Finite Fields and Their Applications 54 (2018) 30–64

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Cryptanalysis of Riccati equation encryption schemes TP-I and TP-II

Jian-Ming Shih [a,1], Lih-Chung Wang [a], Yossi Peretz [b]

[a] *Applied Mathematics, National Dong Hwa University, Taiwan*
[b] *Computer Sciences Department, Jerusalem College of Technology, Lev Academic Center, P.O.B. 16031, Jerusalem, Israel*

ARTICLE INFO

Article history:
Received 5 March 2018
Received in revised form 15 July 2018
Accepted 17 July 2018
Available online xxxx
Communicated by Neal Koblitz

MSC:
94A60
14G50
12Y05
12E20
68Q17
03D15

Keywords:
TP-I (Tsafenat-Paaneah-I)
TP-II (Tsafenat-Paaneah-II)
Public-key encryption schemes
Algebraic Riccati equations

ABSTRACT

TP-I (Tsafenat-Paaneah-I) and TP-II (Tsafenat-Paaneah-II) are two public-key encryption schemes based on simultaneous algebraic Riccati equations over finite fields, which were proposed by Peretz in 2016 [9]. In this research, we discovered the hidden linear structure of TP-I and TP-II, respectively. Hence, we are going to show how can one break the two schemes.

E-mail address: lcwang@gms.ndhu.edu.tw (L.-C. Wang).
[1] PhD student.

https://doi.org/10.1016/j.ffa.2018.07.004
1071-5797/

1. Introduction

Public key cryptosystems (PKC) [5][7][12] have become an important part of our modern communication infrastructure for the last three decades. The security of the mainstream PKC, such as RSA, ECC and ElGamal, depends on hard number-theoretical problems such as factoring integers or discrete logarithms. Ever since Shor proposed the quantum computer attack algorithm, and the approach of the quantum computer realization, post-quantum cryptography [1] has become noticeable. There are 4 known alternative approaches for post-quantum cryptography, namely multivariate, lattice based, code based and signature based public key cryptography. Multivariate public key cryptography is a promising alternative [2][6][11][13][14]. Multivariate public key cryptosystems rely on the difficulty of solving systems of nonlinear algebraic equations, which is an NP-complete problem in general. However, it is not easy to find a good trap door for an encryption scheme. So far, there are still a small number of schemes which have not been broken.

TP-I and TP-II are two public-key encryption schemes based on simultaneous algebraic Riccati equations [8] over finite fields, which were proposed by Peretz in 2016 [9]. An algebraic Riccati equation arises in the context of infinite-horizon optimal control problems continuous time or discrete time control systems. Riccati equations over finite fields are the analog of the original problem. Riccati equation is given as follows. $Y = \mathcal{R}(X) := XCX + XD - AX - B$ where A, B, C, D and X are matrices. Hence it is a system of quadratic equations. In general, it is hard to solve the Riccati equation. Peretz has proved that NSARE (Nonsymmetric Simultaneous Algebraic Riccati Equations) problem is NP-complete over any finite field in [9]. In order to make a trap door, the structure of A, B, C, D and X are specially chosen in [9]. However, owing to the chosen structure of A, B, C, D and X, we discovered the hidden linear structure of TP-I and TP-II [3][4]. Hence, we found the ways to break these two schemes. The original paper of TP-I and TP-II gave no suggestion of the system parameters. Hence, we only show how to break the toy examples and use the complexity estimate of our attacks to show them unsafe.

Riccati equations are appealing because any future Riccati based cryptosystem would have fantastic time in parallel implementation since matrix multiplication and matrix summation have time-optimal algorithms in parallel (an $n \times n$ matrix summation takes $O(1)$ in parallel when using n^2 processors and matrix multiplication takes $O(log_2(n))$ when using n^3 processors). Therefore, from the perspective of efficiency, Riccati equations are very appealing for the design of efficient cryptosystems as was indicated in [9][10].

This paper is organized as follows: introducing TP-I encryption scheme in Section 2; describing how to attack TP-I in Section 3; explaining TP-II encryption scheme in Section 4; detailing how to attack TP-II in Section 5; finally a conclusion is given in Section 6.