Lattice Based Group Signatures: Achieving Anonymity in Post Quantum World

Jayadev C.O Sekhar, Sangeetha Jose

Dept. of Information Technology, Government Engineering College Idukki, Kerala, India

***Abstract*—Group signature, as the name specifies is a special kind of signature scheme which allows a group of users to sign a message by preserving the constraints of anonymity and traceability. There are a lot of such schemes proposed by using number theoretic concepts. The emergence of quantum computers in the near future is making the existence of number theory based cryptographic constructions under scrutiny. Since lattice based cryptography overcomes the drawbacks of number theory based constructions, the post quantum world is interested in the lattice theory based constructions. This paper discusses about different lattice based group signatures.**

***Keywords*—Group signatures; lattice based crypto; post quantum crypto; quantum computers; number theory**

I. INTRODUCTION

Lattice based cryptography [10] finds its importance in the post quantum world, where the computational power is exponentially increased. Present world crypto systems does not consider the threat posed by the quantum computational power. The chances of breaking such systems using quantum computational power is very high. This is because of the fact that such systems are depending on hard problems which are breakable with quantum computational power. This raises the need for a good alternative, lattice based cryptography. It is making use of the hardness of some problems characterized by taking specific vector distances in the lattices. Quantum computational power seems to be insufficient for solving these problems. This feature of lattice problems can be used for the construction of post quantum crypto systems.

The algorithms that provide solution to the lattice problems takes exponential computational time. But the same algorithms, once given with quantum power can break the conventional number theoretic constructions in polynomial time, making them vulnerable to attacks by quantum computers [8]. So, lattice based cryptography seems to be the most attractive alternative for the post quantum world which is not so far away. The importance of lattice based cryptography also relies on the factors like worst case hardness, efficient implementations and relatively simple constructions. The research on the field of lattices have shown that there exist no polynomial time algorithm that approximates lattice problems to within polynomial factors. The security of all lattice based cryptographic constructions depends on this conjecture. Also, the development of lattice algorithms for solving these problems does not see any progress from the early 1980s.

II. CATEGORIES OF LATTICE CRYPTOGRAPHY

Lattice based cryptographic constructions can be divided in to two categories based on the security they provide. First one includes efficient practical proposals, but they lack a proof of security. Second one consist of constructions with strong provable security guarantees, but they are very inefficient when it comes to the practical implementation. The strong security guarantees given by the latter type is due to the worst case hardness of the lattice based problems. Worst case hardness indicates that the breaking of a cryptographic construction is equivalent in hardness to solving more than one lattice problems in worst case [9].

The worst case hardness mentioned above seems to be the distinguishing characteristic of lattice based cryptography. All other cryptographic systems are based on average case hardness, making the choice of lattices much better for security. At present, once if a system is based on the hardness of factoring, it implies the ability of factoring some numbers, not the ability to factor all the numbers. Worst case hardness ensure that attacks are likely to be effective only for a small set of parameters. That is it can assure that flaws in the construction are avoided. It also guides in making design decisions. Along with the above mentioned improvements in the design of the system, worst case hardness can also help in selection of concrete parameters for the cryptosystem.

Lattice based cryptography become the answer to the security threats raised in the post quantum world because there are currently no quantum algorithms for solving lattice problems which are better than known non quantum algorithms [10]. This does not imply that lattice problems can never be solved using quantum algorithms. Actually they are seemingly good candidates to be solved by such algorithms, because lattice problems are found to be not NP hard for approximation factors. Also, the Fourier transform, commonly used by quantum algorithms is very close to lattice duality. The periodicity finding technique used by the quantum algorithms does not seems to be feasible to solve the lattice problems, thanks to the geometrical structure followed by them.

III. GROUP SIGNATURES

Users of the group are allowed to sign messages on behalf of a group administered by some manager in the case of group signature schemes ([4]-[6]).The group manager initializes the group and he is responsible for the generation of public and

secret keys. Each of the users are given with unique personal secret keys by the manager. A member of the group can sign a message using their personal secret key, enabling anyone who knows the public key to verify that some group member signed the message. Group signatures are required to satisfy two requirements: given some group signature the group manager should be able to determine which member of the group signed the message (traceability), but no one other than the group manager should be able to know the identity of the signer (anonymity). Only the group manager can revoke the anonymity of a group member.

A. Types of Group Signatures

Based on the admissibility of new members in to the group, group signatures are of two types, static [6] and dynamic group signatures [5]. In static scheme, the number of group members is fixed during the initialization stage. The computation of secret signing keys for each member is done in this stage by the group manager. Static schemes are having different algorithms for signing, verification and opening of the signer identity. There exist only one group manager, who takes care of computing the secret signing keys of group members and of opening their signatures. In static schemes the key generation algorithm generates public key of the group, private key of the group manager allowing the latter to open group signatures, and a personal secret signing key for all members of the group. In case of dynamic group signatures, it is possible to add and revocate the members to and from the group. This is achieved by special algorithms for joining, revocation and for issuing keys for new users.

IV. A DETAIED STUDY ON GROUP SIGNATURES

A. Digital Signatures

Digital signatures [1] can be seen as the public-key alternative of message authentication. It is a technique that unites a person's identity/entity to the digital data. There exist a wide range of signature schemes for different applications in the real world. Proxy signatures [1] provides a kind of delegation for the signing capability of the signer. That is, the signer assigns his signing ability to a trusted third party and this party signs all the messages for the original signer. This simplifies the signing process for high computational framework. The concept of ring signature [2], gives the precedence of signing of a message to a group of users, who jointly decides on the signing capability. A subgroup of the members from the group signs the message and the verification is also done by the same group of members only. Here, the message is signed by the group of persons on behalf of the entire group. This scheme makes the common terminology of the need for peer signing better in terms of the computational requirements. Multi signature schemes [3], gives a new approach to the simplification of the common signatures. Here, a group of users signs a message by combining the individual signatures in to one signature. This makes the signature more compact in terms of the size as well as the structure of formation. These schemes makes the impact of signing the message by a group of members more effective and secure. Also, the complexity of the signing functionality is reduced by the construction of special group based signature schemes.

B. Group Signature

The group signature scheme, conveyed by Chaum and Heyst [4] proposed a methodology for signing a message by a single member of the group on behalf of the entire group. This led to the generation of signatures which took the identity of a group instead of an individual, still signed by an individual. The verification of the signature was still the same, as in the case of common signature schemes. Hence, the group signatures provided a level of simplicity for the signing process in special cases, where the signature has to be generated by a specified group of persons. The individual who signs the message for the group is also having the constraint of not revealing the identity at any moment of time during the whole process. So, one of the important feature of a group signature scheme is the anonymity of the signer. It should be preserving this property at any cost so that the possibility of forge ability can be reduced to minimum. The revealing of the identity of the signer is required during special cases in the scheme. For example, when the signature is causing some kind of a legal dispute for the group of members, the identity of the original signer will have to be revealed without any hesitation. This is done for avoiding the problem that may arise due to the judicial action taken against the generated signature. Instead of making the entire group members responsible for such an incident, it is favored to follow such an in need opening strategy, taken only during the special cases. The group is of course in need of a specified member who can manipulate such actions within the group, relating to the members, who can be called as the group manager. This group manager is having the responsibility of taking care of all the actions being taken by the group members. It can be seen that such a group manager is having the duty of addition and revocation of the members to/from the group. Along with managing the membership constraints of the group, this group manager is also responsible for the opening the identity of the signer of a specified signature, during cases of legal disputes. So, anonymity of the member can be broken only by the group manager. None other than the group manager should be capable of doing that at any moment of time.

C. Number Theoretic Constructions

Different kinds of group signatures [5] have been proposed based on the constraints of membership to the group. The main two categories are the static and dynamic group signatures. The static type is the kind of group signature in which the group is not changing. That is, neither addition nor revocation of members is possible in such a scheme. It will be having a specified group of members assigned for the signing process, which cannot be changed at any instance. In this case, only one group manager will be required for the purpose of opening the identity of the signer.

The working of a common static group signature scheme is given in [6]. The first stage in the scheme is the key generation stage, where the security parameters are used to generate the keys used in the scheme. This step is followed by the signature generation step, where the member generates a signature on a message using the private key assigned to him. The verification is done by the group public key on the generated signature. Opening of the signature is accomplished using the group manager's private key, which reveals the identity of the signer.

The Properties and the working of a number theory based dynamic group signature are specified in [7]. The only difference from the static case is that the later allows the admission of new members in to the group and the revocation of existing members. In this case, the responsibility of the group manager is distributed. It is not feasible to depend on a single group manager for performing both opening as well as membership management in the group. So, dynamic schemes always comprise of two group managers, one for the identity revealing and the second for the addition/revocation of members. The only difference in the action being performed from the static case is the addition of a specified joining algorithm. This algorithm is specifying the members who can join the group. Also the members get their private signing keys only after the joining step. So, in case of dynamic scheme, the key generation phase is divided in between the joining and the actual key generation phase.

D. Lattice based Cryptography

The need for lattice based cryptography is specified in [8]. The comparison between number theory and lattices showed the strength of lattices in terms of efficiency as well as the hardness of the underlying hard problems. The hard problems based on number theory are susceptible to attacks with quantum computational time. That is it is possible to solve the hard problems in polynomial time with quantum computers. In case of lattices, the lack of use of algebraic constructions and lack of vulnerability to recursive programming make them harder. So, the hard problems on lattices are not breakable by quantum computers, making them the best choice as an alternative to number theory in the post quantum world.

The main advantages of using lattice based cryptography are proposed in [9]. The security of the constructions are found to be provable in nature. That is, a set of well-defined hard problems can be used for achieving the security constraints. This makes the constructions even simpler to understand and implement. The security of the construction is based on some assumptions, which are worst case in nature. It can also be seen that the computations used in lattices do not depend on modular arithmetic. They are always making use of geometrical problems within the lattice structure, making the computation even simpler.

E. Lattice Based Cryptography- Hard Problems

The prime hard problem derived from lattices namely, the shortest vector problem is specified in [10]. It is defined as finding the shortest vector in a lattice, using only the basis is infeasible in polynomial time. The closest vector problem in lattices is given in [12]. This problem asks to find the closest point in the lattice from a point given in real space. This is found to be more computationally complex than the shortest vector problem. GapSVP problem [13], which asks to find whether the shortest vector is less than a particular value is a hard problem in lattices. Another variant of this, the shortest independent vector problem, asking for 'n' shortest vectors is used as a hard problem instance in the work of [14].

F. Lattice Based Group Signatures

The first work which proposed a static group signature scheme based on lattices is [15]. They followed the conventional strategies of signing specified in the work of Chaum and Heyst [4]. They made use of the Learning with Errors problem proposed by [15] as an instance of the basic shortest vector problem. It was possible to construct the static scheme, but the dynamicity was not added in the scheme.

A modified version of the above said scheme by the addition of the revocation feature is proposed by [15]. This was accomplished using a registration table for keeping track of all the activities of the group members. It was followed by a joining only scheme of [17]. This work proposes a similar construction of group signature, which achieves dynamicity of adding members in to the group only. Here, the revocation of members is not supported. So, new members could be added in to the group for the signing action, but the existing ones can never be discarded from the group. These two proposals were incomplete as far as the notion of fully dynamic group signature is concerned. This led to the development of the first ever fully dynamic group signature scheme from lattices by [18]. They proposed a fully dynamic scheme, as an extension of the above mentioned revocation only scheme. For the incorporation of admission of new members, they used an updated version of the Merkele tree accumulator. Along with the LWE problem, they included the Short Integer Solution problem for the easiness of the joining process with the tree accumulator. The use of two hard problem instances makes the construction questionable in terms of the worst case hardness posed by it.

V. CONCLUSIONS

The emergence of quantum computational power adversely affects the existence of existing cryptographic constructions based on number theory. The hard problems of number theory are breakable in polynomial time with quantum computational power. This gives rise to the need of an efficient alternative in the post quantum era. Lattice theory finds the space here, thanks to the worst case hardness posed by the lattice problems. This nature makes them harder than the number theory counterparts. The group signatures are important cryptographic constructions, finding many applications in

different fields of importance. There exist efficient static group signatures based on lattice assumptions. But only one full dynamic scheme is present which makes use of lattices. The development of more such schemes based on lattices, which allow joining as well as revocation of members to and from the group is still a much open problem.

ACKNOWLEDGMENT

We thank all the anonymous referees for their useful suggestions. Also, we are great full to our teachers, and friends for aiding us in conducting this survey.

REFERENCES

[1] Kim, Seungjoo, Sangjoon Park, and Dongho Won. (1997). Proxy signatures, revisited. International Conference on Information and Communications Security. Springer Berlin Heidelberg.

[2] Zhang, Fangguo, and Kwangjo Kim (2002). ID-based blind signature and ring signature from pairings. Advances in cryptology—ASIACRYPT 2002: 629-637.

[3] Yi, Lijang, Guoqiang Bai, and Guozhen Xiao.(2000) Proxy multi-signature scheme: a new type of proxy signature scheme. Electronics Letters 36.6 : 527-528.

[4] Chaum, David, and Eugène Van Heyst(1991).Group signatures. Advances in Cryptology—EUROCRYPT'91. Springer Berlin/Heidelberg.

[5] Bellare, Mihir, Haixia Shi, and Chong Zhang(2005). Foundations of group signatures: The case of dynamic groups. Cryptographers' Track at the RSA Conference. Springer, Berlin, Heidelberg.

[6] Abdalla, Michel, and Bogdan Warinschi(2004). On the minimal assumptions of group signature schemes. Information and Communications Security: 1-13.

[7] Zhou, Xuanwu (2007). Dynamic group signature with forward security and its application. Grid and Cooperative Computing, GCC 2007. Sixth International Conference on. IEEE.

[8] Micciancio, Daniele, and Oded Regev(2009). Lattice-based cryptography.Post-quantum cryptography. Springer Berlin Heidelberg, 147-191.

[9] Regev, Oded(2006). Lattice-based cryptography. CRYPTO. Vol. 4117.

[10] McKenzie, Ralph N., George F. McNulty, and Walter F. Taylor(1987). Algebras, lattices, varieties. Vol. I. The Wadsworth & Brooks/Cole Mathematics Series. Wadsworth & Brooks.

[11] Ajtai, Miklós(1998). The shortest vector problem in L 2 is NP-hard for randomized reductions. Proceedings of the thirtieth annual ACM symposium on Theory of computing. ACM.

[12] Peikert, Chris.(2009) Public-key cryptosystems from the worst-case shortest vector problem. Proceedings of the forty-first annual ACM symposium on Theory of computing. ACM,.

[13] Micciancio, Daniele, and Shafi Goldwasser(2002). Closest vector problem. Complexity of Lattice Problems. Springer US, 45-68.

[14] Gordon, S. Dov, Jonathan Katz, and Vinod Vaikuntanathan(2010). A group signature scheme from lattice assumptions. ASIACRYPT. Vol. 6477..

[15] Regev, Oded(2010) The learning with errors problem. Invited survey in CCC (2010): 15.

[16] Langlois, Adeline, et al.(2014) Lattice-Based Group Signature Scheme with Verifier-Local Revocation. Public Key Cryptography. Vol. 8383.

[17] Libert, Benoît, et al(2016). Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II 22. Springer Berlin Heidelberg.

[18] Ling, San, et al.(2017). Lattice-Based Group Signatures: Achieving Full Dynamicity with Ease. IACR Cryptology ePrint Archive 2017: 353.