Technology to securely turn biometric data into a cryptographic key

October 27 2015

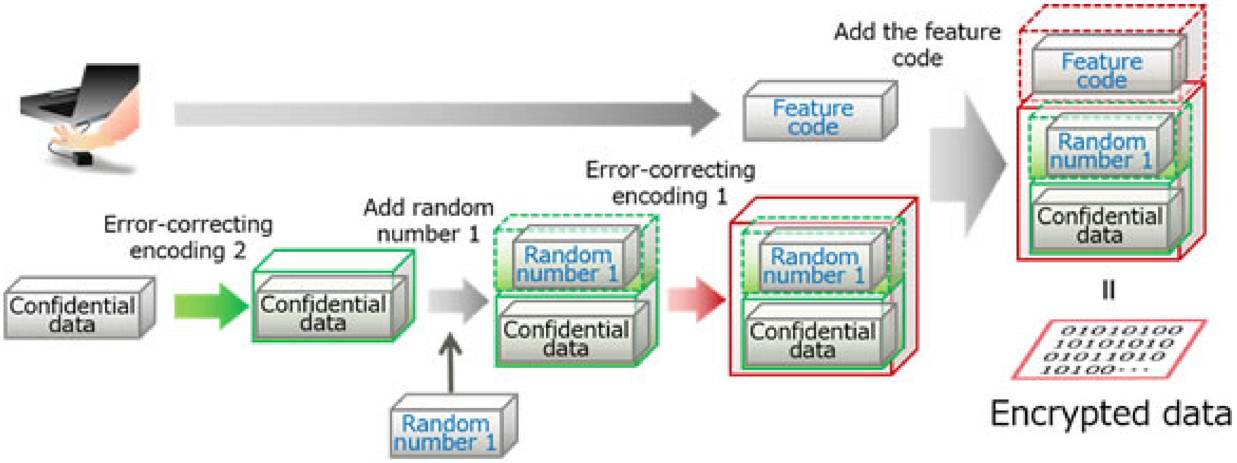

Figure 1: Diagram of the encryption process

Fujitsu Laboratories Ltd. today announced the development of a technology that turns biometric data, such as palm veins, into a cryptographic key. This newly developed technology enhances the security of the encryption method and protects confidential data, such as IDs and passwords. Conventional technologies that use biometric data to encrypt information require that the biometric data be used as-is when retrieving confidential data.

This means that for confidential data managed in a cloud service, for example, it would be necessary to send the biometric data through the network, raising issues of the network's security. Now, Fujitsu Laboratories has developed a technology that uses randomized numbers, each different, to convert biometric data into a cryptographic key for use in encryption and decryption. This makes it possible to simply and securely manage an individual's confidential data using biometric data, while preventing the unconverted biometric data from passing through the network. Fujitsu Laboratories anticipates that using this technology will make it easier and more convenient to carry out biometric authentication to verify the identity of a person accessing confidential data managed on the Internet.

Details of this technology will be presented, in conjunction with Kyushu University and Saitama University, at the 8th International Symposium on Foundations & Practice of Security (FPS 2015), to be held in Clermont-Ferrand, France, starting Monday, October 26th.

Development Background

The volume of IDs, passwords and other personal confidential data is increasing along with the growth of Internet services. All of this confidential data, being difficult to remember, is increasingly managed with encryption, such as by using AES, the current standard encryption technology. With current technologies, it has been necessary for users to manage cryptographic keys in order for them to decrypt encrypted data by storing cryptographic keys on an IC card or by validating cryptographic keys stored within a PC through password authentication. This therefore elicits a need for a technology that can securely encrypt and manage an individual's confidential data, using biometric data for personal authentication that is inseparable from the individual.

Issues

Contactless palm vein authentication technology, first developed by Fujitsu Laboratories in 2003, is used around the world in fields such as identity verification for ATMs in financial institutions, computer access, and facilities access management, owing to its excellent authentication capability. If confidential data could be encrypted using biometrics, the cryptographic key management of earlier encryption technologies would become unnecessary, and confidential data could be simply and securely managed. Biometric authentication works by extracting feature data from biometric data. With previous technologies, confidential data was encrypted with this feature data, but when decrypting, the feature data extracted from biometric data would usually be matched with the encrypted data as-is. This does not present a problem when used within a personal device, such as a PC or smartphone, but when used across an open network such as in the cloud, a more secure decryption technology is necessary to prevent leaks of biometric data.

Newly Developed Technology

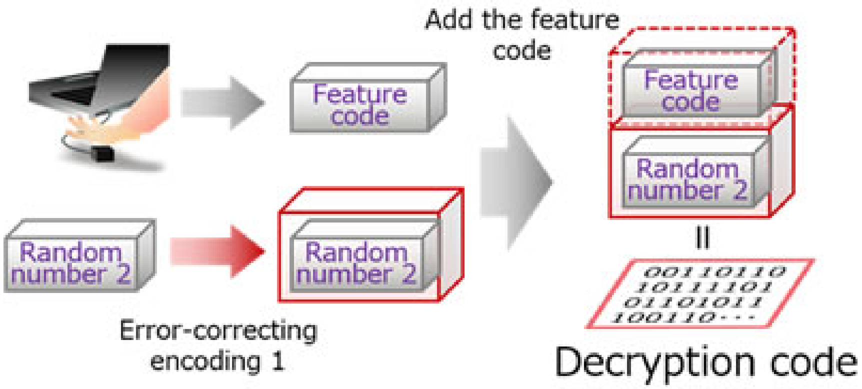

Figure 2: Diagram of decryption processing (client device)

For encrypting and decrypting data, Fujitsu Laboratories developed technology to decrypt confidential data that has been encrypted using biometric data converted using random numbers. As a result, confidential data can be encrypted and decrypted just with the user's biometric data, obviating the need for cryptographic key management. Fujitsu Laboratories applied widely used error-correcting codes for the encryption method as the technology to compensate for errors that are typically generated in the transmission route. The system randomly determines different random numbers for encryption and decryption, and using this protects the confidential data and biometric data. The features of the newly developed technology are as follows.

1. Technology to protect biometric data using error-correcting codes and random numbers

In encryption, confidential data is converted with an error-correcting code, and a random number is added to the whole. That data is then further converted using an error-correcting code, the feature code(1) extracted from the biometric data is added to generate the encrypted data, and this encrypted data is then registered in the server (Figure 1).

A decryption code is used as the key when decrypting encrypted data. For decryption, the decryption code, after being converted into secure data, is sent from the device to the server. The decryption code is generated by first converting a random number using an error-correcting code, and then adding the feature code extracted from the biometric data (Figure 2). As different random numbers are used for encryption and decryption, a different, secure decryption code can be generated.

2. Confidential data recovery technology using two-stage error-correcting technology

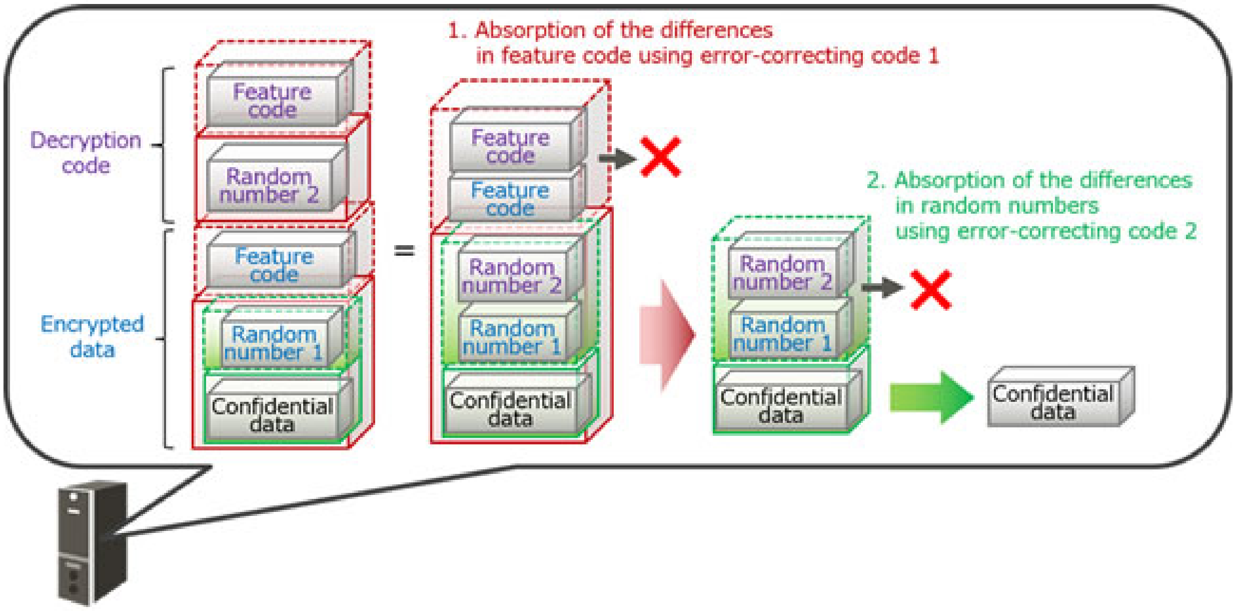

Figure 3: Diagram of decryption processing (server)

Variations in one's motion or position when inputting biometric data can generate slight discrepancies. This leads to discrepancies when calculating the feature code for decryption from the feature code for encryption, but the discrepancy can be absorbed because it is converted using an error-correcting code in advance (1 in Figure 3). Moreover, the discrepancy caused when calculating the random number used in decryption from the random number used in encryption will similarly be corrected when using error-correcting code 2, enabling recovery of the confidential data (2 in Figure 3). In this way, as the biometric data input for encryption and decryption are similar sufficiently, so long as they are both from the same person, the confidential data can be retrieved from the encrypted data using error-correcting technology.

Effect

Using this newly developed technology, the cryptographic key management that had been needed for existing encryption technologies becomes unnecessary. Furthermore, because the biometric data used for encryption and decryption are converted with random numbers, it is now possible to simply and securely manage an individual's confidential data using biometric data, while preventing the unconverted biometric data from leaking over the network. This means that the use of encryption technology using biometrics, which had previously been generally limited to use within a personal device, such as a PC, can now expand to cloud services across open networks.

Fujitsu Laboratories will continue to improve the speed of decryption processing and expand the types of information that can be encrypted, while also examining this technology's applicability to a number of potential use cases such as the Social Security and Tax Number system in Japan, with the goal of commercialization during fiscal 2017. It will also examine the development of the feature code, and work to expand the types of applicable biometrics, such as fingerprints.

Provided by Fujitsu

Citation: Technology to securely turn biometric data into a cryptographic key (2015, October 27) retrieved 8 April 2024 from https://phys.org/news/2015-10-technology-biometric-cryptographic-key.html