様式 C-7-2

自己評価報告書

平成 23 年 5 月 12 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：計算機代数、公開鍵暗号、多変数

１．研究計画の概要

計算機代数と暗号理論の学際的研究として、多変数を用いた各種公開鍵暗号に対し、計算機代数的アプローチによる攻撃手法の提案を目指すことで安全性評価を行い、安全性と効率性を考慮しながら、脆弱性のない暗号の設計を目指す。

２．研究の進捗状況

研究計画に基づき、多変数を用いた各種公開鍵暗号について、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（ASC07）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、計算機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 構成を、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、発表した。その応用として、ASC04 と ASC07 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 ASC07 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、現時点において安全性が保たれている。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した。そこで問題を組み合わせ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いた。しかし、単項簡約を行わなくても、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、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。これにより、公開鍵のサポートの制約条件の適切さが分かり、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、計算機代数分野で重要な Groebner 基底の計算に使われる単項簡約を利用して、ASC07 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。

３．現在までの達成度

②おおむね順調に進展している。

（理由）まだ解決すべき問題も多いが、研究の進捗状況に述べたように、計算機代数と暗号理論の学際的研究として、多変数を用いた暗号に対して計算機代数的アプローチで攻撃手法の提案を目指し、安全性評価を行っている。

４．今後の研究の推進方策

多変数を用いた公開鍵暗号に関してさらに幅広く調査し、計算機代数の各種アルゴリズムを適した形に改良して攻撃手法の提案を行い、その成果をふまえ、安全性と効率性を考慮しながら、脆弱性のない暗号の設計を目指す。

５． 代表的な研究成果
（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５件）

① 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), 印刷中, 査読無

② 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

③ 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

④ 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

⑤ 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

〔学会発表〕（計９件）

① 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, Kyoto, Japan

② 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

③ 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

④ Maki IWAMI,
Towards applications of computer algebra for attacking cryptosystems, Combinatorics Summer school 2009, September 1, 2009, Wakkanai Hokusei Gakuen University, Japan

⑤ Maki IWAMI,
Series solution and Cryptography, 18th Jssac meeting, June 12, 2009, Ryukoku University, Japan

⑥ 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.

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

⑧ 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.

⑨ 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.