On multivariable asymmetric public-key cryptography based on simultaneous algebraic Riccati equations over finite fields

Y. Peretz[1]

[1] *Computer Sciences Department, Lev Academic Center, Jerusalem, Israel. yosip@g.jct.ac.il*

Many encryption schemes based on Multivariable Quadratic Equations (MQE) over finite fields were suggested in the last three decades and many were broken (see [1]). Apparently, the broken systems were based on some hidden structure, which on one hand enabled the efficient invertibility of the system, but on the other hand was found to be vulnerable to algebraic attacks. Almost all the MQE based encryption schemes that were proved to be insecure, share the common drawback that some quadratic forms associated to their central maps have low rank (see [2]) and therefore are vulnerable to the Min-Rank Attack (see [3]). On the other hand, the belief that random quadratic systems are hard to solve on average (see [4], [5] and references therein), points towards designing trap-door primitives based on randomness, which raises difficulties in designing immune invertible primitives. Little was done in this direction in the context of asymmetric public-key cryptography (see [4]).

An overview of Multivariate Public-Key Cryptography (MPKC) is given in [6], where the authors call for a unifying framework for cryptanalysis of MPKC systems in order to build confidence in their security. They also point out to potential applications of such systems in the realm of limited computing power (e.g. in Radio Frequency Identification Devices (RFID) and in Wireless Sensing (WS)), where other cryptographic systems (e.g. RSA, ELGAMAL, ECC) are irrelevant. A summary of the main developments in the cryptanalysis of multivariate cryptosystems is given in [7] and [5].

Let $\mathbf{F}$ denote any finite field. Non-symmetric Algebraic Riccati Equation (ARE) over $\mathbf{F}$ is an equation of the form:

$$XCX + XD - AX - B = 0, \tag{1}$$

where A, B, C, D are $m \times m, m \times n, n \times m, n \times n$ matrices and the solution X is a $m \times n$ matrix over $\mathbf{F}$. The complexity of computing X is equivalent to the complexity of the constrained generalized eigenvalue-eigenvector problem defined by:

$$T \begin{bmatrix} X \\ I \end{bmatrix} = \begin{bmatrix} X \\ I \end{bmatrix} L, \tag{2}$$

where

$$T = \begin{bmatrix} A & B \\ C & D \end{bmatrix}, \tag{3}$$

and $L = CX + D$ is $n \times n$ matrix. The Non-symmetric Simultaneous Algebraic Riccati Equations problem (NSARE) is the following: given t quadruples

$$(A_i, B_i, C_i, D_i), i = 1, \ldots, t, \tag{4}$$

find X such that all the equations:

$$XC_iX + XD_i - A_iX - B_i = 0, \tag{5}$$

are satisfied simultaneously for $i = 1, \ldots, t$. The NSARE is known to be NP-complete over any finite field and NP-hard over any infinite field (see [8]).
It follows that any set of multivariable polynomial equations can be reduced (by polynomial-time reduction) to the NSARE problem (the converse is obvious) and thus any encryption scheme based on multivariable polynomial set of equations can be crypt-analyzed to vulnerabilities by investigating the related equivalent NSARE problem.

Based on the NSARE problem, pubic-key encryption schemes were defined, with the following features (see [8]):

1. The security of the systems is based on provable NP-complete problem.

2. The suggested schemes fit to the age of post-quantum cryptography.

3. The systems involves truly (pseudo) random choice of the coefficients of the core equations.

4. The suggested scheme is very flexible in the ability of matching the security level to the needs and to the given computing power.

5. The suggested systems fit to the realm of limited-power computing devices since they involve only matrix summation and multiplication (matrix inversion is made once for the whole system life).

6. The suggested systems has a very fast encryption and decryption time. It has several magnitudes of improvement over the RSA for equivalent level of security.

7. The suggested schemes are highly parallelizable in parallel software or hardware and thus the encryption and decryption time can be speeded-up to a fantastic time.

Finally, the urgent call for new multivariable public-key cryptosystems (see [9]) and the call for a unifying framework for cryptanalysis of MPKC systems (see [6]) are also fulfilled by this research.

References

[1] C. Wolf, B. Preneel, *Taxonomy of Public-Key Schemes based on the Problem of Multivariate Quadratic Equations*, Cryptology ePrint Archive, Report 2005/077, http://eprint.iacr.org/ (2005).

[2] C. Tao, A. Diene, S. Tang and J. Ding, *Simple Matrix Scheme for Encryption*, PQCrypto 2013, LNCS 7932, pp. 231-242 (2013).

[3] A. Kipnis, A. Shamir, *Cryptanalysis of the HFE public key cryptosystem by relinearization*, CRYPTO 1999, LNCS 1666, pp. 19-30 (1999).

[4] N. T. Courtois, *General Principles of Algebraic Attacks and New Design Criteria for Cipher Components*, Advanced Encryption Standard - AES 2005, LNCS 3373, pp. 67-83 (2005).

[5] O. Billet, J. Ding, *Overview of Cryptanalysis Techniques in Multivariate Public Key Cryptography*, Inbook: Gröbner Bases, Coding, and Cryptography, Editors: M. Sala, T. Mora, L. Perret, S. Sakata and C. Traverso, Springer-Verlag Berlin Heidelberg, pp.263-283 (2009).

[6] J. Ding, B. Y. Yang, *Multivariate Public Key Cryptography*, Inbook: Post Quantum Cryptography, Editors: D. J. Bernstein, J. Buchmann and E. Dahmen, Springer-Verlag Berlin Heidelberg, pp.193-234 (2009).

[7] Jintai Ding, Jason E. Gower, Dieter S. Schmidt, *Multivariate Public Key Cryptosystems*, Series: Advances in Information Security, Editor: Sushil Jajodia, Springer (2006).

[8] Y. Peretz, *On mulivariable encryption schemes based on simultaneous algebraic Riccati equations over finite fields*, Finite Fields and Their Applications, 39, pp. 1-35 (2016).

[9] W. Shen, S. Tang, *TOT, a Fast Multivariable Public Key Cryptosystem with Basic Secure Trapdoor*, Cryptology ePrint Archive, Report 2013/771, http://eprint.iacr.org/ (2013).