Susceptibility of Digital Signature Schemes Based on Error-Correcting Codes to Universal Forgery

Mohssen Alabbadi and Stephen B. Wicker

Coding and Information Theory Laboratory
School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, Georgia 30332 USA
+1 (404) 894-3129 (Voice)
+1 (404) 853-9959 (FAX)
wicker@ee.gatech.edu

Abstract. Xinmei's digital signature scheme and the scheme's modified version as proposed by Harn and Wang have been shown by the authors and others to be susceptible to several different attacks. The authors have since devised and presented a scheme that is impervious to the attacks that were successfully applied to the earlier schemes. It is shown in this paper that this new scheme and Xinmei's scheme are vulnerable to universal forgeries. Equipped with this attack and the earlier ones, general remarks about digital signature schemes based on linear error-correcting block codes are presented.

1 Introduction

In 1990, Xinmei presented a true trapdoor digital signature scheme based on linear error-correcting block codes. The scheme was later modified by Harn and Wang to reduce the threat of selective forgery. Both schemes were subsequently shown by the authors and others to be susceptible to a variety of attacks. The authors then devised a scheme that is impervious to the attacks that were successful on the previous schemes. It is shown in this paper that this new scheme as well as Xinmei's scheme are vulnerable to universal forgeries. Equipped with this attack and the previous ones, general remarks about digital signature schemes based on linear error-correcting block codes are concluded. These remarks may be used as guidelines to construct a secure scheme. The next two sections contain brief reviews of Xinmei's and the authors' digital signature schemes. This is followed by a discussion of two efficient attacks that result in universal forgery for both schemes. The final section sets out several requirements for a truly secure digital signature scheme based on linear block error correcting codes.

2 Xinmei's Digital Signature Scheme

In Xinmei's digital signature scheme [13], each user, say user A, chooses an (n, k) binary Goppa code C_A that has the ability to correct t_A errors. A $k \times n$ binary

generator matrix G_A and an $(n-k) \times n$ binary parity check matrix H_A are then selected for C_A. User A finds an $n \times k$ binary matrix G^* such that $G_A G_A^* = I_k$, where I_k is the $k \times k$ identity matrix. User A selects two nonsingular binary matrices: an $n \times n$ matrix P_A and a $k \times k$ matrix S_A, then he/she computes the following matrices:

$$J_A = P_A^{-1} G_A^* S_A^{-1} \tag{1}$$

$$W_A = G_A^* S_A^{-1} \tag{2}$$

$$T_A = P_A^{-1} H_A^T. \tag{3}$$

User A publishes J_A, W_A, T_A, H_A, t_A, and t'_A where $t'_A < t_A$, but $S_A G_A$ and P_A constitute the private key.

User A obtains the n-bit signature $\underline{c}_j$ of the k-bit message $\underline{m}_j$ by computing

$$\underline{c}_j = (\underline{e}_j \oplus \underline{m}_j S_A G_A) P_A, \tag{4}$$

where $\underline{e}_j$ is a random n-bit error vector of Hamming weight $w_H(\underline{e}_j) = t'_A < t_A$. The receiver validates the signature $\underline{c}_j$ by applying the Berlekamp-Massey algorithm on the syndrome $\underline{c}_j T_A = \underline{e}_j H_A^T$ to obtain $\underline{e}_j$, which must have weight of t'_A. Then J_A, W_A, and $\underline{e}_j$ are used to recover $\underline{m}_j$ by computing the expression

$$\underline{m}_j = \underline{c}_j J_A \oplus \underline{e}_j W_A. \tag{5}$$

In [1] the linearity of the code and knowledge of the error vectors are exploited in a chosen-message attack that results in a total break of Xinmei's scheme. The attack transforms the cryptanalytic problem into a pair of systems of linear equations: one containing n equations in n variables, and the other containing k equations in k variables. The complexity of this attack is thus $O(n^3)$.

It was observed by Harn and Wang in [5] that the combination of valid signatures of some messages yields a valid signature for another message; Xinmei's scheme is thus vulnerable to selective forgeries. Harn and Wang proposed a modification of Xinmei's scheme that appears to secure it against selective forgery. Their scheme has been shown to be totally breakable under known-message attack [2]. In [12] van Tilburg devised a direct attack that totally breaks both the Xinmei scheme and the Harn-Wang modified version of Xinmei's scheme. Under such attack the private key is directly obtained from the public key.

3 The Authors' Scheme

The authors have presented a scheme [3] that overcomes the weaknesses of Xinmei's scheme and the Harn-Wang scheme. In the authors' scheme, each user, say user A, selects an (n, k) binary irreducible Goppa code C_A that has the ability to correct t_A errors. User A then selects a $k \times n$ binary generator matrix G_A and an $(n-k) \times n$ binary parity check matrix H_A for the code C_A. The user then finds G_A^* such that $G_A G_A^* = I_k$, where I_k is the $k \times k$ identity matrix. A nonsingular

binary $n \times n$ matrix P_A is then generated, and the matrices $G'_A = P_A^{-1} G_A^*$ and $H'_A = P_A^{-1} H_A^T$ are computed. Finally, user A selects an $n \times l$ binary matrix R_A of rank n, where $n < l$, and determines R_A^* such that $W_A W_A^* = I_n$. The public key consists of G'_A, H'_A, H_A, R_A^*, t_A, and t'_A, where t'_A is an integer such that $t'_A < t_A$. The private key consists of the matrices G_A, P_A, G_A^*, and R_A. Furthermore, a nonlinear noninvertible function $f(\underline{x}, \underline{y})$ is made available to all users, where $\underline{x}$ is a binary k-tuple, $\underline{y}$ is a binary n-tuple, and the output value is a binary k-tuple. The function f can be implemented in a similar fashion to the DES [10].

A k-bit message $\underline{m}_j$ is signed in the following manner. A random binary error vector $\underline{z}_j$ of length n and weight t'_A is selected. A random l-bit vector $\underline{e}_j$ of arbitrary non-zero weight is also selected. The l-bit signature $\underline{s}_j$ is then computed using the expression

$$\underline{s}_j = [(\underline{z}_j \oplus [f(\underline{m}_j, \underline{z}_j) \oplus \underline{z}_j G_A^*] G_A) P_A \oplus \underline{e}_j R_A^*] R_A \oplus \underline{e}_j. \tag{6}$$

$\underline{s}_j$ and $\underline{m}_j$ are transmitted. The signature is validated by first computing

$$\underline{v}_j = \underline{s}_j R_A^* = (\underline{z}_j \oplus [f(\underline{m}_j, \underline{z}_j) \oplus \underline{z}_j G_A^*] G_A) P_A. \tag{7}$$

The Berlekamp-Massey algorithm is then applied to the syndrome $\underline{v}_j H'_A = \underline{z}_j H_A^T$ to obtain $\underline{z}_j$, which must have weight of t'_A. Then G'_A is used to recover $f(\underline{m}_j, \underline{z}_j)$ as $\underline{v}_j G'_A$. Finally $\underline{v}_j G'_A$ is compared with the hashing function value $f(\underline{m}_j, \underline{z}_j)$ obtained using the received $\underline{m}_j$ and the computed $\underline{z}_j$. The signature is accepted if the two are identical.

The scheme is impervious to the attacks that are successful on Xinmei's scheme and the Harn-Wang scheme. However, this scheme as well as the previous ones are vulnerable to universal forgery as will be shown in the next section. We will first show that the matrix R_A has no cryptographic significance and the problem is reduced to generating an n-bit vector $\underline{v}_j$ that is accepted by the validation process, for there exits an $n \times l$ binary matrix R' such that $R' R_A^* = I_n$ and $\underline{s}_j$ is then obtained as $\underline{s}_j = \underline{v}_j R'$. The matrix R' can be found in polynomial time as follows. n linearly independent rows of W_A^* are selected (this can be done by row reduction of the matrix W_A^*, requiring $O(ln^2)$ bit operations). Let the n linearly independent rows be numbered as $l_1, l_2, \cdots, l_n$. The n linearly independent rows are then inverted in $O(n^3)$ bit operations. The columns of the inverted matrix correspond to columns $l_1, l_2, \cdots, l_n$ of R' and the other $l - n$ columns of R' are filled with zeros.

4 Universal Forgery

4.1 Attack I

Knowledge of the error vectors alone could jeopardize the security of the schemes; a known-message attack is devised that allows the cryptanalyst to universally forge signatures. We begin by noting that, in Xinmei's scheme,

$$\underline{c}_j = (\underline{e}_j \oplus \underline{m}_j S_A G_A) P_A = \underline{e}'_j \oplus \underline{m}_j E_A, \tag{8}$$

where $\underline{e}'_j = \underline{e}_j P_A$ and $E_A = S_A G_A P_A$. Similarly, in the other scheme,

$$\underline{v}_j = (\underline{z}_j \oplus [f(\underline{m}_j, \underline{z}_j) \oplus \underline{z}_j G_A^*] G_A) P_A = \underline{z}'_j \oplus f(\underline{m}_j, \underline{z}_j) E'_A, \tag{9}$$

where $\underline{z}'_j = \underline{z}_j P_A \oplus \underline{z}_j G_A^* G_A P_A$ and $E'_A = G_A P_A$.

Thus if E_A (respectively E'_A) and at least one $\underline{e}'_j$ (respectively $\underline{z}'_j$) are known, then the user's signature can be universally forged in Xinmei's scheme (respectively the other scheme). For example, if the message $\underline{m}_l$ is to be signed, then the cryptanalyst can produce the signature $\underline{c}_l$ as $\underline{c}_l = \underline{e}'_j \oplus \underline{m}_l E_A$ in Xinmei's scheme (respectively as $\underline{c}_l = \underline{z}'_j \oplus f(\underline{m}_l, \underline{z}_j) E'_A$ in the other scheme). Furthermore, if E_A (respectively E'_A) is known, then $\underline{e}'_j$ (respectively $\underline{z}'_j$) can be readily found. Hence the cryptanalyst needs only to find E_A (respectively E'_A).

Let $\underline{c}_j$ and $\underline{c}_{j'}$ (respectively $\underline{v}_j$ and $\underline{v}_{j'}$) be the signatures of the messages $\underline{m}_j$ and $\underline{m}_{j'}$ under Xinmei's scheme (respectively the other scheme), where $\underline{e}_j$ (respectively $\underline{z}_j$) is the error vector used in both signatures. Then $\underline{c}_j \oplus \underline{c}_{j'} = (\underline{m}_j \oplus \underline{m}_{j'}) E_A$ (respectively $\underline{v}_j \oplus \underline{v}_{j'} = (\underline{m}_j \oplus \underline{m}_{j'}) E'_A$). Now the cryptanalyst needs k pairs of signatures such that each pair uses the same error vector. The k expressions $\{\underline{c}_j \oplus \underline{c}_{j'} = (\underline{m}_j \oplus \underline{m}_{j'}) E_A\}_{1 \le j, j' \le k}$ (respectively $\{\underline{v}_j \oplus \underline{v}_{j'} = (\underline{m}_j \oplus \underline{m}_{j'}) E'_A\}_{1 \le j, j' \le k}$) form a linear system which allows us to solve for E_A (respectively E'_A) in $O(k^3)$ provided that set of the messages $\{\underline{m}_j \oplus \underline{m}_{j'}\}_{1 \le j, j' \le k}$ are linearly independent. The cryptanalyst can then find one or more $\underline{e}'_j$'s (respectively $\underline{z}'_j$'s) by using E_A (respectively E'_A).

The efficiency of this attack can be expressed as the number of signatures l that must be obtained before the attack succeeds. It is assumed that the signatures generated by a user are uniformly distributed. Let N be the number of possible error vectors that can be invoked by the signer. Clearly

$$N = \binom{n}{t'_A}. \tag{10}$$

The problem exhibits a great resemblance to the birthday paradox. We expect the number of signatures required for this universal forgery attack to be $O(\sqrt{N})$. To support this argument, we take an approach similar to the one given in [4, pp. 279–281].

Let the signatures be grouped into r sets such that each set contains s signatures, where $s^2 \le N$. For any two sets, the total number of comparisons is s^2 and the probability that a comparison would yield a match is $1/N$ (the match event refers to the event when two signatures from two different sets have the same error vector, a match within a set is not considered here). Thus the probability of a match between any two sets is approximately s^2/N. By making $s = \sqrt{N}$, there is then a match between any two sets with overwhelming probability (it was mentioned in [9] that there are at least three elements in common between any two such sets). Furthermore, r is chosen such that $\binom{r}{2} \ge k$, and thus $r = \left\lceil \frac{1 + \sqrt{1 + 8k}}{2} \right\rceil$. The total number of signatures needed is thus $l = O(r\sqrt{N})$.

The attack requires two tables: one containing the signatures and another containing the error vectors. The space requirement is thus $O[l(n + \lceil log_2 N \rceil)]$ bits, where each error vector requires $\lceil log_2 N \rceil$ bits. $O(Nk)$ comparisons are needed for this attack. But this complexity can be dramatically reduced, however, by sorting the whole l signatures instead of comparing the elements one by one. This sorting technique would have a complexity of $O(l \log_2 l)$ comparisons and since each comparison involves two $\lceil log_2 N \rceil$-bit numbers. It follows that the bit complexity is $O(\lceil log_2 N \rceil l \log_2 l)$ bit operations.

Finally we must consider the question of whether the set of the messages $\{\underline{m}_j \oplus \underline{m}_{j'}\}_{1 \le j,j' \le k}$ are linearly independent. It is to be noted that the number of $k \times k$ binary invertible matrices is $0.29 \times 2^{k^2}$, and the number of $k \times k$ binary matrices is 2^{k^2}. Thus the probability of randomly selecting any $k \times k$ binary matrix and having it be invertible is thus 0.29, and the expected number of repetitions is thus 3.4. The number of signatures that must be collected is thus increased on the average by a factor slightly more than 3.

4.2 Attack II

In Xinmei's scheme, $\underline{c}_j$ must satisfy the equations $\underline{c}_j T_A = \underline{e}_j H_A^T$ and $\underline{c}_j J_A = \underline{e}_j W_A \oplus \underline{m}_j$. This leads to $\underline{c}_j [T_A \mid J_A] = [\underline{e}_j H_A^T \mid \underline{e}_j W_A \oplus \underline{m}_j]$, or simply $\underline{c}_j X = Y$, where $Y = [\underline{e}_j H_A^T \mid \underline{e}_j W_A \oplus \underline{m}_j]$ is an $n \times n$ matrix and $X = [T_A \mid J_A]$ is an $n \times n$ matrix which is publicly known. Similarly, in the authors' scheme, $\underline{v}_j$ should satisfy $\underline{v}_j H'_A = \underline{z}_j H_A^T$ and $\underline{v}_j G'_A = f(\underline{m}_j, \underline{z}_j)$. This leads to $\underline{v}_j [H'_A \mid G'_A] = [\underline{z}_j H_A \mid f(\underline{m}_j, \underline{z}_j)]$, or simply $\underline{v}_j X' = Y'$, where $Y' = [\underline{z}_j H_A \mid f(\underline{m}_j, \underline{z}_j)]$ is an $n \times n$ matrix and $X' = [H'_A \mid G'_A]$ is an $n \times n$ matrix which is publicly known.

The analyst computes Y (respectively Y'), where $\underline{m}_j$ is the message to be forged and $\underline{e}_j$ (respectively $\underline{z}_j$) has weight t'_A, then $\underline{c}_j$ (respectively $\underline{v}_j$) can be easily obtained as $\underline{c}_j = YX^{-1}$ (respectively $\underline{v}_j = Y'X'^{-1}$), provided that X (respectively X') is full rank. The following lemma shows that X and X' are both full rank matrices, and thus signatures can be universally forged in both schemes.

Lemma 1 *X and X' are full rank matrices.*

Proof: We will only prove the lemma for X; the result for X' can be proven in a similar manner. Let $\underline{w}$ be an n-bit column vector and partition $\underline{w}$ into two vectors, an $(n-k)$-bit column vector $\underline{w}_1$ and a k-bit column vector $\underline{w}_2$. Thus $X\underline{w} = [T_A \mid J_A]\underline{w} = [P_A^{-1} H_A^T \mid P_A^{-1} G_A^* S_A^{-1}]\underline{w} = P_A^{-1} H_A^T \underline{w}_1 \oplus P_A^{-1} G_A^* S_A^{-1} \underline{w}_2$. If it holds that $X\underline{w} = 0_{n \times 1}$ (the all-zero n-bit column vector) if and only if $\underline{w} = 0_{n \times 1}$, then X has rank n. For $\underline{w} = 0_{n \times 1}$, we have $X\underline{w} = 0_{n \times 1}$. For $X\underline{w} = 0_{n \times 1}$, we have $P_A^{-1} H_A^T \underline{w}_1 \oplus P_A^{-1} G_A^* S_A^{-1} \underline{w}_2 = 0_{n \times 1}$. Premultiplying by $G_A P_A$, we obtain $G_A H_A^T \underline{w}_1 \oplus G_A G_A^* S_A^{-1} \underline{w}_2 = 0_{k \times 1}$. Since H_A is the null space of G_A, we have $G_A H_A^T = 0_{k \times (n-k)}$ and hence $G_A G_A^* S_A^{-1} \underline{w}_2 = 0_{k \times 1}$, or $S_A^{-1} \underline{w}_2 = 0_{k \times 1}$ and thus $\underline{w}_2 = 0_{k \times 1}$, for S_A is nonsingular. Hence $H_A^T \underline{w}_1 = 0_{n \times 1}$. Since H_A^T has rank $n-k$, then $\underline{w}_1 = 0_{(n-k) \times 1}$. ∎

Li [7] mentioned that if the public key in Xinmei's scheme is chosen such that X is not a full rank matrix, then the scheme is secure. Lemma 1, on the contrary, shows that X is always full rank, regardless of the selection of the public key.

5 Conclusion

Examining the previous digital signature schemes based on linear error-correcting block codes, the following can be concluded:

- The linearity of the code allows selective forgery [5]. This, however, can be prevented by signing the image of the message under a nonlinear noninvertible transformation [5] instead of signing the message itself. It is essential that the transformation is a function of the error vector [3] to prevent the chosen-message attack devised in [1].
- Revealing the error vectors permits universal forgery as shown in this paper (attack I). This attack can be prevented if the error vectors are not revealed or the parameters of the code are chosen properly to make this attack infeasible.
- Revealing information about the right inverse of the generator matrix is equivalent to revealing some information about k linearly independent columns of the generator matrix. This is the reason for the success of the direct attack on the Xinmei and Harn-Wang schemes [12] and the universal forgery attack (attack II) described here. (It is to be noted that the probabilistic ciphertext-only attacks launched on McEliece's system [8] as described in [6, 8, 11] are all based on searching for k linearly independent columns of the generator matrix). Thus the public key should not contain information (even in scrambled form) about k linearly independent columns of the generator matrix.

References

1. M. Alabbadi and S. B. Wicker. Cryptanalysis of the Harn and Wang modification of the Xinmei digital signature scheme. *Electronics Letters*, 28(18):1756–1758, 27th August 1992.
2. M. Alabbadi and S. B. Wicker. Security of Xinmei's digital signature scheme. *Electronics Letters*, 28(9):890–891, 23rd April 1992.
3. M. Alabbadi and S. B. Wicker. Digital signature schemes based on error-correcting codes. In *IEEE International Symposium on Information Theory*, January 17-22 1993. San Antonio, Texas, U.S.A.
4. D. W. Davies and W. L. Price. *Security for Computer Networks.* John Wiley and Sons, 1989.
5. L. Harn and D. -C. Wang. Cryptanalysis and modification of digital signature scheme based on error-correcting codes. *Electronics Letters*, 28(2):157–159, 16th January 1992.
6. P. J. Lee and E. F. Brickell. An obsevation on the security of McEliece's public-key cryptosystem. In C. G. Gunther, editor, *Lecture Notes in Computer Science # 330, Advances in Cryptology-Eurocrypt '88 Proceedings*, pages 275–280, Davos, Switzerland, May 25-27 1988. Springer-Verlag.

7. Yuan-Xing Li. An attack on Xinmei's digital signature scheme. In *IEEE International Symposium on Information Theory*, January 17-22 1993. San Antonio, Texas, U.S.A.
8. R. J. McEliece. Public-key cryptosystem based on algebraic coding theory. JPL DSN Progress Report 42-44, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, U.S.A, Jan. & Feb. 1978. Pages 114-116.
9. J. Meijers and J. van Tilburg. On the Rao-Nam private-key cryptosystem using linear codes. In *IEEE International Symposium on Information Theory*, page 126, June 24-28 1991. Budapest, Hungary.
10. National Bureau of Standard. *Data Encryption Standard, Federal Information Processing Standard (FIPS) Publication 46*, January 1977. U.S. Department of Commerce, Washington, D.C.
11. J. van Tilburg. On the McEliece public-key cryptosystem. In S. Goldwasser, editor, *Lecture Notes in Computer Science # 403, Advances in Cryptology-Crypto '88 Proceedings*, pages 119–131, Santa Barbara, Ca., Aug. 21-25 1988. Springer-Verlag.
12. J. van Tilburg. Cryptanalysis of Xinmei digital signature scheme. *Electronics Letters*, 28(20):1935–1936, 24th September 1992.
13. W. Xinmei. Digital signature scheme based on error-correcting codes. *Electronics Letters*, 26(13):898–899, 21st June 1990.