Fujitsu develops technology capable of searching encrypted data to maintain privacy

January 15 2014

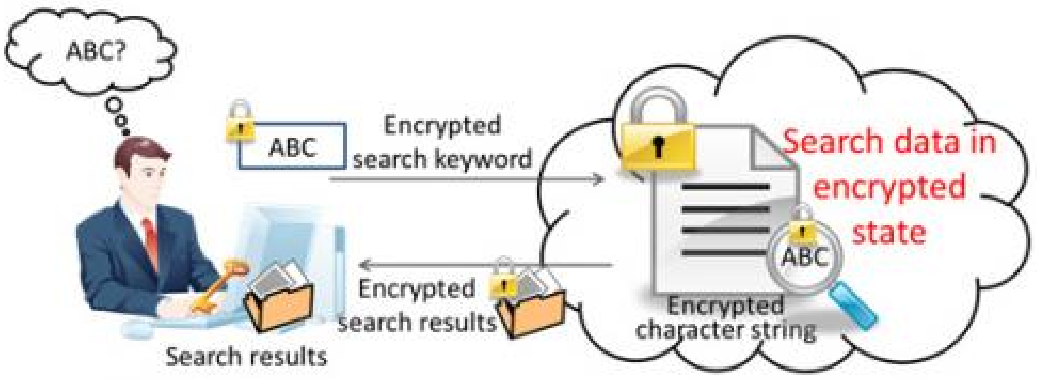

Figure 1. Private data search in the cloud

Fujitsu Laboratories today announced the development of a technology that can perform concealed searches of encrypted data in its encrypted form. Searching data while it is encrypted makes it possible to maintain a high level of privacy with no risk of leaks – particularly important for personal data such as DNA, medical data, biological data, and educational records. Through outsourcing, searches of confidential data can be carried out safely as text data and keyword search terms kept private. Whether or not search hits are obtained also remains undisclosed.

Based on homomorphic encryption which allows computations to be performed on confidential encrypted data without disclosure, Fujitsu has developed a new batch search method that accelerates the processing speed of searching for matches on the encrypted data. The new technology can search 16,000 characters in one second, and does not need an index of searchable keywords to be generated in advance. Instead, it makes discretionary searches of the encrypted text directly for any search key.

Details of this technology are being presented at the Fujitsu North America Technology Forum 2014, opening January 22 in Mountain View, California, and also at the Symposium on Cryptography and Information Security (SCIS2014), opening January 21 in Kagoshima, Japan.

With advances in cloud-based data storage and big-data analysis, information services for individual customers, such as healthcare administration, are appearing, however issues of peoples' private data being disclosed have been increasing. Fujitsu Laboratories has been working on technologies that enable more effective utilization of information while protecting privacy at the same time.

While there are encryption technologies, such as homomorphic encryption, that make it possible to perform calculations on data in an encrypted state, in order for data in the cloud to be useful, statistical calculations alone are not enough. For the data to be truly useful, technology that enables the data to be searchable has been needed (Figure 1).

Technological Issues

There are already a number of methods for searching data in an encrypted state, but these rely on pre-registering searchable keywords, and do not allow for freeform searching. These searches face certain implementation problems as well. As search results are unencrypted, this creates the potential for unwanted disclosure on the search engine. In addition, the search process is time-consuming.

About the Technology

Fujitsu Laboratories has developed a technology that can search encrypted character strings in their encrypted state. This method is based on homomorphic encryption, which makes it possible to perform statistical calculations on encrypted character strings, but takes that approach a step further by performing multiple encrypted calculations in a single process, working in batch mode to determine whether the search key appears in the character string being searched. Because of the nature of homomorphic encryption, searchable keywords do not need to be registered in advance, so the data remains secret throughout the search process, which can cover 16,000 characters per second. Features of this technology are as follows.

1. Searches encrypted character strings directly for matches, eliminating need to pre-register keywords

Fujitsu Laboratories has developed a technology that matches encrypted text using an extension to the private calculation functions in homomorphic encryption. Because the process of finding matches between the search key and the encrypted character string is carried out while the character string is encrypted, there is no need for searchable keywords to be registered in advance. Also, the use of homomorphic encryption means that the entire search process is carried out using encrypted character strings. Even the search results are encrypted, so that they can only be read by someone with the decryption key, further heightening security.

2. Batch-mode calculations accelerate search process

Past search methods could only search for character strings one string at a time. Fujitsu Laboratories has developed a way to search the entire character strings in batch mode, resulting in dramatically faster processing (Figure 2). This method makes it possible to search 16,000 characters of character strings in one second or less (Figure 3).

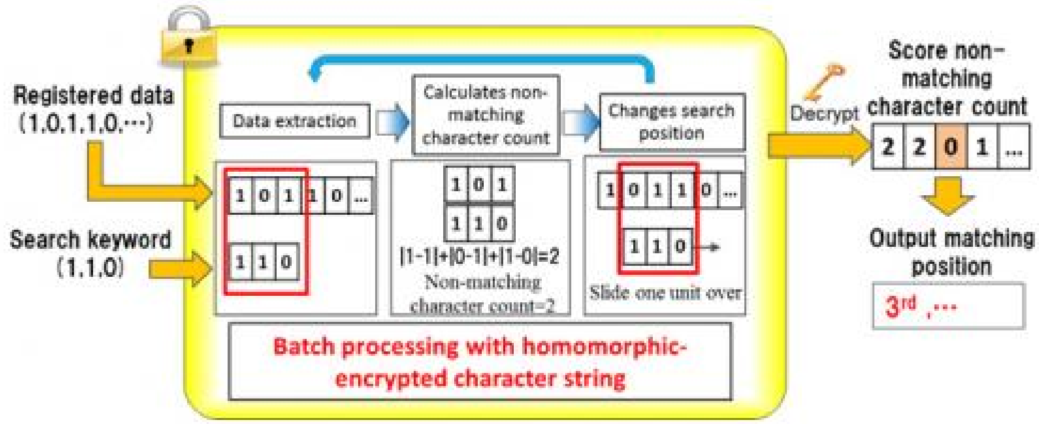

Figure 2. Calculating different parts of multiple-character strings simultaneously

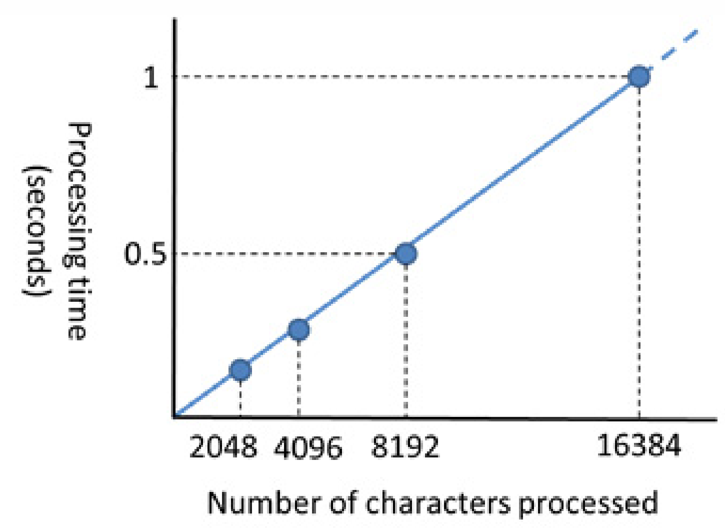

Figure 3. Processing time in private searching

This technology makes it possible to search encrypted data for any arbitrary search key, while keeping not only the source data itself encrypted but also the search key and even the search results. When applied to searching for a certain base sequence in a DNA strand, for example, this technology allows for a person's DNA information to remain private while finding whether or not it contains a certain sequence (Figure 4). This will also make it possible to achieve new analytical results obtained from medical records or base sequences collected from multiple hospitals, all while encrypted, which has the potential to make new drug development more efficient. Even data that has particularly sensitive privacy implications, such as medical records, can now be searched in full, thanks to this technology. The technology has potential applications outside of biology and medicine, as well, such as, for example, in aggregating results from multiple educational institutions for analysis. It could be used in a variety of situations where the privacy of data needs to be protected, or where data protection has been a problem (Figure 5).

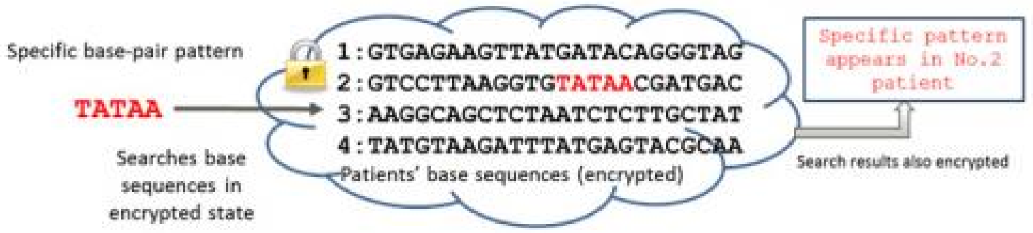
Specific base-pair pattern
TATAA
Searches base sequences in encrypted state
1 : GTGAGAAGTTATGATACAGGGTAG
2 : GTCCTTAAGGTGTATAACGATGAC
3 : AAGGCAGCTCTAATCTCTTGCTAT
4 : TATGTAAGATTTATGAGTACGCAA
Patients' base sequences (encrypted)
Specific pattern appears in No.2 patient
Search results also encrypted

Figure 4. Custom medical application of private character string-search technology

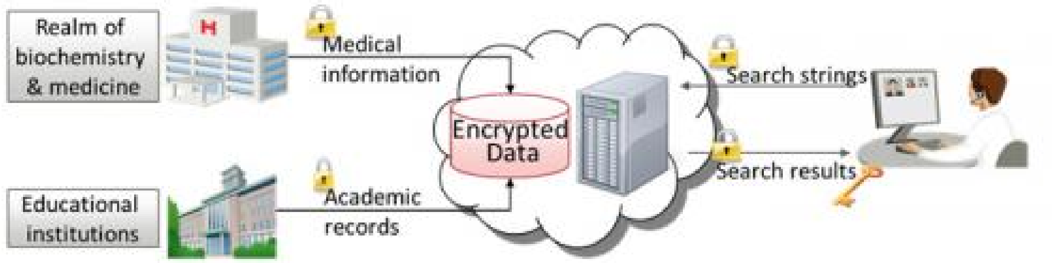

Figure 5. Potential uses for private search technology

Fujitsu Laboratories is continuing with practical testing of this technology, with a goal of commercial implementation in 2015. It is the company's intention to see this technology widely used as a way to maintain the security of personal information in a world that is increasingly driven by data, and as a tool for creating benefits to society by making data more useful while defending privacy.

Provided by Fujitsu

Citation: Fujitsu develops technology capable of searching encrypted data to maintain privacy (2014, January 15) retrieved 24 April 2024 from https://phys.org/news/2014-01-fujitsu-technology-capable-encrypted-privacy.html