Cryptanalysis of the AA_β Cryptosystem based on Linear Diophantine Equation Discrete Log Problem

Yanbin Pan and Yingpu Deng

Key Laboratory of Mathematics Mechanization
Academy of Mathematics and Systems Science,Chinese Academy of Sciences
Beijing 100190, China
panyanbin@amss.ac.cn, dengyp@amss.ac.cn

Abstract. Very recently, Ariffin and Abu proposed a new version of the AA_β cryptosystem based on linear diophantine equation discrete log problem. However, we give an efficient simple ciphertext-only attack to show that it is not secure.

Keywords: Public-Key Cryptosystem, linear diophantine equation discrete log problem, matrix decomposition

1 Introduction

In 2009, Ariffin and Abu[1] proposed a chaos-based public key cryptosystem which they call the AA_β cryptosystem. However, it was broken by Blackburn [3].

Very recently, Ariffin and Abu [2] proposed a new version of the AA_β cryptosystem based on linear diophantine equation discrete log problem and matrix decomposition problem. However, we give an efficient simple ciphertext-only attack to show that it is not secure.

The remainder of the paper is organized as follows. In Section 2, we describe the AA_β cryptosystem. In Section 3, we give our very simple attack. Finally, we give a short conclusion.

2 Description of the AA_β Cryptosystem

Key Generation:
B first selects a *singular* 2×2 matrix G_B and two nonsingular 2×2 matrix B_1, B_2, then he computes

$$E_{1B} = G_B B_1, E_{2B} = G_B B_2.$$

Public Key: E_{1B}, E_{2B}.
Private Key: B_1, B_2.
Encryption:
A wants to encrypt a message $M \in \mathbb{Z}^{2\times 2}$ to B. He first choose a fix constant Δ, and let $U = \Delta E_{2B}$, $A_3 = U - E_{1B}$. Then he randomly chooses $A_4 \in \mathbb{Z}^{2\times 2}$ and let

$$E_{AB} = A_4 A_3.$$

Finally, he computes

$$C_1 = A_4U, C_2 = A_4E_{2B}, C_3 = M + E_{AB}$$

and sends (C_1, C_2, C_3) to B.

Decryption: When getting (C_1, C_2, C_3), B first computes $E_{BA} = (C_1B_1^{-1} - C_2B_2^{-1})B_1$. It can be simply concluded that $E_{BA} = E_{AB}$. So B can get M by computing $C_3 - E_{BA}$.

Ariffin and Abu gave some methods to generate the needed random matrices and also an example. What's more, they defined the LDEDLP problem which is to solve E_{AB} from $(E_{1B}, E_{2B}, C_1, C_2, C_3)$ and assume that it is hard. However, we next give an efficient attack to show that the cryptosystem is not secure. Furthermore, LDEDLP is easy.

3 Our Attack

Our purpose is to recover E_{AB}. Once having done this, we can get M easily.

Notice that Δ can be easily obtained, since $U = \Delta E_{2B}$, $C_1 = A_4U$, $C_2 = A_4E_{2B}$, it is obvious that $C_1 = \Delta C_2$. After we have Δ, U is known and so is A_3.

We claim that

Proposition 1. *We can find a matrix $K \in \mathbb{Q}^{2\times 2}$ in polynomial time, such that*

$$A_3 = E_{2B}K.$$

Proof. First we prove that such K must exist. Since $A_3 = U - E_{1B} = \Delta E_{2B} - E_{1B} = E_{2B}(\Delta I - B_2^{-1}B_1)$, we can let $K = \Delta I - B_2^{-1}B_1$, where I is the identity matrix.

Second we show how to find such K. We have

$$\begin{aligned} A_{3_{11}} &= E_{2B_{11}}K_{11} + E_{2B_{12}}K_{21} \\ A_{3_{12}} &= E_{2B_{11}}K_{12} + E_{2B_{12}}K_{22} \\ A_{3_{21}} &= E_{2B_{21}}K_{11} + E_{2B_{22}}K_{21} \\ A_{3_{22}} &= E_{2B_{21}}K_{12} + E_{2B_{22}}K_{22}. \end{aligned}$$

Since E_{2B} is singular, we only focus on the first two linear equations

$$\begin{aligned} A_{3_{11}} &= E_{2B_{11}}K_{11} + E_{2B_{12}}K_{21} \\ A_{3_{12}} &= E_{2B_{11}}K_{12} + E_{2B_{12}}K_{22}. \end{aligned}$$

Without loss of generality, we suppose $E_{2B_{12}} \neq 0$, so we we can fix any K_{11}, K_{12} first, then compute the corresponding K_{21}, K_{22} to get the complete K. Notice that K may be different from $\Delta I - B_2^{-1}B_1$.

It is obvious that $C_2K = A_4E_{2B}K = A_4A_3 = E_{AB}$.

We give the whole attack below:

Input: $E_{1B}, E_{2B}, C_1, C_2, C_3$
Output: M
1. Compute $\Delta = C_{1_{ij}}/C_{2_{ij}}$, where $C_{2_{ij}} \neq 0$.
2. Compute $A_3 = \Delta E_{2B} - E_{1B}$.
3. Compute K such that $A_3 = E_{2B}K$.
4. Compute $E = C_2K$.
5. Compute $M = C_3 - E$, output M

4 Conclusion

The new version of the AA_β cryptosystem is not secure.

References

1. M.R.K. Ariffin and N.A. Abu, "AA_β-Cryptosystem: A chaos based public key cryptosystem", Int. J. Cryptology Research 1 (2009) 149-163.
2. M.R.K. Ariffin and N.A. Abu, "Linear Diophantine Equation Discrete Log Problem, Matrix Decomposition Problem and the AA_β-Cryptosystem", available at http://eprint.iacr.org/2011/145.
3. S.R. Blackburn, "The Discrete Log Problem Modulo 1: Cryptanalyzing the Ariffin-Abu cryptosystem," J. Mathematical Cryptology, vol. 4, pp. 193-198, 2010.