論　文　の　要　旨

題 目　A Study on Privacy-Enhancing User Authentication Systems with Efficiency Improvements
（プライバシーを保護したユーザ認証システムの効率改善についての研究）

氏名　Shahidatul Sadiah Binti Abdul Manan

The internet has currently become a ubiquitous channel for data hub and dissemination since the networking infrastructure has grown to connect computers all over the world through cloud applications and online services. In such services, user authentications are required to permit only access from a valid user. On the other hand, through the authentication, service providers collect a large amount of information about the users and their online activities. This information can be beneficial for the service providers, but the way of handling them might also present challenges to user's privacy.

One of cryptographic solutions to protect the users' privacy in the authentication is an *anonymous credential scheme*. This scheme allows an issuer to issue each user a certificate as a proof of the qualification that contains the user's attributes. The user can anonymously convince any verifier for the possession of the certificate, where the selected attributes can be disclosed without revealing any other information about the user's privacy. In general, complex relations on attributes can be proved. Previously, an anonymous credential system with constant size proofs was proposed, where a user can prove any Conjunctive Normal Form (CNF) formulas, i.e., an ANDs of ORs, on attributes. However, this system still suffers from inefficiency in the case of numerous OR literals, due to the less expression capability of CNF formulas. To achieve the constant-size proof, this system utilizes an *accumulator* that compresses multiple attributes of a formula into a single value. In the compression, the accumulator requires that all public parameters assigned to the attribute values of OR literals in the formula are multiplied which cause a large delay in the proof generation.

In the first part of this thesis, we propose an extended accumulator to prove *monotone formulas* on attributes and apply it to the anonymous credential system in order to obtain more efficiency in the proof generation. The monotone formula is a logic formula that contains any combination of AND and OR relations without negations. That is, CNF formula is a limited type of the monotone formulas. Thus, in the cases that proved formulas require longer sizes in the representation of CNF formula than monotone formula, the proposed system has more efficient computation costs. We ensure this in the implementation, where the experimental result shows that the proposed scheme reduced the proving time from 969.11*ms* to 63.04*ms* and the verifying time is reduced from 376.97*ms* to 132.57*ms* in a practical example.

Another cryptographic solution to protect the users' privacy in the authentication is a *group signature scheme*, which is the digital signature version of the anonymous credential. In the scheme, a group member is allowed to sign a message anonymously on behalf of the group. There are two types of authorities engage: A *group manager*, (GM) who adds users into the group, and an *opener* who can identify the signer from the signature when necessary. One important function in the group signature scheme is *revocation*, where the user's privilege to sign a message is removed. The revocation is a critical issue, which has been broadly studied.

Previously, Libert et al. proposed a revocable group signature scheme, where for number of users N, the scheme has achieved $O(1)$ signature size, $O(1)$ signing/verification costs, $O(1)$ membership certificate size, and $O(\log N)$ public key size. However, the scheme still needs an improvement on the $O(R)$ revocation list (RL) size, where R is the number of revocations. This is because the signer needs to fetch the RL for every revocation epoch, thus, the large size will cause delay in mobile environment. Later, Nakanishi et al. proposed a scheme with compact RL using an accumulator. In this scheme, GM accumulates T subsets in the SD method and signs the accumulated value for any integer T. Thus, the number of signatures is reduced by $1/T$ and the RL size is $O(R/T)$. However, the signing time, the public key size and membership certificate size are increased, when T is increased.

On the second part of this paper, we extend the scheme proposed by Libert et al.. In the proposed scheme, similarly to the scheme by Nakanishi et al., we partition the subsets into a number of blocks and compress it using a *vector commitment*. Since the compression is simpler than the accumulator, we can reduce the RL size to $O(R/T)$ while maintaining the membership certificate size as $O(1)$. However, the signing cost still depends on T, and the verification has constant overhead costs, since there are more proofs of the zero-knowledge fashion. This scheme seems to be practical on the RL size, but the practicality of the signing time for concrete values of T, and the overheads in the verification time are unknown. To clarify that, we implemented the scheme with some efficiency improvements to show the time efficiency. From the experimental results, the signing time is less than 500 ms for $T = 400$, but the verification time is about 1.5 s. We consider that the implemented scheme is practical in a mobile environment due to lower user computation time and storage.