NEWS RELEASE

NTT

October 25, 2005

# World's Fastest Secure Circuit Evaluation Algorithm Enabling Arbitrary Operation on Encrypted Data

World's first implementation has led to major advancement toward practical use of secure aggregation of questionnaires and tamper-resistant software

Nippon Telegraph and Telephone Corporation (hereafter NTT, headquartered in Chiyoda-ku, Tokyo, Japan; President and CEO: Norio Wada) announced that it has developed the world's fastest secure circuit evaluation algorithm and anticipates practical level performance from the provably-secure circuit evaluation technology that is implemented and evaluated based on NTT's advanced cryptographic implementation technology. Toward the commercialization of the technology, this is the world's first implementation of secure circuit evaluation technology that enables arbitrary operation on encrypted data without decryption. Algorithms of secure circuit evaluation technology, in which arbitrary operation is possible while input data and operation logics are left encrypted, have been studied for over ten years and up until now, because of their high computational complexity, the technology has been limited to only theoretical study. NTT has developed an algorithm that has the world's lowest computation and communications costs. Based on the advanced cryptographic implementation technology cultivated by NTT, we achieved the world's first implementation and measured the processing times for the basic operations of the technology. NTT made significant progress in the practical application of this technology and based on the results, we estimated that a software-only authentication token, not a tamper-proof hardware (*1) token, for two-way authentication such as that used in a virtual private network (VPN) is feasible. Furthermore, we estimate that it is feasible to run aggregational operations on encrypted data without decryption. This is useful when dealing with sensitive information such as medical information. In the future, this technology is expected to be applied to preventing illegal reverse engineering of programs, intellectual property protection such as digital rights management, preventing information leakage, and privacy protection in enterprises, public authorities, and educational institutions. The results of the implementation evaluation of this technology are slated for presentation at the Computer Security Symposium, hosted by the Information Processing Society of Japan, taking place from October 26 in Matsuyama-shi, Ehime, Japan.

## BACKGROUND OF SECURE CIRCUIT EVALUATION TECHNOLOGY AND OUR CONTRIBUTION

When dealing with information, there are cases where only specific information is disclosed and other information is kept unrevealed. For example, when outsourcing computations in which confidentiality is required, not only the data, but also the logic of the computation requires secrecy. Furthermore, from the viewpoint of protecting

personal information, in regard to varieties of questionnaires, aggregate data that contain no information specific to any individual may be disclosed. However, there are cases where measures must be taken to ensure that no individual data of the questionnaire is revealed. By making use of the secure circuit evaluation technology, since arbitrary operation of the information while it is encrypted becomes possible, the level of security of this type of computation and aggregation can be rapidly increased. Although theoretical research has been conducted worldwide on the technology for more than ten years, because of the computational complexity level, up until now a practical implementation could not even have been considered. NTT Information Sharing Platform Laboratories, which performs world leading cryptography research including Camellia previously adopted as an IETF standard, has this time developed a basic algorithm for secure circuit evaluation that executes at the world's lowest costs both in computation and communications. Based on advanced cryptography implementation technology, we were successful in measuring the processing performance of the secure circuit evaluation for the first time in the world. As a result, the road was opened to practical use of new security systems the level of security of which was increased significantly compared to existing schemes.

## APPLICATION FIELDS FOR THIS TECHNOLOGY

The following are the assumed applications in the current status.

(1) Software Authentication Token
When performing two-way authentication for encrypted communications such as over VPNs, hardware authentication tokens (*2) such as IC cards, USB keys, and one-time password generators have been used as a device to provide higher security. These hardware tokens guarantee higher-level security because the operations and data used for authentication are processed inside the tamper-proof hardware token that is practically impossible to analyze. However, the cost of purchasing and delivering token devices represents a great barrier to their introduction. If the secure circuit evaluation technology is available, by using only software, authentication tokens that are practically impossible to analyze become feasible. By using the software authentication token, since the authentication program is executed under encrypted status, data and operations used for authentication cannot be revealed. Furthermore, thanks to its software-only nature, the tokens can be delivered through networks, and we can expect that the costs will be reduced and the degree of convenience improved.

(2) Privacy-Preserving Aggregation of Questionnaires (Fig.1)
Up to now, for cases when outsourcing the aggregation of questionnaires, generally the data require additional processing so that no individual can be specified from the data. However, this additional processing is laborious, and in some cases, it disables the desired aggregational operation. Moreover, due to the recent enactment of the personal information protection act, many more precautions are required for the treatment of individual data of questionnaires, etc.
If the secure circuit evaluation technology is employed, arbitrary operations can be performed while individual data in the questionnaires are kept encrypted and thus not leaked. Therefore, privacy-preserving aggregation can be achieved by simply letting an outsourcee run arbitrary computations and present only the results of the computations.

## CHARACTERISTICS OF SECURE CIRCUIT EVALUATIONS

(1) Various operations are possible without decrypting the encrypted data (Fig. 2)

Arbitrary operations can be performed where the input data are kept encrypted. No decryption is performed on the input, only the output is decrypted.
In addition, the same technology can be used to execute the encrypted operation logics where the logics are kept encrypted.

(2) Multiparty Model
Based on the multiparty protocol theory (*3), secure circuit evaluation is guaranteed to be cryptologically secure. The protocol requires the cooperation of multiple participants where each is delivered a secret key. Unless more than a specified number of participants collude, it is ensured cryptologically that the input data and logics cannot be revealed. The collusion threshold can be specified at any number with the requirement of each application instance.

## FUTURE PLANS

We are aiming at the achievement of a commercial system employing the secure circuit evaluation technology in three years. Furthermore, by improving the performance of this technology, we plan to develop advanced applications such as information retrieval and data mining on encrypted databases, and tamper resistant digital rights management. Through such efforts, we want to contribute to the establishment of a safe and secure information society.

## TERMINOLOGY

*1 Tamper-Proof Hardware
A physical device that is able to prevent unauthorized access to confidential contents (data and programs) inside it.

*2 Authentication Token
A set of data and programs that require authentication. In order to prevent attacks such as impersonation, it is desired that the data and programs are protected.

*3 Multiparty Protocol
A protocol that enables "operation of encrypted data" and "execution of encrypted operation logics" only when at least K participants out of the total of N participants cooperate. In general, the level of security becomes higher as K increases.

- Fig. 1.Application example: Privacy-preserving aggregation of questionnaires
- Fig. 2.Outline of secure circuit evaluation technology

## CONTACT INFORMATION

Chizuka, Sano, Ida
Public Relations Section
Planning Department
NTT Information Sharing Laboratory Group
Nippon Telegraph and Telephone Corporation
Phone: 0422-59-3663
E-mail: koho@mail.rdc.ntt.co.jp