009), Springer-Verlag, 13-23. 査読有

5. K. Emura, A. Miyaji and K. Omote, "A Certificate Revocable Anonymous Authentication Scheme with Designated Verifier", The First International Workshop on Recent Innovations and Breakthroughs in Cryptography, RIBC 2009, 769-773. 査読有

6. M. S. Rahman, M. Soshi and A. Miyaji, "A Secure RFID Authentication Protocol with Low Communication Cost", The 3rd International Workshop on Intelligent, Mobile and Internet Services in Ubiquitous Computing, IMIS 2009, 559-564. 査読有

7. A. Miyaji, S. Zrelli, Y. Shinoda, and T. Ernst, "Security and Access Control for Vehicular Communications Networking and Communications", IEEE International Conference on Wireless and Mobile Computing, WIMOB '08, 561-566. 査読有

8. A. Miyaji, K. Omote and K. Kato, "Simple Certificateless Signature with Smart Cards", International Workshop on Security in Ubiquitous Computing Systems, SECUBIQ'08, IEEE, 2008, 査読有

9. A. Miyaji, A. Waseda, T. Takagi, and M. Soshi, "Quantum Secret Sharing between Multiparty and Multiparty against the Attack with Single Photons or EPR-pair", The 2008 International Symposium on Information Theory and its Applications, Proceedings of ISITA 2008, 査読有

10. A. Miyaji and K. Mizosoe, "Revisited (Hyper)-Elliptic Curve Scalar Multiplication with a Fixed Point", IPSJ Trans vol. 49, No.9 (2008), 2975-2988. 査読有

11. A. Miyaji, "Generalized Scalar Multiplication Secure against SPA, DPA, and RPA", IEICE Trans., Fundamentals. vol. E91-A, No.10 (2008), 2833-2842. 査読有

12. A. Miyaji, "Ancestor Excludable Hierarchical ID-based Encryption and Its Application to Broadcast Encryption", IPSJ Trans, vol. 48, No.9 (2007), 2999-3013. 査読有

13. T. Hinoue, A. Miyaji, and T. Wada, "The security of RC6 against asymmetric chi-square test attack", IPSJ Trans, vol. 48, No.9(2007), 2966-2975. 査読有

14. A. Miyaji, "Generalized MMM-algorithm Secure against SPA, DPA, and RPA", ICISC 2007, Lecture Notes in Computer Science, 4817 (2007), Springer-Verlag, 282-296. 査読有

15. W. Hasegawa, M. Soshi, A. Miyaji, "Mobile Agent Security with Efficient Oblivious Transfer In International Conference on Security and Cryptography", SECRYPT 2007, July 2007. 299-304. 査読有

16. A. Miyaji, Y. Takano, "Evaluation of the security of RC6 against the x^2-attack", IEICE Trans., Fundamentals. vol. E90-A, No.1 (2007), 22-28. 査読有

17. A. Miyaji, H. Mamiya, H. Morimoto. "Secure elliptic curve exponentiation against RPA, ZRA, DPA, and SPA", IEICE Trans., Fundamentals, vol.89-A, No.8 (2006), 2207-2215. 査読有

18. H. Mamiya and A. Miyaji, "Fixed-Hamming-Weight Representation for Indistinguishable Addition Formulae", IPSJ Trans, vol.47, No.8 (2006), 2430-2439. 査読有

19. T. Terada, M. Soshi, and A. Miyaji, "An IP Traceback Scheme with Variably Probabilistic Packet Marking", The 2006 International Symposium on Information Theory and its Applications, Proceedings of ISITA 2006, 査読有

20. 宮地充子, 「双線形写像に基づく暗号に適した(超)楕円曲線の構造」, 東京大学院大学数理科学研究科「代数幾何・数論及び符号・暗号」研究会報告書, 2006, 42-58. 査読無

21. A. Miyaji and K. Umeda, "Efficient Group Signature Scheme based on a Modified Nyberg-Rueppel Signature", IPSJ Trans., Vol.46, No.8 (2005), 1889-1902. 査読有

22. A. Miyaji and Y. Sakabe and M. Soshi, "Java Obfuscation -- Approaches to Construct Tamper-Resistant

Object-Oriented Programs”, IPSJ Trans., vol. 46, No.8 (2005), 2107-2119. 査読有

23. A. Waseda, M. Soshi, and A. Miyaji, “n-state quantum coin flipping protocol”, International Conference on Information Technology - ITCC2005 ,Volume II, pp.776-777, 2005. 査読有

24. A. Miyaji and Y. Takano,“On the Success Probability of chi^2-attack on RC6”, Proceedings of ACISP 2005, Lecture Notes in Computer Science, 3089 (2005), Springer-Verlag, 310-325. 査読有

25. H. Mamiya and A. Miyaji, “Fixed-Hamming-Weight Representation for Indistinguishable Addition Formulae”, ACNS 2005, 776-777. 査読有

〔学会発表〕(計 21 件) (招待講演含む)
1. 平澤 庄次郎, 宮地 充子, “埋め込み次数を事前に決定できる楕円曲線の改良″, IEICE Japan Tech. Rep., ISEC2008-137 (2009-3), 223-229, March 9-10th 2009, 公立はこだて未来大学.

2. Atsuko Miyaji, “The recent tendency of research and standardization of elliptic curve cryptosystems”, The 4th Franco-Japanese Computer Security Workshop, December 6th 2008, 慶應義塾大学.

3. 平澤 庄次郎, 宮地 充子, “埋め込み次数を事前に決定できる楕円曲線″, IEICE Japan Tech. Rep., ISEC2008-82 (2008-11), 63-66, November 13-14th 2008, 名古屋能楽堂.

4. Atsuko Miyaji, “Elliptic Curve Cryptosystem for the Privacy Protection: Theory and International Standardization”, UK-JAPAN Symposium on “Privacy and Security in the Information Society”, November 4th 2008, 東京大学大学院.

5. Atsuko Miyaji, “Generalized EBRIP ″, IEICE Japan Tech. Rep., ISEC2007-122 (2007-12), 67-78, December 19th 2007, 東京 (機会振興会館).

6. 宮地 充子, 「楕円曲線を用いた暗号の最近の研究動向」, 奈良女子大学「魅力ある大学院教育」イニシアティブ, 女性先端科学セミナー, October 29th 2007, 奈良女子大学.

7. 宮地 充子, (チュートリアル講演)「ペアリング利用に適した楕円曲線の研究及び標準化動向」, 電子情報通信学会, ソサイエティ大会 2007, AT2-2, September 13th 2007, 鳥取大学.

8. 宮地 充子, 「双線型写像応用に適した楕円曲線の最新の技術及び標準化動向」, RSA Conference, April 25th 2007, 東京.

9. 溝添健次, 宮地充子, 亀井利明. “3 つの基底を用いた効率的な楕円ベキ倍算″, IEICE Japan Tech. Rep., ISEC2007-16 (2007-03), 81-86, March 1-2nd 2007, 九州産業大学.

10. 宮地充子, 「数論応用と楕円曲線暗号の構築について」, 電子情報通信学会信学技報 IT2006-11, 1-6, November 28th 2006, 函館.

11. 宮地 充子, 「双線形写像暗号に適した楕円曲線の構成」, 日本応用数理学会 2006 年度年会講演予稿集, 104-107, September 16th 2006, 筑波大学.

12. 宮地充子, 「双線形写像暗号に適した楕円曲線の構成」, 日本応用数理学会 2006 年度年会, 講演予稿集 (2006), 104-107, September 9th 2006, 筑波大学.

13. 宮地充子, 清宮健, “Address-bit DPA に強力な BRIP アルゴリズムの改良″, IEICE Japan Tech. Rep., ISEC2005-118 (2005-12), 47-52, December 16th 2005, 東京 (機会振興会館).

６. 研究組織
(1)研究代表者
宮地 充子 (Miyaji Atsuko)
北陸先端科学技術大学院大学・情報科学研究科・教授
研究者番号：10313701

(2)研究分担者

(3)連携研究者