JSIAM Letters Vol.3 (2011) pp.53–56 ©2011 Japan Society for Industrial and Applied Mathematics JSIAM Letters

On the reduction attack against the algebraic surface public-key cryptosystem(ASC04)

Satoshi Harada[1], Yuichi Wada[2], Shigenori Uchiyama[3] and Hiro-o Tokunaga[3]

[1] NRI SecureTechnologies, Ltd., Tokyo 105-7113, Japan
[2] Waseda Junior & Senior High School, Tokyo 162-8654, Japan
[3] Tokyo Metropolitan University, Tokyo 192-0397, Japan

E-mail *s2-harada@nri.co.jp, uchiyama-shigenori@tmu.ac.jp*

Received May 10, 2011, Accepted June 25, 2011

Abstract

In 2004, Akiyama and Goto proposed an algebraic surface public-key cryptosystem (ASC04) which is based on the hardness of finding sections on fibered algebraic surfaces. In 2007, Uchiyama and Tokunaga gave an efficient attack, which is called the reduction attack, against ASC04 under some condition of a public-key of the scheme. In 2008, Iwami proposed its improved attack. In this paper, we point out a flaw in Iwami's attack and propose a generalized reduction attack. The attack is based on Iwami's attack, and the flaw is fixed. We also discuss our experiments of the attack.

Keywords multivariate public-key cryptography, algebraic surface, section finding problem, Gröbner basis, elimination ideal

Research Activity Group Algorithmic Number Theory and Its Applications

1. Introduction

In 1994, Shor proved that the integer factorization problem and the discrete logarithm problem can be solved in probabilistic polynomial time by using quantum computers [1]. Thus, once a quantum computer is realized, public-key cryptosystems based on them would not be secure. For this reason, cryptographic schemes which are expected to have resistance against quantum computers have been researched actively [2]. Algebraic surface public-key cryptosystems (ASCs for short) [3,4], proposed by Akiyama and Goto, is one of the candidates for such schemes. ASC is based on the hardness of finding sections on fibered algebraic surfaces. This problem is called the section finding problem (SFP for short). SFP is the following problems. (Let $k := \mathbb{F}_p$ be a finite prime field of p elements.)

Let $X(x, y, t) = 0$ be an algebraic surface over k, the problem is to find two polynomials $u_x(t), u_y(t) \in k[t]$ such that $X(u_x(t), u_y(t), t) = 0$.

Two of the authors, Uchiyama and Tokunaga, proposed an efficient attack, which is called the reduction attack, against the ASC04 (which is the first implementation of ASC proposed in 2004) in 2007 [5]. They make use of some fundamental properties of Gröbner basis. The correctness of the reduction attack can be proven under a certain condition of the leading term of a public-key $X(x, y, t)$ with respect to a monomial order in $k[x, y, t]$. Moreover, Ivanov and Voloch proposed a so-called trace attack in 2008 [6]. Then, Iwami proposed an improved reduction attack [7]. In this paper, we point out a flaw in Iwami's scheme, and propose a generalized reduction attack against the ASC04. The attack is based on Iwami's attack, and the flaw is fixed by our proposal. The correctness of our proposed attack is proven without any conditions. Moreover, we discuss our experiments of the proposed attack.

2. ASC04

In this section, we briefly review the ASC04. See [3] for the detail.

2.1 Secret-Key

Two different curves D_1 and D_2 parameterized with t in $\mathbb{A}^3(k)$:

$$D_1 : (x, y, t) = (u_x(t), u_y(t), t),$$
$$D_2 : (x, y, t) = (v_x(t), v_y(t), t).$$

2.2 Public-Key

- Algebraic Surface X:
  $X(x, y, t) := \sum_{(i,j)\in\Lambda_X} c_{ij}(t)x^i y^j = 0$ $(\in k[x, y, t])$
  $(\Lambda_X := \{(i, j) \in (\mathbb{Z}_{\geq 0})^2 \mid c_{ij}(t) \neq 0\})$ satisfying
  $$X(u_x(t), u_y(t), t) = X(v_x(t), v_y(t), t) = 0.$$
- l: an integer satisfying the following condition.
  $\deg_t X(x, y, t) < l$, and l is the minimum degree of a monic irreducible polynomial $f(t) \in k[t]$ given for encryption.
- d: an integer satisfying the following condition.
  $$d \geq \max\{\deg u_x(t), \deg u_y(t), \deg v_x(t), \deg v_y(t)\}.$$

2.3 Encryption

Divide a plaintext m into l blocks as $m = m_0||m_1||\cdots||m_{l-1}$ and embed m_i $(0 \leq m_i < p$ $(i = 0, \ldots, l-1))$ within coefficients of a plaintext polynomial $m(t) \in k[t]$.

Choose a monic irreducible polynomial $f(t) \in k[t]$ of degree greater than or equal to l and randomly choose

Table 1. Reduction attack.

Input: Public-Key $X \in k[x,y,t]$, Ciphertext $F \in k[x,y,t]$.
Output: Plaintext m corresponding to ciphertext $F(x,y,t)$.
1. Find the remainder $R_1 \in k[x,y,t]$ by dividing F by X.
2. Randomly choose some terms of R_1 with $c_{ij}(t)x^iy^j$ $((i,j) \neq (0,0), c_{ij}(t) \notin k)$, and let its coefficients $c_{ij}(t)$ be $C(\subset k[t])$.
3. Factorize elements of a set C, and let the set of irreducible factors of degree l or more be $G(\subset k[t])$.
4. Choose $g \in G$, and find the remainder $n \in k[t]$ by dividing R_1 by g. If $n \notin k[t]$, we choose another $g \in G$.
5. Let $n(t) = n_{k-1}t^{k-1} + \cdots + n_1t + n_0 \in k[t]$, and compute $m = n_0 \| n_1 \| \cdots \| n_{k-1}$.

two polynomials $r(x,y,t), s(x,y,t) \in k[x,y,t]$ with some conditions about its degree. The ciphertext $F(x,y,t) \in k[x,y,t]$ is defined as follows:

$$F(x,y,t) := m(t) + f(t)s(x,y,t) + X(x,y,t)r(x,y,t).$$

2.4 Decryption

Substituting sections D_1, D_2 into $F(x,y,t)$, we obtain:

$$h_1(t) := F(u_x(t), u_y(t), t) = m(t) + f(t)s(u_x(t), u_y(t), t),$$

$$h_2(t) := F(v_x(t), v_y(t), t) = m(t) + f(t)s(v_x(t), v_y(t), t).$$

Factorize $h_1(t) - h_2(t)$ and choose $f(t)$ as an irreducible polynomial with largest degree. Then, $m(t)$ is obtained by dividing $h_1(t)$ by $f(t)$. Finally, we obtain the plaintext m from $m(t)$.

3. Reduction attack

3.1 Reduction attack

In 2007, Uchiyama and Tokunaga proposed an efficient attack, which is called the reduction attack, against the ASC04 [5]. (See Table 1.) They make use of fundamental properties of Gröbner basis. For the proof of its correctness, the following condition is assumed:

Condition 1 *For the defining equation of the algebraic surface X, the leading term of X as $LT(X)$ w.r.t. a monomial order in $k[x,y,t]$ is in the form of $cx^\alpha y^\beta$ $(c \in k, (\alpha,\beta) \neq (0,0))$.*

3.2 Iwami's reduction attack

In 2008, Iwami generalized the reduction attack [7], and claimed Condition 1 can be dropped.

We implemented the attack. However we could not obtain the valid plaintexts. So there is a flaw in Iwami's scheme. See [7] for the detail.

Proposition 2 *In Iwami's attack, we have $n = 0$ in Step 5.*

Proof For $^\forall g \in G$ in Step 4, $g(t) \in k[t] \subset k(t) \subset k(t)[x,y]$. Therefore, $g(t)$ is a unit in $k(t)[x,y]$. Thus, we obtain as follows:

$$R_1 = (1/g(t))R_1 g(t).$$

Since $(1/g(t))R_1 \in k(t)[x,y]$, we obtain $n = r = 0 \in k$ in Step 5. Thus, we cannot obtain the valid plaintext m.

(QED)

Table 2. Generalized reduction attack.

Input: Public-Key $X \in k[x,y,t]$, Ciphertext $F \in k[x,y,t]$.
Output: Plaintext m corresponding to ciphertext $F(x,y,t)$.
1. Assume the public-key $X \in k(t)[x,y]$, and compute $Y := X/\mathrm{LC}(X)$. $(Y \in k(t)[x,y], \mathrm{LC}(X) \in k[t])$
2. Find the remainder $R_1 \in k(t)[x,y]$ by dividing F by Y.
3. Randomly choose some terms of R_1 with $c_{ij}(t)x^iy^j$ $((i,j)$ $(0,0), c_{ij}(t) \notin k)$, changing its coefficients $c_{ij}(t)$ to equivalent fractions with a common denominator, and let the numerators be $C(\subset k[t])$.
4. Factorize elements of a set C, and let the set of irreducible factors of degree greater than or equal to l be $G(\subset k[t])$.
5. Choose $g \in G$, and compute a Gröbner basis for an idea $\langle g, X\rangle$ w.r.t. the lex order $(x > y > t)$ in $k[x,y,t]$. Find the remainder $n(t) \in k[t]$ by dividing F by the basis.
6. Let $n(t) = n_{k-1}t^{k-1} + \cdots + n_1t + n_0 \in k[t]$, and compute $m = n_0 \| n_1 \| \cdots \| n_{k-1}$.

4. Generalized reduction attack

4.1 Generalized reduction attack

In this section, we propose a generalized reduction attack (GRA for short). This attack is based on Iwami's attack, and the flaw is fixed. See Table 2.

4.2 Analysis of the generalized reduction attack

We can prove the correctness of the generalized reduction attack without using Condition 1 based on the following two theorems.

Theorem 3 *In Step 4 of our attack, $^\exists g \in G$ s.t. $g = f(t)$.*

Proof Let $I := \langle Y \rangle \subset k(t)[x,y]$ be an ideal generated by Y. Then, $\{Y\}$ is a Gröbner basis. Since I is a principal ideal, $^\forall a \in I$, $a = \bar{G}Y$ $(\bar{G} \in k(t)[x,y])$. Therefore, $^{\exists 1}G_1, R_1 \in k(t)[x,y]$ s.t. $F = G_1Y + R_1$. This R_1 is clearly equal to R_1 in Step 2. Similarly, $^{\exists 1}G_2, R_2 \in k(t)[x,y]$ s.t. $s(x,y,t) = G_2Y + R_2$. Therefore, the cipher text $F(x,y,t) = m(t) + f(t)s(x,y,t) + X(x,y,t)r(x,y,t)$ is as follows: (Note that $X = \mathrm{LC}(X)Y$)

$$\begin{aligned} F &= m(t) + f(t)(G_2Y + R_2) + \mathrm{LC}(X)Yr \\ &= m(t) + f(t)R_2 + Y(f(t)G_2 + \mathrm{LC}(X)r). \end{aligned}$$

Then, each term of $m(t) + f(t)R_2$ can not be divided by $\mathrm{LT}(Y)$. Therefore, we obtain $R_1 = m(t) + f(t)R_2$ by the uniqueness of R_1.

Now, we assume $R_2 = R_2(t) \in k(t)$. Then, we evaluate the cipher polynomial F at sections D_1 and D_2, we obtain:

$$h_1(t) = F(u_x(t), u_y(t), t) = m(t) + f(t)s(u_x(t), u_y(t), t),$$

$$h_2(t) = F(v_x(t), v_y(t), t) = m(t) + f(t)s(v_x(t), v_y(t), t).$$

Since $X(u_x(t), u_y(t), t) = \mathrm{LC}(X)Y(u_x(t), u_y(t), t) = 0$ and $\mathrm{LC}(X) \neq 0$, we obtain $Y(u_x(t), u_y(t), t) = 0$. Therefore, $s(u_x(t), u_y(t), t) = G_2Y(u_x(t), u_y(t), t) + R_2 = R_2$. Similarly, we have $s(v_x(t), v_y(t), t) = R_2$. Thus, we obtain:

$$h_1(t) = m(t) + f(t)R_2 = h_2(t).$$

Therefore, we cannot decrypt because of $h_1(t) = h_2(t)$, and this is a contradiction.

Thus, $^{\exists}x^iy^jt^k$ $((i,j) \neq 0, k \geq 0)$ in the numerator of R_2 and $R_1 (= m(t) + f(t)R_2)$. Then, we randomly choose some terms of R_1 satisfying Step 3, and change them to equivalent fractions with a common denominator. Let the numerators be a set C. Since any element of C can be divided by $f(t)$, we obtain $f(t) \in G$. **(QED)**

Note: In what follows, we use f instead of g since we can obtain $f(t) = g$ $(\in G)$ by Theorem 3.

Theorem 4 *$n(t)$ in Step 5 is the plaintext polynomial $m(t)$.*

Proof Let an ideal I be $I := \langle X, f \rangle$, and let a Gröbner basis for I be $GB(I) := \{f_1, \ldots, f_s\}$. Moreover, the Gröbner basis for $I \cap k[t]$ is equal to $GB(I) \cap k[t]$ by the elimination ideals. Then, we gather $f_i \in GB(I) \cap k[t]$ from $GB(I)$, then change the indices of f_i in ascending order of degree. We obtain $GB(I) \cap k[t] = \{f_{i_1}, \ldots, f_{i_l}\}$. Since we can regard $GB(I) \cap k[t]$ as the reduced Gröbner basis, we have:

$$GB(I) \cap k[t] = \{f_{i_1}\}.$$

Now, we will prove $f_{i_1}(t) = f(t)$. First, we shall prove that $f_{i_1}(t)$ is divisible by $f(t)$. $^{\exists}a(x,y,t), b(x,y,t) \in k[x,y,t]$ s.t. $f_{i_1}(t) = a(x,y,t)X(x,y,t) + b(x,y,t)f(t)$ since $f_{i_1} \in I \subset k[x,y,t]$. Then, substitute the secret-key $(x,y,t) = (u_x(t), u_y(t), t)$ into f_{i_1}, and we have: (Note that $X(u_x(t), u_y(t), t) = 0$)

$$f_{i_1}(t) = b(u_x(t), u_y(t), t)f(t).$$

We assume $\tilde{b}(t) := b(u_x(t), u_y(t), t)$, and we obtain:

$$f_{i_1}(t) = \tilde{b}(t)f(t) \quad (\tilde{b}(t) \in k[t]).$$

Secondly, we shall prove that $f(t)$ is divisible by $f_{i_1}(t)$. Since $f \in I \cap k[t]$, f_{i_1} is a Gröbner basis. Then, we have:

$$f(t) = c(t)f_{i_1}(t) \quad (c(t) \in k[t]).$$

Therefore, we have:

$$f(t) = c(t)f_{i_1}(t) = c(t)\tilde{b}(t)f(t).$$

Since $c(t)\tilde{b}(t) = 1$ and $\tilde{b}, c \in k$, we obtain $GB(I) \cap k[t] = \{f(t)\}$.

Thus, we obtain $GB(I) = \{f(t), f_2, \ldots, f_s\}$ s.t. $f_i = x^{\alpha}y^{\beta}t^{\gamma}$ $(2 \leq i \leq s, (\alpha, \beta) \neq 0, \gamma \geq 0)$. Since we compute a Gröbner basis for an ideal I w.r.t. the lex order $(x > y > t)$ in $k[x,y,t]$, we have:

$$\mathrm{LT}(f) \in k[t], \quad \mathrm{LT}(f_i) \notin k[t] \quad (2 \leq i \leq s).$$

Then, we shall consider about dividing the cipher text $F = m(t) + sf + Xr$ by $GB(I)$. Any terms of the $m(t) \in k[t]$ can not be divided by $\mathrm{LT}(f_i)$ $(2 \leq i \leq s)$. Furthermore, any terms of the $m(t) \in k[t]$ can not be divided by $\mathrm{LT}(f)$ because of $\deg m(t) = l - 1$ and $\deg f(t) = l$. Since $sf + Xr \in I$, $sf + Xr$ is divisible by $GB(I)$.

Thus, by the uniqueness of the reminder of dividing by Gröbner basis, the reminder of dividing the cipher text F by $GB(I)$ makes $m(t)$. **(QED)**

Table 3. Improved generalized reduction attack.

Input: Public-Key $X \in k[x,y,t]$, Ciphertext $F \in k[x,y,t]$.
Output: Plaintext m corresponding to ciphertext $F(x,y,t)$.

1. Assume the public-key $X \in k(t)[x,y]$, and compute $Y := X/\mathrm{LC}(X)$. $(Y \in k(t)[x,y], \mathrm{LC}(X) \in k[t])$
2. Find the remainder $R_1 \in k(t)[x,y]$ by dividing F by Y.
3. Randomly choose some terms of R_1 with $c_{ij}(t)x^iy^j$ $((i,j) \neq (0,0), c_{ij}(t) \notin k)$, changing its coefficients $c_{ij}(t)$ to equivalent fractions with a common denominator, and let the numerators be $C (\subset k[t])$.
4. Factorize elements of a set C, and let the set of irreducible factors of degree greater than or equal to l be $G (\subset k[t])$.
5. Choose $g \in G$, and compute a normal form n of F by $\{g, X\}$ w.r.t. the lex order $(x > y > t)$ in $k[x,y,t]$. If the remainder n is a univariate polynomial $n(t) \in k[t]$, go to Step 7. Otherwise go to Step 6.
6. Choose $g \in G$, and compute a Gröbner basis for an ideal $\langle g, X \rangle$ w.r.t. the lex order $(x > y > t)$ in $k[x,y,t]$. Find the remainder $n(t) \in k[t]$ by dividing F by the basis.
7. Let $n(t) = n_{k-1}t^{k-1} + \cdots + n_1t + n_0 \in k[t]$, and compute $m = n_0 || n_1 || \cdots || n_{k-1}$.

By Theorems 3 and 4, we can prove that this algorithm is effective for ASC04.

5. Efficiency of the generalized reduction attack

When we implement the GRA, since it takes many times to compute a Gröbner basis, the GRA is not so efficient in many cases. From a practical point of view, we need to reduce its running time. Here we propose some improved methods for the GRA by adding some step just before Step 5 in the Table 3. We call this attack IGRA for short. See Table 3 for the detail.

If $n(t) \in k[t]$ in Step 5, then the $n(t)$ is a plaintext polynomial $m(t)$. We have the following theorem.

Theorem 5 *If a normal form of F by $\{f, X\}$ w.r.t. lex order is a univariate polynomial $n(t) \in k[t]$ in Step 5 of Table 3, $n(t)$ is the plaintext polynomial $m(t)$ for ASC04.*

Proof Let an ideal I be $I := \langle X, f \rangle$, and let a Gröbner basis for I be $GB(I) := \{f_1, \ldots, f_s\}$. As shown at the proof of Theorem 4,

$$GB(I) \cap k[t] = \{f(t)\}.$$

Therefore, we can assume $f_1 = f(t)$ and $\mathrm{LT}(f_i) = x^{\alpha_i}y^{\beta_i}t^{\gamma_i}$ $(2 \leq i \leq s, (\alpha_i, \beta_i, \gamma_i) \in \mathbb{Z}^3_{\geq 0}, (\alpha_i, \beta_i) \notin (0,0))$. By Theorem 4, since we can obtain the valid plaintext polynomial $m(t)$ by dividing the ciphertext $F(x,y,t)$ by $GB(I)$, we have:

$$F(x,y,t) = m(t) + f_1g_1 + f_2g_2 + \cdots + f_sg_s$$
$$(\mathrm{LT}(f_i) \nmid m(t), g_i \in k[x,y,t], 1 \leq {}^{\forall}i \leq s).$$

Moreover, we can obtain a univariate polynomial $n(t)$ by a normal form of F by $\{f, X\}$, and we have:

$$F(x,y,t) = n(t) + fh_1 + Xh_2 \ (h_1, h_2 \in k[x,y,t]).$$

Therefore, we compute difference of the both members, and we obtain: (Note that $f_1 = f(t)$)

$$n(t) - m(t) = f_1(g_1 - h_1) + f_2g_2 + \cdots + f_rg_r - Xh_2.$$

Table 4. IGRA.

p	d	l	**avg. [s]**	**memory [MB]**
17	20	160	0.152	11.78
17	50	400	0.572	15.02

Table 5. $p = 17$, $d = 5$, $l = 50$.

	GRA	**IGRA**
time [s]	521.350	0.010

Since $f_1(= f), f_2, \ldots, f_s, X \in I$, we obtain $n(t) - m(t) \in I \cap k[t]$ $(= \langle f(t) \rangle)$. Moreover, since $\deg m(t) < l \leq \deg f(t)$ and $\deg n(t) < \deg f(t)$, we obtain $f(t) \not| (n(t) - m(t))$. Therefore, we obtain:

$$n(t) - m(t) = 0 \Longleftrightarrow n(t) = m(t).$$

(QED)

By Theorem 5, we do not need to compute a Gröbner basis if $n(t) \in k[t]$, and we can find a plaintext m efficiently.

6. Implementation

In this section, we will show some experimental results about the GRA (Table 2) and the IGRA (Table 3). We used a system of Solaris10 with 2GHz CPU (AMD Opteron246), 4GB memory, and 160GB hard disk. Moreover, we used Magma [8](Ver. 2.16-4) as a software for writing the program.

(a) IGRA We describe the experimental results about the IGRA. For each (p, d, l), we generate 100 sets (X, f, s, r, m) randomly. See Table 4 for the results. We could efficiently find the valid plaintext m for larger size parameters. The above results of the IGRA could compute $m(t) \in k[t]$ at Step 5. Thus, we do not need to compute a Gröbner basis at Step 6. Here we note that, there exist some cases we need Step 6.

(b) GRA v.s. IGRA We compared with the GRA and the IGRA. As stated in the previous section, it takes many times to compute a Gröbner basis generally in the GRA. Actually, there exist some parameters, which take more than several hours to compute a Gröbner basis in the GRA. Now, we show some experimental results. See Table 5 for the results. In Table 5, for IGRA, the average running time is shown. Here, we generate randomly 100 sets (X, f, s, r, m) for $p = 17, d = 5, l = 60$. On the other hand, for GRA, the fastest running time in the experiments is only shown since its running time was too long, and we had to terminate the program before finished in most cases.

7. Conclusion

We proposed a generalized reduction attack against ASC04, and the flaw in Iwami's attack was fixed by our proposal. Also we showed some experimental results about our proposed attack. One of our future works is to evaluate the computational complexity of the generalized reduction attack according to [9] which is an attack against ASC09, where the ASC09 is an another implementation of the ASC [4, 10].

Acknowledgments

The authors would like to thank the reviewers for their valuable comments. This work was supported in part by Grant-in-Aid for Scientific Research (C)(20540125).

References

[1] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput., **26** (1997), 1484–1509.
[2] T. Okamoto, K. Tanaka and S. Uchiyama, Quantum Public Key Cryptosystems, in: Proc. of Crypto2000, LNCS 1880, pp. 147–165, Springer, 2000.
[3] K. Akiyama and Y. Goto, A Public-Key Cryptosystem using Algebraic Surfaces, in: Proc. of PQCrypto2006, pp. 119–138, 2006.
[4] K. Akiyama, Y. Goto and H. Miyake, An Algebraic Surface Cryptosystem, in: Proc. of PKC2009, LNCS 5443, pp. 425–442, Springer, 2009.
[5] S. Uchiyama and H. Tokunaga, On the Security of the Algebraic Surface Public-Key Cryptosystems (in Japanese), in: Proc. of SCIS2007, 2C1-2, 2007.
[6] P. Ivanov and J. F. Voloch, Breaking the Akiyama-Goto Cryptosystem, in: Proc. of AGCT11, Contemporary Math. 487, pp. 113–118, 2009.
[7] M. Iwami, A Reduction Attack on Algebraic Surface Public-Key Cryptosystems, in: Proc. of ASCM2007, LNCS 5081, pp. 323–332, Springer, 2008.
[8] Magma, `http://magma.maths.usyd.edu.au/magma/`.
[9] J-C. Faugère and P-J Spaenlehauer, Algebraic Cryptanalysis of the PKC'2009 Algebraic Surface Cryptosystem, in: Proc. of PKC2010, LNCS 6056, pp. 35–52, Springer, 2010.
[10] K. Akiyama and Y. Goto, An improvement of the algebraic surface public-key cryptosystem, in: Proc. of SCIS2008, 1F1-2, 2008.