Functional Encryption Enabling Secure Leasing of Private Keys

Ryo Nishimaki

Abstract

Proving the non-existence of something is a difficult proposition called "the devil's proof." However, quantum mechanics can be used to prove that private keys used in functional encryption have been deleted (do not exist). It can also be used to prevent duplication of private keys. In this article, the method that my research colleague and I proposed at an international conference held by the International Association for Cryptologic Research in 2022 is overviewed, and the innovations expected when this method is implemented are described.

Keywords: cryptography, quantum computation, deletion of information

1. Advanced cryptography and private keys for the cloud era

One of the cryptographic methods used for one-to-many communication is called public-key cryptography. Anyone can encrypt a message without sharing a key in advance, and a private key is used to decrypt the message. Various *intelligent cryptosystems* that embed advanced logic in public-key cryptosystems are currently being proposed. A well-known example is attribute-based encryption in which user attributes are set in a private key and its decryption capability is based on those attributes. For example, if the encryption incorporates the conditions "personnel department" and "section chief," only the person holding the key with exactly the same attributes can decrypt it. Confidentiality of the message is protected because keys with attributes such as "personnel department/subsection chief" or "sales department/section chief" that only partially meet the conditions cannot decrypt the ciphertext above.

Functional encryption, which is studied by my research colleague and I in a paper titled "Functional Encryption with Secure Key Leasing" [1] published in January 2023, is a more-powerful type of intelligent cryptography. In contrast to attribute-based encryption, which can only obtain entire plaintext, functional encryption can obtain processed information computed from plaintext by decrypting ciphertext (**Fig. 1**). If functional encryption is practically applied, it will, for example, make it possible to calculate only statistical information from an encrypted database stocked with medical information on patients with intractable diseases in a manner that does not infringe the privacy of the patients. Advanced cryptography is expected to be a powerful tool for assuring information security in the cloud era.

Private keys can be generated on current computers.

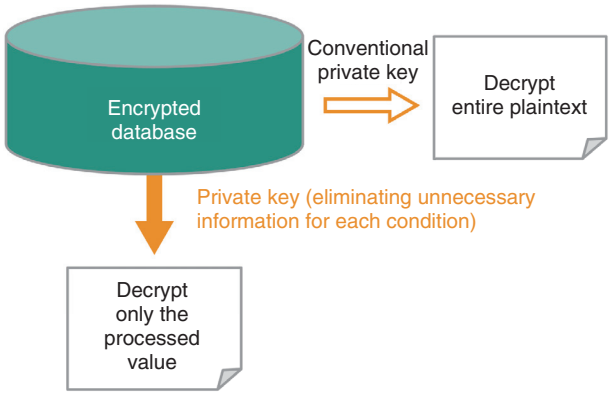


Fig. 1. Functional encryption.

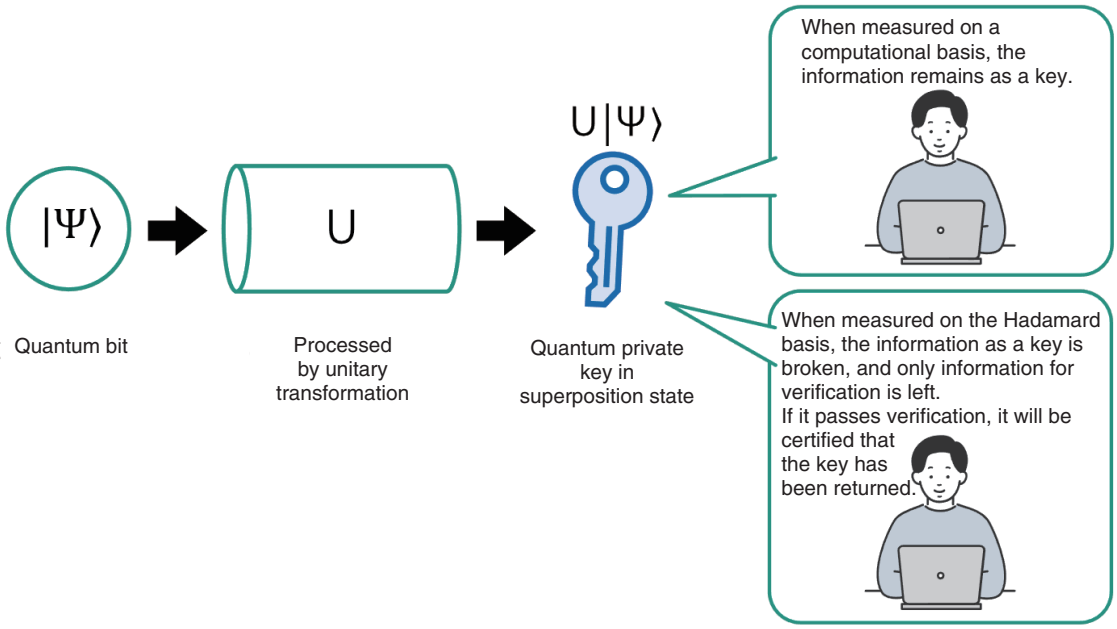


Fig. 2. How a quantum private key works.

However, it is impossible to prevent copying of key data once the key has been distributed. Even if the user insists the key is returned or deleted, the ciphertext can still be decrypted if the duplicate key is hidden. With that possibility in mind, we therefore applied the principle of quantum mechanics to prove mathematically that private keys of functional encryption can be deletable and uncopiable and proposed a secure key leasing based on that principle.

2. Using the uncertainty principle to delete the key by measurement

As a premise, it is assumed that both the host (who lends the key) and the user (who borrows the key) are using quantum computers. A quantum computer with a memory that can store quantum states and execute arbitrary algorithms is now in practical use, and private keys lent to users are also expressed in terms of quantum states. A private key is in a *superposition state* that changes on observation.

To delete such a private key, the quantum bit (qubit) of the key is first processed by a unitary transformation[*1] to generate a quantum key. During that transformation, information remains as a key when the key's superposition state is measured on a computational basis[*2] ($|0\rangle$, $|1\rangle$) but is deleted when it is measured on the Hadamard basis[*3] ($|+\rangle$, $|-\rangle$).

When the time comes to return the key, the user is asked to measure the quantum key on the Hadamard basis. If the superposition state is correctly measured, the key information is deleted in accordance with the uncertainty principle to leave behind only the classical information described as 0s or 1s (called certificate), and the certificate can be submitted as evidence of deletion.

If the measurement method differs from the specified one, the key information remains, and the key is not considered to have been returned. Therefore, changing the method of observing the superposition state makes it possible to delete part of the key information and delete the function of the key (**Fig. 2**).

There is a simple method for proving that a private key has been deleted and provide "the devil's poof." When the private key is deleted, a classical certificate is submitted as evidence of its deletion. After verifying the certificate, the host sends a new ciphertext to

*1 Unitary transformation: Changing an input qubit by applying an operation.

*2 Computational basis: A basic measurement to obtain information from the quantum state. A superposed qubit is represented as $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, and if the qubit is measured by the computational basis, a measurement value of 0 will be obtained with probability $|\alpha|^2$ and the state will be $|0\rangle$ or 1 will be obtained with probability $|\beta|^2$ and the state will be $|1\rangle$.

*3 Hadamard basis: Whether the quantum state is $|+\rangle$ or $|-\rangle$ is measured. Hadamard operation converts $|0\rangle$ to $|+\rangle$ and $|1\rangle$ to $|-\rangle$.

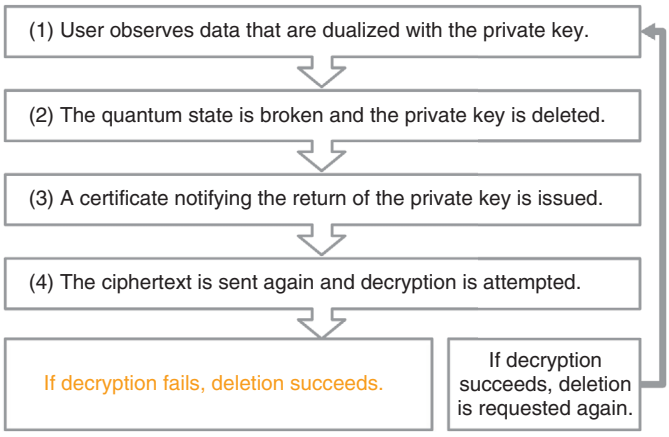


Fig. 3. Proof of deletion of quantum private key.

the user for decryption. If decryption fails, it is judged that the key does not exist; in other words, decryption failure equals deletion. This procedure/method is formulated in **Fig. 3**.

3. Copy protection from no-cloning

3.1 Private-key copy protection

Quantum mechanics are used to prevent copying of private keys. A quantum state created by oneself can be duplicated; however, according to the no-cloning theorem, an unknown quantum state given by another person cannot be duplicated. Even if an adversarial user attempts to duplicate an unknown quantum state, they will not be able to correctly decrypt a ciphertext by one of two quantum keys.

With this quantum key, it is impossible to extract the information that enables us to decrypt ciphertext. This status is explained by the fact that, as mentioned above, the uncertainty principle states that the state of the key will change at the moment it is observed to be copied, and the key will be lost. The only option is to leave the key in the quantum state without trying to measure it. Therefore, we have formulated and proved copy protection for such a private key.

The security of cryptography is classified into computational security, which is proven by computationally hard problems, and information-theoretic security, which is unbreakable even by an attacker with unlimited computational power. The proposed method, functional encryption with secure key leasing, guarantees computational security because it uses both quantum properties and computationally secure cryptography (**Fig. 4**).

3.2 Cryptographic technology for the future quantum society

Today, the cloud model is regarded as more important than the on-premises[*4] model, and quantum computers released in the US and Canada are operated by cloud services. Stronger cryptographic technologies are thus required in such one-to-many communication environments. Several technologies for revoking key data on classical computers have been proposed; however, they are inefficient and inconvenient if the private key is re-created for each generation of ciphertext. Moreover, if the ciphertext is updated all at once, various costs are incurred in proportion to the volume of the original data. The risk of old data is also a concern. We therefore thought that applying quantum mechanics to advanced cryptography would be an effective way to alleviate the costs and risks associated with encryption. We expect the scope of research on encryption procedures and theories for developing specific technologies to continue expanding.

4. Expansion into content services and the "right to be forgotten"

In the future, we believe that it will be possible that something based on the method reported in this article (i.e., functional encryption with secure key leasing) will become an international standard and be implemented in society. We say this because if the National Institute of Standards and Technology

*4 On-premises: Information systems are installed and operated in facilities managed by the user (e.g., a company).

Fig. 4. Copy protection of a quantum private key.

(NIST) in the US selects functional encryption as a next-generation encryption method, it will be standardized worldwide.

Although we are limiting ourselves to private keys in this article, our ultimate goal is to provide proof of program deletion and copy protection. When proof of program deletion and copy protection are implemented, they will change the way companies conduct research and development, manage information, and provide content services. In an example implementation, a quantum key is given to the customer and is valid only during the service usage period, and the key is invalidated when the contract period expires. These next-generation encryption technologies will also increase trust in third-party servers and cloud services and provide stronger protection for copyrights and other rights.

If old ciphertext remaining in search engines could be deleted completely, functional encryption may also be applicable to the "right to be forgotten" stipulated in Article 17 of the General Data Protection Regulation (GDPR) of the EU. We currently have no choice but to trust the other party's claim that "I deleted it," but quantum mechanics may enable us to respond technically to new concepts of rights (**Fig. 5**).

However, applying quantum mechanics is only possible if quantum computers are universal and used by general users. Considering the current error-correction capability, we believe that implementation of quantum-mechanics-based cryptographic technology is still some way off and requires further engineering in the development stage.

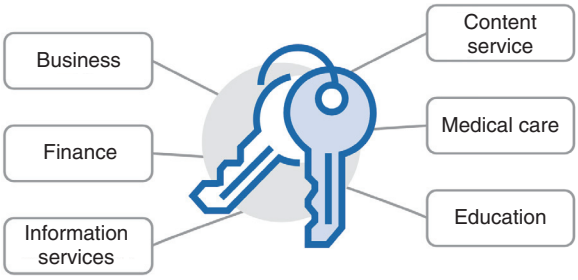


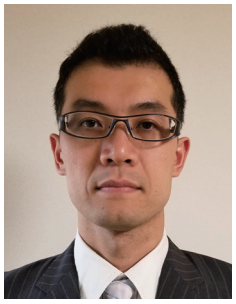
Fig. 5. Example categories in which functional encryption can be implemented.

Once quantum-mechanics-based cryptographic systems start working, the cryptographic technology will become global, so updating it will not be easy. From formulating theories to developing technologies and implementing them in society, various elements are intertwined, and we believe that process

will take a considerable amount of time.

Reference

[1] F. Kitagawa and R. Nishimaki, "Functional Encryption with Secure Key Leasing," Proc. of ASIACRYPT 2022, LNCS, Vol. 13794, pp. 569–598, 2022. https://doi.org/10.1007/978-3-031-22972-5_20



Ryo Nishimaki
Distinguished Researcher, Cryptography Research Laboratory, NTT Social Informatics Laboratories.
He received a B.E. and M.I. from Kyoto University and D.S. from Tokyo Institute of Technology in 2005, 2007, and 2010. He joined NTT in 2007. His research is focused on design and foundation of cryptography. He is currently researching cryptography and information security at NTT Social Informatics Laboratories.