International Journal of Information & Network Security (IJINS)
Vol.3, No.2, April 2014, pp. 92~97
ISSN: 2089-3299

Multiplicative Learning with Errors and Cryptosystems

Gu Chun-sheng*, **
* School of Computer Science and Technology, University of Science and Technology of China
** School of Computer Engineering, Jiangsu University of Technology

Article Info

Article history:

Received Aug 12th, 2012
Revised Dec 20th, 2013
Accepted Mar 26th, 2014

Keyword:

Multiplicative Learning with Errors
Private-Key Encryption
Public-key Encryption
LWE on Abelian Group

ABSTRACT

We first introduce a new concept of multiplicative learning with errors (MLWE), which is multiplicative version of the learning with errors (LWE). Then we reduce that the hardness of the search version for MLWE to its decisional version under the condition of modulo of a product of sufficiently large smoothing prime factors. Next we construct the MLWE-based private-key and public-key encryption schemes, and prove that the security of our schemes is based on the worst-case hardness assumption of MLWE. Finally, we discuss the LWE on additive group to the LWE on general abelian group and approximate lattice problem on abelian group.

Corresponding Author:

Gu Chun-sheng,
School of Computer Engineering,
Jiangsu University of Technology,
1801 Zhongwu Main Road, Zhonglou District, Changzhou City, Jiangsu Province, China, 213001.
Email: guchunsheng@gmail.com

1. INTRODUCTION

After the concept of public-key cryptosystem is presented, very few convincingly secure public-key schemes have been discovered despite considerable research efforts. Now standard cryptographic assumptions are mainly based on the hardness of computational problems such as integer factoring problem [1-2], discrete logarithm problem [3-4], elliptic curve problem [5-6] and lattice problem [7]. Recently, Regev [8] extended learning parity with noise (LPN) to learning with errors (LWE) over larger modulo, and described a different class of cryptosystem based on LWE. In the search version of LWE, the goal is to solve for an unknown vector *s* on Z_p^n which is often chosen uniformly at random, given any desired *m*=poly(*n*) independent 'noisy random inner products' $(a_i, b_i =< a_i, s > +e_i) \in Z_p^n \times Z_p$, $i \in [m]$, where $a_i \in Z_p^n$ and each e_i the error distribution *X*. In the decisional version, the goal is merely to distinguish between noisy inner products as described above and uniformly random samples from $Z_p^n \times Z_p$. Moreover, Regev constructed an elementary reduction from the search version to decision version for the LWE problem when prime *p*=poly(*n*).

The multiplicative learning with error (MLWE) problem is a multiplicative version of LWE. It is parameterized by a dimension *n*, a modulus *p*, and an error distribution *X* over Z_p, where *X* is often considered as a Gaussian-like distribution that is relatively concentrated around 0. In the search version of MLWE, the goal is to solve for an unknown vector *s* on some subset of Z_p^n which is often chosen uniformly at random, given any desired *m*=poly(*n*) independent 'noisy random exponential inner products' $(a_i, b_i = (a_i \wedge^r s) \times e_i = \prod_{j=1}^n a_{i,j}^{s_j} \times e_i \in Z_{p^*}^n \times Z_{p^*}$, $i \in [m]$, where $a_i \in Z_{p^*}^n$, e_i the error distribution *X*. In the decisional version, the goal is to distinguish between noisy random exponential inner products and uniformly random samples from $Z_{p*}^{n} \times Z_{p*}$.

Related Work. After Regev introduces LWE and construct an elementary public key cryptosystem, many works (e.g. [9-19]) have focused on how improve and design various cryptographic primitive under the hardness of LWE.

Our work is inspired by Ref. [8]. Regev [8] defines the additive learning with error, whereas we generalize LWE on the additive group to the MLWE on the multiplicative group. Moreover, we also extend the work of [18] from exponential error noise to directly multiplicative noise error in the public key and ciphertext. Namely, the problem defined in [18] is equivalent to the LWE problem if there is an oracle solving the discrete logarithm problem, whereas MLWE we here introduce is not equivalent the LWE problem even if supposing the discrete logarithm oracle. We show the difference between them in the following Remark 2.1. Furthermore, we construct respectively public key and private key cryptosystems based on MLWE and discuss how to generalize LWE on additive group to LWE on general abelian group. To our knowledge, the leaning with error problem on the abelian group does not obtain the attention for researchers. We believe this contribution is of independently interest.

Our Results. Our main contribution is to introduce the concept of MLWE and prove that the hardness of the search version of MLWE is equal to its decisional version. Our second contribution is to construct MLWE-based private-key and public-key encryption schemes, whose securities are based on the worst-case hardness assumption of MLWE.

Organization. We describe notations and definitions in Section 2; we prove the hardness of MLWE in Section 3; we construct MLWE-based public key and private key cryptosystems in Section 4; and we extend LWE to the LWE on the abelian group and approximate lattice problem on abelian group in Section 5; we finally conclude this paper and give open problem in Section 6.

2. Preliminaries

We denote $[p]=\{1,2,...,p\}$, $-[p]=\{-1,-2,...,-p\}$, $Z_p=\{\lceil -p/2\rceil,...,\lfloor (p-1)/2\rfloor\}$, $Z_{p*}=\{a \mid \gcd(a,p)=1, and\ a \in Z_p\}$. We denote column vectors $x,y \in Z^n$, $x^c=(x_1^c,...,x_n^c)$, $x/c=(x_1/c,...,x_n/c)$, $x \oplus y=(x_1 \oplus y_1,...,x_n \oplus y_n)$, and $x * y^{-1}=(x_1 \times y_1^{-1},...,x_n \times y_n^{-1})$, where the c is a non-zero constant.

We assume $X,Y \in Z_p^{m\times n}$, $X \wedge^r Y^T=(a_{i,j})$ with $a_{i,j}=\prod_{k=1}^{n} x_{i,k}^{y_{j,k}}$, $X \wedge^l Y^T=(a_{i,j})$ with $a_{i,j}=\prod_{k=1}^{n} y_{j,k}^{x_{i,k}}$, $X*Y=(a_{i,j})$ with $a_{i,j}=x_{i,j}y_{i,j}$, $Y^{-1}=(a_{i,j})$ with $a_{i,j}=y_{i,j}^{-1}$, $kX+c=(a_{i,j})$ with $a_{i,j}=kx_{i,j}+c$, $g^X=(a_{i,j})$ with $a_{i,j}=g^{x_{i,j}}$.

We denote $\lambda(p)$ the Carmichael's λ-function for p, $\varphi(p)$ Euler's φ-function for p.

Definition 2.1 (Learning With Error LWE$_{p,s,X}$ [8]). Suppose $n>1$, p be a positive integer and consider a list of equations with errors $<a_i,s>+e_i=b_i (\bmod p)$, $i\in[m]$, $m \le poly(n)$ where a_i, s are chosen independently from the uniform distribution on Z_p^n, e_i is independently drawn from the error distribution X and $b_i \in Z_p$. Let LWE$_{p,s,X}$ denote the problem of recovering s from such equations, A$_{p,s,X}$ the probability distribution generated by LWE$_{p,s,X}$.

Definition 2.2 (**Multiplicative Learning With Error MLWE$_{p,s,X}$**). Assume n, m, p be positive integers, $a_i, i\in[m]$ are chosen independently from the uniform distribution on Z_{p*}^n, s is chosen independently from the uniform distribution on $Z_{\varphi(p)}^n$, $b_i=(a_i \wedge^r s)\times e_i \bmod p$, where each e_i is independently drawn from the error distribution X on Z_p. Let MLWE$_{p,s,X}$ denote the problem of recovering s from such equations with errors, MA$_{p,s,X}$ the probability distribution generated by MLWE$_{p,s,X}$.

Remark 2.1. Notice that MLWE$_{p,s,X}$ is not equivalent to LWE$_{p,s,X.}$ For example, assume $p=29$, A,s,e,b be an input instance for MLWE$_{p,s,X}$, A_1,e_1,b_1 be the discrete logarithm $\log_2$ of A,e,b. It is easy to see that the error distribution e_1 on $Z_{\varphi(p)}$ is different from the one of e on Z_p.

$$A=\begin{pmatrix}3&7&4&11\\6&9&17&24\\5&26&20&18\\16&3&2&13\end{pmatrix},\quad s=\begin{pmatrix}5\\10\\23\\11\end{pmatrix},\quad e=\begin{pmatrix}3\\2\\-1\\5\end{pmatrix},\quad b=(A\wedge^r s)*e=\begin{pmatrix}10\\4\\12\\3\end{pmatrix}\bmod 29,$$

$$A_1=\log_2 A=\begin{pmatrix}5&12&2&25\\6&10&21&8\\22&19&24&11\\4&5&1&18\end{pmatrix},\quad e_1=\log_2 e=\begin{pmatrix}5\\1\\14\\22\end{pmatrix}, b_1=A_1s+e_1=\begin{pmatrix}23\\2\\7\\5\end{pmatrix}\bmod 28.$$

3. Hardness of MLWE

In this section, we show the equivalence between the decisional version and the search version for MLWE when *p* is a product of sufficiently large smoothing prime factors.

Theorem 3.1 Let $n>1$ be an integer, $p=p_1...p_t$ for distinct primes $p_i=poly(n)$. There is a probabilistic polynomial time reduction from solving the search MLWE$_{p,s,X}$ problem with overwhelming probability to distinguishing MA$_{p,s,X,e}$ from $U(Z_{p*}^n\times Z_{p*})$ for arbitrary $s\in Z_{\lambda(p)}^n$ with overwhelming probability.

Proof: Assume D to be an efficient distinguisher that distinguishes MA$_{p,s,X}$ from *U* for modulus p_1. Given input samples $(a_i,b_i=a_i\wedge^r s\times e_i), i\in[m]$ generated by the distribution MA$_{p,s,X}$. The goal is to solve s from (a_i,b_i). Due to $p_1=poly(n)$, we can compute the order of $a_{i,j}$. Without loss of generality, let the order of $a_{i,j}$ be p_1-1. First, choose m random $r_i\in Z_{p_1-1}$, and for any $k\in Z_{p_1-1}$, factor $k=xy\bmod(p_1-1)$ such that $x\neq 1, y\neq 1$ and $\gcd(y,p_1-1)=1$ except with $k=0\bmod(p_1-1)$. Then, compute $a_{i,1}^{'}=a_{i,1}^{x+r_i}$, $a_{i,j}^{'}=a_{i,j}, j>1$, $b_i^{'}=b_i\times a_{i,1}^{r_iy}$. Finally, call D with the parameters $(a_i^{'},b_i^{'})$. If $D((a_i^{'},b_i^{'}))=1$, then $s_1=k$, otherwise $s_1\neq k$. If $s_1=xy$, then $s_1+r_iy=(x+r_i)y$, namely $(a_i^{'},b_i^{'})\in MA_{p_1,s,X}$. If $s_1\neq xy$, the probability that $(s_1+r_iy)/(x+r_i)=(s_1+r_jy)/(x+r_j)$ is at most $1-1/(6\ln\ln(p_1-1))+1/(p_1-1)$. When $(s_1-xy)(r_i-r_j)=0\bmod(p_1-1)$, $s_1\neq xy$, and $r_i\neq r_j$, the probability of $\gcd(r_i-r_j,p_1-1)>1$ is at most $1-1/(6\ln\ln(p_1-1))$. Moreover, the probability of $r_i=r_j$ is $1/(p_1-1)$. So, the probability that $(s_1+r_iy)/(x+r_i)=(s_1+r_jy)/(x+r_j)$ and $s_1\neq xy$ for all (r_i,r_j) is at most $(1-1/(6\ln\ln(p_1-1))+1/(p_1-1))^{m-1}$ and negligible. In other words, if $s_1\neq xy$, there does not exist an integer z such that $z=(s_1+r_iy)/(x+r_i)\bmod(p_1-1)$ for all i with overwhelming probability. In this case, $b_i^{'}$ is uniformly random by applying the fact the order of $a_{i,1}$ is p_1-1 and $\gcd(y,p_1-1)=1$, namely, $r_i^{'}=r_iy\in U(Z_{p_1-1})$. Hence, we can decide whether $k=s_1$ by using D and $1\leq s_1\leq p_1-1$=$poly(n)$. If all $1\leq k<p_1-1$ is not equal to s_1, then $s_1=0\bmod(p_1-1)$, for the input samples are from the distribution $MA_{p_1,s,X}$. So, we can add a random number to s_1, then decide s_1. Finding all other coordinates is similar for modulus p_1 and $p_2,...,p_t$. Finally, we recover $s\in Z_{\lambda(p)}^n$ via the Chinese remainder theorem.■

Lemma 3.1 (Decisional Average-case to Worst-case). If there is a distinguisher that distinguishes MA$_{p,s,X}$ from *U* for a non-negligible fraction of all possible *s*, then there is an efficient algorithm that for all *s* accepts with probability exponentially close to 1 on inputs from MA$_{p,s,X}$ and rejects with probability exponentially close to 1 on inputs from *U*.

Lemma 3.2 (Search Average-case to Worst-case). If there exists an efficient algorithm that solves MLWE$_{p,s,X}$ for a non-negligible fraction of all possible *s*, then there exists an efficient algorithm that for all *s* solves MLWE$_{p,s,X}$ with probability exponentially close to 1.

Proof: The proofs of Lemma 3.1, 3.2 follow the adaptive ones of Lemma 4.1, 4.2 of Ref. [8]. ■

4. Cryptosystems

In this section, we present a private-key encryption scheme and a public-key encryption scheme based on the decisional MLWE problem, respectively. By using Theorem 3.1, we know their securities depend on the hardness of the MLWE problem.

4.1 Private-Key Encryption Scheme

Let n be the security parameter. $m = n^c$ where $c > 0$ is a constant, $p = poly(n)$ is a prime, $q = \lfloor \sqrt{p} \rfloor$.

Key Generation Algorithm: On input 1^n, choose a uniformly random secret key $s \in Z_p^n$.

Encryption Algorithm: On input a secret key $s \in Z_p^n$ and a message $y \in \{0,1\}^m$. Choose $A \in_R Z_{p*}^{m\times n}$ uniformly at random and an error vector $e \in_R (-[q-1]) \cup [q-1]$ where $|e_i| \in [q-1]$, output the ciphertext $c = (A, (A \wedge^r s) * e * q^y \bmod p)$.

Decryption Algorithm: On input a secret key $s \in Z_p^n$ and a ciphertext $c = (A, b)$. The decryption algorithm computes $x = b * (A \wedge^r s)^{-1} \bmod p$ and it deciphers as follows: if $-(q-1) \le x_i \le q-1$, then it deciphers $y_i = 0$, otherwise it deciphers $y_i = 1$.

Correctness: The decryption algorithm computes $x = b * (A \wedge^r s)^{-1} = e * q^y$. Thus, if $y_i = 0$, then $-(q-1) \le x_i \le q-1$. If $y_i = 1$, $q \le x_i = (e_i \times q) \bmod p \le p - q$. We here use the absolutely least residue for modulo p.

Efficiency: The size of ciphertext $c = (A, b)$ has $mn\lg p + m\lg p$ bits. The expansion of ciphertext is $(mn\lg p + m\lg p)/m = n\lg p + \lg p$ for each message bit.

Proposition 3.1 (Security). The symmetric encryption scheme is semantically secure assuming that the MLWE$_{p,s,U}$ problem is hard.

4.2 Public-key Encryption Scheme

Let n be the security parameter. $m = 2n$, $p = p_1 \ldots p_t > 2^{4n\lg n + 12n}$ such that $p_i = poly(n)$ are distinct primes, $q = \lambda(p)$.

Key Generation: Choose uniformly at random $A \in \square_{p*}^{m\times n}$, $S \in Z_q^{m\times n}$, $E \leftarrow U_{[s]}^{m\times m} \bigcup U_{\text{-}[s]}^{m\times m}$, where $s = \lfloor 8\sqrt{n} \rfloor$. Output the secret key $sk = (S)$, and the public key $pk = (A, B)$ where $B = (A \wedge^r S^T) * E \bmod p$.

Encryption: Given the public key $pk = (A, B)$ and a message $y \in \{0,1\}^m$. Choose uniformly at random $x \in \{0,1\}^m$ and output the ciphertext $c = (c_1, c_2)$, where $c_1 = (x \wedge^l A) \bmod p$, $c_2 = (x \wedge^l B) \times M \bmod p$,
$M = diag(q^{y_1}, q^{y_2}, \ldots, q^{y_m})$, and $q = \lfloor p^{1/2} \rfloor$

Decryption: Given the secret key $sk = (S)$ and a ciphertext $c = (c_1, c_2)$. Compute $w = c_2 * (c_1 \wedge^r S^T)^{-1}$, and output $y_i = 0$ if $|w_i| < q$ modulo p and $y_i = 1$ otherwise.

Correctness. Since $w = c_2 * (c_1 \wedge^r S^T)^{-1} = (q^{y_1} \prod e_{i,1}^{x_i}, q^{y_2} \prod e_{i,2}^{x_i}, \ldots, q^{y_m} \prod e_{i,m}^{x_i}) \bmod p$,

$|\prod e_{i,j}^{x_i}| \le \prod(\sqrt{n}\times 8\sqrt{n}) = 2^{2n\lg n+6n} < q,\ j\in[m]$. Thus, if $y_i = 0$, then $|w_i| < q$, if $y_i = 1$, then $|w_i| \ge q$.

Efficiency. The size of the public key $pk = (A,B)$ has $O(m^2\lg p) = O(n^3\lg n)$ bits. The size of the secret key $sk = (S)$ is $O(mn\lg p) = O(n^2\lg n)$ bits. The size of the ciphertext $c = (c_1, c_2)$ is $O(m\lg p) = O(n^2\lg n)$ bits. The expansion of ciphertext is $O(n^2\lg n/n) = O(n\lg n)$ for each message bit.

Proposition 3.2 (Security). The public key encryption scheme is secure assuming that the MLWE$_{p,s,U}$ problem is hard when *p* is a product of sufficiently large smoothing prime factors.

5. Extension

5.1 LWE on Abelian Group

The LWE problem is the additive group defined on Z_p^n, the MLWE problem is the multiplicative group defined on Z_{p*}^n. So, it is not difficult to generalize the LWE on additive group to the LWE on general abelian group. Assume G is an abelian group, × operator of G. The LWE problem on G is defined as follows: given any desired *m*=poly(*n*) independent 'noisy random inner products' $(a_i, b_i = \prod_{j=1}^{n} a_{i,j}^{s_j}\times e_i)\in G^n\times G$, $i\in[m]$, where $a_i\in G^n$ and each e_i the error distribution *X* on G, $a_{i,j}^{s_j} = a_{i,j}\times a_{i,j}\ldots\times a_{i,j}$, find s. In the search version, the goal is to solve for an unknown vector *s* on G^n which is often chosen uniformly at random. In the decisional version, the goal is merely to distinguish between noisy inner products above and uniformly random samples from $G^n\times G$. It is easy to verify the LWE problem on the abelian group can be used to construct the public key cryptosystem if there is a norm for the group elements in G. So, we believe it is very interesting to study the hardness of LWE on the general abelian group.

5.2 Approximate Lattice Problem on Abelian Group

We can further generalize LWE into an approximate lattice problem on general abelian group. Without loss of generality, we assume that G is an abelian group, × operator of G. The approximate lattice problem on G is defined as follows: given any *m*=poly(*n*) independent 'noisy random inner products' $b_i = (s_i\wedge A)\times e_i \in G^n$, $i\in[m]$, where $a_i\in G^n$ and each e_i the error distribution *X* on G, $s_i\wedge A = \prod A_{i,j}^{s_{i,j}}$, $a_{i,j}^{s_j} = a_{i,j}\times a_{i,j}\ldots\times a_{i,j}$, find s. In the search version, the goal is to solve for an unknown vector *s* on G^n which is often chosen uniformly at random. In the decisional version, the goal is merely to distinguish between noisy inner products above and uniformly random samples from $G^n\times G$. Similarly, the approximate lattice problem on the abelian group can be used to construct the public key cryptosystem if there is a norm for the group elements in G.

6. Conclusion and Open Problem

We introduce the concept of MLWE and construct the public key and private key schemes based on MLWE, whose securities are based on the worst-case hardness assumption of MLWE. Furthermore, we also discuss the generalization of LWE to LWE over the Abelian group. An interesting open problem is to reduce the hardness of solving MLWE to the hardness of the general lattice problem.

ACKNOWLEDGEMENTS

This work is supported by National Natural Science Foundation of China Grants (No. 61142007), by Changzhou application research foundation (No.CJ20120021), and by Foundation of Jiangsu University of Technology (No. KYY12027).

REFERENCES

[1] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communication of the ACM*, 21(2), 1978, pp. 120-126.

[2] S. Pradhan and B. K. Sharma, "An Efficient RSA Cryptosystem with BM-PRIME Method", *International Journal of Information & Network Security (IJINS)*, Vol.2, No.1, 2013, pp. 103~108.

[3] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", *the 4th Annual International Cryptology Conference (CRYPTO'84)*, LNCS 196, 1984, pp. 10–18.

[4] C. Meshram and S. A. Meshram, "PKC Scheme Based on DDLP", *International Journal of Information & Network Security (IJINS)*, Vol. 2, No. 2, 2013, pp. 154-159.

[5] F. Amounas and E.H. El Kinani, "Construction Efficiency of the Elliptic Curve Cryptosystem using Code Computing for Amazigh Alphabet", *International Journal of Information & Network Security (IJINS)*, Vol.2, No.1, 2013, pp. 43~53.

[6] F. Amounas and E.H. El Kinani, "A Novel Encryption Scheme of Amazigh Alphabet Based Elliptic Curve using Pauli Spin ½ Matrices", *International Journal of Information & Network Security (IJINS)*, Vol. 2, No. 3, 2013, pp. 190-196.

[7] M. Ajtai and C. Dwork, "A public-key cryptosystem with worst-case/average-case equivalence", *The 28th ACM Symposium on Theory of Computing (STOC 1997)*, 1997, pp. 284-293.

[8] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography", *The 36th ACM Symposium on Theory of Computing (STOC 2005)*, 2005, pp. 84–93.

[9] A. Kawachi, K. Tanaka, and K. Xagawa, "Multi-bit cryptosystems based on lattice problems", *The 10th IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2007)*, LNCS 4450, 2007, pp. 315–329.

[10] C. Peikert, V. Vaikuntanathan, and B. Waters, "A framework for efficient and composable oblivious transfer", *the 28th Annual International Cryptology Conference (CRYPTO 2008)*, LNCS 5157, 2008, pp. 554–571.

[11] A. Akavia, S. Goldwasser, and V. Vaikuntanathan, "Simultaneous hardcore bits and cryptography against memory attacks", *The Sixth Theory of Cryptography Conference (TCC 2009)*, 2009, pp. 474–495.

[12] C. Peikert and B. Waters, "Lossy trapdoor functions and their applications", *The 39th ACM Symposium on Theory of Computing (STOC 2008)*, 2008, pp. 187–196.

[13] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions", *The 39th ACM Symposium on Theory of Computing (STOC 2008)*, 2008, pp. 197–206.

[14] B. Applebaum, D. Cash, C. Peikert, A. Sahai, "Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems", *the 29th Annual International Cryptology Conference (CRYPTO 2009)*, LNCS 5677, 2009, pp. 595-618.

[15] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problem", *The 40th ACM Symposium on Theory of Computing (STOC 2009)*, 2009, pp. 333-342.

[16] A. R. Klivans and A. A. Sherstov, "Cryptographic hardness for learning intersections of halfspaces", *Journal of Computer and System Sciences*, 75(1):2–12, 2009.

[17] S. Goldwasser, Y. Kalai, C. Peikert and V. Vaikuntanathan, "Robustness of the Learning with Errors Assumption", *The First Symposium on Innovations in Computer Science (ICS'10)*, 2010, pp. 230-240.

[18] Gu Chunsheng, "Public Key Cryptosystems from the Multiplicative Learning with Errors", *2010 International Conference on Multimedia Information Networking and Security (MINES'10)*, 2010, pp.456-459.

[19] Gu Chun-sheng, Wu Fang-sheng, "On Fully Homomorphic Encryption, Approximate Lattice Problem and LWE", *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*, Vol.2, No.1, 2013, pp. 1-15.

BIOGRAPHY OF AUTHOR

Gu Chun-sheng received his Ph.D. Degree from University of Science and Technology of China in 2005. Since 2008 he has been an associate professor in the School of Computer Engineering, Jiangsu University of Technology. His research interests are in the cryptanalysis and design of public key cryptosystems.