情報保護學會論文誌
第14券 第1號, 2004. 2

Goldreich-Goldwasser-Halevi 전자서명의 선택 평문 공격*

양 대 헌†
인하대학교

Chosen Message Attack Against Goldreich-Goldwasser-Halevi's Lattice Based Signature Scheme

DaeHun Nyang†
Inha Univ.

요 약

이 논문에서는 Crypto97에 발표된 잘 알려진 lattice 문제에 기반한 Goldreich-Goldwasser-Halevi(GGH)의 전자 서명을 암호해독한다. GGH의 서명방법에 선택 평문공격을 수행하고 제안하는 공격방법에 취약함을 보인다. 암호해독 방법에서는 서로 선형 독립적인 n개의 lattice 점을 모아서 원래 lattice의 sub-lattice를 생성하는 새로운 basis를 생성한다. 이 sub-lattice가 유효한 서명을 생성하는데 사용될 수 있음을 보인다. 이 공격방법의 유효성을 실험을 통해서 보이고, 마지막으로 비밀키를 생성하는데 사용되는 cube-like parameter가 안전성에 좋지 않은 영향을 미침을 보인다.

Abstract

The Goldreich-Goldwasser-Halevi(GGH)'s signature scheme from Crypto '97 is cryptanalyzed, which is based on the well-known lattice problem. We mount a chosen message attack on the signature scheme, and show the signature scheme is vulnerable to the attack. We collects n lattice points that are linearly independent each other, and constructs a new basis that generates a sub-lattice of the original lattice. The sub-lattice is shown to be sufficient to generate a valid signature. Empirical results are presented to show the effectiveness of the attack. Finally, we show that the cube-like parameter used for the private-key generation is harmful to the security of the scheme.

Keywords: *Public-key cryptography, Lattice, Closest Vector Problem, GGH's Cryptosystem, Chosen message attack*

I. Introduction

Recent researches have found that Closest Vector Problem(CVP) and Shortest Vector Problem(SVP) may be useful in the public-key cryptography. The CVP was shown by van Emde Boas to be NP-hard in 1981.[7] In 1996, Ajtai introduced a function that is provably one-way if approximating the shortest non-zero vector(SVP) in a lattice is hard in the worst case, and invented a public-key cryptosystem using the lattice problem.[1,2]

Being motivated by Ajtai's work, Gold-

접수일: 2003년 9월 24일; 채택일: 2003년 12월 24일
* The author would like to acknowledge the comment of S. Halevi.
† nyang@inha.ac.kr

reich, Goldwasser, and Halevi proposed a public-key cryptosystem using lattice reduction problems.[4] Their cryptosystem shed light on the possibility of new cryptosystems based neither on the factorization nor on the discrete logarithm problems. Even better, their cryptosystem is superior to existing schemes in that it encrypts a message and writes a signature in $O(n^2)$ operations, while RSA encrypts a message in $O(n^3)$ operations for security parameter n, at the expense of key sizes. The speed gain obtained by long key sizes looks quite attractive for the upcoming high speed network environments such as ATM(Asynchronous Transfer Mode). Also, it has a novel property that it can process an analogue signal. In [6], their encryption scheme was attacked and P. Nguyen showed that it would be dangerous to use a dimension less than 400 even though we fix the flow, which limits our interests in the encryption scheme. P. Nguyen's attack depends on two weaknesses: one is that the error vectors are always quite shorter than the vectors in the lattice, and the other is the regular form of the error vectors. These two weaknesses do not appear in GGH's signature scheme. Thus, their signature scheme still works well. As far as we know, there has not been any published challenge on GGH's signature scheme.

In this paper, we cryptanalyze the GGH's public-key signature scheme, of which security depends on the approximability of the close lattice point within a bound. A key observation of the cryptanalysis is that for a message which consists of small elements, a signing oracle returns as a signature a lattice point whose Euclidean length is short. Properly collected n lattice points with a signing oracle may be used as a new basis for the lattice. Unfortunately, randomly collected n lattice points do not make the same lattice as that generated from the public or private basis, but they are likely to generate a sparser lattice than the original one. The second observation is that we do not have to use the same lattice as the lattice generated from the public or private-key to write a valid signature. That is, we can make use of the *sub-lattice* as a private-key. Especially, we show that in case of a private basis with non-zero cube-like parameter, the original private basis can be completely restored(The cube-like parameter represents how cube-like a private basis is. A private basis is generated as $R = k \cdot I + rand(\pm l)$, where k is the cube-like parameter.).

Set of real numbers and set of integers are denoted by R and Z, respectively in this paper. We denote real numbers by small Greek letters and integers by lowercase letters such as $i, j, k, \ldots$. Column vectors are denoted by bold-face lowercase (e.g. $\mathbf{b}$, $\mathbf{c}$, $\mathbf{e}$ etc.), and matrices are denoted by capital letters (e.g. B, H, R, etc.), all of which are $n \times n$ matrices.

II. Brief Survey of GGH's Public-key Cryptosystem

GGH's cryptosystem encrypts a message by encoding it into $\mathbf{u} \in L$ and adding a small noise to $\mathbf{u}$, where L is the carefully selected lattice. Decryption is the process to eliminate the added noise from the lattice point and decode the result. Before we summarize the GGH's cryptosystem, let's define the lattice.

Definition 1. *Lattice* Given a set of n linearly independent column vectors in R^n, $B = \{\mathbf{b}_1, \ldots \mathbf{b}_n\}$, we define the lattice spanned by the basis B as the set of all linear

combinations of the $\mathbf{b}_i$'s with integral coefficients, namely

$$L(B)=\{\sum_i k_i\mathbf{b}_i : k_i \in Z \text{ for all } i\}$$

One of the important facts about lattice is that all the bases of a given lattice have the same determinant.

Definition 2. *Orthogonality Defect* Let B be a non-singular $n\times n$ matrix. Then the orthogonality defect of B is defined as

$$\text{orth-defect}(B)=\frac{\prod_i \|\mathbf{b}_i\|}{det(B)},$$

where $\|\mathbf{b}_i\|$ is the Euclidean norm of the i'th column in B.

Definition 3. *Dual Orthogonality Defect* Let B be a non-singular $n\times n$ matrix. Then the dual orthogonality defect of B is defined as

$$\text{orth-defect}^*(B)=\frac{\prod_i \|\mathbf{b}_i\|}{det(B^{-1})}=\det(B)\cdot\prod_i \|\mathbf{b}_i\|,$$

where $\|\mathbf{b}_i\|$ is the Euclidean norm of the i'th row in B^{-1}.

The dual orthogonality defect plays a crucial role in the security of GGH's cryptosystem.

GGH's cryptosystem uses two bases B and R of the same full rank lattice in Z^n, and a positive real number σ. Here, B has a high dual orthogonality defect, whereas R has a low dual orthogonality defect. (B, σ) is the public-key, and R plays a role as the private-key in their settings. Refer to [4] how (B, R, σ) are generated.

The ciphertext corresponding to an encoded plaintext v is obtained by computing $c=Bv+e$, where $\mathbf{e}$ is a randomly chosen vector from R^n whose each entry has zero-mean and variance σ^2. Deciphering is performed by evaluating $T\lfloor R^{-1}\mathbf{c}\rceil$, where $T=B^{-1}R$ is a unimodular matrix.

They also provided a public-key digital signature scheme. Their scheme signs a vector $\mathbf{u}$ in R^n by finding a lattice point $\mathbf{v}$ that is sufficiently close to the vector. The lattice point is represented as a linear combination of the columns of B, and the verifier can verify the signature by comparing τ and the distance between the message vector and the vector $\mathbf{v}$.

To sign a message s, we encode the message into $\mathbf{u}\in R^n$ by an encoding function $Enc(s)=\mathbf{u}$. Now, a lattice point near $\mathbf{u}$ is easily found by computing $v = T\lfloor R^{-1}\mathbf{u}\rceil$, where $(T=B^{-1}R,\ R^{-1})$is a private-key. A signature is verified by computing Euclidean distance of $B\mathbf{v}-\mathbf{u}$ and comparing it with τ. If the distance is shorter than τ, the signature is regarded valid, otherwise not. τ must be carefully determined, since it takes greatly effect both on the security of the signature scheme and on the verification error probability.

Ⅲ. Cryptanalysis of GGH's Signature Scheme

3.1 Idea: Sub-lattice Attack

We begin with the simple fact that a GGH's signing oracle returns a sufficiently close lattice vector for a given random vector $\mathbf{u}\in R^n$. For a vector $\mathbf{u}\in R^n$ whose element ranges from $-k$ to k, the signing oracle gives a signature, or a lattice point of which Euclidean distance from $\mathbf{u}$ is smaller than the public value τ. In this setting, we mount the chosen message attack against the signature scheme by providing many short messages and collecting the results. The collected signatures can be used to construct a new private basis,

even though they are likely to generate a different lattice from the lattice generated from the original public-key or the private -key. More exactly, they have large probability to make a sub-lattice of the original lattice. Even though the newly constructed basis spans only a subset of the original lattice, we can still utilize it as a private-key. Using the new basis, we can write a valid signature for an arbitrary message. Define the "error vector"

$$\mathbf{e}=\lceil H^{-1}\mathbf{u}\rfloor-H^{-1}\mathbf{u},$$

and, $Round_H(\mathbf{u})=H\lceil H^{-1}\mathbf{u}\rfloor$, where H is an $n\times n$ basis of a lattice. Then the distance between $\mathbf{u}$ and $Round_H(\mathbf{u})$ is $\|H\mathbf{e}\|$, the Euclidean norm of the vector $H\mathbf{e}$. Clearly, the i'th entry ε_i in $\mathbf{e}$ is less than or equal to 1/2 for all i, because of the rounding-off. Thus, we would prefer to the sub-lattice whose elements are small enough to make $\|H\mathbf{e}\|$ smaller than τ. The effort to find another basis H can be taken by gathering many short signatures. Intuitively, submitting a short random vector $\mathbf{u}$ to a signing oracle gives us a short lattice point.

Now, the problem how short the vector must be is solved. Given a message $\mathbf{u}$, a signing oracle returns $\mathbf{v}=B^{-1}R\lceil R^{-1}\mathbf{u}\rfloor$, and the cryptanalysist can collect many signatures $B\mathbf{v}=R\lceil R^{-1}\mathbf{u}\rfloor$. Note that if $\mathbf{u}$ is carefully selected, the vector $\mathbf{d}=\lceil R^{-1}\mathbf{u}\rfloor$ will consist of almost 0's except one or a few ±1's. Then, the signature of the $\mathbf{u}$ is either exactly one of the columns of R or a sum of a few columns of R, the private basis. From now on, *sum of several vectors* $\mathbf{r}_i$ means

$$\sum_{i=1}^{n} c_i\times\mathbf{r}_i,\ \text{where } c_i\in\{0,\pm1\},$$

where ε/n portions of c_i's are ±1 for a small constant ε.

With n signatures collected in this way, we can construct a new basis, though the basis is likely to generate the sub-lattice of $L(R)$ rather than $L(R)$ itself.

To make $\mathbf{d}=\lceil R^{-1}\mathbf{u}\rfloor$ have almost 0's and only a few of ±1's, we must constrain the range of elements of $\mathbf{u}$. We use the Hoeffding bound. Let's denote the i'th entry in $\mathbf{d}$ and $\mathbf{u}$ by δ_i and μ_i respectively. Also, we denote the i,j 'th element in R^{-1} by ρ_{ij}, and the maximum L_∞ norm of the rows in R^{-1} by $\Upsilon/\sqrt{n}$, where Υ will be roughly estimated by any randomly generated basis with the maximum entry size of R and its cube-like parameter.

$$Pr(|\delta_i|>1/2)<2exp(-\frac{1/4}{2n(k\Upsilon/\sqrt{n})^2})=\varepsilon/n \quad (1)$$

where $\delta_i=\sum_j\rho_{ij}\mu_i$ and $|\mu_i|\le k$.

$$Pr(|\delta_i|>3/2)<2exp(-\frac{9/4}{2n(k\Upsilon/\sqrt{n})^2})=\beta, \quad (2)$$

where β is set to a very small value such as 10^{-10}.

If we limit k such that it satisfies equation (1) and (2), δ_i will be composed of almost 0's and ε number of ±1's, and entries whose absolute values are greater than 1 will be occurred with β probability. By giving a random vector whose element ranges from $-k$ to k to a signing oracle, we can extract either exactly one of the columns of R or a *sum of a several* columns of R.

To get a numerical sense, consider the parameters $n=140$, $\varepsilon=5$, $\beta=10^{-10}$, $\Upsilon=1/30$. Evaluating the equation (1), (2) yields $|k|<6$ and $|k|<7$, respectively. However, the effective value of $|k|$ in the experiment is twice as large as those values.

Let H be the newly constructed basis.

To write a signature, we need another matrix, that is $T=B^{-1}R$, the unimodular matrix. But in our case, we can construct $T'=B^{-1}H$. Our T is not a unimodular matrix, but it is composed of only integer elements. This is because $L(H)$ is a sub-lattice of $L(B)$ (sometimes, $L(B)$ itself), and H's determinant(equally, the volume of the parallelepied of $L(H)$) is the integer multiple of B's determinant(the volume of the parallelepied of $L(B)$). Now, we can write a signature for any message with the newly generated private-key,(H,T'). For a message $\mathbf{m}$, the distance between $\mathbf{m}$ and the signature $T\lfloor H^{-1}\mathbf{m}\rceil$ is expressed in the following equation.

$$\| \mathbf{m}-BT'\lfloor H^{-1}\mathbf{m}\rceil \| = \| \mathbf{m}-H\lfloor H^{-1}\mathbf{m}\rceil \| = \| H(H^{-1}\mathbf{m}-\lfloor H^{-1}\mathbf{m}\rceil \| = \| H\mathbf{e} \|$$

To make $\| H\mathbf{e} \|$ much smaller, we can apply a lattice reduction algorithm like LLL reduction to H.[5]

It is high time to estimate the distance between the message and the signature that is written by (H,T') .

Let's denote L_1 norm of i-th row in R and that in H by γ_{Ri} and γ_{Hi}, respectively. Every column of our newly constructed basis H is constructed from the vector $\mathbf{d}=\lfloor R^{-1}\mathbf{u}\rceil$ that has less than or equal to ε number of ± 1's and at least one ± 1. For the worst case analysis, we assume that $\mathbf{d}$ consists of exactly ε number of ± 1's. Under the assumption of uniform distribution of ± 1 in $\mathbf{d}$, we can obtain

$$\gamma_{Hi} = \varepsilon * \gamma_{Ri}$$

Thus,

$$\| H\mathbf{e} \| = \varepsilon \| R\mathbf{e} \| \quad (3)$$

As seen in the equation (3), a signature generated with (H,T') is ε times farther from the message than the signature generated with (R,T) is. Equation (3), however, is the worst case estimation for the distance between a message and its corresponding signature. As stated previously, $\mathbf{d}$ has less than or equal to ε number of ± 1's. Furthermore, many of them contain only one ± 1. Thus, the distance in the experiment is much nearer than that in the above estimation.

3.2. Description of the Procedure

We describe the cryptanalyzing procedure of GGH's signature scheme that finds H, a basis for a sub-lattice of $L(R)$ and T'. Fig. 1 describes an algorithm to find out a new private-key.

The parameter q determines when the algorithm stops. The more columns are substituted, the lower the probability for B' to remain fully ranked is. Because we replaced longer columns first, a few remaining columns will not degrade the quality of H.

Writing a signature with (H,T') for an encoded message $\mathbf{m}$ is the same as that with (R,T). For a message $\mathbf{m}$ to be signed, a signer generates the signature $\mathbf{v}=T'\lfloor H^{-1}\mathbf{m}\rceil$. The signature is verified by comparing τ with $\| \mathbf{m}-B\mathbf{v} \| (= \| H\mathbf{e} \|)$.

Instead of using the Babai's round off algorithm to get the lattice point near the message, we can use his nearest plane algorithm to decrease more distance between the signature generated by H and the message.[3]

Now, we estimate the algorithm's running time.

First, we approximate the number of repetitions of the main loop. We must consider the probability for B' to remain fully ranked after substituting $B\mathbf{v}$ for one of its columns, $\mathbf{b}_c$. Assume the matrix U obta-

ined by substituting zero column vector with one of columns of U, which is $R^{-1}B'$. If we transform U into echelon form, every i-th column has a non-zero i-th entry except one column, which is a zero column vector.

Input: A signing oracle A, a signature verifying box V, A public-key (B, σ), q: the trade-off parameter between the running time and the quality of H.
Output: A new private-key (H, T')
1. Perform a lattice reduction algorithm such as LLL reduction to B, and let the result B.
2. Compute b_i , the Euclidean distance of every column of B and assign the smallest one η.
3. Sort b_i with decreasing order according to b_i and store the sorted index to $p[i]$.
4. $H = B$, $c = 1$.
5. Do the following until q columns of H are replaced.
 (a) Generate a random vector u, of which elements are uniformly distributed over $[-k, k]$, where k is determined by equation (1)(2).
 (b) Evaluate a signature $v = A(u)$ by submitting u to the signing oracle A.
 (c) Check whether the signature v is zero-vector. If so, goto step (a).
 (d) Check whether the signature v is valid. If not, goto step (a).
 (e) If Bv is larger than or equal to η, goto step (a).
 (f) Check whether B' obtained by substituting the $p[c]$-th column of H with Bv forms a basis. That is, check whether the rank of B' is n or not.
 (g) If B' forms a basis, then let $H = B'$, and increase c by one.
 (h) If not, then $B' = H$.
6. Apply the Lattice reduction algorithm to H.
7. Compute $T' = B^{-1}H$.

Fig. 1 Algorithm 1 to find out an equivalent private key

Thus, when we replace the zero column with a new vector $\mathbf{d}=\lfloor R^{-1}\mathbf{u} \rfloor$ that has only 0's and ε number of ± 1's, $\mathbf{d}$ would make U be fully ranked with high probability if the i-th element of $\mathbf{d}$ is not zero. Thus, if we assume that ε number of ± 1's are uniformly distributed in $\mathbf{d}$, the probability for one of ± 1 to hit the i-th position is ε/n.

Within the loop 4, the most time consuming part is an operation to check whether the resultant matrix is fully ranked or not, and it takes $O(n^3)$.

Finally, we get the average running time of our algorithm.

$$O(\frac{n^4}{\varepsilon}) \tag{4}$$

3.3. Empirical Results

In this section, we show empirical results of our attack. To get the empirical results, we used the LiDIA package.[8] In the experiments, we let $l=4$, the entry size of R and the cube-like parameter $=l\times\lfloor 1+\sqrt{n} \rfloor$. To generate the public basis from R, we performed $2n$ number of mixing steps, where each step is performed by a uni-modular matrix whose all elements in its diagonal

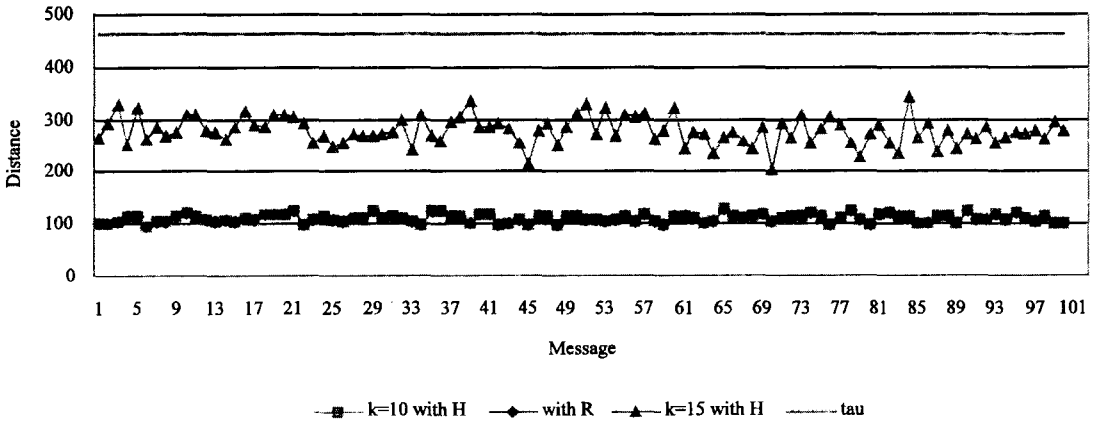

Fig. 2 Quality of signatures generated with H, Dimension=80

are 1 and one of its columns is composed of {-1, 0, 1}. The column has a bias toward 0 and Pr[1]=Pr[-1]=1/7.

These parameter settings are the same as those of.[4] The messages are uniformly distributed in the range of [-200,200].

Fig. 2-5 show τ (for $\varepsilon = 2^{-30}$), distances between 100 messages and corresponding

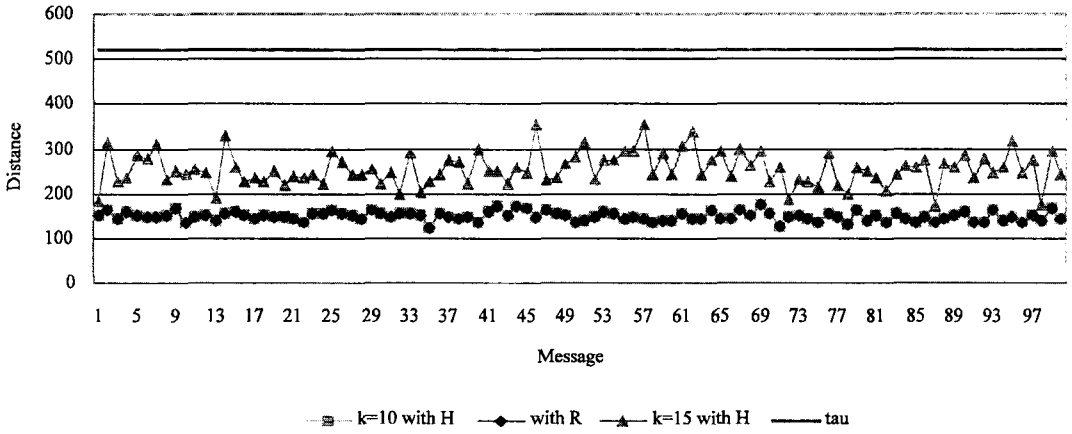

Fig. 3 Quality of signatures generated with H, Dimension=100

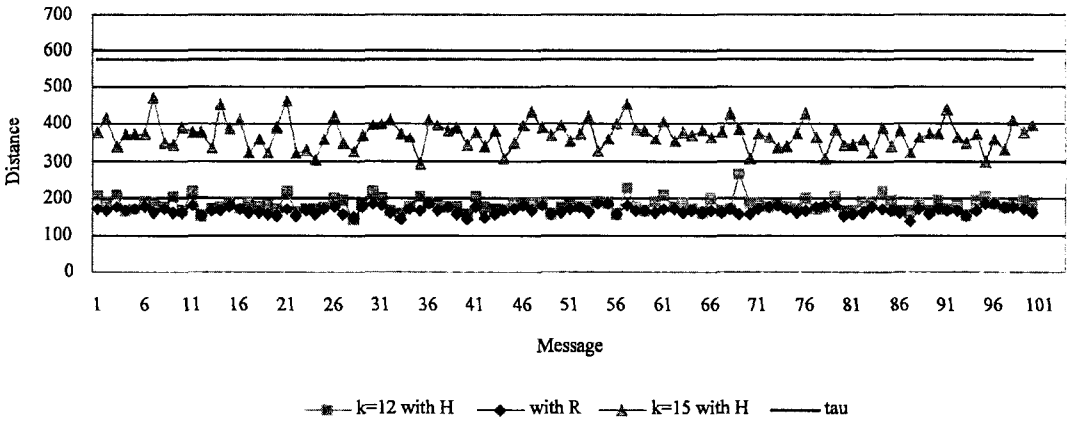

Fig. 4 Quality of signatures generated with H, Dimension=120

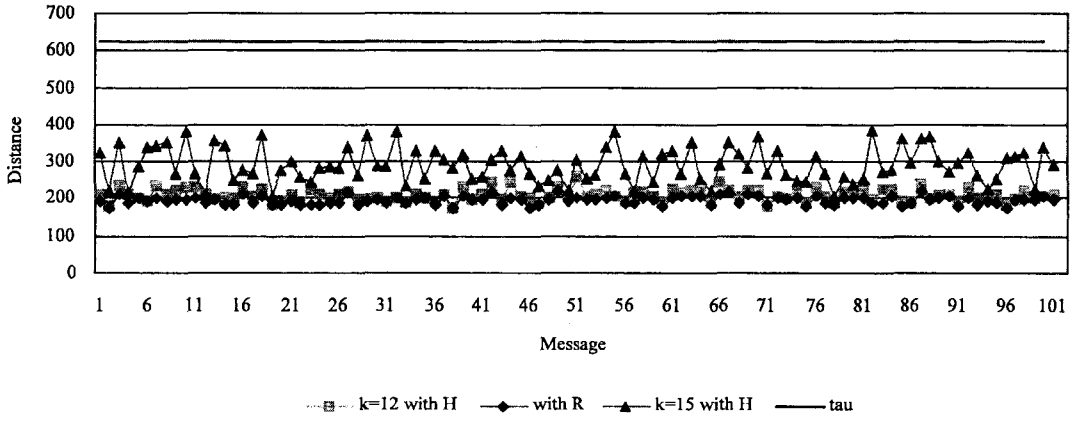

Fig. 5 Quality of signatures generated with H, Dimension=140

Table 1. Summary of the Experiments

(Dimension, k, rc)	pc	AD(H)/AD(R)	Det(H)/Det(R)	(B/R, H/R)
(80, 10, 80)	2534	1	1	(0.33e49, 1)
(80, 15, 80)	563	2.53	≈ 0.24e15	(0.33e49, 0.19e31)
(100, 10, 99)	1991	1	1	(0.13e84, 0.45e12)
(100, 15, 100)	289	1.71	673	(0.13e84, 0.66e21)
(120, 12, 120)	1633	1.09	2	(0.34e120, 3857.66)
(120, 15, 120)	183	2.24	≈ 0.12e15	(0.34e120, 0.64e39)
(140, 12, 137)	1145	1.07	16	(0.14e172, 0.61e10)
(140, 15, 140)	787	1.49	36	(0.14e172, 0.21e21)

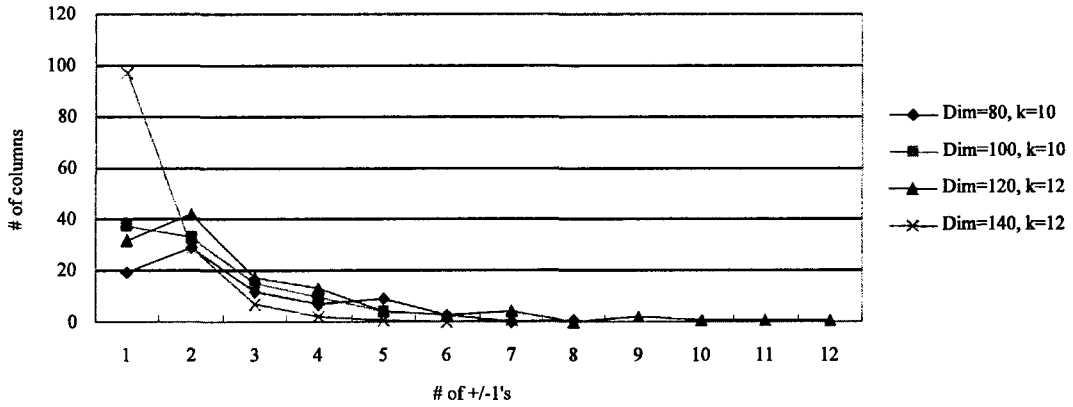

Fig. 6 Cardinalities of $M(H, k)$ for varying parameters

signatures with H and R for dimensions 80, 100, 120 and 140. For dimension 80 and 100 with $k=10$, the algorithm found the same basis as R. With $k=15$, the distances between the signatures with H and the messages are short enough for the signatures to be regarded as valid ones, though they are rather longer than those with R. With $k=10$ or $k=12$, signatures with H cannot be discriminated from the signatures with R.

Table 1 summarizes various metrics regarding the quality of signatures generated with H. In the table, AD(B) is the average distance from the messages and the signatures generated by the basis B, and Det(B) is the determinant of B. rc and pc is the number of replaced columns in each trial and the number of messages consumed, respectively. We didn't count messages that derive signatures to be zero. B/R means the orthogonality defect ratio between B and R, and H/R means that between H and R, where both B and R are LLL-reduced.

From these empirical results, we can conclude that the new basis obtained in the way of section 3 has enough quality to generate a signature that is sufficiently close to the submitted message.

Finally, fig. 6 shows that the cardinality of

$$M(H, k)=\{column \mid S(H, column)=k\}$$

has a light-tailed distribution. The light-tailed distribution means that almost every

columns of H are those of R and only a few columns are *sum of several columns* of R. This property of $M(H,k)$ takes a positive effect not only on the quality of the signature with H, but also on the restoration of the private basis in the attack of the signature scheme, which will be described in the following section.

3.4 Complete Restoration of the Private Basis

In this section, we show that with a rectangular private basis, the signature scheme may reveal its private basis. Regardless of the cube-like parameter, we can attack the signature scheme by the sublattice, and we showed by experiment that it generates the basis with enough quality.

However, as pointed in,[4] non-zero cube-like parameter is preferable to zero cube-like parameter, because that much increases the dual orthogonality defect ratio of public basis and private basis. In this section, we show that we can completely restore the original private basis R if the signature system uses the non-zero cube-like parameter.

We can obtain the exact R from the approximated H by solving a simultaneous equation. For the establishment of simultaneous equation, we take advantage of the fact that the cube-like parameter is $\lceil 1+\sqrt{n} \rfloor$ times larger than l. The key observation is that $B\mathbf{v}=R\lfloor R^{-1}\mathbf{u} \rfloor$, that is the signature for $\mathbf{u}$ is a *sum of several columns* of R, and we can observe in a $B\mathbf{v}$ several peaks resulted from the *biased* diagonals of R.

As shown in section 3.1, the vector $\lfloor R^{-1}\mathbf{u} \rfloor$ has only a few ± 1's and other large portions are filled with 0's. Also, note that the i-th element of the i-th column of R is biased by the cube-like parameter, while others are not. Thus, by counting the peak elements of $B\mathbf{v}$, we can guess how many columns are combined to construct the signature $B\mathbf{v}$, and by observing positions of the peaks, we can guess which columns of R are involved to make a signature. By collecting n-linearly independent pairs of such $B\mathbf{v}$, we can establish the following simultaneous equations and recover R by solving it.

$$RX=H \tag{5}$$

where X is an $n\times n$ matrix whose columns are made up of $\{0,\pm 1\}$ and constructed from linearly independent $B\mathbf{v}$'s by Algorithm 2 and 3.

In this scenario, however, we must not disregard that the number of combined columns of R to make $B\mathbf{v}$ does matter in the attack. If the number of columns combined exceeds a certain threshold, that is, lots of columns are linearly combined, we cannot discriminate the peak points in the vector $B\mathbf{v}$ because every elements in get equally large.

Following is the worst case approximation for the number of columns to be combined, x. In the worst case, the biased point is subtracted by xl, while others are added by xl, where l is the maximum entry size of R. Thus, to make the peak points still greater than others, following must be satisfied.

$$l\lceil 1+\sqrt{n} \rfloor - xl > xl$$

Rewriting the above equation for x, we get

$$x < \frac{\lceil 1+\sqrt{n} \rfloor}{2} \tag{6}$$

For dimension 100, $x=5$, for 120, $x=6$, and for 200, $x=8$, etc. Equation(6) is the worst-case approximation for x. Since all ele-

ments in R are unformly distributed in $[-l, l]$ except the diagonal, each element in the vector that is made by summing x number of columns of R up would likely to be around 0 except the peak points. So, we can set x much larger than the approximated value in equation(6).

Because the permitted x is proportional to ε of the equation(4), we can attack faster with a larger x.

Let us describe how to find the peak points. It consists of two phases. One is finding how many columns of R are combined to be $B\mathbf{v}$, and the other is searching the positions where the peaks are located. Followings are those procedures.

First, we describe how *columns* the number of columns combined can be found. By equation(6), we assume that *columns* is less than $\frac{\lceil 1+\sqrt{n} \rceil}{2}$.

Now, the following procedure outputs positions and polarities of the peaks.

From n linearly independent $B\mathbf{v}$'s, we can get n linearly independent $\mathbf{x}$'s (equally, $\lceil R^{-1}\mathbf{u} \rfloor$'s) and make the matrix X in equation(5). Since X is fully ranked, its inverse does exist and we can easily find the exact R from equation(5).

Fig. 6 shows that $M(H, k)$ has a light-tailed distribution, and it ensures that our attack should succeed to restore the private basis. Consequently, the cube-like parameter is not desirable for the security of GGH's signature scheme.

Input : $B\mathbf{v}$, l and n
Output : *columns*
1. Set *columns* = $\frac{\lceil 1+\sqrt{n} \rceil}{2}$
2. Do the following loop while *columns* > 0
 (a) Count the number of elements of $B\mathbf{v}$ whose absolute value is less than or equal to $l \times$ *columns* and set it to w.
 (b) If $n - w$ is not equal to *columns*, then *columns* = *columns* $- 1$ and goto step (a).
 (c) else return *columns* $= n - w$
3. If *columns* $= 0$,
 then Print "$B\mathbf{v}$ is not an appropriate vector. Choose another one.".

Fig. 7 Algorithm 2 to find out *columns*

Input : *columns* and $B\mathbf{v}$
Output : Column vector $\mathbf{x} = (x_1, x_2, \ldots, x_n)$
1. $i = 1$ and set $\mathbf{x}$ to be a zero vector.
2. Do the following loop while $i \leq$ *columns*
 (a) Find the element m whose absolute value is i-th largest and its position p in $B\mathbf{v}$.
 (b) if $m > 0$, then set $x_p = 1$
 (c) else set $x_p = -1$
3. return the vector $\mathbf{x}$.

Fig. 8 Algorithm 3 to find out x

Ⅳ. Conclusion

In the paper, we presented an effective attack against GGH's signature scheme. The chosen message attack against the signature scheme uses the fact that a signing oracle returns a short lattice point for a short message vector and gathering those lattice points can construct a good basis to write a valid sign. Especially, the cube-like parameter is shown to be harm for the security of the cryptosystem.

We believe that the running time can be reduced by starting from the null basis, filling columns of it one by one with a short lattice point while checking whether the lattice point increases the rank of the basis. Also, the attack has inherently very high parallelism and its running time can be easily improved by the distributed computing.

References

[1] M. Ajtai, Generating hard instances of lattice problems, In *Proceedings of 28th STOC*, Philadelphia, 1996, pp. 99-108.
[2] M. Ajtai, and C. Dwork, A public-key cryptosystem with worst-case/average-case equivalence, In *Proceedings of 29th STOC*, Texas, 1997, pp. 284-293.
[3] L. Babai, On Lovasz lattice reduction

and the nearest lattice point problem, *Combinatorica*, Vol.6, No.1, 1986, pp. 1-13.

[4] O. Goldreich, S. Goldwasser, and S. Halvei, Public-key cryptosystems from lattice reduction problems, In *Proceedings of CRYPTO'97*, Santa Barbara, CA, 1997, pp. 112-131.

[5] A. K. Lenstra, H. W. Lenstra, L. Lovasz, Factoring polynomials with rational coefficients, *Mathematische Annalen* 261, 1982, pp. 515-534.

[6] P. Nguyen, Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto '97, In *Proceedings of CRYPTO'99*, Santa Barbara, CA, 1999, pp. 112-131.

[7] P. Van Emde Boas, Another NP-complete problem and the complexity of computing short vectors in a lattice, Report 81-04, Mathematische Institut, University of Amsterdam, 1981.

[8] LiDIA, A C++ Library For Computational Number Theory, Available from http://www.informatik.th-darmstadt.de/TI/LiDIA/Welcome.html.

〈著者紹介〉

양 대 헌 (DaeHun Nyang)

1994년 2월: 한국과학기술원 과학기술대학 전기 및 전자 공학과 졸업
1996년 2월: 연세대학교 컴퓨터 과학과 석사
2000년 8월: 연세대학교 컴퓨터 과학과 박사
2000년 9월~2003년 2월: 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재: 인하대학교 정보통신대학원 전임강사
〈관심분야〉 암호이론, 암호프로토콜, 인증 프로토콜, 무선 인터넷 보안