6278

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

A Digital Signature Scheme Constructed with Error-correcting Codes

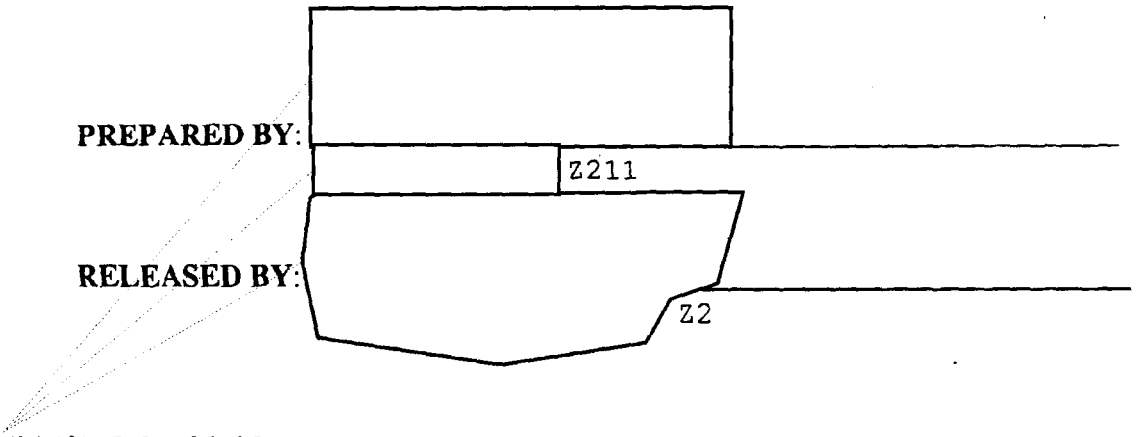
Z2-TSR-06-93

30 March 1993

A9585A.3-79

DOCID: 3097967

Z2-TSR-06-93
30 March 1993



(b)(3)-P.L. 86-36

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY NSA/CSSM 123-2	3. DISTRIBUTION/AVAILABILITY OF REPORT THIS REPORT CANNOT BE RELEASED OR REPRODUCED WITHOUT PERMISSION OF THE ISSUING OFFICE.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE ORIGINATING AGENCY'S DETERMINATION REQUIRED	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) Z2-TSR-06-93	5. MONITORING ORGANIZATION REPORT NUMBER(S) (b)(1) (b)(3)-P.L. 86-36
6a. NAME OF PERFORMING ORGANIZATION	6b. OFFICE SYMBOL (If applicable) Z2
7a. NAME OF MONITORING ORGANIZATION	
6c. ADDRESS (City, State, and ZIP Code) DIRNSA Ft. Meade, MD 20755-6000 Attn: Z2	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION	8b. OFFICE SYMBOL (If applicable)
9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER	
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO.
11. TITLE (Include Security Classification) A Digital Signature Scheme Constructed with Error-correcting Codes (b)(3)-P.L. 86-36	
12. PERSONAL AUTHOR(S) Z211, translator	
13a. TYPE OF REPORT TSR	13b. TIME COVERED FROM_____ TO_____
14. DATE OF REPORT (Year, Month, Day) 1993 March 30	15. PAGE COUNT 9
16. SUPPLEMENTARY NOTATION	

17. COSATI CODES		
FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
Signature schemes, Error-correcting codes, public-key cryptosystems

19. ABSTRACT (Continue on reverse if necessary and identify by block number)
(U) A digital signature scheme based on error-correcting codes is proposed

(b)(3)-P.L. 86-36

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT [X] UNCLASSIFIED/UNLIMITED [ ] SAME AS RPT. [ ] DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE (Include Area Code) 963-6421 / 22c. OFFICE SYMBOL

DD Form 1473, JUN 86 *Previous editions are obsolete.* SECURITY CLASSIFICATION OF THIS PAGE

COMPUTER FACSIMILE -CONFIDENTIAL//MR-

UNCLASSIFIED

A Digital Signature Scheme Constructed with Error-correcting Codes

The authors of this paper, LI Yuanxing and LIANG Chuanjia, are at the Xi'an Electronics, Science, and Technical University. The paper appeared in Acta Electronica Sinica, volume 19 (1991), no. 4, p. 102-104. The translation was carried out by [redacted] *Z211, then corrected and improved by* [redacted] *W3152. The manuscript, representing a doctoral-level research topic funded by the National Education Commission, was first received by the publishers in January of 1990; the final form was received in December 1990.*

Abstract. In this paper a digital signature scheme based on error-correcting codes is proposed for the first time.

1. Introduction

In 1978, McEliece for the first time used error-correcting codes to construct a type of public-key cryptosystem [1], combining encryption with error-correcting codes. In the following ten years or so, much research by Chinese and foreign scholars has been devoted to the relation between encryption and error-correcting codes, and abundant research results have been obtained [2-6]. However, there have so far been no open-source research papers on how to use error-correcting codes to construct digital signature schemes. This paper proposes a type of digital signature scheme based on error-correcting codes. The paper analyzes a few performance norms of the scheme and gives requirements which the parameters should satisfy for the scheme's security. Research shows that the scheme is secure, is easily designed and implemented, has speed advantages, and its public and secret keys are not too large. Of course the information rate of the scheme is comparatively low.

2. The construction of the digital signature scheme

We let A and B be two users, and A wants to transmit to B a message which needs to have a digital signature.

2.1. Generating the public and secret keys

To allow A to implement a message signature, we first choose a linear (n, k, t) block code over a suitable $GF(q)$. Here q and n, k, t represent respectively a prime power and the code length, dimension, and error-correcting capability of the error-correcting code. Let A choose randomly an (n, k, t) Goppa code over $GF(q)$ and denote the $k \times n$ generator matrix and the $(n-k) \times n$ parity-check matrix over $GF(q)$ be denoted by G and H respectively. As usual $n \leq q^m$, and $k \geq n - mt$; m is a positive integer. A further randomly chooses an $n \times n$ permutation matrix P over $GF(q)$. Compute $H' = HP$. Let H' be public, but keep H and P secret.

2.2. Achieving the signature

Let L be the set of n-dimensional vectors over $GF(q)$ which have Hamming weight not exceeding t. Then

$$|L| = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i,$$

where $|L|$ denotes the number of elements in L. We know from coding theory that a block code with error-correcting capability t can theoretically correct q^{n-k} error patterns but in practice, using the fast decoding algorithm, we can guarantee correct decoding only for those error patterns belonging to L. That is, given an $(n-k)$-dimensional syndrome vector, since the actual decoder decodes incompletely, one cannot guarantee an n-dimensional vector, i.e., that the error patterns give a 1-1 correspondence. However, for an arbitrary $E \in L$, there is a unique corresponding syndrome S, and $EH^T = S$. H^T denotes the transpose of H. Conversely, when the decoder decodes this S, we obtain uniquely the original $E \in L$. Hence A, before achieving the above signature, should do the following preparatory operations.

(I) First divide the message which requires a signature into l-long groups over $GF(q)$. This length l must satisfy: if A randomly chooses in L a subset U comprising q^l elements, and computes for every element in U a corresponding syndrome, then this can be accomplished in a reasonable time.

(II) A randomly chooses in L a subset U comprising q^l elements, and computes for every element in U a unique syndrome. Namely, for $E \in U$, compute $EH^T = S$.

(III) Establish a 1-1 correspondence between the q^l l-dimensional message vectors and the q^l syndromes, and make it public.

It is easy for A to accomplish each of the above three steps. Then A can achieve the signature for his message by using the following three-step procedure.

(1) let M be an arbitrary l-dimensional message vector. Based on the published correspondence relation, find the corresponding syndrome S. Feed S into the Goppa code decoder, and obtain uniquely the n-dimensional error pattern E. Namely $S = EH^T$. Also the weight of E does not exceed t.

(2) Right-multiply E by $(P^T)^{-1}$, thus obtaining the signature C for M, where $C = E(P^T)^{-1} = EP$. [The last equality is valid only if $P^T = P^{-1}$, which we should not require. I think he should have omitted this last equality. — edit.]

(3) Transmit C to B.

2.3. Verifying the signature

(1) When B receives C, he uses A's public key H' to compute $C(H')^T$. $C(H')^T = EPP^TH^T = S$. [Note that this does not require $C = EP$; instead $C = E(P^T)^{-1}$ is the critical matter. — edit.]

(2) Based on A's public correspondence relation, from S find M, thus accurately recovering the message vector, and achieving the verification.

Obviously, any other user could emulate B, using A's public key and public correspondence relation, to verify A's signature.

3. A proof of the security of the scheme

We may as well let the adversary employ the following methods as he tries to forge A's signature.

1. If he can from the public key H' factor out H and P, then A's signature can be forged. However, H and P are both randomly generated by A, so the possible number of H and P respectively are I_t and $n!(q-1)^n$. Here [7]

$$I_t = \frac{1}{t}\sum_{d|t}\mu(d)(q^m)^{\frac{t}{d}}.$$

Also the factors of H' are not unique. Therefore, to factor out the secret keys H and P from H' the computational complexities respectively are $C_{\mathrm{LM1}} =$

$O(q^{mt})$ and $C_{\mathrm{LM2}} = O(n!(q-1)^n)$. [Of course one need not perform *both* of these tasks. And nonuniqueness does not favor the cryptographer! — edit.]

2. Based on the public H' and the already known S (i.e., M), he could try to obtain the signature C from solving the equations $C(H')^T = S$. However, H' represents a general linear block code, and $C \in L$, thus trying to obtain the signature by solving equations is an NP-complete problem [8].

3. Based on L, he could try to guess the signature of M directly. The computational complexity of guessing the signature is $C_{\mathrm{LM3}} = O(|L|)$.

If n, k, and t satisfy definite requirements, C_{LM1}, C_{LM2}, and C_{LM3} become very large in magnitude, so it will be difficult for the adversary's methods to forge A's signature to prove effective.

4. Design of parameters and analysis of the scheme's performance

From security analysis we know that the computational complexities of the possible analytic methods are respectively C_{LM1}, C_{LM2}, and C_{LM3}. For simplicity, take $q = 2$; then $C_{LM1} = O(2^{mt})$, $C_{LM2} = O(n!)$, and $C_{LM3} = O(\sum_{i=0}^{t} \binom{n}{i})$.

Let A choose an irreducible (n, k, t) Goppa code over $GF(2)$; then $n = 2^m$ and $k \geq n - mt$. Obviously if we choose $m > 6$ and $t > 10$ then C_{LM1} and C_{LM2} both exceed $O(2^{60})$. In this case $n > 64$ and $n - R > 60$. [R. mentioned below, is the information rate $\frac{l}{n}$. — edit.]

Below we analyze conditions which n and t should satisfy so that C_{LM3} exceeds $O(2^{60})$. Since $2t = d - 1 \leq n - k$,

$$\frac{t}{n} \leq \frac{1}{2}\left(1 - \frac{k}{n}\right) < \frac{1}{2}.$$

From [9] we get

$$\sum_{i=0}^{\frac{t}{n}\cdot n} \binom{n}{i} \geq \frac{2^{nH_2(t/n)}}{\sqrt{8t(1-t/n)}} \tag{1}$$

where

$$H_2(t/n) = -\frac{t}{n}\log_2\frac{t}{n} - \left(1 - \frac{t}{n}\right)\log_2\left(1 - \frac{t}{n}\right).$$

Thus

$$C_{LM3} \geq O(2^{nH_2(t/n)}). \tag{2}$$

For $0 < \frac{t}{n} < \frac{1}{2}$, $H_2(t/n)$ is a monotone increasing function; if $\frac{t}{n} = 0.1$ then $H_2(t/n) = 0.469$. If we choose $n = 128$ then $n \cdot H_2(t/n) \approx 60.03$, so if we choose $n = 128$ and $\frac{t}{n} \geq 0.1$ then $C_{LM3} > O(2^{60})$.

Integrating the requirements on C_{LM1} and C_{LM2}, if we choose $n = 128$ and $t \geq 13$, then the signature scheme will have sufficient security. In this case $n - k \geq 91$.

For example, A can choose an irreducible degree-13 polynomial $g(x)$ over $GF(2^7)$, from which he can generate an irreducible (128,37,13) Goppa code. Using this code, A can perform digital signatures.

The following analysis describes several performance norms of the scheme.

(1). Achieving the complexity

Achieving the above scheme is very convenient. Provided that A has a Goppa code decoder he can sign messages. The signature process is also fast. Because the decoding speed of the Goppa code decoder has ([9]) a complexity of about $O(n \log_2^2 n)$, a single message vector signature requires only about $n \log_2^2 n$ arithmetic operations. Also verification of the received C involves only adding the corresponding columns chosen in H'. Since $C \in L$, verification is at most the addition of t n-dimensional column vectors, so requires at most tn arithmetic operations. Thus verification is also very fast.

(2). The quantity of public and secret key

The quantities of public and secret key are respectively $(n - k) \times n$ bits and $(2n - k) \times n$ bits. If we use the above example, then the quantities of public and secret key respectively are only about 11,000 bits and 28,000 bits. In addition to wanting to publish H', A will also need to publish the correspondence between the message vectors and their syndromes. If A agrees on a permutation sequence of message vectors, with agreement based on the decimal-based integers from 0 to $2^l - 1$ in increasing order, then A will also need to publish this quantity of $(n - k)2^l$ bits. Again employing the above example, and choosing $l = 15$, A will need to publish about 2,980,000 bits of syndromes. (note: in the M_s public-key system the quantity of public key is about 2,840,000 bits [2]).

(3). The information rate

The information rate of the scheme is $R = \frac{l}{n}$. In the above example, $R \approx 0.12$. The comparatively low information rate of this scheme is a weakness. By increasing l, R can be raised to a certain extent. If $l = 30$ then $R \approx 0.23$.

Another point we need to address is as follows. Prior to performing the signature, A needs to compute in advance the 2^l syndromes of the n-dimensional vectors in U. A can use the Goppa code decoder to accomplish this (computing the syndromes corresponds to the first step of decoding), in time already included in the $n \log_2^2 n$ arithmetic operations needed for a single signature. Hence if A computes in advance the 2^l syndromes, it cannot increase the time and difficulty to achieve the scheme.

5. Concluding remarks

Error-correcting coding theory has continued to mature since its origins in the '50s. More and more, research on the application of error-correcting codes is becoming of value to the public. In this paper error-correcting codes were used to construct a type of digital signature scheme, pointing out an important application of error-correcting codes in cryptologic research, thereby having significance in both theory and practice. New applications of error-correcting codes in cryptology are attracting people to conduct new and more profound research.

We warmly thank professors WANG Xinmei and HU Zheng for beneficial discussions.

Bibliography

1. R. J. McEliece, DSN Progress Report 42-44 (1978), 114-116.

2. WANG Xinmei, Acta Electronica Sinica 11 (1986), no. 4, 84-90. [in Chinese]

3. WANG Xinmei, J. China Inst. Communic. 7 (1986), no. 5, 1-6. [in Chinese]

4. WANG Xinmei, J. China Inst. Communic. 10 (1989), no. 4, 1-6. [in Chinese]

5. R. J. McEliece et al., Communic. ACM, 24 (1981), 583-584.

6. WANG Xinmei, J. China Inst. Communic. 8 (1987), no. 4, 1-9. [in Chinese]

7. E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, 1968.

8. E. R. Berlekamp et al., IEEE Trans. Info. Theo. 24 (1978), 384-386.

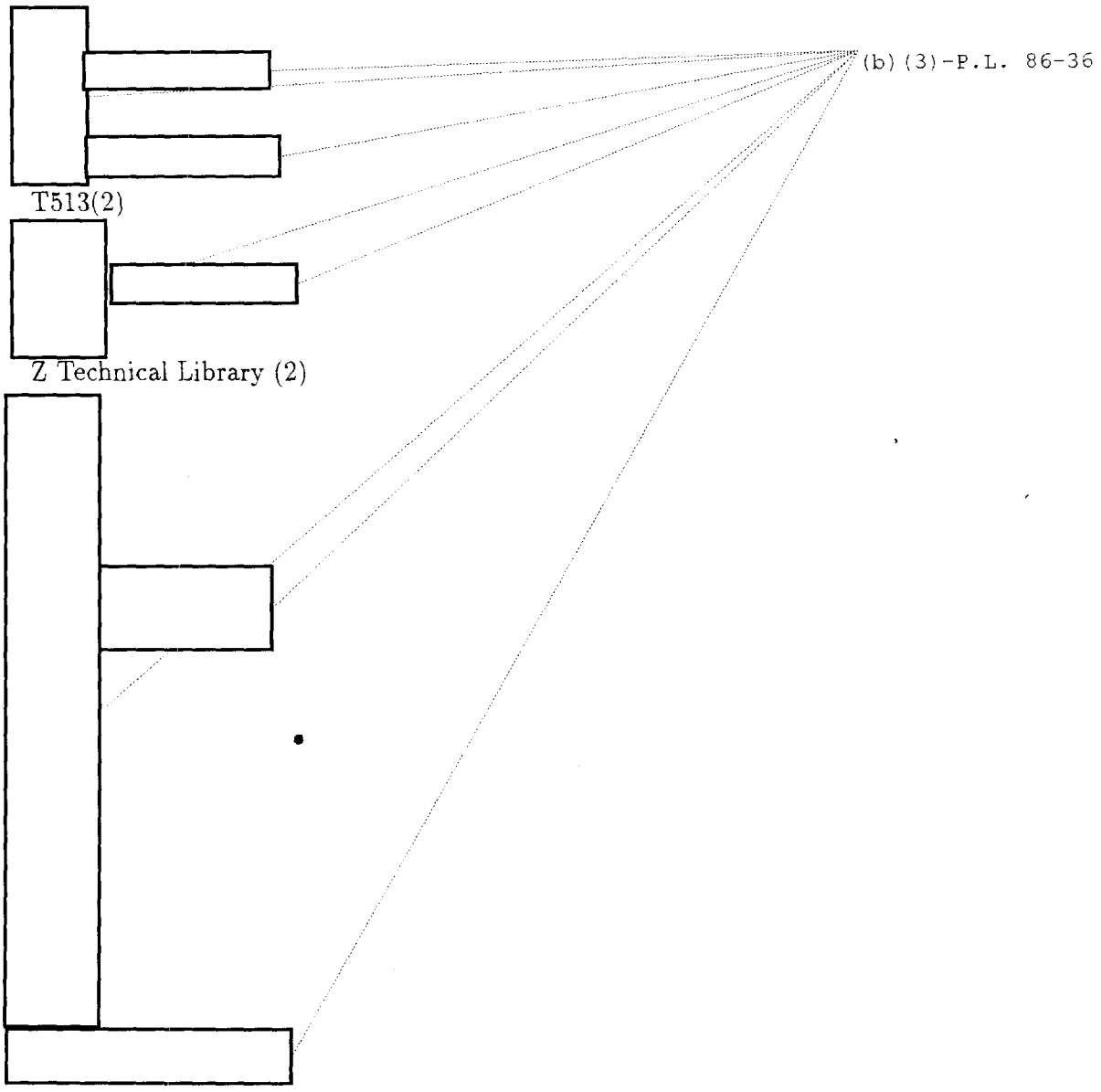
9. F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-correcting Codes, North-Holland, 1977.

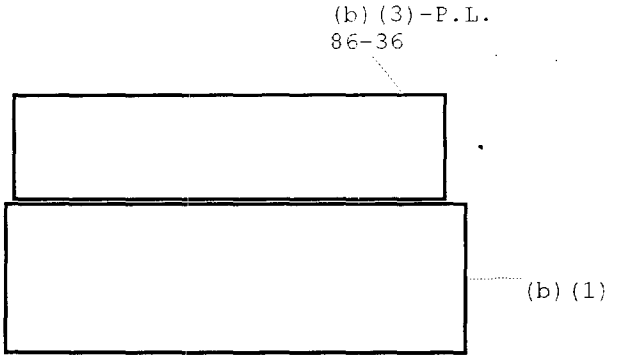
DISTRIBUTION:

C61

C7

E42




(b)(3)-P.L.
86-36
(b)(1)