Theoretical Computer Science 730 (2018) 1–20

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

A lattice-based group signature scheme with verifier-local revocation [☆]

San Ling [a], Khoa Nguyen [a,*], Adeline Roux-Langlois [b], Huaxiong Wang [a]

[a] Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore
[b] CNRS/IRISA, 263 avenue du Général Leclerc, 35042 Rennes, France

ARTICLE INFO

Article history:
Received 16 August 2017
Received in revised form 17 February 2018
Accepted 29 March 2018
Available online 4 April 2018
Communicated by G. Persiano

Keywords:
Group signatures
Verifier-local revocation
Lattice-based cryptography
Zero-knowledge arguments
Bonsai tree signature

ABSTRACT

Support of membership revocation is a desirable functionality for any group signature scheme. Among the known revocation approaches, verifier-local revocation (VLR) seems to be the most flexible one, because it only requires the verifiers to possess some up-to-date revocation information, but not the signers. All of the contemporary VLR group signatures operate in the bilinear map setting, and all of them will be insecure once quantum computers become a reality. In this work, we introduce the first lattice-based VLR group signature, and thus, the first such scheme that is believed to be quantum-resistant. In comparison with existing lattice-based group signatures, our scheme has several noticeable advantages: support of membership revocation, logarithmic-size signatures, and milder hardness assumptions. Moreover, our construction works without relying on public-key encryption schemes, which is an intriguing feature for group signatures.

1. Introduction

Group signatures have been an important research topic in public-key cryptography since their introduction by Chaum and van Heyst [15]. In these schemes, all the potential signers form a group, where each signer can anonymously issue a signature on behalf of the whole group (anonymity). On the other hand, in cases of disputes, there is a tracing mechanism which can link a given signature to the identity of the misbehaving member (traceability). These two attractive features allow group signatures to find applications in various real-life scenarios, such as anonymous online communications, digital right management, e-commerce systems, and much more. Over the last two decades, many group signature schemes with different security models, different levels of efficiency and functionality have been proposed ([16,4,5,8,9,6,21,28],...).

One desirable functionality of group signatures is the support for membership revocation. For example, misbehaving members who issue signatures for documents, which they are not allowed to sign, should be revoked from the group. In these cases, if a group signature scheme does not support revocation, then the whole system has to be re-initialized, which is obviously an unsuitable solution in practice. Currently there are two main revocation approaches for group signatures. The first approach requires all the unrevoked members to update their signing keys after each revocation ([4,12,8,11],...). At the same time, all the signature verifiers need to download the up-to-date group public key. As a consequence, it is sometimes inconvenient to practically implement such schemes. The second approach, that is group signatures with

[☆] This manuscript is the full, corrected version of a paper published in the proceedings of PKC 2014.
[*] Corresponding author.
E-mail address: khoantt@ntu.edu.sg (K. Nguyen).

https://doi.org/10.1016/j.tcs.2018.03.027
0304-3975/© 2018 Elsevier B.V. All rights reserved.

verifier-local revocation (VLR), only requires the verifiers to possess some up-to-date revocation information, but not the signers. Since in most of real-life scenarios, the number of signature verifiers is much smaller than the number of signers, this revocation approach is more flexible and more practical. Moreover, it is akin to that of the traditional Public Key Infrastructures, where the verifiers use the latest Certificate Revocation List to check the public key of the signer. The notion of VLR group signatures was introduced by Brickell [10], then formalized by Boneh and Shacham [9], further investigated and extended by Nakanishi and Funabiki [38,39], Libert and Vergnaud [29], and Bichsel et al. [7]. It is worth mentioning that all the existing VLR group signatures scheme operate in the bilinear map setting. Furthermore, all these schemes will be insecure once quantum computers become a reality [46]. Thus, constructing a VLR group signature schemes which is secure against quantum computers, or even outside of the bilinear map setting, is a challenging open question.

Lattice-based group signatures. Lattice-based cryptography is currently considered as the most promising candidate for post-quantum cryptography. As opposed to classical cryptography (i.e., based on the hardness of factoring or discrete log problems), lattice-based cryptography is widely believed to be resistant against quantum computers, moreover, it enjoys provable security under *worst-case* hardness assumptions ([1,44,19,36]). Designing secure and efficient lattice-based cryptographic constructions (and group signatures, in particular) becomes an intriguing challenge for the research community looking forward to the future. To the best of our knowledge, three lattice-based group signature schemes have been proposed, but none of them supports membership revocation. The first one was introduced by Gordon et al. [20] in 2010. While their scheme is of great theoretical interest, its signatures have size $\mathcal{O}(N)$, where N is the number of group users. In terms of efficiency, this is a noticeable disadvantage if the group is large, e.g., group of all employees of a big company. Camenisch et al. [13] later proposed lattice-based anonymous attribute tokens system, a primitive that can be considered as a generalization of group signature. However, in their construction, the signatures size is still linear in N. Recently, Laguillaumie et al. [23] designed a scheme featuring signature size $\widetilde{\mathcal{O}}(\log N)$, which is the first lattice-based group signature that overcomes the linear-size barrier. We remark that all the above mentioned schemes follow the traditional sign-and-encrypt-and-prove paradigm: to enable the tracing mechanism, these schemes require the signer to encrypt some private information via certain type of public-key encryption (PKE) based on the Learning With Errors (LWE) problem, and then generate a sophisticated proof to prove particularly that the ciphertext is well-formed. Relying on PKE to construct group signatures may imply two troublesome issues: firstly, it makes the construction less efficient; secondly, since the whole system is secure only if the underlying PKE scheme is secure, it sometimes does lead to a relatively strong hardness assumption. In particular, the recent scheme by Laguillaumie et al. [23] is only provably secure if there is no quantum algorithm to approximate the Shortest Independent Vectors Problem (SIVP_γ) on lattices of dimension n to within certain $\gamma = \widetilde{\mathcal{O}}(n^{8.5})$. This yields several interesting open questions in this direction: Is it possible to construct a scheme that supports membership revocation? Can lattice-based group signature schemes be free of LWE-based PKE? How to design a more efficient scheme based on weaker security assumptions?

Our contributions. In the present work, we reply to all the above open questions positively. In particular, we introduce the first group signature with verifier-local revocation from lattice assumptions, and thus, the first such scheme that is believed to be quantum-resistant. In comparison with known lattice-based group signatures, while the schemes from [20], [13] and [23] follow the CPA-*anonymity* and CCA-*anonymity* notions from [8,5], our construction satisfies the (weaker) notion of *selfless-anonymity* for VLR group signatures from [9]. Nevertheless, our scheme has several remarkable advantages over the contemporary counterparts:

1. Functionality: Our scheme is the first lattice-based group signature that supports membership revocation. As discussed above, this is a desirable functionality for any group signature scheme.
2. Simplicity: Our scheme is conceptually very simple. Each group signature roughly consists of an LWE instance and an all-in-one argument of knowledge, made non-interactive using Fiat–Shamir paradigm [18]. Moreover, the scheme departs from the traditional paradigm, and is free of LWE-based public-key encryptions.
3. Efficiency: For a security parameter n and for a group of N members, the group public key and the signature have bit-sizes $\widetilde{\mathcal{O}}(n^2) \cdot \log N$ and $\widetilde{\mathcal{O}}(n) \cdot \log N$, respectively. This level of asymptotic efficiency is comparable to that of [23], and is a noticeable improvement over those of [20] and [13].
4. Security assumption: Our scheme is proved to be secure (in the random oracle model) based on the worst-case hardness of approximating the Shortest Independent Vectors Problem, for general lattices of dimension n, to within a factor $\gamma = \widetilde{\mathcal{O}}(n^{2.5})$. That is, in contrast to [23], we achieve logarithmic-size signatures without having to pay a heavy cost in terms of hardness assumptions.

Overview of our techniques. The main building block of our VLR group signature scheme is a Stern-like [47] interactive argument system allowing a signer to convince the verifier in zero-knowledge that: (i) the signer is a certified group member (i.e., he possesses a valid secret signing key); (ii) the "revocation token" assigned to the signer is correctly committed via a function that is injective, one-way and pseudo-random. The argument system is repeated many times to make the soundness error negligibly small, and then is converted to a signature scheme via Fiat–Shamir heuristic [18]. If the produced signature is generated by an honest signer whose revocation token is unavailable to the verifier, then it should be