Post-quantum Secure Hybrid Ring Signcryption Scheme from Lattice Assumption

WANG Chunxiao[1, 2,a], Wang Fenghe [1,b]

[1] Deptment of Mathematics and physics. Shandong Jianzhu University, Jinan 250101, China

[2]College of Engineering, Qufu Normal University, Rizhao 276800, China

[a]xiao2166@126.com, [b]fenghe2166@163.com

Keywords: Ring signcryption, Signcryption tag-KEM, Lattice cryptography, Learning with errors problem, Short integer solution.

Abstract. The signcryption tag-KEM/DEM construction is naturally extended to the ring signcryption in this paper. The security model of hybrid ring signcryption which is constructed by ring signcryption tag-KEM/DEM is given in this paper. A hybrid ring signcryption from lattice theory is proposed which satisfies anonymity and identity authenticity. Moreover, based on the hardness of the learning with errors problem and the short integer solution problem, confidentiality and unforgeability of the proposed scheme is proven in the random oracles model.

1. Introduction

Signcryption concept was first proposed by Zheng [1] in 1997. Since then, a lot of new signcryption schemes [2-6] have been proposed. Ring signcryption scheme is proposed by combining the conceptions of ring signature and signcryption together which provides not only confidentiality and authenticity but also the anonymity of the sender. However, the identity authenticity of the actual signer may be important in practical applications [7-9]. To achieve identity authenticity in a different way, we make a natural extension from signcryption tag-KEM [6] to ring signcryption tag-KEM. And we also show how to build a hybrid ring signcryption scheme over lattice. In our proposed scheme, an actual signer can prove that he has generated the ciphertext by providing the symmetric key of the symmetric algorithm. Because that, besides the receiver, only the actual user knows the symmetric key of the symmetric algorithm.

Our work

Our main work is described as follows:

1. We adapt the signcryption tag-KEM + signcryption DEM construction [6] to the ring signcryption.
2. We extend the concept of ring signcryption to lattice-based cryptography[10-15] and build a hybrid ring signcryption scheme using lattice cryptographic tools. We also prove that the proposed hybrid ring signcryption scheme satisfies confidentiality, unforgeability, anonymity and identity authenticity.

2.Preliminaries

2.1. Lattice and Lattice Problem

Let $\mathbf{B}=\{\mathbf{b}_1,\mathbf{b}_2,\cdots\mathbf{b}_n\}\subset R^n$ be a set of n linearly independent vectors. The n-dimensional lattice generated by **B** is $\Lambda=\{\mathbf{Bc}=\sum_{i\in[n]}c_1\mathbf{b}_1+c_2\mathbf{b}_2+\cdots+c_n\mathbf{b}_n,c_i\in Z_q\}$, where **B** acts as a basis for this lattice. For a prime q and a vector $\mathbf{y}\in Z_q^n$, two special lattices are defined as follows: $\Lambda_q^{\perp}(\mathbf{A})=\{\mathbf{x}\in Z_q^m:\mathbf{Ax}=\mathbf{0}(\bmod q)\}$ and $\Lambda_q^{y}(\mathbf{A})=\{\mathbf{x}\in Z_q^m:\mathbf{Ax}=\mathbf{y}(\bmod q)\}$.

Definition 1 (SIS Problem). For parameters (*n*, *m*, *q*), $\mathbf{A}\in Z_q^{n\times m}$, and a real number *β*, the SIS problem is defined to find a nonzero vector $\mathbf{v}\in Z_q^m$ satisfies **Av**=0 (mod*q*) and $\|\mathbf{v}\|<\beta$ [10,12].

Definition 2 (LWE Problem). For (*n*, *m*, *q*), $\mathbf{s}\in Z_q^n$ and χ is an error distribution over Z_q^m. Let $\mathrm{A}_{s,\chi}$ be a distribution obtained from $\{\mathbf{A},(\mathbf{A}^T\mathbf{s}+\mathbf{x})(\mathrm{mod}\,q)\}\in Z_q^{n\times m}\times Z_q{}^m$ where $\mathbf{A}\in Z_q^{n\times m}$ is chosen uniformly and randomly and errors vector **x** is chosen according to distribution *χ*. The LWE problem is defined as follows: Given a sample from $\mathrm{A}_{s,\chi}$, output $\mathbf{s}\in Z_q^n$ with noticeable probability. The decision variant of the LWE problem is to distinguish $\mathrm{A}_{s,\chi}$ from the uniform distribution over $Z_q^{n\times m}\times Z_q{}^m$.

2.3. Some Results on Lattice

We recall some main results in lattice cryptography as the following Propositions.

Proposition 1 (PSF) [10].

Let *n, m, q* be positive integers so that *q*=*poly*(*n*) and *m*>5*n*log*q*. There exists a probabilistic polynomial-time (PPT) algorithm SamplePre such that on input (**A**, **T**, **y**, **s**), where $\mathbf{A}\in Z_q^{n\times m}$ and $\mathbf{y}\in Z_q^n$, T is a basis of $\Lambda_q^{\perp}(\mathbf{A})$, an integer $s\geq\|\tilde{\mathbf{T}}\|\cdot\omega(\sqrt{\log m})$ ($\tilde{\mathbf{T}}$ denotes **T**'s the Gram-Schmidt orthogonalization), outputs **e** which satisfies **Ae**=**y**(mod*q*). Furthermore, the distribution of **e** is within negligible statistical distance of $\mathrm{D}_{\Lambda_q^{y}(\mathbf{A}),s,0}$. Moreover, with overwhelming probability, $\|\mathbf{e}\|\leq s\sqrt{m}$.

Proposition 2 (Trapdoor sampling algorithm) [14].

For any prime *q*=*poly*(*n*) and *m*>5*n*log*q*, there is a PPT algorithm that, on input 1^n, outputs a matrix $\mathbf{A}\in Z_q^{n\times m}$, and $\mathbf{S}\subset\Lambda_q^{\perp}(A)$, where the distribution of **A** is statistically close to the uniform distribution over $Z_q^{n\times m}$ and $\|\boldsymbol{S}\|\leq O(\sqrt{n\lg q})$. Moreover, **S** can be efficiently converted to a "short" basis **T** of $\Lambda^{\perp}(A)$.

2.4 Hybrid Ring Signcryption

A hybrid ring signcryption scheme consists of two parts: ring signcryption tag-KEM and ring signcryption DEM. A ring signcryption tag-KEM is defined as tuple of six algorithms.

$Gen=(Gen_c,Gen_u,Gen_r)$, These three algorithms generate the common parameter, the key of the user and the keys of the receivers, respectively. Sym algorithm is used to generate the symmetric key. Encap algorithm is a probabilistic key encapsulation algorithm. Decap is a deterministic key decapsulation algorithm.

A ring signcryption DEM consists as two polynomial-time algorithms: a deterministic encryption algorithm, Enc, and a deterministic decryption algorithm, Dec.

This paper focuses on the IND-CCA2 security which is given in [8]. The IND-CCA2 security is defined by a game between the challenger and a three stages attacker $\mathcal{A}$=($\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{A}_3$).

3. The Proposed Lattice-based Hybrid Ring Signcryption Scheme

3.1 Lattice-based Ring Signcryption tag-KEM

Our proposed ring signcryption tag-KEM is described as follows:

--- Gen_c. Let *n* be a main secure parameter. q>2 and $m=(1+\beta)n\log q$ for some constant $\beta\geq 0$. Let *l* be a integer and bounded by *poly*(*n*). A Gaussian parameters $s=\tilde{L}\omega(\sqrt{\log n})$ where $\tilde{L}=O(\sqrt{n\log q})$. In our construction, we need two secure hash functions as follows $h_1:\{0,1\}^*\rightarrow Z_q^n$, $h_2:Z_q^m\rightarrow\{0,1\}^l$.

--- Gen_r. The receiver generates $(\mathbf{B}_{10},\mathbf{T}_{10})\in Z_q^{n\times m}\times Z_q^{m\times m}$ and $(\mathbf{B}_{11},\mathbf{T}_{11})\in Z_q^{n\times m}\times Z_q^{m\times m}$ by proposition 2, where $\mathbf{T}_{10},\mathbf{T}_{11}$ are short basises of the relate lattice. The receiver randomly chooses 2*l*-2 matrixes $\mathbf{B}_{ib}\in Z_q^{n\times m}$ where $2\leq i\leq l, b\in\{0,1\}$.Then, $pk_r=\{\mathbf{B}_{ib}\},i\in[l],b\in\{0,1\}$, $sk_r=\{\mathbf{T}_{10},\mathbf{T}_{11}\}$.

---Gen_u. Every ring user U_i uses the random lattice sample algorithm in proposition 2 to generate matrices $(\mathbf{A}_i,\mathbf{T}_i)$. Let $pk_i=\mathbf{A}_i, sk_i=\mathbf{T}_i$. Let the ring public key $pk=(pk_1,pk_2,\cdots pk_l)$.

---Sym. Suppose ring user U_i wants to send a message to the receiver on behalf of the ring group. He acts as follows:

1. Randomly chooses and computes $K=h_2(\mathbf{s})$. 2. Set $\omega=(\mathbf{s},pk_r,pk_i,pk)$.

---Encap

1. U_i randomly chooses $\tau\in\{0,1\}^l$ and computes $h_1(\mathbf{s},\tau)$

2. U_i chooses $i-1$ random errors vectors $\mathbf{e}_k\leftarrow D_{Z^m,\alpha}$, and computes $\mathbf{A}_k\mathbf{e}_k \bmod q$.

3. Let $\mathbf{y}=(h_1(\mathbf{s},\tau)-\sum_{k=1}^{i}\mathbf{A}_k\mathbf{e}_k)\bmod q$, $\mathbf{e}_i\leftarrow \Pr eSample(\mathbf{A}_i,\mathbf{T}_i,\mathbf{y})$.

4. For $\tau=(\tau_1,\tau_2,\cdots,\tau_i)$, $\mathbf{b}_k=\mathbf{B}_{i\tau_k}^T\mathbf{s}+\mathbf{e}_k(\bmod q)$ where $k=1,2,\cdots,i$. Let $(\tau,\mathbf{b}=(\mathbf{b}_1,\cdots,\mathbf{b}_i))$ be the encapsulation of the symmetric key K.

---Decap:

1. Parses $\mathbf{b}=(\mathbf{b}_1,\cdots,\mathbf{b}_i)$ where $\mathbf{b}_k\in Z_q^m$, If **b** cannot be parsed in this way, rejects it.

2. Computes **s** and $\mathbf{e}_i$ from $\mathbf{b}_i$ with the help of the trapdoor $\mathbf{T}_{i\tau_i}$, and then computes others $\mathbf{e}_k$. Checks $\|\mathbf{e}_k\|\le s\sqrt{m}$, otherwise, rejects it.

3. Checks $h_1(\mathbf{s},\tau)=\sum_{k=1}^{i}\mathbf{A}_k\mathbf{e}_k \bmod q$. If not, rejects it..

4. Computes $K=h_2(\mathbf{s})$ as a symmetric key of the signcryption DEM.

3.2 Ring Signcryption DEM

---Enc: Let $M\in\{0,1\}^l$ be a message, $K+M=c(\bmod 2)$, ---Dec: Computes $K+c=M(\bmod 2)$

4. Analysis of the Proposed Scheme

4.1 Confidentiality

Theorem 1. The proposed ring signcryption tag-KEM is IND-CCA2 secure under the hardness of the learning with errors problem.

Proof. Our proof proceeds in a sequence of games which are unindistinguished each other.

Game 0 This is the original IND-CCA2 game of the ring signcryption tag-KEM between the adversary and the challenger. Let suppose the challenge tag is τ^* in step 4

Game 1 This is the same as the Game 0, but the decapsulation oracle is modified to output an errors symbol if on inputting challenge tag. τ^* .

Game 2 It is the same as the precious Game 1, but, the Gen_r algorithm is modified as follows: $\mathbf{B}_{k\tau_k}$ are random matrixes, and $\mathbf{B}_{k(1-\tau_k)}$ are the outputs of the algorithm in proposition 2 .

Game 3 It is the same as the precious game, but the vector b of the challenge encapsulation $(\tau^*,\mathbf{b}=(\mathbf{b}_1,\cdots,\mathbf{b}_i))$ is chosen uniformly in step 5.

4.2 Unforgeability

Theorem 2. In the random oracle model, the proposed ring signcryption tag-KEM is sUF-CMA secure under the short integer solution problem intractability assumption.

Proof. If there is an adversary $\mathcal{A}$ can attack the sUF-CMA security of proposed scheme with advantage ε, then a challenger $\mathcal{B}$ can solve the SIS problem with probability ε. We omit the details.

4.3 Anonymity and Authentication

Vector **e** is statistically close to Gaussian distribution,which leaks no information about the signer. The actual ring user can prove its identity by providing K and **s**.

5. Summary

In this paper, a lattice-based ring signcryption scheme is designed using ring signcryption tag-KEM + ring signcryption DEM technique whose security is proven in the random oracle model.

Acknowledgements

The authors thank the anonymous referees for their helpful comments. This work was supported by the National Natural Science Foundation of China (Grant No. 61303198, 61173151) and Natural Science Foundation of Shandong Province (No. ZR2013FQ031).

References

[1] Y. L.Zheng, Digital signcryption or how to achieve cost(signature and encryption) <<cost(signature) + cost(encryption). In CRYPTO,1997, 165-179.

[2] X.Boyen, Multipurpose Identity-Based Signcryption. In: CRYPTO '03, Berlin: Springer, LNCS 2729, 2003, pp. 383-399.

[3] B. Libert, J.J. Quisquater, Efficient signcryption with key privacy from gap diffie-hellman groups. In Public Key Cryptography, 2004, pp. 187-200.

[4] B. Libert, and J.J. Quisquater, Improved signcryption from q-diffie-hellman problems. In International Conference on Security in Communication Networks, SCN, LNCS 3352, volume 4, 2004, pp. 220-234.

[5] Dent A. W., Hybrid signcryption schemes with insider security. In Information Security and Privacy -ACISP 2005, LNCS 3574, Springer, 2005, pp. 253-266.

[6] Dent A. W. Hybrid signcryption schemes with outsider security. In Proceedings of ISC 2005, LNCS 3650, Springer,2005, pp. 203-217.

[7] T. E. Bjostad , A.W.Dent, Building better signcryption schemes with tag-KEMs. In Public Key Cryptography-PKC 2006, LNCS 3958, Springer-Verlag, 2006, pp. 491-507.

[8] K.L. Chung, G.M. Yang, D. S. Wong, X. Deng, S. S.M. Chow, An efficient signcryption scheme with key privacy and its extension to ring signcryption, Journal of Computer Security, 2010(18): 451-473.

[9] F. Li, M. Shirase, T. Takagi, Analysis and Improvement of Authenticatable Ring Signcryption Scheme, Journal of Shanghai Jiaotong University, 2008, 13(6): 679-683.

[10] C. Gentry , C. Peikert, V. Vaikuntanathan, Trapdoors for Hard Lattices and New Cryptographic Constructions. In: STOC, Victoria, British Columbia, 2008, pp. 197-206.

[12] Cash D, Hofheinz D, Kiltz E, peikert C. Bonsai Trees, or How to Delegate a Lattice Basis. In Eurocrypt, H. Gilbert (Ed.), LNCS 6110, 2010, pp. 523-552.

[13] O. Regev, On Lattice, Learning with Errors, Random Linear Codes, and Cryptography. In: STOC, Baltimore, 2005, pp. 84-93.

[14] J. Alwen, C. Peikert, Generating Shorter Bases for Hard Random Lattices [C]. In: STACS, volume 09001, 2009, pp. 75-86.

[15] F. Wang, Y. Hu, B. Wang, Lattice-based Linearly Homomorphic Signature Scheme over Binary Field, Science China Information Science. 2013, 56(11): 112108:1-112108:9.