2009 Third International Conference on Network and System Security

Weakness on Cryptographic Schemes based on Chained Codes

Omessaad Hamdi
SYSTEL laboratory of of Higher School of Communication of Tunis
Tunisia
hamdi@univ-tln.fr

Ammar Bouallegue
SYSCOM Laboratory of the National School of Engineering of Tunis
Tunisia
ammar.bouallegue@enit.rnu.tn

Sami Harari
SYSCOM South University of Toulon-Var, La garde,
France
harari@univ-tln.fr

***Abstract*—We propose a method to recover the structure of a randomly permuted chained code and how to cryptanalyse cryptographic schemes based on these kinds of error coding. This result prohibits the use of chained code on cryptography.**

***Keywords*-Cryptography, Chained Codes, Attack, Complexity.**

I. Introduction

RSA and McEleice are the oldest public key cryptosystems. They are based respectively on intractability of factorization and syndrome decoding problems [1]. However, McEliece [2] was not quite as successful as RSA, partially due to its large public key and to the belief that McEleice could not be used in signature. In 2001, Courtois, Finiasz and Sendrier [3] show a new method to build practical signature schemes with the McEliece public key cryptosystem. This scheme has the drawback of a high signature cost. One idea to counter this drawback consists in replacing Goppa code by other codes which have faster decoding algorithms like chained codes.

In this paper, we show an invariant in the structure of chained codes which makes a weakness in cryptographic schemes based on chained codes. Our approach is based on the fact that any given chained equivalent code can be transformed in a systematic code which has a special generator matrix representation.

II. Chained Code

A chained code C is defined as a direct sum of γ elementary codes C_i. This code is of length $N = \sum_{i=1}^{\gamma} n_i$ and of dimension $K = \sum_{i=1}^{\gamma} k_i$.

$$C = \bigoplus_{i=1}^{\gamma} C_i = \{(u_1, ..., u_\gamma); \quad u_1 \in C_1, ..., u_\gamma \in C_\gamma\}$$

To encode an information $m = (m_1, ..., m_\gamma)$, where m_i is k_i bits, we simply multiply it by the generator matrix to obtain the codeword $u = m.G = (u_1, ..., u_\gamma)$ with u_i is the n_i bits codeword obtained from m_i using the elementary code C_i. So, G is a diagonal matrix in blocs and whose diagonal is formed by elementary generator matrices G_i of the codes C_i.

We assume that we have an efficient decoding algorithm for each elementary code C_i. To decode $u = (u_1, ..., u_\gamma)$, we apply for each codeword u_i its correspondent decoding algorithm $dec_{C_i}()$. The decoded word is $m = (m_1, m_2, ..., m_\gamma)$ with $m_i = dec_{C_i}(u_i), \quad i = 1..\gamma$.

We define the support of a non zero word $x = (x_1, x_2..., x_n)$, denoted $supp(x)$, as the set of its non zero positions. $supp(x) = \{i \in \{1, ..., n\} | \quad x_i \neq 0\}$ and the support of a set $S = \{y_1, y_2, ..., y_\gamma\}$ as the union of the supports of its words. $supp(S) = \cup_{y_i \in S, i=1..\gamma} \quad supp(y_i)$. So the support of a code $C(N, K)$ is the union of its 2^K codewords supports.

Two words x and y are said to be connected if their supports are not disjoints i.e $supp(x) \cap supp(y) \neq \oslash$ and two sets I and J are said to be disjoints if there is no connection subset between them.
A non zero codeword x of C is said to be minimal support if there is no codeword $y \in C$ such that $supp(y) \subset supp(x)$.

Two codes $C(N, K)$ and $C'(N, K)$ are said to be equivalents if there is a permutation σ of $\{1, ..., N\}$ such as: $C' = \sigma(C) = \{(c_{\sigma(1)}, ..., c_{\sigma(N)}) | (c_1..., c_N) \in C\}$. In other words, C and C' are equivalents if there is a permutation matrix such as for any generator matrix G of C, the matrix $G' = GP$ is a generator matrix of C'.

III. Chained codes and Cryptography:

As we mentioned in the introduction, the drawback of the unique digital signature scheme based on error coding is the high signature complexity which is due to Goppa decoding algorithm. One idea to counter this drawback consists in replacing Goppa code by chained code which have faster decoding algorithm.

Generally, the secret key of a cryptographic scheme based on error coding is the code itself, for which an efficient decoding algorithm is known, and the public key is a transformation of the generator or parity check matrices.

We consider a digital signature scheme based on chained code, then we develop an algorithm to discover the private

978-0-7695-3838-9/09 $26.00 © 2009 IEEE
DOI 10.1109/NSS.2009.22

key from public key. This attack is applicable for every cryptographic scheme since it is a structural attack.

Secret key	S is a random $(K \times K)$ non singular matrix called the scrambling matrix. G is a $(K \times N)$ generator matrix of a chained code P is a random $(N \times N)$ permutation matrix
Public key	$G' = S.G.P$ is a randomly scrambled et permuted generator matrix. It is a generator matrix of an equivalent non structured code to the chained code. $\sum_i c_i$ is the completed correction capacities calculated as [3]. $h()$ is a hash function
Signature	The signer, first, calculates $y = h(M).P^{-1}$, where $h(M)$ is the N bit message, P^{-1} is the inverse of P. Then he uses the completed decoding algorithm [3] for the original chained code C to obtain $x = S.\sigma$. Finally, the receiver obtains the signature by computing $\sigma = S^{-1}.x$ where S^{-1} is the inverse of S.
Verification	The verifier calculates $\rho' = \sigma.G'$ and $\rho = h(M)$ The signature is valid if $d(\rho, \rho') < \sum_i (c_i)$.

We have introduced a digital signature scheme and then we present the weakness of this scheme. This weakness is due to the fact that chained codes have an invariant. Code equivalence means that one generator matrix is a permutation of the other, because matrix S does not change the code but only performs a modification on the basis of the linear subspace. Canteaut showed that the matrix S may be important to hide the systematic structure of the Goppa codes, therefore having an important security role [4]. However, Heiman was the first to study this point and states that the random matrix S used in the original McEliece scheme serves no security purpose concerning the protection [5]. We confirm this argument and we show that the random matrix S has no security role for cryptographic schemes based on linear codes. We state also that disjoint elementary code supports is an invariant by permutation.

To avoid exhaustive attack, we used at least five different elementary codes and to avoid attack by information set, we used a chained code with length at least equal to 900 bits.

The attack explores the characteristics of the code transformation in order to identify its building blocks. Its input is a generating matrix G' of a randomly permuted chained code of length N and dimension K. Its output is a structured chained code. The algorithm's steps are:

- Apply a Gauss elimination to the rows of the matrix G' to obtain the systematic form $G_0 = (I_d, \quad Z)$.
  Sendrier shows that rows of any systematic generator matrix of a code C are minimal support codewords of C and that any minimal support codeword of C is a row of a systematic generator matrix of C [4].
  The systematic chained code support is formed by disjoint sets. Each set represents the support of an elementary code. The transformation of any randomly permuted chained code generator matrix into a systematic matrix by linear algebraic algorithms will allow us to find these supports and thus elementary codes.
- Search the disjoint sets of rows of the systematic matrix G_0. Each set forms the elementary code support.
- Use elementary decoding algorithms to decode every message.

IV. Results:

The security of cryptographic schemes based on error coding is highly dependent on the class of used codes. Some class of codes reveal their characteristics even when they go through the permutation used to construct the public code. It is the case of chained codes. The starting point was the observation that any systematic matrix is formed by small weight codeword and that chained code contains so many minimal support codewords. These two properties lead to a structural attack of digital signature scheme based on chained code. Figure1 IV shows the complexity of the attack of some cryptosystems using chained codes. The complexity is always less 2^{45} even with so long codes ($N = 3000$). This complexity prohibits using chained code in cryptography.

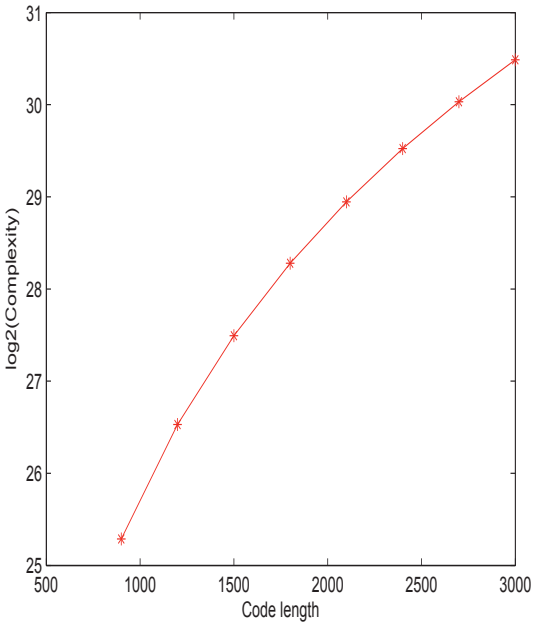

Figure 1. Attack complexity on chained linear codes

V. Conclusion

In this paper, we discussed the structure of a randomly permuted chained code. We explored potential threats from

systematic generator matrix that have particular structure. Chained code generator matrices have the properties of disconnected elementary code supports. This property is invariant by permutation, which make this kind of code useless in cryptography.

REFERENCES

[1] E.R. Berlekamp, R.J. McEliece, and H.C.A. van Tilborg, "On the inherent intractability of certain coding problems", IEEE Transactions on Information Theory, Vol.24, No.3,1978, pp.384-386.

[2] R.J. McEliece, "A public-key cryptosystem based on algebraic coding theory"; DSN Prog. Rep., Jet Propulsion Laboratory, California Inst. Technol., Pasadena, CA, pp. 114-116,January 1978.

[3] N. Courtois, M. Finiasz, and N. Sendrier, "How to achieve a McEliece-based digital signature scheme", In C. Boyd, editor, Asiacrypt 2001, volume 2248 of LNCS, pages 157-174. Springer-Verlag, 2001.

[4] N.Sendrier, "On the structure of a linear code". AAECC, Vol.9, n3, 1998, pp.221-242.

[5] A. Canteaut "Attaques de cryptosystmes mots de poids faible et construction de fonctions t-rsilientes" . PhD thesis, Universit Paris 6, October 1996.

[6] R. Heiman 'On the security of Cryptosystems Based on Linear Error Correcting codes' MSc. Thesis, Feinberg Graduate School of the Weizmann Institute of Science. August 1987.