Analysis of the errors in the recent attacks on DSA and ECDSA using lattice theory

Khúc Xuân Thành, Nguyễn Duy Anh, Nguyễn Bùi Cương

***Abstract*— Recently, in the attacks on DSA and ECDSA which based on the lattice have some new results that are published by Poulakis in [1, 2] and Draziotis in [3]. However, these papers still have some of the errors in the numerical computation examples, the definitions, and the feasibility of the attack. Namely, Poulakis [1] has an error in the numerical computation example. Draziotis [3] incorrectly defines polynomials that construct rows of matrices in the attack. Attack of Poulakis in 2016 [2] is less feasible and the numerical computation example on this paper is incorrect. We discussed with Poulakis and Draziotis about the above errors. They recognized these errors. The computationally verifiable results have made on the MAGMA Algebra Toolkit [4].**

***Tóm tắt*— Gần đây, trong các tấn công lên lược đồ chữ ký DSA và ECDSA dựa trên lý thuyết lưới đã có các kết quả mới được công bố của Poulakis trong [1, 2] và Draziotis trong [3]. Tuy vậy, trong các bài báo đó vẫn tồn tại một số sai sót trong tính toán bằng số, định nghĩa và tính khả thi của tấn công. Cụ thể, Poulakis năm 2011 [1] đã thực hiện nhầm ví dụ tính toán bằng số, Draziotis năm 2016 [3] định nghĩa chưa chính xác các đa thức xây dựng các hàng của ma trận trong tấn công. Tấn công Poulakis năm 2016 [2] là ít có tính khả thi và ví dụ tính toán bằng số mô tả tấn công trong bài báo này cũng được thực hiện chưa đúng. Các sai sót này đã được chúng tôi trao đổi lại với chính các tác giả của các bài báo trên và đã nhận được sự công nhận về những nhầm lẫn này. Các kết quả kiểm chứng tính toán đã được chúng tôi thực hiện trên bộ công cụ tính toán đại số MAGMA [4].**

Từ khóa— Tấn công DSA, ECDSA; Lưới; Thuật toán LLL.

Keywords— Attack on DSA, ECDSA; Lattice, LLL algorithm.

This manuscript is received on 1/7/2017. It is commented on 3/7/2017 and is accepted on 7/7/2017 by the first reviewer. It is commented on 17/8/2017 and is accepted on 30/8/2017 by the second reviewer.

I. INTRODUCTION

The lattice theory was studied about 100 years ago under the name "geometry of numbers", but its applications were actually developed since the lattice basis reduction algorithm was discovered by three mathematicians Arjen Lenstra, Hendrik Lenstra, László Lovász (LLL) [5]. The LLL algorithm is immediately considered one of the key algorithms in number theory when it points to a polynomial time algorithm for analyzing integer polynomials and solving simultaneous Diophantine equations. One of the first applications of the LLL algorithm in cryptography is to disrupt the Merkle-Hellman cryptosystem. In addition, the LLL algorithm is used to break other cryptosystems such as RSA [6, 7], DSA, ECDSA [8].

In the attacks on DSA and ECDSA based on the lattice theory, there are emerged a series of the papers [1], [2], [3]. These papers [1] and [2] show that if the long-term key a and the ephemeral key k of a signed message which satisfies $a, a^{-1}, k, k^{-1} < q^{1/3}$ or $a, a^{-1}, k, k^{-1} > q - q^{1/3}$ then they can easily be recovered. These results are different from the attack of Blake [14] that can recover the signature keys $a, k < q^{1/2}$ or $a, k > q - q^{1/2}$. Hence, the keys can be secure in the attack of Blake but it may be insecure in the attack of [1], [2] and vice versa.

However, [1], [2] and [3] still have some inaccuracies regarding the numerical computation example to description practical attacks the definition and the infeasibility of the attack. Therefore, in this paper, we analyze the details of these errors. The authors of the above papers agreed with us about these errors. Moreover, the verifiable results have made on the MAGMA Algebra toolkit.

The paper is organized as follows. In Section II, we recall DSA, ECDSA signature scheme, ideal to construct the attack on the signature

scheme based on lattice and some results in [1], [2] and [3]. Section III analyzes an error numerical computation example of [1]. Section IV analyzes the errors in [3] and introduce how to fix it. Section V analyzes the reason attacks of [2] are infeasible and error numerical computation example. The conclusion is presented in Section VI.

II. DSA, ECDSA SIGNATURE SCHEME

DSA and ECDSA [9] are known as two versions of the US signature schemes. In DSA, signer chooses two prime numbers p and $q \mid p-1$. The element g is a generator the order q subgroup G of $\mathbb{Z}_p^*$. The public parameter of the signer is (p,q,g,A), where $A = g^q \bmod q$ and $a \in_R \{1,\ldots,q-1\}$ is long-term key. To sign a message m that has the hash value $h(m) \in \{0,\ldots,q-1\}$, he chooses a random number $k \in \{1,\ldots,q-1\}$, which is the ephemeral key, and computes

$$r = (g^k \bmod p) \bmod q, \text{ and}$$

$$s = k^{-1}(h(m) + ar) \bmod q.$$

The signature of m is a pair (r,s). The signature is valid only if r,s is belong to $[1,q-1]$ and the below equation is hold:

$$r = (g^{s^{-1}h(m) \bmod q} A^{s^{-1}r \bmod q}) \bmod p \bmod q.$$

The ECDSA uses an elliptic curve E over $\mathbb{F}_p$ and a point $P \in E(\mathbb{F}_p)$ with a prime number q. The public parameter of signer is (p,E,P,q,Q), where $Q = aP$ and $a \in_R \{1,\ldots,q-1\}$ is long-term key. To sign a message m that has the hash value $h(m) \in \{0,\ldots,q-1\}$, he chooses a random number $k \in \{1,\ldots,q-1\}$ which is the ephemeral key and computes $kP = (x,y)$. Next, he computes:

$$r = x \bmod q \text{ and}$$

$$s = k^{-1}(h(m) + ar) \bmod q.$$

The signature of m is a pair (r,s). For the verification of the signature one computes. One check whether r,s is belong to $[1,q-1]$, compute:

$$u_1 = s^{-1}h(m) \bmod q,\ u_2 = s^{-1}r \bmod q,$$

$$u_1P + u_2Q = (x_0, y_0).$$

The signature is valid only if $r = x_0 \bmod q$.

The common feature of the attacks on DSA and ECDSA signature schemes is solving the equation $s = k^{-1}(h(m) + ar) \bmod q$ to find keys a,k. However, this is a hard problem. On the other hands, we have efficient methods to solve the equation in the integer ring. The question is "Can we transfer from solving the equation in the modulo q to do in $\mathbb{Z}$ and, if so, how to do?"

Fortunately, the Howgrave-Graham lemma [7] said that a such transfer is possible and gives the idea for this transfer.

Lemma 1. *(Howgrave-Graham) ([7], p. 4) Let* $h(x,y) = \sum_{i,j} h_{i,j} x^i y^j \in \mathbb{R}[x,y]$ *be a polynomial which is a sum of at most* n *monomials. A norm of polynomial* $h(x,y)$ *is* $\|h(x,y)\| = \sum_{i,j} h_{i,j}^2$. *Let* X,Y *be positive integers, and integer* x_0, y_0 *such that* $|x_0| < X, |y_0| < Y$. *If one of the below two cases is satisfied:*

1, $h(x_0,y_0) = 0 \bmod q$ *and* $\|h(xX,yY)\| < q/\sqrt{n}$,

2, $h(x_0,y_0) \in \mathbb{Z}$ *and* $\|h(xX,yY)\| < 1/\sqrt{n}$.

then $h(x_0,y_0) = 0$ *holds over the integer.*

Proof. See [7], p. 4-5.

In particular, we need to find polynomials that accepts keys $\overline{a}, \overline{k}$ (or $\overline{k^{-1}}$) as the solutions (with $a \in [1,\ldots,q], \overline{a} = a$ if $a > q/2$, otherwise $\overline{a} = a - q$). In addition, these polynomials must have coefficients small enough such that its standard too. Hence, if the polynomial satisfies one of the two cases of Lemma 1 then it accepts a,k (or k^{-1}) as the solution over the integer.

In [1], Poulakis finds a conic equation $B + Cy + Dxy = 0,\ (B,C,D \in \mathbb{Z})$ that has $\overline{a}, \overline{k^{-1}}$ as the solutions. Poulakis presents a method to solve such conic equation based on assumption the factorization of B is known.

Finally, Poulakis show that if there are integers $X > 0$ and $Y > 0$ satisfying $\overline{a} < X, \overline{k^{-1}} < Y$ and $XY^2 < q/6^{3/2}$ then there is a deterministic algorithm which computes a and k.

The attack of Draziotis [3] is an improvement of [1] by increasing the dimension of the lattice. However, the increasing dimensions of the lattice break the form of the conic equation. Hence, we need one more polynomial that has $\overline{a}, \overline{k^{-1}}$ solutions to constructing the system equation which has two variables. Draziotis if there are integers $X > 0$ and $Y > 0$ satisfying $\overline{a} < X, \overline{k^{-1}} < Y$ and $X^{1,26}Y^2 < 0,262 \cdot q^{1,157}$ then there is a deterministic algorithm which computes a and k.

Poulakis [2] is a different approach to the two above attacks. In particular, instead of using Lemma 1 and the lattice reduction algorithm, [2] builds a special lattice that every nonzero vector has a lower bound. Later, the author finds a long-term key a based on solving the shortest vector problem in the lattice. However, this attack is not feasible in practice. These issues are analyzed in Section 5 in this paper.

III. ATTACK BY POULAKIS 2011

In [1] Section 5, page 355, Poulakis performs a numerical computation example that describes the finding of a long-term key a on the ECDSA signature scheme. Specifically, he presents the following: (the italic words are quoted from the paper of Poulakis).

We consider the elliptic curve given in [10, Example 3, p. 182]. We have the prime

$$p = 2^{160} + 7$$

and the elliptic curve E defined over $\mathbb{F}_p$ by the equation:

$y^2 = x^3 + 10x + 1230929586093851880935//$
$564157041535079194.$

The number of points of $E(\mathbb{F}_p)$ is:

$q = 1461501637330902918203683 51//$
$8218126812711137002561.$

The problem that we want to mention in this example is that prime q is incorrect. Indeed, through verifiability on the MAGMA, the number of points of this curve is

$q = 1461501637330902918203686 25//$
$1257451235345756695486.$

Since p is incorrect, the signature (r, s) that [1] computes later is also wrong. Returning to the document [10], we found that the [1] mistakenly referred to the elliptic curve of Example 2, p. 182 in [10].

As such, the curve is accurate to take the number of points

$q = 1461501637330902918203683 5182//$
$18126812711137002561.$

that is

$y^2 = x^3 + 10x + 1343632762150092499701 63//$
$7438970764818528075565078.$

Therefore, the section 5 in [1] has been incorrectly computed. We have asked Poulakis about this problem. In response email, he has recognized that choosing wrong parameters of the elliptic curve E is a typo.

IV. ATTACK BY DRAZIOTIS 2016

In [3], Draziotis offers a lighter condition for the attack recovering the long-term key. However, Draziotis incorrectly defined the polynomials for constructing the row vectors of the matrix that made up the lattice. Although, later in the proof, he still constructed the correct matrix. To analysis this error, we recall the definitions that are used in [3].

Let $f(x, y) \in \mathbb{R}[x, y]$ and m, t be some positive integer. We define $g_{i,k}(x, y) = x^i f(x, y)^k$ ($k = 0,1,\ldots,m$, $i = 0,1,\ldots,m-k$) is x-shift polynomials of $f(x, y)$ and $h_{j,k}(x, y) = y^j f(x, y)^k$, ($k = 0,\ldots,m$, $j = 0,\ldots,t$) is y-shift polynomials of $f(x, y)$. Next, Draziotis constructs a matrix M_m as the following ([3], p. 543):

Lemma 2.4. *[3]. Let* $f(x, y) = q^{-1}(x(y + A) + B)$ *and the vector* $\mathbf{b}_{i,k} = (g_{i,k}X^iY^k)_{i,k}$, $k = 0,1,\ldots,m$, $i = 0,1,\ldots,m-k$, *for some* $m \in \mathbb{Z}_{\geq 0}$ *and* $g_{i,k}$

the coefficients of the x-shift polynomial of $f(x,y)$. Let the matrix $M_m = (\mathbf{b}_{i,k})_{i,k}$.

Then

$$\det M_m = q^{-\alpha(m)} X^{2\alpha(m)} Y^{\alpha(m)},$$

where $\alpha(m) = m(m+1)(m+2)/6$.

Proof: M_m is the matrix

$$\begin{array}{c} \\ 1 \\ x \\ f \\ x^2 \\ \vdots \\ f^m \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & x & xy & x^2 & \dots & x^m y^m \end{array} \\ \begin{pmatrix} 1 & & & & & \\ & X & & & & \\ q^{-1}B & qAX^{-1} & q^{-1}XY & & & \\ & & & X^2 & & \\ \vdots & \vdots & \vdots & \vdots & \ddots & \\ * & * & * & * & * & q^{-m}X^mY^m \end{pmatrix} \end{array}$$

The dimension of M_m is $(m+1)(m+2)/2$. Since

$$\begin{aligned} &\#\ (i,k) : k = 0,1,\dots,m,\ j = 0,1,\dots,m-k \\ &= (m+1) + m + \dots + 1 \end{aligned}$$

Also M_n is lower triangular

$$\det M_m = \prod_{k=0}^{m} \prod_{i=0}^{m-k} q^{-k} X^{k+i} Y^k.$$

.

We can easily see that the matrix M_m in the proof of lemma differs from the matrix which is stated in Lemma 2.4. Indeed, considering the third row of the matrix M_m $(k=0, i=1)$ as defined in Lemma 2.4, we have

$$\begin{aligned} g_{0,1}X^0Y^1 = fY &= q^{-1}(x(y+A)+B)Y \\ &= Bq^{-1}Y + Aq^{-1}Yx + q^{-1}Yxy \end{aligned}$$

Then, the vector $(q^{-1}BY, q^{-1}AY, q^{-1}Y, 0, \dots, 0)$ is the third row of M_m. This row is different from the third row of matrix M_m in the proof of Lemma 2.4. Hence, the determinant of M is different from that of Lemma 2.4.

Through the review of the article [7] which is referred by Draziotis. We find that the matrix in the proof of the Lemma 2.4 is correct, but M_m as defined in lemma is inaccurate. Moreover, we make an edit of this lemma as follows:

Let $f(x,y) = q^{-1}x(y+A)+B$. Let the matrix $M_m = (\mathbf{b}_{i,k})_{i,k}$, where $\mathbf{b}_{i,k}$ is the coefficients of polynomials $g_{i,k}(xX, yY) = (xX)^i f(xX, yY)^k$ $k = 0,1,\dots,m$, $i = 0,1,\dots,m-k$ for some positive integer m. Then

$\det M_m = q^{-\alpha(m)} X^{2\alpha(m)} Y^{\alpha(m)}$, where $\alpha(m) = m(m+1)(m+2)/6$.

According to the new statement, we have the matrix M_m similar to the matrix in the proof. Indeed, for $k=1, i=0$, we have:

$$\begin{aligned} g_{0,1}(xX, yY) &= (xX)^0 f(xX, yY)^1 \\ &= q^{-1}(xX(yY + A) + B) \\ &= q^{-1}B + q^{-1}AXx + q^{-1}XYxy. \end{aligned}$$

Hence, the third row of the matrix M_m is $(q^{-1}B, q^{-1}AX, q^{-1}XY, 0, \dots, 0)$.

Draziotis [3] also makes the same mistake in the lemma below ([3], p. 543):

Lemma 2.5 [3] *Let $f(x,y) = q^{-1}(x(y+A)+B)$, and $\mathbf{c}_{j,k} = (h_{j,k}X^jY^k)_{i,k}$, $k = 0,1,\dots,m$ $j = 0,1,\dots,t$ for some $m, t \in \mathbb{Z}_{\geq 0}$ and $h_{j,k}$ the coefficients of y-shift polynomials of $f(x,y)$. Let $R_{t,m} = (\mathbf{c}_{j,k})_{j,k}$ and $\hat{R}_{t,m}$ be the right block of $R_{t,m}$ of dimension $(m+1)t$. Then*

$$\det \hat{R}_{t,m} = q^{-t\beta(m)} X^{t\beta(m)} Y^{t(m+1)(m+t+1)/2},$$

where $\beta(m) = (m+1)m/2$.

Based on [7], we are modified Lemma 2.5 as the following:

Let $f(x,y) = q^{-1}(x(y+A)+B)$, and $R_{t,m} = (\mathbf{c}_{j,k})_{j,k}$, where $\mathbf{c}_{j,k}$ is the coefficients of polynomials $h_{j,k}(xX, yY) = (yX)^j f(xX, yY)^k$, $k = 0,1,\dots,m$, $j = 0,1,\dots,t$ for some $m, t \in \mathbb{Z}_{\geq 0}$ Let $\hat{R}_{t,m}$ be the right block of $R_{t,m}$ dimension $(m+1)t$. Then

$$\det \hat{R}_{t,m} = q^{-t\beta(m)} X^{t\beta(m)} Y^{t(m+1)(m+t+1)/2},$$

where $\beta(m) = (m+1)m/2$.

We also asked Draziotis about the incorrect definition of these matrix $M_m, R_{t,m}$. In response email, he has agreed with our remark and has updated his paper in [11].

V. ATTACK BY POULAKIS 2016

In [2], Poulakis presents a new method of attacking the signature scheme based on the shortest vector problem in the lattice. He offers an attack scenario that finds a long-term key a without having to rely on ephemeral key k. However, the ability to find the case for successful attack succeeds is difficult. Therefore, this attack is less feasible.

Attack of Poulakis 2016

Input: The known values $(m_j, r_j, s_j)(j = 1,\ldots,t)$.

Output: The long-term key a.

Step 1: Compute $C_j = -r_j s_j^{-1} \bmod q$ and $D_j = -s_j^{-1} h(m_j) \bmod q$.

Step 2: Select integers $A_i (i = 1,\ldots,n)$ with $2^{i-1} q^{i/(n+1)} < A_i < 2^i q^{i/(n+1)}$.

Step 3: Compute $B_{ij} = A_i D_j C_j^{-1} \bmod q$ $(i = 1,\ldots,n, j = 1,\ldots,t)$

Step 4: Denote by M the set of map

$$\mu : \{1,\ldots,n\} \to \{1,\ldots,t\}.$$

For every $\mu \in M$, the vector

$$\mathbf{v}_\mu = (x_\mu, y_{1\mu(1)}, \ldots, y_{n\mu(n)})$$

is the solution of congruence equation

$$y_i + A_i x + B_{i,\mu(i)} = 0 \bmod q \quad (i = 1,\ldots,n)$$

Step 5: If $\|\mathbf{v}_\mu\| < q^{n/(n+1)}/16$ then set $a = x_\mu$, where $\|\mathbf{v}_\mu\|$ is Euclidean norm of $\mathbf{v}_\mu$.

For the remainder of this paper, we present the reason why it is difficult to find cases of successful execution of the attack and wrong numerical computation example in [2]. First, we recall the main idea of this attack.

Let n be a positive integer, $n \le \log\log q - 1$. Suppose that we have $t \le n$ signed messages $m_j (j = 1,\ldots,t)$. The pair (r_j, s_j) is respectively signatures of messages m_j, where $r_j = x(k_j P) \bmod q$ in ECDSA signature scheme or $r_j = (g^{k_j} \bmod p) \bmod q$ in DSA signature scheme, $k_j \in_R \{1,\ldots,q-1\}$ and $s_j = k_j^{-1}(h(m_j) + a r_j) \bmod q$

In [2], a condition is required to successfully execute the attack that can recover the long-term key a ([2], p. 140).

Proposition 4.1. [2] *Put* $k_{ij} = k_j A_i C_j^{-1} \bmod q$ $(i = 1,\ldots,n, j = 1,\ldots,t)$. *Suppose there is* $\mu \in M$ *such that*

$$\left\|(a, k_{1\mu(1)}, \ldots, k_{n\mu(n)})\right\| < \frac{q^{n/(n+1)}}{16}, \qquad (1)$$

then the algorithm Attack of Poulakis 2016 compute a

Proposition 4.1 is based on a strong assumption that there are existence $\mu \in M$ is satisfied (1). The question is: "how to find such a mapping μ?

We can see that the left of inequality (1) depending on the values A_i since k_j, C_j^{-1} is fixed. Hence, we must find $A_i \in 2^{i-1} q^{i/(n+1)}, 2^i q^{i/(n+1)}$ for $i = 1,\ldots,n$ to satisfy (1). This is very hard problem. For example, consider ECDSA signature scheme with $q = 160$ bit. Suppose we have $n = 3$ signed messages. Then, in order to perform the attack, one must select the values $A_1 \in (2^{40}, 2^{41})$, $A_2 \in (2^{81}, 2^{82})$ and $A_3 \in (2^{122}, 2^{123})$ at the same time such that

$$\left\|a, k_{1\mu(1)}, k_{2\mu(2)}, k_{3\mu(3)}\right\| < \frac{2^{120}}{16}. \qquad (2)$$

Since A_1, A_2, A_3 belong to the too big interval, it is very difficult to choose the values A_i to satisfying (2). In particular, we have tested exhaust to find the value A_1, A_2, A_3 on MAGMA Software installed on Core i7-3.4 GHz computer

within 7 days but still have not found satisfactory value.

In this regard, we have discussed with Poulakis. In response email, he also recognized that choosing A_i to satisfy equation (1) is hard. In addition, he "believed" that one can choose such A_i values at any one time. However, how long it takes to get A_i so he has not answered yet.

In addition to the uncertainty above, Poulakis made the mistake of performing numerical calculations to describe the attack. Specifically, in [2] page 142 performs an attack on ECDSA with the curve parameters and calculated as follows: the italic words are quoted from the paper of Poulakis [2].

We consider the elliptic curve E give in [10, p.182, Example 3] defined over the finite field $\mathbb{F}_p$, where $p = 2^{160} + 7$ is a prime by the equation

$y^2 = x^3 + 10x + 1343632762150092499701637 4//$
$3897076481852807556507 8.$

The number of points of $E(\mathbb{F}_p)$ is the 160-bit prime is:

$q = 1461501637330902918203683 51//$
8218126812711137002561

Consider the point $P = (x_P, y_P)$ of $E(\mathbb{F}_p)$ order q, where:

$x_P = 8587134810530702787791 68//$
$0329206136803600475352 71$
$y_P = 3649383213503922650381 82//$
$0515032797267482241840 66$

We take a long-term key the 160-bit integer

$a = 8749846680322117333113 868//$
$4130667374933323658617 8.$

The public key is $Q = (x_Q, y_Q)$ where:

$x_Q = 5971622468928720560343 153//$
$3045295063632474169153 6$

$y_Q = 1181877329208353060566 9692//$
$6675892475754968435739 0$

Let m_1, m_2, m_3 be three messages with hash values:

$h(m_1) = 1238458437157734227527 8//$
$2500471850527123502491 6418$
$h(m_2) = 1028653949698644928576 6//$
$3757255096126671808621 3222$
$h(m_3) = 1359253753908721564345 0//$
$8691938914544947951071 3328$

Suppose that the following ephemeral keys k_1, k_2, k_3 have been used respectively for the generation of the signatures of the three messages:

$k_1 = 4660805433228896888835467 11//$
$5835518398826523750031,$

$k_2 = 7307508186654514591018424 1//$
$6358141509827966271589,$

$k_3 = 7307508186654514591018424 1//$
$6358141509827966279681.$

We have the points:

$R_i = k_i P = (x(R_i), y(R_i))$

$x(R_1) = 1254157729089443995418 1//$
$2383252380827703131394 962,$

$y(R_1) = 2310994211717652956752 55//$
$1725361664908710994104 0,$

$x(R_2) = 7251443779102468855346 16//$
$7067566994041955076632 31$

The signature of m_i is (r_i, s_i), where $s_i = k_i^{-1}(h(m_i) + ar_i) \bmod q$ and $r_i = x(R_i) \bmod q$

$s_1 = 1363805341335356352807 6508//$
$2369015455265391445111 9,$

$s_2 = 1286644068312084224467 9891//$
$9343676926547176728457 1$

$s_3 = 1357235540051781293143 7202//$
$3275275184067724775409 0.$

By re-computation, we see that the signature s_2, s_3 is incorrect. The exact values of s_2, s_3 must be:

$s_2 = 7598778819913345317823 3407//$
$4560701681542665509 15$

$s_3 = 7873335166031067195461 5951//$
3684578275599629418244

Since s_2, s_3 are wrong, the values $C_i, D_i (i = 2,3)$ in [2] are also incorrect. Besides, we tried to recalculation $C_i, D_i (i = 2,3)$ with the wrong values of s_2, s_3 in [2], we can not find $C_i, D_i (i = 2,3)$ the same as in [2]. Moreover, Poulakis chooses $A_1 = D_1 = 34359738369$ but this value does not belong the interval $[q^{1/4}, 2q^{1/2}]$. About these problem, we also dicused with Poulakis. In response email, explain the wrong s_2, s_3, D_2, D_3, Poulakis attributed to the printing error. Also, when asked why the A_1 was not in the range $q^{1/4} < A_1 < 2q^{1/2}$ Poulakis said that it was possible to re-select $A_1 = q^{1/4} + 1$. However, when checking condition (1), this value is also not satisfied.

VI. CONCLUSION

In this paper, we have analyzed some of the error in [1], [2], [3] attacking on the DSA and ECDSA signature schemes based on the lattice theory. In particular, the errors of choosing the elliptic domain parameter in Poulakis [1] can arise from the typo. We corrected the incorrectly defines polynomials that construct rows of matrices in Draziotis 2016 [3]. Based on the experimental verification of the attacks as well as the author's responses, we see that the attacks in [1], [3] actually serious when the signature keys can easily be recovered if it satisfies the certain condition. Therefore, we need to be more cautious in choosing the long-term key and the ephemeral in DSA and ECDSA to avoid such attacks. In Poulakis [2], since the attack based on a very strict assumption, this attack is infeasible. Moreover, the errors in the numerical computation example and the unclear response of Poulakis about choosing A_i make us strongly believe that the attack is not available.

REFERENCES

[1] D. Poulakis, "Some lattice attacks on DSA and ECDSA," Applicable Algebra in Engineering, Communication, and Computing, vol. 22, no. 5, pp. 347-358, 2011.

[2] D. Poulakis, "New lattice attacks on DSA schemes," Journal of Mathematical Cryptology, vol. 10, no. 2, pp. 135-144, 2016.

[3] K. A. Draziotis, "DSA lattice attacks based on Coppersmith's method," Information Processing Letters, vol. 116, no. 8, pp. 541-545, 2016.

[4] J. Cannon, W. Bosma, C. Fieker, and A. Steel, "Handbook of MAGMA functions," Edition, vol. 2, 2006.

[5] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," Mathematische Annalen, vol. 261, no. 4, pp. 515-534, 1982.

[6] A. May, "Using LLL-reduction for solving RSA and factorization problems," in The LLL algorithm: Springer, pp. 315-348, 2009.

[7] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than N/sup 0.292," IEEE transactions on Information Theory, vol. 46, no. 4, pp. 1339-1349, 2000.

[8] I. F. Blake and T. Garefalakis, "On the security of the digital signature algorithm," Designs, Codes and Cryptography, vol. 26, no. 1, pp. 87-96, 2002.

[9] P. Gallagher, "Digital signature standard (DSS)," Federal Information Processing Standards Publications, volume FIPS, pp. 186-3, 2013.

[10] I. F. Blake, G. Seroussi, and N. Smart, Elliptic curves in cryptography. Cambridge university press, 1999.

[11] K. Draziotis. (2017). DSA lattice attacks based on Coppersmith's method. Available: http://users.auth.gr/drazioti/extension_of_poulakis_11_elsevier.pdf

AUTHORS PROFILE

B.S. Khúc Xuân Thành

Workplace: Institute of Cryptography Science and Technology.

Email: khucxuanthanh@gmail.com

The education process: has received a mathematical bachelor degree in Ha Noi University of Science, in 2013.

Research today: Public-key cryptography, Lattice-based cryptography.

B.S. Nguyễn Duy Anh

Email: duyanhural567@gmail.com

The education process: has received a computer science bachelor degree in Ha Noi University of Science, in 2017.

Research today: Cryptography, Computer science

M.Sc. Nguyễn Bùi Cương

Workplace: Institute of Cryptography Science and Technology.

Email: nguyenbuicuong@gmail.com

The education process: has received a mathematical bachelor degree in Ha Noi National Universiy of Education, in 2004, and has received a mathematical master degree in Ha Noi University of Science, in 2008.

Research today: Secret-key cryptography.

Thư mời viết bài cho Chuyên san "Nghiên cứu khoa học và công nghệ trong lĩnh vực an toàn thông tin" số 06 (02.2017)

Kính gửi quý độc giả, các nhà nghiên cứu, nhà quản lý, cán bộ, giảng viên của các cơ sở đào tạo và các Viện nghiên cứu trong lĩnh vực An toàn thông tin.

Đến nay, 5 kỳ Chuyên san Nghiên cứu khoa học và công nghệ trong lĩnh vực An toàn thông tin của Tạp chí An toàn thông tin, Ban Cơ yếu Chính phủ đã được xuất bản. Ban biên tập Chuyên san trân trọng cám ơn các nhà khoa học đã gửi bài và tham gia nhận xét, đánh giá bài báo, cám ơn các quý độc giả đã đóng góp những ý kiến quý báu cho Chuyên san trong thời gian qua.

Theo Kế hoạch, Chuyên san số 06 (02.2017) của Tạp chí An toàn thông tin dự kiến sẽ được xuất bản vào tháng 12/2017. Tạp chí trân trọng kính mời các nhà nghiên cứu, giảng viên của các cơ sở đào tạo và các Viện nghiên cứu trong lĩnh vực An toàn thông tin gửi bài báo khoa học cho Chuyên san số 06. Bài viết gửi đăng trên Chuyên san xin vui lòng gửi trước ngày 15/11/2017.

Các bài báo khoa học cần được soạn thảo bằng phần mềm MS.Word hoặc Latex theo mẫu định dạng của Tạp chí (được cung cấp tại trang web www.antoanthongtin.vn, hoặc liên hệ để nhận bản mẫu qua email thukychuyensan@bcy.gov.vn). Bài viết sẽ được gửi đến các nhà khoa học đúng chuyên ngành đánh giá, phản biện theo đúng quy trình công bố công trình khoa học của Hội đồng Chức danh Giáo sư nhà nước. Tác giả có bài báo được đăng sẽ được nhận nhuận bút theo quy định của Tạp chí cùng 01 cuốn Chuyên san số có bài viết và bản mềm (PDF) của các số khác nếu có nhu cầu.

Các bài báo sau khi được xuất bản sẽ được giới thiệu tóm tắt trên trang web của Tạp chí An toàn thông tin (www.antoanthongtin.vn) và sau 3 tháng sẽ cho phép độc giả tải toàn bộ nội dung bài báo để phục vụ công tác đào tạo và nghiên cứu.

Các bài viết đã đăng trong Chuyên san là các công trình nghiên cứu khoa học, ứng dụng công nghệ mới, các thành tựu khoa học, kỹ thuật mới về lĩnh vực bảo mật và an toàn thông tin, chưa gửi đăng trên bất kỳ tạp chí hoặc kỷ yếu hội nghị nào.

Mọi thông tin chi tiết vui lòng liên hệ:

Tạp chí An toàn thông tin - Chuyên san khoa học

Địa chỉ: 105 Nguyễn Chí Thanh, Đống Đa, Hà Nội

Thư ký hành chính: Hoàng Nhật Minh , Di động: 0916.811.488

Trần Ngọc Mai, Di động: 0989.455.838

E-mail: thukychuyensan@bcy.gov.vn