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 6 月 19 日現在

機関番号：34427
研究種目：若手研究（Ｂ）
研究期間：2008～2012
課題番号：20700016
研究課題名（和文）　安全で効率的な新しい多変数公開鍵暗号の設計に関する研究

研究課題名（英文）　A study on Secure and Efficient Multivariate Public Key Cryptosystems

研究代表者
岩見　真希　（IWAMI MAKI）
大阪経済法科大学・教養部・准教授
研究者番号：00422197

研究成果の概要（和文）：
安全で効率的な多変数を利用した公開鍵暗号の設計に向けて、暗号理論と計算代数の両分野がどのように相互作用しながらアルゴリズムが改良され、多種多様な分類にわかれてきたのか、幅広く調査･研究を行った。そして、計算代数分野の各種アルゴリズムの応用可能性を探りながら、最先端の研究結果を調査し、攻撃手法の提案に向けてアルゴリズムを適した形に改良して実験･検証を行い、暗号理論と計算代数の学際的研究を行った。

研究成果の概要（英文）：
To construct secure and efficient multivariate public key cryptosystems (MPKC), this research has focused attention on the interactions between MPKC and Computer Algebra which cause the improvement of their algorithms and various types of MPKC. To suggest algorithm to attack, we have researched leading-edge study by interdisciplinary approach, investigating the possibility of application of computer algebra techniques, modified them to fit and verified the effectiveness by experiments.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	900,000	270,000	1,170,000
2009 年度	900,000	270,000	1,170,000
2010 年度	1,770	531	2,301
2011 年度	698,230	209,469	907,699
2012 年度	700,000	210,000	910,000
総　計	3,200,000	960,000	4,160,000

育児休業等に伴い 2010 年度研究中断、2011 年度再開、1 年度繰り下げ

研究分野:計算代数
科研費の分科・細目：情報学･情報学基礎
キーワード：計算代数、セキュリティ、多変数、公開鍵暗号

１．研究開始当初の背景

素因数分解や離散対数問題の困難性に安全性の根拠をおく RSA 暗号、ElGamal 暗号、楕円曲線暗号などの公開鍵暗号が広く使われているが、量子コンピュータが実現すると、その特有の性質を利用して素因数分解や離散対数問題を効率的に（多項式時間で）解けるようになるため、安全性が崩壊することが

分かっている。よって、他の困難な数学的問題（NP 困難）である多変数連立方程式の求解問題、格子最短ベクトル問題、線形符号の復号問題などに安全性の根拠をおく公開鍵暗号が次世代の耐量子コンピュータ暗号として盛んに研究されている。こうした背景のもと、様々な暗号方式が提案されているが、その開発･改良過程で重要な役割を果たしてきたのが、計算代数分野の各種テクニックを利用した攻撃手法である。しかし、計算代数分野では応用を意識することなく純粋にアルゴリズムの研究そのものが独自の進化を遂げているものが多く、暗号分野で使われているのはごく一部にすぎない。よって、暗号分野と計算代数分野の学際的な研究が重要である。

２．研究の目的

次世代の耐量子コンピュータ暗号のうち、多変数連立方程式の求解問題に安全性の根拠をおく公開鍵暗号について、暗号分野と計算代数分野の学際的な調査・研究を行う。

３．研究の方法

多変数を利用した公開鍵暗号について、幅広く最新動向の調査を行う。そして、計算機代数分野の既存の各種アルゴリズムを、応用可能性を探りながら、それらに適用可能な形に改良することで、新たな攻撃手法を提案し、安全性評価を行う。

４．研究成果

多変数を用いた各種公開鍵暗号について、MI にはじまり、HFE、近年では ASC など、数百件にのぼる論文が発表され、様々な方式が提案・改良されているが、その進化の過程でみられる計算代数の各種テクニックを利用した攻撃手法、たとえばグレブナー基底を用いた方法や、その改良版の F_4,F_5 アルゴリズム、differential attack などに着目し、また、他の計算代数の各種テクニックの応用可能性を探りながら、幅広く調査を行った。

その中から、代数曲面公開鍵暗号（ASC04）および 2008 年に発表された改良版代数曲面公開鍵暗号（ASC09）に対し、計算機代数の側面から、既知の方法以外に脆弱性がないか、確認を行った。まず、計算代数の手法の暗号系への拡張として、標数 0 における手法である多変数展開基底法と拡張 Hensel 構成について考察した。暗号では標数 p（p は素数）がよく用いられるため、アルゴリズムを精査し、標数に依存するところを標数 p に拡張して発表した。その応用として、ASC04 と ASC09 に対して、標数 p での多変数展開基底法や拡張 Hensel 構成の展開テクニックを利用して代数曲面の零点にあたる Puiseux 級数根を計算し、平文を求める過程で必要な多項式を得るために利用した。しかし ASC09 に関しては、Puiseux 級数根を利用して線形方程式を解く提案手法は、公開鍵である代数曲面上の多数の有理点を利用して未定係数法による線形方程式を解く Voloch による方法と同じく、線形方程式の解空間の次元が大きいため、解を一意に特定するのが難しく、安全性が保たれることが確認できた。そこで、これらの攻撃手法の後に、単項簡約を行うことで制約条件を増やし、線形方程式の解空間の次元を下げようと試みた。その途中で、問題を組み合わせて最適化問題に帰着させ、整数格子の基底簡約による方法を用いて解く工夫を行った。しかし、公開鍵の一部である各多項式のサポートの制約条件を利用すれば、単項簡約を行わなくても同じ解空間の次元まで下げることができることが判明した。よって、公開鍵のサポートの制約条件の適切さ、および上記線形方程式を解く攻撃手法に対する安全性を確認した。その他、代数曲面のパラメータ表示を利用した攻撃手法についても検討した。また、計算代数分野で重要なグレブナー基底の計算に使われる単項簡約を利用して、ASC09 の公開鍵におけるランダムな多項式間の脆弱性となりうる条件を明らかにした。その後、Faugère と Spaenlehauer により、セキュリティパラメータに関して多項式時間で実行可能な有効な攻撃手法が提案された(PKC2010)。この手法では、実用上のパラメータ設定では、途中の線形方程式系の方程式の数が未知数の数より多いため、通常は解が一意に定まるとされ、実験でも確認されている。画期的なのは ①２つの暗号文の差と公開鍵を生成元とするイデアルを素イデアルに分解（実際の計算では消去イデアルのグレブナー基底計算または暗号文の差と公開鍵の終結式計算で得られた結果を因数分解）して攻撃に重要な役割を果たすある未知の多項式に紐づけられた因子を検出して利用していること、②新しい変数を導入して途中で経由する有理関数体における不定性を解消していること、の２点である。しかしながら、①の素イデアルに分解するステップで、多くのケースでは問題ないと言及されているが、セキュリティパラメータによっては素イデアルにならない（つまりこの手法が有効ではない）ケースがあることにも注意すべきであり、検討の余地があるといえる。

また、これらは ASC の特徴を用いた攻撃手法であり、安全性の根拠である求セクション問題を解いているわけではないため、求セクション問題は、効率的解法の探求や暗号への利用という点で今なお興味深い問題といえる。

さらに、その他の暗号についても、安全で効率的な新しい多変数公開鍵暗号の設計のために、両分野がどのように相互作用し、ア

ルゴリズムが改良されながら、多種多様な分類にわかれてきたのかを、幅広く調査・研究した。

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 6 件）

① Maki IWAMI,
Computer Algebra Techniques in the Development of Public-Key Cryptosystems using Multivariate Polynomials, 大阪経済法科大学論集,Vol.105, 2013, 掲載予定, 査読無

② Maki IWAMI,
An improvement of Voloch’s rational point attack on improved algebraic surface cryptosystem, 京都大学数理解析研究所講究録(RIMS Kokyuroku), Vol.1759, pp.105-114, 2011, 査読無
http://hdl.handle.net/2433/171329

③ Maki IWAMI,
Series solution and Cryptography, 数式処理(Bulletin of the Japan Society for Symbolic and Algebraic Computation), Vol.16, No.2, pp.127-130, 2009, 査読無
http://ci.nii.ac.jp/naid/1002679198 3

④ Maki IWAMI,
Applying expansion techniques of multivariate expansion base method and extended Hensel construction to cryptography, Abstracts of Papers Presented to the American Mathematical Society, Vol.30, No.1, Issue 155, pp.152-153, 2009, 査読有

⑤ Maki IWAMI,
Breaking the Improved Akiyama-Goto Algebraic Surface Public-key Cryptosystem, 数式処理(Journal of the Japan Society for Symbolic and Algebraic Computation), Vol.15, No.2, pp.124-127, 2008, 査読無
http://ci.nii.ac.jp/naid/1002390261 5

⑥ Maki IWAMI,
An Attack on Improved Algebraic Surface Public-key Cryptosystem, ACM Communications in Computer Algebra (Poster Abstracts ECCAD 2008), Issue 164, Vol.42, No.2, pp.71-74, 2008, 査読無
http://www.sigsam.org/cca/issues/is sue164.html

〔学会発表〕（計 10 件）

① Maki IWAMI,
Computer Algebra Techniques in the Development of Public-Key Cryptosystems using Multivariate Polynomials, March 29,2013, Application of Fundamental Mathematics to Computer Science from Algebraic Perspective (大阪経済法科大学科学研究費採択課題合同研究会), Osaka University of Economics and Law, Japan

② Maki IWAMI,
An improvement of Voloch’s rational point attack on improved algebraic surface cryptosystem, RIMS Workshop on Developments in Computer Algebra Research, July 9, 2010, Research Institute for Mathematical Sciences, Kyoto University, Japan

③ Maki IWAMI,
Surface Parametirizaion and Cryptography (poster presentation), The 11th International Workshop on Computer Algebra in Scientific Computing, September 14 and 19, 2009, Kobe University, Japan

④ Maki IWAMI,
Computer Algebra and Cryotography, 稚内北星学園大学 数学・数理科学談話会, September 4, 2009, Wakkanai Hokusei Gakuen University, Japan

⑤ Maki IWAMI,
Towards applications of computer algebra for attacking cryptosystems, Combinatorics Summer school 2009, September 1, 2009, Wakkanai Hokusei Gakuen University, Japan

⑥ Maki IWAMI,
Series solution and Cryptography, 18th Jssac meeting, June 12, 2009, Ryukoku University, Japan

⑦ Maki IWAMI,
Applying expansion techniques of multivariate expansion base method and extended Hensel construction to cryptography, Joint Mathematics Meetings 2009, Meeting #1046, January 8, 2009, Washington, DC, U.S.A.

⑧ Maki IWAMI,
Breaking the Improved Akiyama-Goto Algebraic Surface Public-key Cryptosystem, June 7, 2008, 17th Jssac meeting, Josai University, Japan

⑨ Maki IWAMI,
An Attack on Improved Algebraic Surface Public-key Cryptosystem,

ECCAD (East Coast Computer Algebra Day) 2008 (poster presentation), May 10, 2008, Shepherd University, U.S.A.

⑩ Maki IWAMI,
Breaking the Akiyama-Goto Algebraic Surface Public-key Cryptosystem and a Short Introduction to Multivariate Analytic Factorization, Symbolic Computation Seminar, North Carolina State University, Mathematics Department, May 7, 2008, North Carolina State University, U.S.A.

〔その他〕
ホームページ等
http://researchmap.jp/read0104915/

６．研究組織
(1)研究代表者
岩見　真希　(IWAMI MAKI)
大阪経済法科大学・教養部・准教授
研究者番号：00422197