Available online at www.qu.edu.iq/journalcm

JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS

ISSN:2521-3504(online) ISSN:2074-0204(print)

New trend for LWE application in different computer science fields

Bushra Kamil Hilal [a],Mohammad Q.Jawad[b] , Dr. Ahmed W.Shehab[c]

Department of Computer information systems , College of Computer Science and information technology /University of Qadisiyah
Department of Biomedical InforMatics ,College of Biomedical Informatics University of IT & Communication ,Baghdad.Iraq
Department of Biomedical InforMatics ,College of Biomedical Informatics University of IT & Communication ,Baghdad.Iraq

bushra.k.h@qu.edu.iq
Mohammad.qassim 2002@uoitc .edu .iq
AHMED @uoitc .edu .iq

ARTICLE INFO

Article history:
Received: 03 /03/2023
Rrevised form: 14 /04/2023
Accepted : 19 /04/2023
Available online: 30 /06/2023

Keywords:

ring learning with error (RLWE), linkable ring signature scheme model , Homomorphic commitment scheme, Fiat-Shamir Transformation .

ABSTRACT

Problems of large keys in the on-lattice ring signature link due to reduce to the lattice, based on the problem of fault-tolerant learning on the ring (RLWE), according to "Homomorphic Commitment→∑-Protocol→Fiat-Shamir Transformation" reconstructs a linkable ring signature scheme on a lattice. First construct a base “Homomorphic commitment scheme” on polynomial ring of RLWE difficult, and use the Fiat-Shamir transformation method. The method converts the ∑-protocol into a linkable ring signature scheme, and suggests linkable ring signature scheme model. It is resistant to quantum computer attacks. compared with the previous linkable ring signature schemes on lattices, proposed methods with high computational, simple and less time frame because the ring elements in the scheme are taken from small polynomials which represents as case of application in computer science.

https://doi.org/10.29304/jqcm.2023.15.2.1230

1- Introduction:

The concept of ring signature was introduced by Rivest et al.[1] First mentioned in 2001 out. This scheme allows signers to anonymously select a signature group. sign the verifier signs the message, and the verifier can only determine that the signer is in the group member, but could not identify which member.

In 2004, Liu et al [2] in the ring an extended attribute called link ability is introduced in the signature, corresponding to ring signature scheme of is Linkable ring signature, while maintaining the anonymity of the signer, can detect two Whether the ring signature was created with similar signer which is same private key.

Linked ring signatures are used in crypto-currency, electronic elections, electronic cash and other applications Scene [3-5] important applications. In 2007, Au et al. [6] will be based on certificate is cryptosystem is certificate based cryptography, CBC) and Combined with chainable ring signatures, a certificate-based chainable Ring signature scheme.

∗Corresponding author

Email addresses:

Communicated by ‘sub etitor’

In 2013, Liu et al. [7] Install linkable ring signature integrity is further improved, and an unconditionally anonymous linkable ring signature is proposed Name scheme (the anonymity of the previous linkable ring signature scheme was calculated by anonymity).

However, the above ring signature schemes on based on the such as the discrete logarithm puzzle [8] and big integers The factorization problem [9], due to the existence of efficient quantum Translation algorithm [10] , if future quantum computers mature, based on classical number theory The cryptosystem of the hard problem will no longer be secure. In this case, the password Scholars in the field began to study post-quantum cryptography. in these alternatives In this case, lattice-based cryptography is highly parallelizable due to its efficiency and simplicity.

It is highly concerned that it can provide strong provable security guarantees Note. Reference [11] proposed an efficient lattice-based ring signature, but main disadvantage is that the length of the public key, private key and signature is large. Literature[12] The first lattice is constructed by "weak pseudo random function" on lattice, accumulator and zero-knowledge proof Chainable ring signature scheme.

The security of the scheme is based on small integers Solution (short integer solution, SIS) puzzle hypothesis [13]. Literature[14] ,∑-protocol framework based on ideal lattice [15] ,Construct A Linkable Ring Signature Scheme on Ideal Lattice Based on Ideal Lattice The shortest vector problem (SVP) prover case security. Reference [16] based on a lattice anti-collision hash function Constructed a linkable ring signature scheme on lattice, the security of the scheme performance is based on the module short integer solution, Module-SIS) hard problems (variants of SIS hard problems) and modules Fault-tolerant learning (module learning with errors, Module-LWE) Hard problem (variant of LWE hard problem). More recently, [17] is based on BLISS (bimodal lattice signature scheme) [18] constructs a lattice unconditionally anonymous scheme of linkable Ring with signature, small integer based on rings as in [19], whose signature length is O(N).

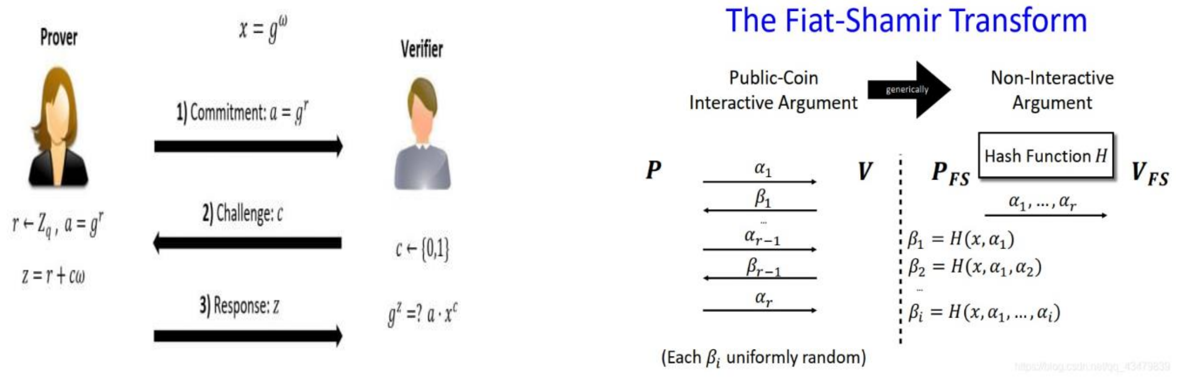
There is usually a key ruler in the cipher on lattice scheme based on LWE hard problem. the ciphertext space is large, and the efficiency is low, (RLWE) as in [20] (Proposed by Lyubashevsky et al. 2010) The two hard problems are is an improved version of the SIS and LWE puzzles on the ring, in the same To the full extent, RLWE puzzles cryptographic are compared The required key lengths for cryptographic schemes for the SIS and LWE problems are higher Shorter and faster to compute.

In order to solve the problem that the key size of the chainable ring signature scheme on the lattice is too long, The problem of low efficiency, this paper is based on the RLWE problem, according to the literature [14] The technical route of reconstructing an on-lattice linkable ring signature scheme And put forward an application scenario - a simple digital currency model. The difference of reference [15] is that reference [14] first constructs an ideal lattice to construct a chainable ring signature, and this paper first constructs a A homomorphic commitment scheme on polynomial rings based on the RLWE problem, then Then combine both Fiat-Shamir & sigma-protocol transformation method for linkable Ring signature.

2- Design proposed solution:

Symbols in this paper are explained, as shown in Figure 1. Figure 1 Symbol description symbol Z m × n q ||·|| Rq ||v||∞ λ∞ 1 (Λ) significance m-row n-column matrix of integers modulo q Euclidean norm of nonzero vectors Integer modulo q polynomial ring, Rq = Zq[x] x n + 1 Infinite norm of a vector ||v||∞ = max i = 0,1,...,n - 1 |vi | Infinity norm of lattice Λ Multiplying two Polynomial Rings x rounded up In addition to the symbols in Table 1, the text also uses symbols such as O, Ơ, ω, etc. , which is a common computational complexity symbol.

(lattice) Let b1,b2, bm be an n-dimensional Euclidean space ℝn The upper m linearly independent vectors, the lattice Λ is defined as the sum of all these vectors Linear combination of integer coefficients, i.e. Λ = ì i î u ý ∑i = 1 þ m xi bi :xi ∈ Z,i = 1,2,⋯,m the set of vectors b1,b2,⋯,bm is called a set of basis of the lattice.



sigma-protocol Fiat-shamir transform

Figure 1: proposed method (sigma-protocol+ Fiat-shamir transform)

2.1 RLWE:

Lyubashevsky et al [20] posed the RLWE problem in 2010, and Point out the worst-case- approximate-shortest-vector problem with ideal lattices of polynomial rings which is (SVP) is quantum normalizable to the computational RLWE problem, which can be a General protocol to decision RLWE (decision ring learning with errors, DRLWE) problems.

1. (RLWE distribution) For the safety parameter n, let f(x) = x n + 1 is the first irreducible polynomial of degree n, where n is a power of 2; Let q = 1 mod 2n be a sufficiently large prime, let the polynomial ring R = Z[x]/f (x) , Rq = R/qR . The error distribution χ is a Gaussian over Rq distributed. Let s ∈ Rq be the secret value, select a ← Rq randomly and uniformly, from Gaussian distribution randomly selects e ← χ , calculates b = a·s + e , and outputs (a, b) , the new distribution consisting of (a,b) is defined as As,χ , and on Rq × Rq The uniform distribution of is defined as U .
2. (computational RLWE problem assumptions) From the As,χ distribution Take a set of mutually independent variables (a,b = a·s + e), solve which contains The value s of , that is, given a, b, the recovery polynomial s is computationally infeasible.
3. (Decisive RLWE problem) is produced by (a,b = a·s + e) The raw distribution As,χ and the uniform distribution U over Rq × Rq are computationally infeasible. Discriminative, that is, to determine whether the parameters (a,b) are taken from the distribution As,χ or from The probability of a uniform distribution U is negligible.
4. (β bounded distribution) If a distribution χ satisfies Pre ← χ [||e|| ∞ < β] ≤ 1 - negl(n) , then it is called a β bounded distribution. 3. This section presents the security model and related security definitions.

2.2 A linkable ring signature:

Scheme in[7,21] by probability polynomials Algorithms (Setup, KGen, Sign, Vfy, Link) are composed.
(1) Setup (1) n) : Input the security parameter n and output the public parameter pp .

(2) KGen(pp): Enter the security parameter pp to generate user authentication key vk and signing key sk .

(3) Sign (ski ,U,μ) : input ring U , signer's private key ski , message μ, the algorithm outputs the signature σ of ring U to message μ.

(4) Vfy(μ,U,σ) : input ring U , message μ and ring signature σ , Accepts output 1; otherwise, outputs 0.

(5) Link(pp,σ,σ') : input public parameter pp , two ring signatures Name σ , σ' , the algorithm is used to verify whether two ring signatures σ , σ' are Generated for the same signer. If generated for the same signer, then Output 1; otherwise, output 0. 3.3.2 The definitions of anonymity and unforgeability are given below:
(anonymity) if message μ is in ring U and key vki0 The signature under is formally with message μ in ring U and key vki1 sign under If the names are exactly the same, the ring signature scheme (Setup, KGen, Sign, 1166 Formally, any adversary A is required to: Pr e e êê ù û úú pp ← Setup(1 n),(μ,i0,i1,U) ← A KGen (pp) b ←{0,1},σ←Signpp,skb (M,R) : A(σ) = b = 1 2 Among them, A chooses i0 , i1 , (vki0 ,ski0) , (vki1 ,ski1) predicted by the key KGen(pp) generates and vki0 ,vki1 ∈ U.

(Unforgeability) “Linkable Ring Signature Scheme” (Setup, KGen,Sign,Vfy,Link) are unforgeable, if attacker A only Knowing the public key and message signature pair, for unasked messages forging ring signatures is infeasible, formally for all probabilistic multinomials A time attacker A: Pr[pp ← Setup(1 n);(μ',U',σ') ← A VKGen,Sign (pp):Vfypp(μ',U',σ') = 1] ≈ 0

1- In the i-th query, VKGen randomly selects ri and runs (vki ,ski) ← KGen(pp,ri) , return vki ;

2- If (vki ,ski) by KGen(pp,ri) and vki ∈ U , then Sign(i,μ,U) returns σ ← Signpp,ski (μ,U);

3- A outputs the ring signature (μ',U',σ'), so that Sign is not signed by (μ', U',*) query, and U contains only the key vki generated by VKGen.

3- RLWE problem:

line analysis and Authenticity for the RLWE problem, that is, taking a set of mutually independent in-dependent variable (a,b = a·s + e) , solve for the value s contained in it, that is, to give Given a and b, it is computationally infeasible to restore the polynomial s, if s is It is regarded as a committed message, and e is regarded as a random number, so that a “Homomorphic commitment scheme” based on RLWE problem [22] .

Specifically, based on The homomorphic commitment scheme of the RLWE problem includes the following two algorithms: Parameter establishment algorithm (KGen): input the safety parameter n, let Rq = Zq[x]/ < x n + 1 > , where q is a sufficiently large common prime number, where n is a power of 2.

Randomly select elements a ← Rq , set the message The space is M= Rq , the random number space R= Rq , generating a Gaussian over Rq Distribution χ, the commitment space is C = Rq, and the commitment key ck ={a,n,q} is generated. Commitment Algorithm (Com): Input a message s ∈ M to be committed, Randomly choose a small error vector e ∈ R , e follows a χ distribution and ||e|| ∞ ≤ β , where β is a positive integer, computes the commitment c = a·s + e ∈ Rq .

1- (The proposed commitment scheme satisfies concealment) It can be seen from the computational RLWE problem that for a given number of group-independent (a,b = a·s + e) , it is not feasible to compute s (specifically Security proof reference [20]), so the proposed commitment scheme hides the It is obvious that, given the commitment value c , we want to calculate the committed value The message s , is computationally infeasible.

2- The proposed commitment scheme satisfies binding:

Let s = ω(lb n) , β < q/2d (d = ϕ(n) is the Euler function number), the proposed scheme satisfies the binding property. Assuming that for different messages s0 , s1 , the same commitment value c can be obtained, that is, for c0 = Com(s0 ; e0) , c1 = Com(s1 ; e1) , there is c0 = c1 . Since each ei = c - asi (i = 0,1) The infinity norm of is at most β, so for e0 - e1 = a(s1 - s0) infinite Norms are ||e0 - e1|| ∞ ≤ ||e0|| ∞ + ||e1|| ∞ < 2β . Since a is from Rq A uniformly randomly selected polynomial in , according to [23] (Lemma 21), The coefficients a of the polynomial ring a can be thought of as in the integer matrix A a column vector for any nonzero vector x ∈ Rn q , there is a very A large probability chooses a vector a with $||ax|| \infty \geq 2\beta$, which is the same as $||e0 - e1|| \infty < 2\beta$ is contradictory, so the commitment scheme in this paper satisfies the binding property.

3- (The proposed commitment scheme satisfies homomorphism) Assuming $s0,s1 \in M$, $e0,e1 \in R$, we have the following equations: $Com(s0 ; e0) + Com(s1 ; e1) =(as0 + e0) +(as1 + e1) = a(s0 + s1) +(e0 + e1) = Com(s0 + s1 ; e0 + e1)$ Therefore, the proposed commitment scheme satisfies additive homomorphism on polynomial rings.

3.1 RLWE commitment scheme

This paper is based on the RLWE commitment scheme, based on the technology of literature [14] route, and reconstruct an on-lattice linkable ring signature scheme. with text The difference from [14] is that this paper is based on the RLWE homomorphic inheritance in Section .

3.2. ∑-protocol and Fiat-Shamir transformation combination method

It used to construct Linkable ring signatures, while the reference [14] is based on the homomorphic inheritance on ideal lattices Nuo "scheme, ∑-protocol with Fiat-Shamir" grouping in [24] transform method to construct Chainable ring signatures.

Linkable ring signatures based on RLWE commitments scheme based on RLWE, R2LRS) includes 5 methods (Setup, KGen,Sign,Vfy,Link), the specific description is as follows: Setup(1 n ,N) : input security parameter n , number of ring members N , adjust Use the KGen algorithm of the homomorphic commitment scheme in Section 4.1 to generate the commitment key ck ={a,n,q} , M= Rq , R= Rq and the "commitment space" is C = Rq , choose a hash function $H: \{0,1\}^* \to \{-1,0,1\}^n$, the final output pp =(n,q,H,a,N) .

KGen(pp) : For the ℓth user, randomly choose $s \leftarrow Rq$ and Randomly sample an error $e \leftarrow \chi$, compute $c\ell = as + e\ell$, let the ℓth The user's verification public key $vk\ell = c\ell$, and the signature private key $sk\ell = e\ell$.

4. links linkable ring signatures (R2LRS):

It based on the RLWE puzzle Propose a new digital currency model. Using the literature [25], a One-time destination address technology, and according ≥ to the route of literature [14], re- Construct a digital currency model based on R2LRS., run R2LRS and public key plus The encryption algorithm (reference [20]) is used to initialize and generate all the Parameter PP. User key generation: This algorithm generates two pairs of public and private keys (epk, esk) and (c,e) .

Destination key generation: the sender chooses a random number $e\ p \leftarrow \chi$ And use the receiver key to generate a one-time destination address cd = c p + c. A complete signature cannot be recovered by anyone other than the recipient name key.. Purpose key recovery: For the receiver, first use the private key to decrypt Decrypt the symmetric key k, then use the symmetric key k to decrypt the hash(epk||ep) , then extract ep , calculate ed = ep + e,c'd , compare c'd = cd , it means that cd is a valid destination address, and ed is the corresponding address of cd valid signing key.

For users A and B, suppose A transfers money to B, and the system first gives Both parties generate a key pair, A uses B's public key to generate a one-time destination address, and then generate public key encryption information Enc(k) and symmetric encryption information hash(epk)||ep , A additionally collects other N - 1 one-time addresses, chain The receiving key, the signing key is generating "linkable ring signature", and finally A outputs Deposit amount, one-time destination address, encrypted information, ring signature and other information A hash operation is performed, and finally A broadcasts this information .

5-Conclusion

The contribution is to first construct a polynomial ring based on the RLWE problem The homomorphic commitment scheme and then combined with ∑-protocol, Fiat-Shamir transformation method to construct linkable ring signatures, and under the random oracle model Based on the computational RLWE problem, the security of the proposed scheme is proved, and the same when the An application scenario - a simple digital currency model due to show security aspects. next count It is planned to carry out experimental analysis on the scheme of this paper, and make further application scenarios.

Future work:

Application in different computer science fields such as in [23] author proposed simultaneously can encrypt multiple plaintext bits with smaller public parameters. also various non-commutative multiplication operations RLWE support error correction coding by larger message space and compares with normal LWE, In [24], finally The supply procedure with output of RLWE hardware implementation as accelerator yields good performance rather than other state of art in [25].

References:

[1] R L. Rivest, A. Shamir, and Y. Tauman, How to leak a secret[C]// LNCS 224, Dec 2001/7th *International Conf*. Theory and Application of Cryptology and Information Security: Advances in Cryptology . Australia. Springer, Berlin, Heidelberg. (2001) p: 552-565.

[2] J K . Liu, V K . Wei, and D S. Wong, Linkable spontaneous anonymous group signature for Ad Hoc groups[C]//LNCS 3108. Springer, Berlin, Heidelberg. pp: 325-335, Jul 2004 /9th *Australasian Conf*. Information Security and Privacy, Sydney, (2004)

[3] J K. Liu, M H . Au, X . Huang, and et al, New insight to preserve online survey accuracy and privacy in big data era[C]// LNCS 8713, Springer, 2014, p: 182-199,Sep 2014/19th European Symposium on Research in Computer Security, Poland,

[4] P P. Tsang, and V K .Wei, Short linkable ring signatures for EVoting, E- Cash and attestation[C]//LNCS 3439, Springer, Berlin, Heidelberg, p: 48-60, Apr 2005/1st International Conference on Information Security Practice and Experience, Singapore,(2005).

[5] S. Noether, Ring signature confidential transactions for monero [EB/OL]. . https://eprint.iacr.org/2015/1098.pdf.

[6] M H. Au, J K. Liu, W. Susilo, and et al. Certificate based (linkable) ring signature[C]//LNCS 4464: Springer, Berlin, Heidelberg, p: 79-92, May2007/ 3rd *International Conf*. on Information Security Practice and Experience, Hong Kong, China,.:

[7] J K. Liu, M H. Au, W. Susilo, and et al, Linkable ring signature with unconditional anonymity[J]. IEEE Transactions on Knowledge and Data Engineering, vol 26, (2014) p: 157-165.

[8] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, vol 31(1985) p: 469-472.

[9] R L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, vol 21(1978) p: 120-126.

[10] P W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Review, vol 41(1999) p: 303-332.

[11] M M.Tian, L S. Huang, and W.Yang, Efficient lattice-based ring signature scheme[J]. Chinese J. Computers, vol 35(2012) p: 712-718.

[12] R . Yang, M H. Au, J. Lai, and et al, Lattice- based techniques for accountable anonymity. abstract protocols and weak PRF. [EB/OL. https://eprint.iacr.org/2017/781.pdf.

[13] Ajtai M. Generating hard instances of lattice problems[C]. ACM. New York. p: 99-108, May 1996. /28th Annual ACM Symposium on the Theory of Computing, Philadelphia.(1969).

[14] H. Zhang, F G. Zhang, H B. Tian, and et al, Anonymous postquantum cryptocash[C]//LNCS 10957: Springer. Berlin. Heidelberg, p: 461-479, Feb 2018 / 22nd International Conference on Financial Cryptography and Data Security, Nieuwpoort, (2018).

[15] J . Groth, and M. Kohlweiss, One-out-of-many proofs: or how to leak a secret and spend a coin[C]//LNCS 9057: Springer, Berlin, Heidelberg,p: 253-280, Apr 2015 /34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Bulgaria, (2015).

[16] C. Baum, H. Lin, and S. Oechsner, Towards practical latticebased one- time linkable ring signatures[C]//LNCS 11149: Springer, Berlin, Heidelberg: p: 303-322, Oct 2018 / 20th International Conference on Information and Communications Security, Lille,(2018).

[17] W A. Torres, R. Steinfeld, A. Sakzad, and et al. Post- quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice RingCT v1.0) [C]//LNCS 10946: Springer, Berlin, Heidelberg, p: 558-576**.**Jul 2018/ 23rd Australasian Conference on Information Security and Privacy, Wollongong, (2018).

[18] L. Ducas, A. Durmus, T. Lepoint, and et al, Lattice signatures and bimodal Gaussians[C]//LNCS 8042: Springer, Berlin, Heidelber, p: 40-56,.Aug 2013/ 33rd Annual Cryptology Conference, Santa Barbara,(2013).

[19] D. Micciancio, Generalized compact knapsacks, cyclic lattices, and efficient one-way functions[J]. Computational Complexity, 16 ,(2007) p: 365-411.

[20] V. Lyubashevsky, C. Peikert, and O.Regev, On ideal lattices and learning with errors over rings[C]//LNCS 6110: Springer. Advances in Cryptology. Berlin, Heidelberg, (2010) p: 43.

[21] J K. Liu, and D S. Wong, Linkable ring signatures: security models and new schemes[C]//LNCS 3481: Springer, Berlin, Heidelberg, p: 614-623.May 2005 / International Conference on Computational Science and Its Applications, Singapore, (2005) p: 614-623.

[22] T P. Pedersen, Non-interactive and information-theoretic secure verifiable secret sharing[C]//LNCS 576: Proceedings 1171

[23] J. Li, P. Jialiang, and Q. Zhiqi , "A Ring Learning with Errors-Based Ciphertext-Policy Attribute-Based Proxy Re-Encryption Scheme for Secure Big Data Sharing in Cloud Environment." Big Data . (2022).unpublished.

[24] Grover, Charles, and et al, "Non-commutative ring learning with errors from cyclic algebras." J. Cryptology. 35. (2022). pp. 1-67.

[25] P.Baidya, M. Swagata, and P. Rourab, "Near Threshold Computation of Partitioned Ring Learning With Error (RLWE) Post Quantum Cryptography on Reconfigurable Architecture." arXiv preprint arXiv:2208.08093 . (2022).unpublished.