氏　　名	MAHARAGE NISANSALA SEVWANDI PERERA
博士の専攻分野の名称	博士（学術）
学位記号番号	博理工甲第 1099 号
学位授与年月日	平成 30 年 9 月 21 日
学位授与の条件	学位規則第 4 条第 1 項該当
学位論文題目	Dynamic Group Signatures using Verifier-local Revocation （検証者の局所的な登録無効化を用いた動的グループ署名）
論文審査委員	委員長　教　授　吉浦　紀晃 委　員　教　授　吉田　紀彦 委　員　准教授　後藤　祐一 委　員　教　授　内田　淳史 委　員　早稲田大学教授 小柴　健史

論文の内容の要旨

Group signatures allow members of the group to sign messages on behalf of the group while being anonymous. On the other hand, the group manager can identify the dispute members. Thus, group signature schemes provide two features, namely, anonymity and traceability. However, gaining strong security for group signature schemes with efficient member revocation mechanism is a quite difficult task. Throughout this thesis, we address the problem of achieving the strong security for fully dynamic group signatures with efficient member revocation mechanism. We use the simplest and efficient member revocation mechanism called Verifier-local revocation (VLR) as the revocation approach and deliver two new security notions and new methods as reasonable solutions for the addressed problems. Moreover, we propose seven schemes with those solutions.

In 2014 the first lattice-based group signature scheme was presented. That scheme used VLR as the member revocation approach. VLR is the most flexible and efficient revocation method at present since it requires only to update the verifiers when a member is revoked. Since the number of verifiers is less than the number of members in a group, passing revoking details to the verifiers are much more efficient than updating the existing members or generating keys newly as required by some other revocation methods. The group members have an attribute called, revocation tokens than the secret signing keys in VLR scheme. The revocation tokens are used to check the active status of the signing member. Once a member is revoked his token is added to a list called revocation list (RL), and RL is passed to the verifiers. However, their scheme relies on a weaker security notion called, selfless-anonymity. Moreover, they have not considered member registration and explicit tracing algorithm which is efficient than the implicit tracing algorithm that they use. On the other hand, in 2015 a much strong security notion called, full-anonymity was proposed. But it serves only for static groups, not for dynamic groups.

Stronger security for VLR schemes can be achieved in two ways. One approach is by using a restricted-version of full anonymity. The other process is changing the methods in the scheme.

In this thesis, we first suggest a new security notion called, almost-full anonymity. The almost-full anonymity provides the group public key and all the group secret signing keys to the adversary as the full anonymity at the anonymity game which we use to measure the security of a scheme. However, VLR schemes deal with another secret attribute called, revocation tokens. The revocation tokens are not available in static groups since they do not provide member revocation. Since we are dealing with VLR schemes, our new security notion the almost-full anonymity should consider managing the revocation tokens. We cannot allow the adversary to access revocation tokens of the indices that are used to generate the challenging signature. If the adversary knows the challenging indices' revocation tokens, then he can identify the owner of the signature easily. Thus, in the almost-full anonymity game, the adversary can request revocation token of any user. But, the requested toekn is only provided if the index of that revocation token is not used to generate the challenging signature. Moreover, at the challenging phase, the challenging signature is created only for the indices that are not used to request revocation tokens. Because of these restrictions, we can say, the almost-full anonymity is a restricted version of the full anonymity.

When employing the almost-full anonymity in schemes, since the almost-full anonymity requires to give all the secret signing keys to the adversary, the revocation token should not be able to generate using the secret signing keys. The previous VLR schemes, use part of the secret signing key as the revocation token. As the next step of our work, we provide a revocation token generation method which creates a revocation token separate to the secret signing keys. In the first scheme we suggested in the thesis, we have provided a new revocation token generation method, and we employed the almost-full anonymity to secure the first scheme.

Next, we consider about fully dynamic group signature schemes that provide both member registration and revocation with VLR. Group signature schemes with member registration present a joining-protocol where new users can interact with the group manager requesting to join the group. The new users who have valid keys can join the group if those keys are not used before. Once the group manager received the information from a new user, he validates the keys and issues the member certification for valid users. Since we use the VLR method, the new members should have member revocation tokens. In the joining protocol, we allow the group manager to produce a revocation token for the valid users. Moreover, when dealing with member registration schemes, we have to consider attacks that may the adversary execute by joining the group. Thus, we suggest another new security notion called, dynamical-almost-full anonymity to serve in the fully dynamic group signature schemes with VLR. The dynamical-almost-full anonymity allows the adversary to add new users to the group. However, even the revocation token should be provided at the time of joining, at the anonymity game we will not give the revocation token to the adversary at the registration query. However, the adversary can request revocation tokens of any member using the revocation query. As same as the almost-full anonymity, the revocation tokens are given to the adversary if only the requested indices are not used to generate the challenging signature, and the challenging signature is not generated for the indices that revocation tokens are revealed. In the anonymity game, the adversary may add the new users before and after the game starts. If the adversary adds the users before the game start as legal users, and if he used those member details at the challenging phase since the revocation tokens are already given, he can win the game. Thus, we have to track the newly added users by the adversary and should allow continuing the game with that information only. For that, we maintain a list called, HU and at the challenging phase, the signature is generated only for the indices which are in HU list. In this manner, in the dynamical-almost-full anonymity game allows to produce the challenging signature for the indices added by the adversary (in HU list) and not used for requesting revocation tokens.

Then we consider using full anonymity by changing the revocation and verification method. Here, the group manager

sign the revocation token before adding to the list. According to that, verifiers have to check whether the tokens in the list are signed by the group manager. Since the adversary does not know the group manager secret key even he has the tokens he cannot add them to the revocation list and check the signer of the given signatures as before. As a result we can directly apply full anonymity that provides all the secret keys including challenging indices tokens to the adversary.

In final step we consider the growth of the revocation list when applying in real life applications and provide a solution with time-bound keys. Thus each key has an expiration time and expired members cannot sign. We use dynamical-almost full anonymity secure our scheme.

In this thesis, using above techniques we proposed seven group signature schemes with VLR that satisfy stronger security than the previous VLR group signature schemes.

論文の審査結果の要旨

学位論文審査委員会は、平成 30 年 8 月 22 日に論文発表会を開催し、論文内容の発表に続いて詳細な質疑と論文内容の審査を行った。以下に審査結果を要約する。

グループ署名とは、グループに属する人が行なった署名から、その署名の検証者がグループの署名であるかを確認できるが、誰が署名したかは特定できない署名方式である。さらに、誰が署名したかを、グループの管理者が確認できることもグループ署名には要求される。グループ署名は暗号を利用して実現されるが、その中でも格子暗号を利用するものが提案されている。格子暗号は量子計算機に対する耐性があると考えられており、強力な暗号である。格子暗号を利用したグループ署名は、2010 年に Gorden らによって提案された。しかし、その鍵と署名のサイズがグループの人数に応じて増加するという問題があった。この問題は Languillaumie らにより解決されたが、そのグループ署名では処理時間が非常に大きくなってしまった。Ling らにより処理時間がより少ないグループ署名が提案されてきたが、グループメンバーの追加や削除などを行うことができない、つまり、グループメンバーが固定されていることが前提となっている。

グループメンバーの変更が可能であるグループ署名の研究としては、Langlois らが 2014 年にメンバーの削除が可能な格子暗号によるグループ署名を提案したのが最初である。この提案手法は、Verifier-localrevocation(VLR) を利用している。VLR では、グループ署名の検証者に、メンバーの削除に関する情報を伝えることだけで、削除されたメンバーが行なったグループ署名を無効とすることができる。他に、メンバーの削除可能なグループ署名には、メンバーの削除の度にメンバーへ署名のための鍵を配布し直す方法などがあるが、VLR が効率良い方法であると考えられている。一方で、Libert らは、メンバーの追加が可能な格子暗号によるグループ署名を提案した。そして、Ling らがメンバーの追加と削除の両方が可能な格子暗号によるグループ署名を初めて提案した。これは、Merkle tree accumulator を用いている。

以上のことを踏まえ、本論文では VLR を用いたメンバーの削除追加が可能な格子暗号によるグループ署名手法を提案する。そして、VLR を用いた従来のグループ署名よりもよりセキュアな手法を提案する。

本論文の構成と内容は次のとおりである。

第 1 章では、本論文の背景、グループ署名とその有効性、グループ署名に関するこれまでの研究、本論文が目標とするグループ署名、そして、本論文の構成について述べている。

第 2 章では、本論文の議論の中で必要となる定義や基本技術を説明している。主に、格子暗号について説明している。

第 3 章では、グループ署名の説明を行なっている。具体的には、メンバーの追加や削除がない場合のグループ署名、メンバーの追加や削除のある場合のグループ署名、メンバー削除の方法である Verifier-local-revocation(VLR) によるグループ署名を説明している。

第 4 章では、グループ署名におけるセキュリティ上の性質について説明している。グループ署名では、グループの誰が署名したかが、署名を検証する人がわからない性質である Full Anonymity、グループ管理者が署名を行なった人が特定できる性質である Full Traceability などいくつかの重要な性質があり、これらを説明している。

第 5 章では、VLR を利用した格子暗号によるグループ署名を提案している。本論文では、7 つのグループ署名を提案しているが、その 1 つ目である VLR によるメンバー削除が可能であり Almost Full Anonymity な性質をもつグループ署名の方法を提案している。Almost Full Anonymity とは本論文で提案した新しい性質であり、従来用いられていた Full Anonymity よりは弱い性質であるが、実用性を考えた場合には十分な

性質であると考えられる。

第６章では、VLR を利用したメンバーの追加と削除が可能なグループ署名を提案している。この章では、メンバーの削除と追加が可能な Almost Full Anonymity なグループ署名を提案した。また、メンバーの削除と追加が可能な Almost Full Anonymity な格子暗号によるグループ署名を提案し、鍵が短い方式、VLR で利用するときの処理が効率的である方式、そして、プロトコルが単純である方式を提案している。

第７章では、メンバーの削除が可能な Full Anonymity な格子暗号によるグループ署名を提案している。この方式は、第５章で提案されているグループ署名と比較してより処理負担が大きくなっているが、セキュアになっている。

第８章では、グループ署名の処理効率を向上させるために、第５章で提案されたグループ署名に対して、Time bound key を導入した新しいグループ署名を提案している。

最後に第９章では、本論文で得られた成果をまとめるとともに、今後の課題を述べている。

以上、要するに、本論文では、グループメンバーの追加と削除が可能となるグループ署名を提案した。このグループ署名は格子暗号に基づいており強度が高い。そして、Almost Full Anonymity というセキュリティ上の性質を導入し、この性質を満たしていることを示した。本論文で得られた成果は、新たなグループ署名の提案となっており、重要な意義があり応用上でも有用である。

本論文の主な内容は、査読付き学術雑誌論文４編（数理電子情報コースにおいて学術雑誌論文相当と見なす査読付き国際会議論文を含む）で公表ないしは受理されている。

以上を総合し、本学位論文審査委員会は、本論文が、博士（学術）の学位を授与するに十分に値するものと認め、「合格」と判定した。