論文 / 著書情報
Article / Book Information

題目(和文)	アドホックグループ上の匿名認証
Title(English)	Anonymous Authentication over Ad-Hoc Groups
著者(和文)	原啓祐
Author(English)	Keisuke Hara
出典(和文)	学位:博士(理学), 学位授与機関:東京工業大学, 報告番号:甲第11712号, 授与年月日:2022年3月26日, 学位の種別:課程博士, 審査員:田中 圭介,伊東 利哉,尾形 わかは,鹿島 亮,安永 憲司
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第11712号, Conferred date:2022/3/26, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	論文要旨
Type(English)	Summary

（博士課程）
Doctoral Program

論 文 要 旨

THESIS SUMMARY

系・コース： Department of, Graduate major in	数理・計算科学　系 数理・計算科学　コース	申請学位（専攻分野）： Academic Degree Requested	博士（理学） Doctor of
学生氏名： Student's Name	原 啓祐	指導教員（主）： Academic Supervisor(main)	田中 圭介
		指導教員（副）： Academic Supervisor(sub)	

要旨（和文 2000 字程度）
Thesis Summary（approx.2000 Japanese Characters ）

近年、SNS などを通して個人がインターネット上に情報を発信することが多くなり、インターネット上で個人の匿名性は保証することは、情報化社会における個人の発言の自由を保護するためには欠かせなく、重要な要件である。その一方で、Tor ネットワークなどの個人に対して無制限な匿名性を与えてしまう機構は、情報化社会において無秩序をもたらし、サイバー犯罪を増長させてしまう恐れもある。このようなサイバー犯罪を防ぐにはユーザに否認不可性を要求することも重要であり、これを実現するにあたっては、電子的に身分を証明するための電子署名技術が広く用いられてきたが、この解決策の問題点は、電子署名を要求することにより署名者の身分が一意に特定されてしまうことである。つまり、今度はユーザに対して匿名性を一切付与できず、上記の個人の匿名性の問題が解決できなくなってしまう。

本論文では、このような現代におけるユーザの匿名性と否認不可性のジレンマを解決するための近年注目されている代表的な高機能署名技術である ring signature 及び (deniable) ring authentication に対する安全性や性能効率の改善に関する様々な提案を行う。

まず、第一の成果として、（人工的な仮定や第三者によるセットアップを仮定しない）Plain Model における情報理論的な匿名性を満たす標準的な仮定に基づくリング署名の一般的構成を提案する。この構成は、（通常の）署名方式、ロッシー暗号、2 ラウンドの対話型証明システムを組み合わせることで構成できる。これらの構成要素は、learning with errors (LWE) 仮定という高次元の格子上で定義される最も標準的な仮定に基づき構成可能である。

次に、第二の成果として、（従来ではランダムオラクルモデルでしか得られていなかった）安全性の根拠とする困難性問題に対してタイトな帰着をつけることができ、かつ、署名サイズがリングのサイズに対して対数的にしか増加しないリング署名方式を、Plain Model において初めて提案する。この構成は、（通常の）署名方式、公開鍵暗号、非対話型証明システム、somewhere perfectly binding hash function を組み合わせることで構成できる。これらの構成要素は、双線形写像群上の最も標準的な困難性仮定の一つである Decision Linear (DLIN) 仮定の下で安全であることが証明可能であり、提案方式の安全性はこれらの構成要素に定数のロスしか発生させずに帰着することが可能である。

最後に、第三の成果として、ランダムオラクルモデルの下で、任意の放送型暗号方式を deniable ring authentication に変換する一般的な手法を提案する。この変換手法を用いることにより、2 ラウンドの通信回数しか必要とせず、各通信量や計算量が最適であり、concurrent deniability を満たす deniable ring authentication の提案が初めて達成される。また、耐量子性を持つ困難性仮定である LWE や（符号理論における）learning parity with noise (LPN) 仮定等からの構成を初めて与えるものでもある。この変換手法は、任意の放送型暗号方式をサポートするため、今後新たな効率の良い放送型暗号方式が得られると、即座に新たな効率の良い deniable ring authentication を得ることを可能とするものである。

備考：論文要旨は、和文 2000 字と英文 300 語を 1 部ずつ提出するか、もしくは英文 800 語を 1 部提出してください。
Note：Thesis Summary should be submitted in either a copy of 2000 Japanese Characters and 300 Words (English) or 1copy of 800 Words (English).

注意：論文要旨は、東工大リサーチリポジトリ(T2R2)にてインターネット公表されますので、公表可能な範囲の内容で作成してください。
Attention: Thesis Summary will be published on Tokyo Tech Research Repository Website (T2R2).

（博士課程）
Doctoral Program

論 文 要 旨

THESIS SUMMARY

系・コース： Department of, Graduate major in	数理・計算科学　系 数理・計算科学　コース	申請学位（専攻分野）： Academic Degree Requested	博士（　理学　） Doctor of
学生氏名： Student's Name	原　啓祐	指導教員（主）： Academic Supervisor(main)	田中　圭介
		指導教員（副）： Academic Supervisor(sub)	

要旨（英文 300 語程度）
Thesis Summary（approx.300 English Words ）

In recent years, people are increasingly sending out information on the Internet, for example, through the social networking services. When we communicate with others through the Internet, we need to make sure that the counter party is the right person and the communication is authenticated. For realizing this, an authentication protocol is one of the most important cryptographic primitives in an Internet-based communication. By using an authentication protocol, a receiver of a message, Bob, can verify that the message received is indeed the one sent by the sender, Alice.

While it is important to consider the authenticity for users, it is also required to ensure the opposite properties, that is, anonymity for users in some real-world applications. In particular, users' anonymity on the Internet is one of the most important requirements for protecting the freedom of personal speech. In fact, in order to meet the demand for anonymity, some technologies providing users with (unlimited) anonymity on the Internet (such as, the Tor network) have been developed.

In order to solve this dilemma between these two properties (authenticity and anonymity), various anonymous authentication primitives have been proposed so far (e.g., group signature, attribute-based signature, anonymous credential, and so on). Among these primitives, in this thesis, we focus on two anonymous authentication primitives over ad-hoc groups of users: ring signature and (deniable) ring authentication.

Specifically, as the first result, we provide a ring signature scheme with unconditional anonymity in the plain model based on the computational assumption over lattices.

Then, as the second result, we provide an efficient and tightly secure ring signature scheme in the plain model based on the computational assumption over bilinear groups.

Finally, as the third result, we provide a generic transformation from broadcast encryption to (deniable) ring authentication in the random oracle model.

備考 ： 論文要旨は、和文 2000 字と英文 300 語を 1 部ずつ提出するか、もしくは英文 800 語を 1 部提出してください。
Note : Thesis Summary should be submitted in either a copy of 2000 Japanese Characters and 300 Words (English) or 1copy of 800 Words (English).

注意：論文要旨は、東工大リサーチリポジトリ(T2R2)にてインターネット公表されますので、公表可能な範囲の内容で作成してください。
Attention: Thesis Summary will be published on Tokyo Tech Research Repository Website (T2R2).