



Title	Secure and efficient post-quantum commitment scheme and its application
Author(s)	宮地, 秀至
Citation	大阪大学, 2023, 博士論文
Version Type	
URL	https://hdl.handle.net/11094/92886
rights	
Note	やむを得ない事由があると学位審査研究科が承認したため、全文に代えてその内容の要約を公開しています。全文のご利用をご希望の場合は、大阪大学の博士論文についてをご参照ください。

The University of Osaka Institutional Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

The University of Osaka

論文内容の要旨

氏 名 (宮 地 秀 至)	
論文題名	Secure and efficient post-quantum commitment scheme and its application (安全で効率的な耐量子暗号を用いたコミットメント方式の構成とその応用)
In recent years, many services that were previously realized in analog form are now realized in digital form. To realize many services securely in digital form, a cryptographic technology called a commitment scheme is indispensable. A commitment scheme can control the timing of decryption and is executed in a commitment phase and a decommitment phase between a sender and a receiver. It is secure by showing the sender and receiver cannot cheat in each phase (hiding and binding properties). In this dissertation, the following three technical issues were proposed to achieve a practical commitment scheme. In the first research, a post-quantum commitment scheme with a small constant of output locality 3 was proposed. The output locality is a natural complexity measure of computational efficiency for boolean functions. If the commitment scheme satisfies k constant output locality, then it is executed at a constant k depth for any input. In other words, a constant low output locality commitment scheme can achieve efficiency. The existing output locality 4 commitment scheme used a randomness extractor to achieve a constant output locality. A randomness extractor requires many random numbers, which made the commitment scheme a more complicated construction. In this proposal, a simple commitment scheme with output locality 3 was realized without using a randomness extractor. Its hiding and binding properties were also proved. Finally, the security parameters of the commitment scheme were also evaluated as well. In the second research, a message-scalable commitment scheme was proposed by using post-quantum cryptography. To prove the binding property of commitment schemes using post-quantum cryptography, some existing research increases the output length by padding zeros to the input length. By expanding the zeros parts to the input length, more messages can be sent, and it becomes a more practical commitment scheme. To achieve the doubled input length, a new assumption is introduced to prove its binding property. In this proposal, a post-quantum commitment scheme that can send twice the input length for the same output length compared to the existing research was proposed. Its hiding property was also proven. Finally, the proposed commitment scheme was compared with other existing research. In the third research, a commitment scheme was applied to social media (SM) for the first time. SM has turned into one of the main communication tools in our society, and various issues related to SM have arisen. One of the issues is a linkable feature and no disclosure feature in SM. In the existing SM, since the post name is linked to the content of the post, it is possible to identify the privacy information of the user from the content of the post, even if the post name is anonymous. Because of this feature, it is not possible to disclose only a part of a post and claim that it is one's own post. SM that satisfies both unlinkability and disclosure has been proposed for the first time by focusing on a commitment scheme. Furthermore, to make the proposed social media practical, the proposed SM was implemented and evaluated. In this dissertation, secure and efficient post-quantum commitment schemes were proposed and its application to social media was shown, which achieved unlinkability and disclosure for the first time.	

論文審査の結果の要旨及び担当者

氏 名 (宮地 秀至)			
	(職)	氏 名	
論文審査担当者	主 査	教授	宮地 充子
	副 査	教授	滝根 哲哉
	副 査	教授	丸田 章博
	副 査	教授	井上 恭
	副 査	教授	田中 雄一
	副 査	教授	鷲尾 隆
	副 査	教授	駒谷 和範
	副 査	講師	王 イントウ
	副 査	教授	河内 亮周 (三重大学工学部情報工学科)

論文審査の結果の要旨

In recent years, our society has become increasingly digitalized. Many services that were previously realized in analog way are now realized digitally. Digitization is not only to services such as ticket reservations, purchases, and tax payments, but also to activities such as bidding, commercial transactions, lectures, and ways of working. However, it is very difficult to achieve digitization in a secure manner, especially digitization of activities. Take bidding, for example. In a bidding process, multiple companies respond to bids, and the company with the highest price wins. In the analog bidding, there is not much of a problem because the bids are written on paper and the bids are not opened until the time of the opening of bids. The digital bidding, on the other hand, requires encryption of the bid value so that no one can know the bid value until the bid opening. This is because the possibility of collusion cannot be ruled out if some people can compound the bid values. In other words, the data must be encrypted in such a way that it cannot be decrypted until a certain point in time. This property is called hiding property. On the other hand, if a bidder can decrypt the data to a value that is different from the encrypted bid, the bidding will not be fair. In other words, it is necessary for the bidder to correctly return to the original bid value when decrypting. This property is called binding property. A scheme that has both these properties is called a commitment scheme, and it is one of the essential security technologies to achieve digitization in a secure manner. Therefore, it is important to construct secure and efficient commitment scheme.

In this dissertation, secure and efficient commitment schemes are studied and a Social Media (SM) with unprecedented features by applying the commitment scheme are proposed. This dissertation consists of the following three contributions.

1. Construction of post-quantum commitment schemes satisfied with theoretical efficiency

To achieve a secure and efficient commitment scheme, a notion of output locality is applied. The output locality is a natural complexity measure of computational efficiency for Boolean functions. If the commitment scheme satisfies k constant output locality, then it is executed to a constant k depth for any input. Based on the notion of output locality, a post-quantum commitment scheme with a small constant output locality 3 is realized. Until this result, the existing commitment has output locality 4, which further used a randomness extractor. A randomness extractor requires complicated construction as well as many random numbers. Compared with the existing best results, this proposal gives the lowest output locality 3 and is a simple commitment scheme without using a randomness extractor. Its hiding and binding properties are also

proved.

2. Construction of a post-quantum message-scalable commitment scheme

Generally, in commitment schemes, the size of output ciphertext tends to be larger than the input plaintext size in order to achieve binding property. This causes a degradation of communication efficiency. To improve communication efficiency, it is desirable to reduce the size of the ciphertext relative to the plaintext. By introducing a new security assumption, this scheme allows the space used for proofs on the binding property to be used for message space. As a result, it is possible to reduce the expansion of the output ciphertext size with respect to the input plaintext size. With some security control, a commitment scheme that allows a larger size of plaintexts to be input at a time is achieved, and the effect is immeasurable.

3. Construction of SM satisfied with flexible and secure privacy control

With the progress of digitization, there has been a change in the way people connect with each other. In recent years, SM has become the important method of communication in society, in addition to face-to-face communication. However, SM has various problems. One of them is the protection of privacy: SM is generally posted under a nickname, which is supposed to protect privacy, but by linking information posted under the same nickname, a person can be identified. The other is the authorship claim to privacy-protected postings. Generally, posts are made anonymously, but there are cases in which authorship may be claimed depending on the contents of the postings. In this case, it is necessary to claim the authorship of a particular posting, but to protect the privacy of others. In other words, existing SM has not been able to realize flexible and secure privacy control. By applying the hiding and binding property of the commitment scheme, the flexible and secure privacy control SM has been realized for the first time. This is the first research to apply the commitment scheme to SM.

As described above, in this dissertation, secure and efficient commitment schemes are realized by applying a notion of output locality and resolving a problem of message-expansion feature and a SM with flexible and secure privacy control. The applications of the proposed commitment schemes are not limited to social media. As mentioned in the beginning, the commitment scheme is one of the essential security technologies to achieve digitization in a secure manner, and their effectiveness is very high. Furthermore, the contribution is not only the application of the commitment scheme to SM, but rather, it has shown how the commitment scheme can be applied to realize secure digitization and clarified the effectiveness of the commitment scheme in digitization. The impact of this research on the further digitization of society in the future is immeasurable.

Therefore, this thesis contributes significantly to the development of the field of information security and engineering and is recognized as a valuable doctoral dissertation.