Send Orders for Reprints to reprints@benthamscience.ae

The Open Cybernetics & Systemics Journal, 2015, *9,* 1033-1037 1033

Open Access

Diffie-Hellman Key Exchange Protocol Based on Ring-LWE

Yu Zhi-Min*, Jing Zheng-Jun and Li Shi-Cun

Key Laboratory of Cloud Computing and Intelligent Information Processing of Changzhou City, Jiangsu University of Technology, Changzhou Jiangsu 213001, China

Abstract: In this paper, we first construct a one-round Diffie-Hellman key exchange protocol based on Ring-LWE. The security of our construction is based on the hardness of the Ring-LWE problem. Second, we adaptively extend our construction from Ring-LWE to LWE. Finally, we efficiently implement our key exchange protocols based on Ring-LWE and LWE.

Keywords: Diffie-Hellman key exchange, LWE, ring-LWE, security.

1. INTRODUCTION

Key exchange protocol is one of the fundamental cryptographic primitive. This protocol allows two or more parties to exchange information over an insecure public network and agree upon a common session key, which can be used for later secure communication between them. So, secure key exchange protocols work as basic building block for constructing other higher-level secure protocols.

Constructing secure key exchange protocol has received much attention [1]. Diffie and Hellman [2] proposed the first 2-party one-round key exchange protocol, whose security depends on the hardness of the discrete logarithm problem. Similarly, one can directly construct a Diffie-Hellman key exchange protocol based on the discrete logarithm over elliptic curve. The breakthrough in key agreement is that Joux [3] constructed a one-round 3-party key agreement protocol using pairings on elliptic curve. But these protocols are insecure in quantum computing setting [4].

Designing lattice-type key exchange protocol is a feasible approach. Ding, Xiang and Lin [5] described a simple provably secure key exchange protocol using a variant of learning with errors (LWE), which is called a small LWE problem. However, their construction is not one-round, but rather a 2-round protocol. Georgescu [6] described a one-round Diffie-Hellman key exchange protocol using the LWE and SIS (short integer solution) problems.

Nevertheless, their protocol cannot be extended to Ring-LWE, and its efficiency is very low and impractical. On the other hand, Garg, Gentry and Halevi [7] recently described a plausible multilinear map using ideal lattices, and constructed a one-round multipartite Diffie-Hellman key agreement protocol based on their multilinear map. But the security of their construction relies on the graded DDH problem, which is a new unconventional assumption. Thus at present, there does not exist LWE-based (or Ring-LWE) one-round Diffie-Hellman key exchange protocol.

Our main contribution is to describe a one-round 2-party Diffie-Hellman key exchange protocol based on Ring-LWE. Our scheme uses a new method to generate a shared information using integers that are close to each other. Namely, our construction is to extract the most significant bits from every coefficient of ring element, whereas their scheme in [5] is to extract the least significant bits. Due to this difference, our scheme is a one-round protocol, whereas their scheme is a two-round protocol.

Our second contribution is to extend our construction from Ring-LWE to LWE. Moreover, we also implement our protocol based on Ring-LWE/LWE.

2. PRELIMINARIES

2.1. Notations

Let λ be the security parameter. For any positive integer n, we define $[n]=\{1,...,n\}$, $|n|$ the bit length of n. By convention, all vectors are in column form and are named using bold lower-case letters (*e.g.* $\mathbf{u}$), and u_i denotes the *i*-th component of $\mathbf{u}$. Matrices are named using bold capital letters (*e.g.* $\mathbf{U}$), and $\mathbf{u}_i$ denotes the *i*-th column vector of $\mathbf{U}$. Let $R=Z[x]/(x^n+1)$, $R_p=R/pR$. For $u\in R$, $\|u\|_\infty$ denotes the infinity norm of its coefficient vector. Let $\gamma_R=n$ be the expansion factor of R, that is, $\|u\times v\|_\infty \le n\cdot\|u\|_\infty\cdot\|v\|_\infty$, where "$\times$" is multiplication in R. We also denote by $|u|$ the bit length of the coefficient of u.

For simplicity, we use the absolute minimum residual system modulo p throughout this paper. For integers p,a, $[a]_p$ denotes $-p/2<[a]_p\le p/2$. Similarly, for $\mathbf{u}\in Z^n$ or $u\in R$, $[\mathbf{u}]_p$ or $[u]_p$ is defined as $[u_i]_p$ for every component of $\mathbf{u}$ or every coefficient of u.

Let $r\leftarrow_\chi S$ denote to choose an element r in S according to the distribution χ. For the distributions A,B,

1874-110X/15 2015 Bentham Open

$A \equiv_c B$ is computationally indistinguishing by arbitrary probabilistic polynomial time algorithm.

2.2. LWE and R-LWE

Definition 2.1 (Learning With Error (LWE) [8]). Let n, p be integers, and χ a distribution over Z_p. Given a list samples (a_i, b_i) of the distribution $D_{n,p,\chi}$ over Z_p^{n+1} such that $a_i \leftarrow Z_p^n$, $s \leftarrow Z_p^n$, $e_i \leftarrow \chi$ and $b_i =< s, a_i > + e_i \bmod p$, the LWE problem $LWE_{n,p,\chi}$ is to distinguish the distribution $D_{n,p,\chi}$ from the uniform distribution over Z_p^{n+1}.

For the coefficient vector $\mathbf{u} = (u_0, u_1, ..., u_{n-1})^T$ of $u \in R$, we define the cyclic rotation $\mathrm{rot}(\mathbf{u}) = (-u_{n-1}, u_0, ..., u_{n-2})^T$, and the circulant matrix $\mathrm{Rot}(\mathbf{u}) = (\mathbf{u}, \mathrm{rot}(\mathbf{u}), ..., \mathrm{rot}^{n-1}(\mathbf{u}))$. $\mathrm{Rot}(\mathbf{u})$ is called the rotation basis of the ideal lattice (u). An ideal $I \subseteq R$ is called principal if it only has a single generator.

Definition 2.2 (Learning with Errors in a Ring of Integers (Ring-LWE) [9]). Let n, p be positive integers, and χ a distribution over R_p. Given a list samples (a_i, b_i) of the distribution $D_{n,p,\chi}$ over $R_p \times R_p$ such that $a_i \leftarrow R_p$, $s \leftarrow R_p$, $e_i \leftarrow \chi$ and $b_i = s \times a_i + e_i$, the RLWE problem $RLWE_{n,p,\chi}$ is to distinguish the distribution $D_{n,p,\chi}$ from the uniform distribution over $R_p \times R_p$.

Theorem 2.1 ([8]). For any integer dimension n, prime integer $p = p(n)$, and $b = b(n) \geq 2n$, there is an efficiently samplable *b*-bounded noise distribution χ such that if there exists an efficient algorithm that solves $LWE_{n,p,\chi}$, then there is an efficient quantum algorithm for solving $\tilde{O}(pn^{1.5}/b)$-approximate worst-case SIVP and gapSVP.

Theorem 2.2 ([9]). For prime integer $p = p(n)$, $b = \omega(\sqrt{n \log n})$, and ring $R = Z[x]/(x^n + 1)$ with n a power of 2, there is an efficiently samplable distribution χ that outputs elements of R of length at most *b* with overwhelming probability, such that if there exists an efficient algorithm that solves $RLWE_{n,p,\chi}$, then there is an efficient quantum algorithm for solving $n^{\omega(1)} \cdot (p/b)$-approximate worst-case SVP for ideal lattices over R.

The classical hardness of LWE obtains progress. Peikert [10] showed that LWE with $p = 2^n$ modulus is as hard as n-dimensional GapSVP using a classical reduction. Recently, Brakerski, Langlois, Peikert, Regev, and Stehlé [11] showed that solving n-dimensional LWE with $\mathrm{poly}(n)$ modulus implies an equally efficient solution to a worst-case lattice problem in dimension $\sqrt{n}$.

The LWE with small parameters remain to be hard. Applebaum, Cash, Peikert, and Sahai [12] showed that LWE becomes no easier to solve when the secret key s's coefficients are sampled from the noise distribution χ, rather than uniformly at random. Moreover, Micciancio and Peikert [13] show the hardness of LWE with small parameters. They prove that LWE remains hard even when the errors are small, if the number of samples is small enough, whereas prior results required the errors to draw from a Gaussian-like distribution and to have magnitude at least $\sqrt{n}$. On the other hand, there is a sub-exponential time algorithm for the LWE with noise less than $\sqrt{n}$ [15], when the number of samples is not restricted.

Theorem 2.3 ([13]). Let n and $m = n(1 + \Omega(1/\log n))$ be integers, and $p \geq n^{O(1)}$ a sufficiently large polynomial bounded (prime) modulus. Then solving LWE with parameters n, m, p and uniformly random errors on set $\{-1, 0, 1\}$ is at least as hard as approximating lattice problems in the worst case on $\Theta(n/\log n)$-dimensional lattices within a factor $\gamma = \tilde{O}(\sqrt{n} \cdot p)$.

3. ONE-ROUND 2-PARTY DIFFIE-HELLMAN KEY EXCHANGE PROTOCOL

In this section, we will first describe our construction, which use a fact that adding a small integer to a large integer does not affect the most significant bit of large integer with high probability. Then we show the security of our construction. Next, we will extend the construction from Ring-LWE to LWE. Finally, we implement our scheme based on Ring-LWE.

3.1. Our Construction

Setup. Choose a random element $f \in R_p = Z_p[x]/(x^n + 1)$ with $p \approx n^t \cdot b^2$ and $t > 2$, output the public parameters $\mathrm{pars} = (p, f)$.

Key Exchange. Assume that Alice and Bob want to decide upon a shared secret key. They perform the following steps.

(1) Alice selects $s_1, e_1 \in R_p$ according to the noise distribution χ, that outputs elements of R of length at most *b* with overwhelming probability, computes $g_1 = s_1 f + e_1$, and sends g_1 to Bob.

(2) Bob selects $s_2, e_2 \in R_p$ according to the noise distribution χ, that outputs elements of R of length at most *b* with overwhelming probability, computes $g_2 = s_2 f + e_2$, and sends g_2 to Alice.

(3) Alice computes a shared key $k_1 = \mathrm{ext}(\lfloor s_1 g_2 \rceil_p)$, and similarly Bob computes a shared secret key

$k_2 = \text{ext}(\lfloor s_2 g_1 \rceil_p)$. Here $\text{ext}(k)$ is a function of bit extracting, which by using half function maps $(-p/2, -p/4] \cup (p/4, p/2] \to 1$ and $(-p/4, p/4] \to 0$ for each coefficient of k.

Correctness: Since $s_1 g_2 = s_1 s_2 f + s_1 e_2$ and $\|f\|_\infty \approx p$, we have $\|s_1 g_2\|_\infty \approx p$. On the other hand, by $\|s_1 e_2\|_\infty \le nb^2$, the most significant part of every coefficient of $s_1 s_2 f$ is identical to that of the corresponding coefficient of $s_1 g_2$ with probability at least $1 - 2^{(|p|-|nb^2|)} \approx 1 - nb^2/p = 1 - 1/n^{t-1}$. So, the probability of $k_1 = k_2$ is at least $1 - 1/n^{t-2}$. When $t = O(\log \log n)$, the probability of correctness is almost 1.

Efficiency. For each party, space required is to store $n \log p$ bits, communication round required is 1 and the number of bits sent is $n \log p$; computation taken is 2 multiplications and 1 addition over the ring, and extracting one bit from every coefficient of one ring element.

Example 3.1. Let $n = 4$, $p = 3079$, $f = -1495 + 147 \cdot x - 816 \cdot x^2 - 863 \cdot x^3$. For simplicity, we interchangeably use ring element and vector without distinction in this example (*e.g.* $f = [-1495 \quad 147 \quad -816 \quad -863]$).

(1) Alice chooses randomly $s_1 = [2 \quad -3 \quad 2 \quad -1]$, $e_1 = [3 \quad -1 \quad -1 \quad -2]$, computes $g_1 = s_1 f + e_1 = [-718 \quad -470 \quad 231 \quad -570]$, and sends g_1 to Bob.

(2) Bob chooses at random $s_2 = [-1 \quad 3 \quad 1 \quad 3]$, $e_2 = [0 \quad 3 \quad 1 \quad 1]$, computes $g_2 = s_2 f + e_2 = [1380 \quad -1318 \quad -727 \quad 236]$, and sends g_2 to Alice.

(3) Alice computes $\lfloor s_1 g_2 \rceil_p = [528 \quad 1272 \quad -649 \quad -1361]$ and extracts a shared secret key $k_1 = \text{ext}(\lfloor s_1 g_2 \rceil_p) = [0 \quad 1 \quad 0 \quad 1]$. For example, $528 \in (-p/4, p/4]$, $1272 \in (-p/2, -p/4] \cup (p/4, p/2]$, so the first and second bits of k_1 are 0 and 1.

Bob computes $\lfloor s_2 g_1 \rceil_p = [525 \quad 1262 \quad -662 \quad -1363]$ and extracts a shared secret key $k_2 = \text{ext}(\lfloor s_2 g_1 \rceil_p) = [0 \quad 1 \quad 0 \quad 1]$. So, the shared secret keys $k_1 = k_2$.

3.2. Security

Theorem 3.1. The above construction is secure against passive PPT adversaries, assuming that the $RLWE_{n,p,\chi}$ is hard.

Proof. Our proof includes two steps. (1) The hardness of RLWE with $s \leftarrow \chi$ is same as the hardness of $RLWE_{n,p,\chi}$ with $s \leftarrow R_p$. This result is proved in [12, 14]. For completeness, we here provide a simple proof. Given two samples $(a_i, b_i = a_i \times s + e_i), i = 1, 2$ from $RLWE_{n,p,\chi}$, assume a_1 is invertible over R_p. Now, we compute $a_2 a_1^{-1} b_1 - b_2 = a_2 a_1^{-1} e_1 + (-e_2)$ and generate a sample $(a_2 a_1^{-1}, a_2 a_1^{-1} e_1 + (-e_2))$ from RLWE with $s \leftarrow \chi$. So, we can reduce $RLWE_{n,p,\chi}$ with $s \leftarrow R_p$ to RLWE with $s \leftarrow \chi$.

(2) Assume a passive PPT adversary A can distinguish the distribution (f, g_1, g_2) from the uniform distribution over $R_p \times R_p \times R_p$, then there is a PPT algorithm B to decide the $RLWE_{n,p,\chi}$ problem. Without loss of generality, given $(a, b_1 = a \times s_1 + e_1)$ with $s_1, e_1 \leftarrow \chi$, B chooses $s_2, e_2 \leftarrow \chi$, computes $b_2 = a \times s_2 + e_2$, and finally calls A with (a, b_1, b_2). This is a contradiction with the assumption that RLWE is hard.

3.3. Extension to LWE

We directly extend the construction above from Ring-LWE to LWE by using matrix form.

Setup. Choose a random matrix $\mathbf{F} \in F_p^{n \times n}$ with $p \approx n^t \cdot b^2$ and $t > 2$.

Key Exchange: Assume that Alice and Bob want to decide upon a shared secret key. They perform the following steps.

(1) Alice selects $\mathbf{S}_1, \mathbf{E}_1 \in F_p^{n \times n}$, each of which is sampled from χ over $F_p^{n \times n}$, computes $\mathbf{G}_1 = \mathbf{S}_1 \mathbf{F} + \mathbf{E}_1$, and sends $\mathbf{G}_1$ to Bob.

(2) Bob selects $\mathbf{S}_2, \mathbf{E}_2 \in F_p^{n \times n}$, each of which is sampled from χ over $F_p^{n \times n}$, computes $\mathbf{G}_2 = \mathbf{F}\mathbf{S}_2 + \mathbf{E}_2$, and sends $\mathbf{G}_2$ to Alice.

(3) Alice outputs $\mathbf{K}_1 = \text{ext}(\lfloor \mathbf{S}_1 \mathbf{G}_2 \rceil)$, and Bob outputs $\mathbf{K}_2 = \text{ext}(\lfloor \mathbf{G}_1 \mathbf{S}_2 \rceil)$. Similarly, $\text{ext}(\mathbf{K})$ is a bit extracting function for every entry of $\mathbf{K}$.

Correctness. It is identical as the construction based on Ring-LWE.

Efficiency. For each party, space required is to store $n^2 \log p$ bits, communication round required is 1 and the number of bits sent is $n^2 \log p$; computation taken is 2 matrix multiplications and 1 matrix addition over F_p, and extracting one bit from every entry of matrix.

Theorem 3.2. The construction based on LWE is secure against passive PPT adversaries, assuming that the $LWE_{n,p,\chi}$ is hard.

Proof. The proof is similar as one of Theorem 3.1.

Table 1. Parameters of one-round Diffie-Hellman key exchange based on ring-LWE/LWE.

n	|p|	|f| or |F|	$\|s_i\|$ or $\|S_i\|$	$\|e_i\|$ or $\|E_i\|$	$\|g_i\|$ or $\|G_i\|$	$j=\|p\|-1$	Security
512	27	27×2^{9}	5	5	27×29	26	Ring-LWE Theorem 2.2
1024	30	30×2^{10}	5	5	30×210	29	
2048	33	33×2^{11}	6	6	33×211	32	
4096	36	36×2^{12}	6	6	36×212	35	
8192	39	39×2^{13}	7	7	39×213	38	
512	18	18×2^{9}	1	1	18×29	17	Ring-LWE Assumption 4.1
1024	20	20×2^{10}	1	1	20×210	19	
2048	22	22×2^{11}	1	1	22×211	21	
4096	24	24×2^{12}	1	1	24×212	23	
8192	26	26×2^{13}	1	1	26×213	25	
512	18	18×2^{18}	1	1	18×218	17	LWE Theorem 2.3 and 2.1
1024	20	20×2^{20}	1	1	20×220	19	
2048	22	22×2^{22}	1	1	22×222	21	
4096	24	24×2^{24}	1	1	24×224	23	
8192	26	26×2^{26}	1	1	26×226	25	

3.4. Implementation

In this section, we implement our construction based on Ring-LWE with small parameters. The parameters of our implementation are in Table **1**, whose unit of length is bit. In Table **1**, the first part is to use the origin parameters defined in [9] to guarantee provable security of our construction. The second part is to use the small parameters defined in [13] to improve its efficiency, but its security is based on the hardness of conjecture on Ring-LWE. The third part is to use LWE with small parameter defined in [13]. For every dimension n in Table **1**, we test 100 experiments to check the success probability of our protocol. The experimentation demonstrates that a shared key in every experiment is generated with probability almost 1.

Under the condition of small parameters, the security of our construction based on LWE depends upon the hardness of the worst-case lattice problem by Theorem 2.3. However, its complexity of communication is increased a factor n. On the other hand, the construction based on ring-LWE has higher efficient, but its security is only conjectured hard. Although the number of samples m is equal to n for ring-LWE, and satisfies to the condition $m = n(1+\Omega(1/\log n))$ in Theorem 2.3, we cannot generalize the result of Theorem 2.3 from LWE to Ring-LWE.

Assumption 3.1. Let n be integers, and $p \geq n^{O(1)}$ a sufficiently large polynomial bounded (prime) modulus. Then solving Ring-LWE with parameters n, p and uniformly random errors on set $\{-1, 0, 1\}$ is at least as hard as approximating ideal lattice problems in the worst case on $\Theta(n/\log n)$-dimensional lattices within a factor $\gamma = \tilde{O}(\sqrt{n} \cdot p)$.

CONCLUSION AND OPEN PROBLEM

We have constructed a one-round Diffie-Hellman key exchange protocol, whose security is based upon the hardness of ring-LWE (or LWE), and is as hard as approximating standard ideal lattice (or lattice) problems in the worst case with polynomial factor.

Our construct only works in two-party Diffie-Hellman key exchange. One interesting open problem is to construct multi-party Diffie-Hellman key exchange using ring-LWE.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This work was financially supported by the basic research Program of Jiangsu University of Technology under Grant (KYY14007/2015). This work was supported by the key laboratory of cloud computing and intelligent information processing of Changzhou City under (CM20123004-KF09).

REFERENCES

[1] Ratna Dutta and Rana Barua. Overview of Key Agreement Protocols. Cryptology ePrint Archive, Report 2005/289, 2005. http://eprint.iacr.org.

[2] W. Diffie and M. E. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

[3] A. Joux, "A One Round Protocol for Tripartite Diffie-Hellman", in Proc. 4th Algorithmic Number Theory Symposium, Leiden, 2000, pp. 385-393.

[4] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM Journal on Computing, vol. 5, no. 26, pp. 1484-1509.

[5] J. Ding, X. Xiang, X. Lin. A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem, Cryptology ePrint Archive, Report 2012/688, 2012. https://eprint.iacr.org.

[6] A. Georgescu, "An LWE-based Key Transfer Protocol with Anonymity", Tatra Mountains Mathematical Publications, vol. 53, no. 3, pp. 119-135, 2012.

[7] S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps from ideal lattices", in Proc. EUROCRYPT 2013, Athens, 2013, pp 1-17.

[8] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography", Journal of the ACM (JACM), vol. 56, no. 6, pp. 1-40, May. 2009.

[9] V. Lyubashevsky and C. Peikert and O. Regev, "On Ideal Lattices and Learning with Errors over Rings", in Proc. EUROCRYPT 2010, Nice, 2010, pp. 1–23.

[10] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problem", in Proc. STOC 2009, Bethesda, 2009, pp. 333–342.

[11] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé, "Classical Hardness of Learning with Errors", in Proc. STOC 2013, New York, 2013, pp. 575–584.

[12] B. Applebaum, D. Cash, C. Peikert, and A. Sahai, "Fast cryptographic primitives and circular-secure encryption based on hard learning problems", in Proc. CRYPTO 2009, Santa Barbara, 2009, pp. 595–618.

[13] D. Micciancio and C. Peikert, "Hardness of SIS and LWE with Small Parameters", in Proc. CRYPTO 2013, Santa Barbara, 2013, pp. 21-39.

[14] R. Lindner and C. Peikert, "Better Key Sizes (and Attacks) for LWE-Based Encryption, Topics in Cryptology", in Proc. CT-RSA 2011, San Francisco, 2011, pp. 319-339.

[15] S. Arora and R. Ge, "New algorithms for learning in presence of errors", in Proc. ICALP 2011, Zurich, 2011, pp. 403–415.

Received: June 10, 2015 Revised: July 29, 2015 Accepted: August 15, 2015