INFORMATICA, 2002, Vol. 13, No. 1, 105–110

Improving the Information Rate of a Private-key Cryptosystem Based on Product Codes

Hung–Min SUN

Department of Computer Science and Information Engineering
National Cheng Kung University
Tainan, Taiwan 701
e-mail: hmsun@mail.ncku.edu.tw

Received: October 2001

Abstract. Recently, Sun proposed a private-key encryption scheme based on the product codes with the capability of correcting a special type of structured errors. In this paper, we present a novel method to improve the information rate of Sun's scheme. This method uses the added error vector to carry additional information. Some information bits are mapped into an error vector with the special structure to be added to a codeword. Once the error vector can be identified, the additional information can be recovered.

Key words: cryptography, data security, private-key cryptosystem, encryption, product codes.

1. Introduction

A number of private-key cryptosystems based on error-correcting codes have been proposed to protect confidential data over the past few years (Alencar *et al.*, 1993; Campello de Souza, 1994; Rao and Nam, 1987a, 1987b; Sun, 1997). However, most of them were shown to be insecure. For example, the Rao–Nam system (Rao and Nam, 1987a, 1987b) is subjected to some chosen-plaintext attacks (Struik and Tilburg, 1988), Alencar *et al.*'s (1993) scheme and Campello de Souza's (1994) scheme were proven to be insecure against some chosen-plaintext attacks in (Sun and Shieh, 1996). In 1995, J. and R.M. Campello de Souza (1995) proposed a private-key encryption scheme which is based on product codes. The idea of their scheme is to use a product code which is capable of correcting a special kind of structured errors and then disguise it as a code that is only linear. This makes it unable to correct the errors as well as their permuted versions. Recently, Sun (1999) showed that J. and R.M. Campello de Souza's scheme is also insecure against chosen-plaintext attacks, and consequently proposed a secure modified scheme. The modified scheme has the disadvantage that the information rate of the scheme is low. In this paper, we address the issue of improving the information rate of the modified scheme.

2. Preliminaries

DEFINITION 1 (J. and R.M. Campello de Souza, 1995). The direct mapping with parameters r and s, denoted $DM_{r,s}(\cdot)$, is the one that maps the vector $V = (v_1, \ldots, v_{rs})$ into the matrix

$$A = \begin{bmatrix} a_{0,0} & \cdots & a_{0,s-1} \\ \cdots & \cdots & \cdots \\ a_{r-1,0} & \cdots & a_{r-1,s-1} \end{bmatrix}_{r\times s},$$

so that $a_{i,j} = v_{is+j+1}$, for $i = 0, 1, \ldots, r-1$, $j = 0, 1, \ldots, s-1$.

DEFINITION 2 (extension from J. and R.M. Campello de Souza, 1995). The vector $E = (e_1, \ldots, e_{rs})$, $e_i \in$ the congruence class modulo 2^t, where $t \geqslant 1$, is said to be a biseparable error, denoted *BSE*(r, s), if (i) its nonzero components are distinct elements in the congruence class modulo 2^t; and (ii) each row and each column of $DM_{r,s}(E)$ contains, at most, one nonzero component.

Theorem 1 (extension from J. and R.M. Campello de Souza, 1995). *A product code PC $(n = (r+1)(s+1)$, $k = rs$, $d = 4)$ in the congruence class modulo 2^t, whose constituent row and column codes are single parity-check codes $C_1(n_1 = r+1$, $k_1 = r$, $d_1 = 2)$ and C_2 $(n_2 = s+1$, $k_2 = s$, $d_2 = 2)$ respectively, can correct a BSE $(r+1, s+1)$ of weight up to $w_{\max}$, where $w_{\max} = \min(2^t - 1, \min(r+1, s+1))$.*

Sun's private-key cryptosystem (Sun, 1999)

Secret key: G is the generator matrix of a PC $(n = (r+1)(s+1)$, $k = rs$, $d = 4)$ in the congruence class modulo 2^t. S is a random binary $(nt) \times (kt)$ matrix, called the scrambling matrix, and P is an $(nt) \times (nt)$ permutation matrix.

Encryption: Let the plaintext M be a binary kt-tuple. That is, $M = (m_1, \ldots, m_{kt})$, where $m_i \in GF(2)$.The ciphertext C is calculated by the sender: $C = \{[M \oplus (E \otimes S)] \cdot G + E\} \otimes P$, where E is a $BSE(r+1, s+1)$ of weight w, $1 \leqslant w \leqslant \min(2^t - 1, \min(r+1, s+1))$. Here we use $\oplus$ and $\otimes$ to denote the XOR operation and the matrix multiplication operation in $GF(2)$, and $+$ and $\cdot$ to denote the vector addition operation and the matrix multiplication operation in the congruence class modulo 2^t. When $\oplus$ and $\otimes$ operations are executed, every bit is regarded as a number in $GF(2)$. When $+$ and $\cdot$ operations are executed, every t-bits is regarded as a number in the congruence class modulo 2^t.

Decryption: The receiver first calculates $C' = C \otimes P^{-1} = M' \cdot G + E$, where $M' = [M \oplus (E \otimes S)]$ and P^{-1} is the inverse of P. Secondly, by using the decoding algorithm of the product code G, the receiver can find and remove the error E embedded in C' to obtain M'. At last, the receiver recovers M by computing $M' \oplus (E \otimes S) = M$.

It is clear that the information rate of this scheme is $\frac{k}{n} = \frac{rs}{(r+1)(s+1)}$.

3. Improving the Information Rate

We can use the added error vector E to carry an additional message block. That is, some additional information bits are mapped into an error vector to be added in the encryption phase. Once the error vector can be identified, the additional message block can be recovered. Therefore, we need a mapping function f such that $f(M')$ is a biseparable error E, and it is easy to compute M' from a given $f(M')$, where M' denotes the additional message block.

For simplicity, we assume that Sun's scheme uses the parameters r, s, and t such that $r = s$, $2^t - 1 \geqslant r + 1$, and E is a $BSE(r+1, r+1)$ of weight $r+1$. Therefore, E depends on which $r+1$ elements are chosen from $\{1, \ldots, 2^t - 1\}$ and which positions of these $r+1$ elements are located in E. The total number of possible combinations for $r+1$ elements chosen from $2^t - 1$ elements is $C_{r+1}^{2^t-1}$. So the amount of information to represent these $C_{r+1}^{2^t-1}$ combinations is $\left\lfloor \log_2 C_{r+1}^{2^t-1} \right\rfloor$. Once these $r+1$ elements are determined, we need to specify the positions of these $r+1$ elements. Because E is a $BSE(r+1, r+1)$ of weight $r+1$, each row (each column) of $DM_{r+1,r+1}(E)$ exactly contains one element of the chosen $r+1$ elements. There are totally $(r+1)!$ possible choices for selecting $r+1$ positions in $DM_{r+1,r+1}(E)$. So the amount of information to represent these $(r+1)!$ choices is $\lfloor \log_2 (r+1)! \rfloor$. In addition, for each choice, there are $(r+1)!$ possible methods to put the chosen $r+1$ elements into the chosen $r+1$ positions in $DM_{r+1,r+1}(E)$. Therefore, the amount of information to represent these $(r+1)!$ methods is $\lfloor \log_2 (r+1)! \rfloor$.

From the above discussion, it is clear that we can carry an additional message block with the length of $\left\lfloor \log_2 C_{r+1}^{2^t-1} \right\rfloor + 2 \lfloor \log_2 (r+1)! \rfloor$ by specifying the error vector E. Thus the information rate of Sun's scheme can be significantly improved. In Table 1, we show the comparison of the information rate between the original scheme and the improved scheme.

In the following, we show how to specify $r+1$ elements from $2^t - 1$ elements by using $\left\lfloor \log_2 C_{r+1}^{2^t-1} \right\rfloor$ information bits. We can use a binary vector of length $(2^t - 1)$ with

Table 1

The comparison of the information rate between the original scheme and the improved scheme, where ‘O’ and ‘N’ denote the original scheme and the improved scheme respectively

t	r	s	Ciphertext	Plaintext(O)	Plaintext(N)	Info. Rate. (O)	Info. Rate. (N)
3	5	5	108 bits	75 bits	95 bits	0.694	0.880
3	6	6	147 bits	108 bits	132 bits	0.735	0.898
4	7	7	256 bits	196 bits	238 bits	0.766	0.930
4	8	8	324 bits	256 bits	304 bits	0.790	0.938

weight $r+1$ to denote those $r+1$ elements out of 2^t-1 elements. Therefore, we need a simple mapping method to transform between $\left\lfloor \log_2 C_{r+1}^{2^t-1} \right\rfloor$-bit and the vector of length (2^t-1) with weight $r+1$. There have been a number of methods proposed to address this problem. The interested reader is referred to (Lin and Fu, 1990; Park, 1989; Sendrier, 1995).

In the following, we show how to specify $r+1$ positions for a biseparable error in $DM_{r+1,r+1}(E)$ by using $\lfloor \log_2 (r+1)! \rfloor$ information bits. We can use a permutation $\{p_1, \ldots, p_{r+1}\}$ of $\{1, \ldots, r+1\}$ to denote these $r+1$ positions which are the (1, p_1)$-$entry, the $(2, p_2)$-entry, …, and the $(r{+}1, p_{r+1})$-entry in the matrix $DM_{r+1,r+1}(E)$. Therefore, we need a simple mapping method to transform between $\lfloor \log_2 (r+1)! \rfloor$-bit and the permutation $\{p_1, \ldots, p_{r+1}\}$ of $\{1, \ldots, r+1\}$.

Here we regard each $\lfloor \log_2 (r+1)! \rfloor$-bit information as a number x.

Algorithm for transforming a number x into a permutation of $\{1, \ldots, r+1\}$:

```
Input: a number $x$.
Output: $S = \{p_1, \ldots, p_{r+1}\}$ which is a permutation of $\{1, \ldots, r+1\}$.
Initial: $T = \{1, \ldots, r+1\}$;
For $i = r, r-1, \ldots, 0$;
{   $j = \lfloor x/i! \rfloor$ ;
    $p_{r+1-i}$ – the $(j+1)$-th item in $T$.
    Delete the $(j+1)$-th item in $T$, and sort $T$ again;
$x = x - j \cdot i!$;
}
```

EXAMPLE. Let $r = 6$ and $x = 010100110011_2 = 1331$. Then the corresponding permutation is (2, 7, 1, 4, 6, 5, 3).

Algorithm for transforming a permutation $\{p_1, \ldots, p_{r+1}\}$ into a number x:

```
Input: $S = \{p_1, \ldots, p_{r+1}\}$.
Output: a number $x$.
Initial: $T = \{1, \ldots, r+1\}, x = 0$.
For $i = 1, \ldots, r+1$;
{ Find the position of $p_i$ in $T$ (we assume $p_i$ is the $j$-th item in $T$);
    $x = x + (j-1) \cdot (r+1-i)!$.
    Delete the $j$-th item in $T$, and sort $T$ again.
}
```

EXAMPLE. Let $r = 6$ and the permutation be (2, 7, 1, 4, 6, 5, 3). Then $x = 1*6! + 5*5! + 0*4! + 1*3! + 2*2! + 1*1! + 0*0! = 720 + 600 + 6 + 4 + 1 = 1331 = 010100110011_2$.

Similarly, specifying the chosen $r+1$ elements into the chosen $r+1$ positions in $DM_{r+1,r+1}(E)$ can be done as the above method by using $\lfloor \log_2 (r+1)! \rfloor$ information bits.

4. Conclusions

In this paper, we have proposed a method to improve the information rate of Sun's private-key cryptosystem based on product codes. By using the proposed method, the information rate of Sun's scheme can be up to around 0.9 or more.

References

Alencar, M.R., A.M.P. Léo, R.M. Campello de Souza (1993). Private-key burst correcting code encryption. In *Proc. of the 1993 IEEE Int. Symp. Information Theory*.

Campello de Souza, J., R.M. Campello de Souza (1995). Product codes and private-key encryption. In *Proc. of the 1995 IEEE Int. Symp. Information Theory*.

Campello de Souza, R.M., J. Campello de Souza (1994). Array codes for private-key encryption. *Electronics Letters*, **30**(17), 1394–1396.

Lin, M.C., H.L. Fu (1990). Information rate of McEliece's public-key cryptosystem. *Electronics Letters*, **26**(1), 16–18.

Park, C.S. (1989). Improving code rate of McEliece's public-key cryptosystem. *Electronics Letters*, **25**(21), 1466–1467.

Rao, T.R.N., K.H. Nam (1987a). Private-key algebraic-coded cryptosystems. In *Advances in Cryptology–CRYPTO'86, Lecture Notes in Computer Science*. Springer–Verlag. pp. 35–48.

Rao, T.R.N., K.H. Nam (1987b). Private-key algebraic-code encryption. *IEEE Trans. on Information Theory*, **35**(4), 829–833.

Sendrier, N. (1995). Efficient generation of binary words of given weight. In *Cryptography and Coding: 5th IMA Conference*. Springer–Verlag. pp. 184–187.

Struik, R., J. Tilburg (1988). The Rao–Nam scheme is insecure against a chosen-plaintext attack. In *Advances in Cryptology–CRYPTO'87, Lecture notes in computer science*. Springer–Verlag. pp. 445–457.

Sun, H.M. (1997). Private-key cryptosystems based on burst-error-correcting codes. *Electronics Letters*, **33**(24), 2035–2036.

Sun, H.M. (1999). On Private-key Encryption Using Product Codes. *Computers & Electrical Engineering*, **25**(6), 439–450.

Sun, H.M., S.P. Shieh (1996). Cryptanalysis of private-key encryption schemes based on burst-error-correcting codes. In *Proc. Third ACM Conference on Computer and Communications Security*. ACM Press. pp. 153–156.

H.–M. Sun received his B.S. degree in applied mathematics from National Chung–Hsing University in 1988, his M.S. degree in applied mathematics from National Cheng Kung University in 1990, and his Ph. D. degree in computer science and information engineering from National Chiao–Tung University in 1995, respectively. He was an associate professor with the Department of Information Management, Chaoyang University of Technology from 1995 to 1999. Currently he is an associate professor with the Department of Computer Science and Information Engineering, National Cheng Kung University. He has published over seventy papers. He was the program chair of 2001 National Information Security Conference and the program committee member of 1997 Information Security Conference, 2000 Workshop on Internet & Distributed Systems, Workshop on the 21st Century Digital Life and Internet Technologies, 1998 and 1999 National Conference on Information Security. His research interests include cryptography, information theory, network security, image compression.

Informacijos perdavimo greičio pagerinimas slaptažodžio kodavime

Hung–Min SUN

Ankstesniuose Sun darbuose pasiūlyta asmens slaptažodžio kodavimo schema grindžiama kodu su galimybe koreguoti specialaus tipo struktūrines klaidas. Šiame straipsnyje autorius pateikia naują metodą, kaip pagreitinantį informacijos perdavimo greitį Sun schemoje. Metodas naudoja klaidos vektorių, nesantį papildoma informacija. Keli informacijos bitai yra atvaizduojami į klaidos vektorių, o priėmus pranešimą – vėl atskiriami.