Yang SHI, Guoyue XIONG
Tongji University

An Asymmetric Multi-Recipient Encryption Scheme

Abstract. *Multi-recipient encryption schemes have many advantages such as high efficiency, low network cost, and flexible object control. An asymmetric multi-recipient encryption scheme with indistinguishability under chosen-ciphertext attack is proposed. The encryption scheme uses an eighth order linear feedback shift register. The main features of this scheme are small size of ciphertext and the overall data communication is also smaller than other asymmetric multi-recipient encryption schemes, hence it is suitable for using in networks of low bandwidth.*

Streszczenie. *W artykule przedstawiono, odporny na ataki sposób szyfrowania asymetrycznego dla wielu odbiorników. Wykorzystany został rejestr przesuwny ze sprzężeniem liniowym ósmego rzędu. Głównymi zaletami algorytmu jest mały rozmiar klucza i mniejsza ilość danych do komunikacji. Szyfrowanie można także wykorzystać w sieciach o małej przepustowości. (**Schemat szyfrowania asymetrycznego dla wielu odbiorców**).*

Keywords: asymmetric encryption, multi-recipient, confidentiality
Słowa kluczowe: szyfrowanie asymetryczne, wielu odbiorców, tajność.

Introduction

Encryption is the most widely used approach to obtain privacy and confidentiality. Multi-recipient encryption is a technology to encrypt messages for several recipients. Multi-recipient encryption schemes have many advantages such as high efficiency, low network cost, and flexible object control.

In order to find an encryption scheme suitable for using in networks of low bandwidth, this paper is aimed at providing an asymmetric multi-recipient encryption scheme with following features:

(1) The size of encryption key is small.
(2) The size of decryption key is small.
(3) The size of ciphertext is small.

With above features, this scheme can be used in applications of relative low network bandwidth such as mobile commerce and so on.

Multi-Recipient Asymmetric Encryption Schemes

An asymmetric multi-recipient encryption scheme $\overline{AE}=\left(CKGen,KGen,\overline{Enc},Dec\right)$ consists of four algorithms [2][3]:

Common-key generation algorithm $CKGen$ takes as input a security parameter $k\in N$ and outputs the common key I in polynomial time $\mathrm{ploy}(k)$. The algorithm is probabilistic.

Key generation algorithm $KGen$ takes as input the common key I and outputs a pair of keys (pk,sk) in polynomial time $\mathrm{ploy}(k)$. The algorithm is probabilistic.

Multi-encryption algorithm $\overline{Enc}$ takes input a public-key vector $pk=(pk[1],\cdots,pk[n])$ and a plaintext vector $M=(M[1],\cdots,M[n])$ and returns a ciphertext vector $C=(C[1],\cdots,C[n])$ in polynomial time $\mathrm{ploy}(k)$. The algorithm is probabilistic.

Decryption algorithm Dec takes as input a private key sk and a ciphertext C, and outputs a message M or a special symbol $\perp$ denoting failure in polynomial time $\mathrm{ploy}(k)$. The algorithm is typically deterministic.

It's clear that the design and analyze of $\overline{Enc}$ are key points of research.

Let $\overline{AE}=\left(CKGen,KGen,\overline{Enc},Dec\right)$ be an asymmetric MRES. Let B be an adversary attacking $\overline{AE}$. B runs the attack experiment $\mathrm{Exp}^{\text{mr-atk-b}}_{\overline{AE},B,n(\cdot)}(k)$ in the following three stages [3][4].

(1) The select stage.
(2) The find stage.
(3) The guess stage.

If atk=cpa ,then $O_i(\cdot)=Enc$ and if atk=cca then $O_i(\cdot)=Dec_{sk_i}(\cdot)$.

The steps of $\mathrm{Exp}^{\text{mr-atk-b}}_{\overline{AE},B,n(\cdot)}(k)$ are as follow:

$$I\overset{\$}{\leftarrow}CKGen\left(1^k\right);\quad \left(1^l,st\right)\overset{\$}{\leftarrow}B\left(select,n(k),I\right)$$

Where $1\le l\le n(k)$

$$\left(pk[i],sk[i]\right)\overset{\$}{\leftarrow}KGen(I),i=1,\cdots,l$$

$$\left(M_0,M_1,M,\mathrm{coins},st\right)\overset{\$}{\leftarrow}B^{O_1(\cdot),\cdots,O_l(\cdot)}\left(find,pk,st\right)$$

Where:

$$|M_0|=|M_1|=l;|M|=n(k)-l;$$

$$|\mathrm{coins}|=n(k)-l;|pk|=l$$

$$\left(pk'[i],sk'[i]\right)\overset{\$}{\leftarrow}KGen\left(I,\mathrm{coins}[i]\right),$$

$$i=1,\cdots,n(k)-l$$

$$pk\leftarrow\left(pk[1],\cdots,pk[l],pk'[l+1],\cdots,pk'[n(k)]\right)$$

$$M\leftarrow\left(M_b[1],\cdots,M_b[l],M[1],\cdots,M[n(k)-l]\right)$$

$$C\overset{\$}{\leftarrow}\overline{Enc}_{I,pk}(M)$$

$$d\overset{\$}{\leftarrow}B^{O_1(\cdot),\cdots,O_l(\cdot)}(\mathrm{guess},C,st)$$

The ind-atk advantage of an adversary B is [3][4]:

$$\mathrm{Adv}^{\text{mr-atk}}_{\overline{AE},B,n(\cdot)}(k)$$

$$=\Pr\left[\mathrm{Exp}^{\text{mr-atk-0}}_{\overline{AE},B,n(\cdot)}(k)=0\right]-\Pr\left[\mathrm{Exp}^{\text{mr-atk-1}}_{\overline{AE},B,n(\cdot)}(k)=0\right]$$

We say that $\overline{AE}$ is IND-CPA (resp. IND-CCA) secure if the function $\mathrm{Adv}^{\text{mr-cpa}}_{\overline{AE},B,n(\cdot)}(\cdot)$ (respectively $\mathrm{Adv}^{\text{mr-cca}}_{\overline{AE},B,n(\cdot)}(\cdot)$) is negligible for any RPTA(randomized, polynomial-time algorithm) B and any polynomial $n(\cdot)$.

A New Multi-Recipient Asymmetric Encryption Scheme

A linear feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state.

Let $d_n = \sum_{i=1}^{8} h_i^{\,n} = \sum_{i=1}^{8} \left(g^{np^{i-1}} \right)$ and $Tr\left(g^n \right) = d_n$.

The coefficients of the LFSR used in this scheme is defined in table 1.

Table 1. Coefficients of the LFSR

Notation	Definition
$\sigma_{1,n}$	d_n
$\sigma_{2,n}$	$\left(2^{-1} \bmod p\right)\left(d_n{}^2 - d_{2n}\right)$
$\sigma_{3,n}$	$\left(6^{-1} \bmod p\right)\left(d_n{}^3 - 3d_n d_{2n} + 2d_{3n}\right)$
$\sigma_{4,n}$	$\left(24^{-1} \bmod p\right)\times\left(d_n{}^4 + 3d_{2n}{}^2 - 6d_n{}^2 d_{2n} + 5d_n d_{3n} - 6d_{4n}\right)$

It can be proved that the 8-th order LFSR defined in table 3 has the following property:

$$d_{n+4} = \sigma_{1,n} d_{n+3} - \sigma_{2,n} d_{n+2} + \sigma_{3,n} d_{n+1} - \sigma_{4,n} d_n$$
$$+\sigma_{3,n} d_{n-1} - \sigma_{2,n} d_{n-2} + \sigma_{1,n} d_{n-3} - d_{n-4}$$

Let $S_n(d) = \left\langle d_{n-3}, d_{n-2}, d_{n-1}, d_n, d_{n+1}, d_{n+2}, d_{n+3}, d_{n+4} \right\rangle$

The new multi-recipient asymmetric encryption scheme is based on a public key cryptosystem proposed in **Błąd! Nie można odnaleźć źródła odwołania.**.

Suppose p and q are big prime numbers and $q \left| p^4 + 1, q \nmid p^i - 1, i = 1, 2, \cdots, 7 \right.$. Let $L = \left(p^4 + 1 \right) / q$ and $k = \left(p^4 - 1 \right) L$, then $kq = \left(p^8 - 1 \right)$. Randomly pickup $a \overset{\$}{\leftarrow} GF\left(p^8 \right) - \{0,1\}$ and let $g = a^k$.

Its common-key generation algorithm is

$$\left\langle p, q, g \right\rangle \overset{\$}{\leftarrow} LFSR\_CKGen\left(1^k\right)$$

The key generation algorithm $LFSR\_KG$ and the decryption algorithm $LFSR\_Dec$ are same as in **Błąd! Nie można odnaleźć źródła odwołania.**. The original encryption algorithm in **Błąd! Nie można odnaleźć źródła odwołania.** is denoted as $C = \left\langle r, c, v \right\rangle \overset{\$}{\leftarrow} LFSR\_Enc\left(p, q, g, R_x(d) \right)$ in this paper.

Suppose that there are n recipients and their public keys are $R_i(d), i = 1, \cdots, n$. The multi-recipient asymmetric encryption algorithm $\overline{LFSR\_Enc}$ is as following:

$s \overset{\$}{\leftarrow} Z_q^*$

$r \leftarrow R_s(d) = \left(d_s^0, d_s, d_{2s}, d_{3s}, d_{4s} \right)$

For $i = 1, \cdots, n$ **do**

$d_{si} \leftarrow \mathrm{Alg}_{8L-2}\left(p, q, g, s, R_i(d) \right)$

$\left\langle K_{1,i}, K_{2,i} \right\rangle \leftarrow KDF\left(d_s, d_{si} \right)$

$c[i] \leftarrow \mathrm{Alg}_{SymEnc}\left(K_{1,i}, M[i] \right)$

$v[i] \leftarrow MAC\left(K_{2,i}, c[i] \right)$

End For

$c \leftarrow \left\langle c[1], \cdots, c[n] \right\rangle$

$v \leftarrow \left\langle v[1], \cdots, v[n] \right\rangle$

Return $\left\langle r, c, v \right\rangle$

Alg_{8L-2} is the algorithm for computing the trace function. Alg_{SymEnc} is a symmetric encryption algorithm with key length of b_1. $MAC : \{0,1\}^{b_2} \times GF\left(p^8 \right) \to \{0,1\}^{b_3}$ is the algorithm for computing message authencation codes. $KDF : GF(p)^2 \to \{0,1\}^{b_1 + b_2}$ is a derived function from a cipherkey linked up with hash functions. Details of these algorithms are given in **Błąd! Nie można odnaleźć źródła odwołania.**, we reuse them to construct the new multi-recipient asymmetric encryption algorithm。

Security Proof

In order to prove the security of the scheme,the reproducibility test should be performed. First several steps of the test $\mathrm{Exp}^{\mathrm{repr}}_{LFSR\_Enc,R}(k)$ are as follows：

$$\left\langle p, q, g \right\rangle \overset{\$}{\leftarrow} LFSR\_CKGen\left(1^k\right)$$

$$\left\langle R_x(d), x \right\rangle \overset{\$}{\leftarrow} LFSR\_KG\left(p, q, g \right)$$

$$\left\langle R_y(d), y \right\rangle \overset{\$}{\leftarrow} LFSR\_KG\left(p, q, g \right)$$

$$M \overset{\$}{\leftarrow} MsgSp\left(p, q, g \right)$$

$$M' \overset{\$}{\leftarrow} MsgSp\left(p, q, g \right)$$

$$s \overset{\$}{\leftarrow} Z_q^*$$

$$C = \left\langle r, c, v \right\rangle \overset{\$}{\leftarrow} LFSR\_Enc_{\langle p,q,g \rangle, R_x(d)}\left(M, s \right)$$

Then the ciphertext C' can be computed by using the following reproduce algorithm R.

$r' = R_s(d) \leftarrow r$

$d_{sy} \leftarrow \mathrm{Alg}_{8L-2}\left(p, q, g, y, R_s(d) \right)$

Extracts d_s from $r' = R_s(d) = \left(d_s^0, d_s, d_{2s}, d_{3s}, d_{4s} \right)$

$\left\langle K_1', K_2' \right\rangle \leftarrow KDF\left(d_s, d_{sy} \right)$

$c' \leftarrow \mathrm{Alg}_{SymEnc}\left(K_1', M' \right)$

$v' \leftarrow MAC\left(K_2', c' \right)$

$C' \leftarrow \left\langle r', c', v' \right\rangle$

With the help of the randomized polynomial-time algorithm R, the test $\mathrm{Exp}^{\mathrm{repr}}_{\overline{LFSR\_Enc},R}(k)$ outputs 1 with probability 1. So the algorithm $LFSR\_Enc$ is reproducable. According to theorem 6.2 of [3], for any randomized polynomial time algorithm B_{CCA}, there exists a randomized polynomial time algorithm A_{CCA} such that for any k:

$$\mathrm{Adv}^{\mathrm{mr\text{-}CCA}}_{\overline{LSFR\_Enc},B_{\mathrm{CCA}},n(\cdot)}(k) \le n(k)\,\mathrm{Adv}^{\mathrm{CCA}}_{LSFR\_Enc,A_{\mathrm{CCA}}}(k)$$

According to proposition 5 of **Błąd! Nie można odnaleźć źródła odwołania.**, if:

(1) The symmetry encryption algorithm and the message authentication code algorithm MAC are secure.

(2) Extracting n from $Tr\left(g^n \right) = d_n \in GF(p)^*$ is computational infeasible.

(3) KDF is a stochastic functio.

Then the public key encryption scheme corresponds to $LFSR\_Enc$ is IND-CCA. Hence the proposed scheme is IND-CCA under the same assumptions.

Scheme analyze

A most important purpose of this scheme is to archive small size of ciphertext and small overall data communication, so here we will focus on the sizes of ciphertext and keys.

Suppose the length of prime number p is l bits, the length of public key of the base algorithm is $3+4l$ bits, the length of plain text is $8l$ bits. Suppose the cipher text is $C=\langle r,c,v\rangle$, then the length of r is $3+4l$ bits, the length of c is $8l$ bits. If the length of v is b bits, then the message expansion rate is $(12l+(b+3))/(8l)$. If b is much smaller than l, then the expansion rate is nearly 1.5. If there are n recipients, the length of cipher text of $\overline{LFSR\_Enc}$ is $(3+4l)+n(8l+b)$, it is only $((3+4l)+n(8l+b))/n(12l+b+3)$ of the length of using $LFSR\_Enc$ n times. If n is not too small and b is much smaller than l, $((3+4l)+n(8l+b))/n(12l+b+3)\approx 2/3$.

Furthermore, if there are n recipients, compared to using $LFSR\_Enc$ n times, the proposed scheme need only 1 time of random number generation $s\overset{\$}{\leftarrow}Z_q^*$ instead of n times. $r\leftarrow R_s(d)$ also only need 1 time instead of n times. Thus, the proposed scheme is more efficiency.

Compared to relative works

Hiwatari et al. concluded parameters of a series of multi-recipient public-key encryption schemes based on randomness reusing in 2009 [6]. Their conclusion is converted into a comparable form in table 2. "-RR" means randomness reusing.

Table 2. Comparison of size

scheme	pk	sk	ciphertext
[1]-RR	24 l	40 l	2n*8 l
[7] -RR	16 l	32 l	2*8 l + n b + n|ske|
[8] -RR	24 l	24 l	n*8 l + n|ske|
[9] -RR	16 l	16 l	n*8 l + n b + n|ske|
[10] -RR	16 l	24 l	n*8 l + b
[11] -RR	32 l	32 l	2n*8 l + n|ske|
[12] -RR	24 l	24 l	n*8 l + n b + n|ske|
This paper	4 l +3	l	n*8 l + n b

It is shown in table 2 that the size of ciphertext of the proposed scheme is smaller than other schemes except [10]-RR. Furthermore, in table 2, the size of public key of the proposed scheme is the smallest one of all those schemes, and the size of private key of the proposed scheme is also the smallest one of all those schemes.

Conclusion

As a most important approach to obtain privacy and confidentiality, encryption is widely used in modern information systems. Multi-recipient encryption is a technology to encrypt messages for several recipients. An asymmetric multi-recipient encryption scheme with indistinguishability under chosen-ciphertext attack is proposed. The encryption scheme is constructed on an eighth order linear feedback shift register. Compare to traditional single-recipient encryption schemes, multi-recipient encryption schemes have many advantages such as higher efficiency, lower network cost and more flexible object control. A complete security proof for the proposed scheme is provided. In the proof, we not only consider outsider attacks, meaning the adversary was not one of the receivers, but also consider insider attacks, meaning the adversary may be allowed to corrupt some fraction of the users and choose secret and public keys for them.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (No. 61202382, 71071114) .

REFERENCES

[1] Cramer R., Shoup V., Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack, SIAM J. Computing, Vol. 33, No.1, 2003, pp.167-226

[2] Bellare M., Boldyreva A., Micali S., Publickey Encryption in a Multi-User Setting: Security Proofs and Improvements, Eurocrypt 2000, LNCS 1807, Springer-Verlag, 2000, pp.259-274

[3] Bellare M., Boldyreva A., Pointcheval D., Multi-Recipient Encryption Schemes: Security Notions and Randomness Re-Use, PKC 2003, LNCS 2567, Springer-Verlag, 2003, pp.85-99.

[4] Bellare M., Boldyreva A., Kurosawa K., Staddon J., Multi-recipient encryption schemes: efficient constructions and their security, IEEE Trans. Inform. Theory, Vol. 53, No. 11, 2007, pp.3927-3943

[5] Ze-hui W., The Provable Security PublicKey Cryptosystem Based on8-th Order LFSR Sequence(In Chinese), ACTA SCIENTIARUM NATURALIUM UNIVERSITATIS SUNYATSEN, Vol. 47, No. 5, 2008, pp28-32

[6] Harunaga H., Keisuke T., Tomoyuki A., Koichi S., Multi-recipient Public-Key Encryption from Simulators in Security Proofs, Lecture Notes in Computer Science, Vol. 5594, 2009, pp.293-308

[7] Kurosawa, K., Desmedt, Y., A new paradigm of hybrid encryption scheme. In: Franklin, M.K. (ed.) CRYPTO 2004, LNCS, Vol. 3152, Springer, Heidelberg , 2004, pp. 426-442

[8] Boyen, X., Mei, Q., Waters, B., Direct chosen ciphertext security from identitybased techniques. In: Atluri, V., Meadows, C., Juels, A. (eds.) ACM Conference on Computer and Communications Security, ACM, New York, 2005, pp. 320–329

[9] Kiltz, E., Chosen-ciphertext secure key-encapsulation based on gap hashed Diffie-Hellman. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, Vol. 4450, Springer, Heidelberg ,2007, pp. 282–297

[10] Hofheinz, D., Kiltz, E., Secure hybrid encryption from weakened key encapsulation, Cryptology ePrint Archive, Report 2007/288, 2007, http://eprint.iacr.org/

[11] Cash, D., Kiltz, E., Shoup, V., The twin Diffie-Hellman problem and applications. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, Vol. 4965, Springer, Heidelberg ,2008, pp. 127–145

[12] Hanaoka, G., Kurosawa, K., Efficient chosen ciphertext secure public key encryption under the computational Diffie-Hellman assumption. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, Vol. 5350, Springer, Heidelberg, 2008, pp. 308–325

***Authors**: Dr. Yang SHI, School of Software Engineering, Tongji University, Sipin Rd. No.1239, 200092, Shanghai, China, E-mail: shiyang@tongji.edu.cn; Dr. Guoyue XIONG (correspondence author), School of Economics and Management, Tongji University, Sipin Rd. No.1239, 200092, Shanghai, China, E-mail: xiongguoyue@tongji.edu.cn;*