Enhancing FinTech Security with Secure Multi-Party Computation Technology

OKAMURA Toshihiko, TERANISHI Isamu

Abstract

As the FinTech revolution gains momentum, a key challenge threatens to bring this progress to a crashing halt: cybersecurity. Given the scope, complexity, and dynamism of FinTech solutions, cyberattacks are inevitable, making enhanced security technology indispensable to ensuring future growth. Information leakage is one of the most common vulnerabilities and is still difficult to be prevented completely. The most promising approach to solving this problem is secure computation, which, thanks to its ability to process encrypted data, has proven to be a robust information leakage prevention technology. This paper discusses NEC's own contribution to Secure Multi-Party Computation (SMPC) technology. In SMPC, data on multiple machines can be processed while maintaining the security of the data on each machine. In addition to explaining the technology itself, we will show how it could work in FinTech applications by reviewing some case studies centering around NEC's high-speed method and protection of information for authentication.

Keywords

security, information leakage prevention, authentication, secure computation, secure multi-party computation

1. Introduction

FinTech has now expanded to the point where its impact is being felt not only by early adopters and businesses, but by just about everyone. A dazzling range of innovative new financial services are rapidly coming onstream, changing the way we live and work. In such an environment, it is critical to develop reliable security measures to protect against cyberattacks. As FinTech becomes more tightly entwined in our daily lives, security breaches have the potential to cause massive financial losses and undermine confidence in the technology itself. In particular, the use of smartphones, which is a key aspect of FinTech and essential to the introduction of convenient services, poses one of the most significant cyberthreats - namely, information leakage. A 2016 study by MacroMill[1)] found that when asked for their impressions about FinTech, users ranked fear of information leakage as the highest.

Since leakage of authentication information can lead to fraudulent settlements and massive leaks through spoofing, especially robust measures are required to prevent this. An industry consortium for passwordless authentication, the FIDO (Fast IDentity Online) Alliance specifies frameworks for safe execution of authentication using users' biometric information and public key cryptography. However, this is based on the assumption that users' biometric templates and secret keys are stored "securely" in user terminals or devices. Once a device has become accessible to an attacker - for example, because the user lost the device or it was penetrated by malware - data security can no longer be guaranteed. Moreover, when we take into consideration the fact that the biometric template is sensitive personal information, it is crucial that effective methods be developed to prevent leakage of this data.

This paper focuses on secure computation, a type of encryption technology that achieves robust prevention of information leakage even against persistent and sophisticated attacks. In particular, we will discuss a type of secure computation called secure multi-party computation on which NEC's Security Research Laboratories is now focusing and introduce NEC's high-speed method and its expected applications in FinTech services.

2. Secure Computation

Encryption is an effective way to prevent information leakage even when data is stolen from the system. Conventionally, however, the encrypted data must be decrypted before it can be processed. This makes it possible for attackers to acquire the original data by restoring it if they are able to gain administrator privileges. In secure computation, the original data is never restored; instead, the encrypted data itself is processed, making it impossible for the information to leak even in the case where an intruder is able to appropriate administrator privileges (**Fig. 1**).

Secure computation can be generally classified into two approaches: one is special encryption such that searchable encryption and homomorphic encryption and the other is Secure Multi-Party Computation (SMPC) (**Fig. 2**). The former, as of now, requires that a different encryption method be designed according to the processing. SMPC, on the other hand, features the ability in principle to handle arbitrary processing by combining SMPC algorithms of basic operations such as "XOR" and "AND".

2.1 Secure Multi-Party Computation (SMPC)

The processing concept of SPMC is shown in **Fig. 3**. First, the owner of data *a* securely distributes *a* to secret shares *x*, *y*, …, and then sends *x*, *y*, … respectively to

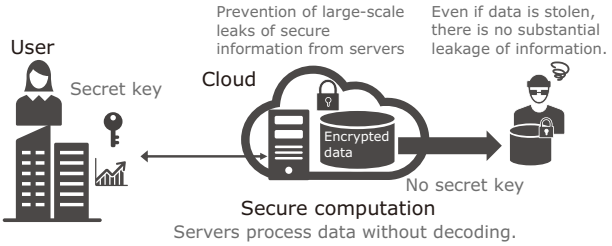

Fig.1 Prevention of information leaks using secure computation.

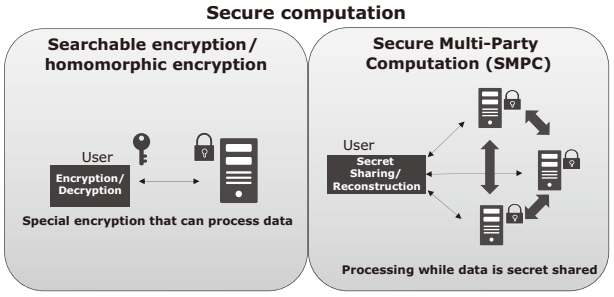

Fig.2 Classification of secure computation.

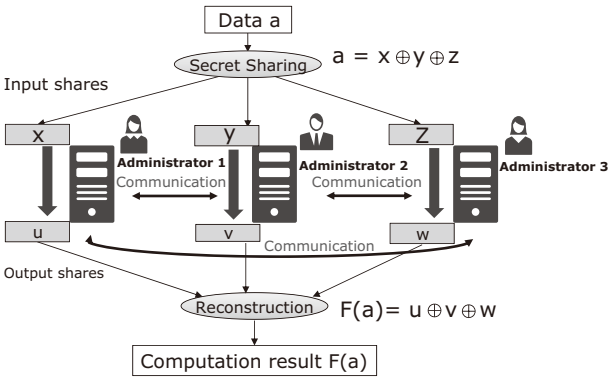

Fig.3 Conceptual diagram of SMPC.

different machines. Computation is performed in a condition where data are always secret shared from inputs to outputs. The result *F(a)* can be reconstructed with the output shares.

Because *a* is secret shared, it cannot be leaked as long as the number of shares stolen by an attacker do not exceed a threshold. Furthermore, SMPC maintains this property even while it is processing the data, so *a* does not even appear in the memory. This means that data security can be guaranteed even if some of the machines are under the control of an attacker. SMPC makes it impossible for an attacker to gain access even in the case of insider threat where the attacker has a privilege and conventional countermeasures like encryption cannot work.

Although SMPC is theoretically capable of handling the situation described above, it has until recently remained in the theoretical realm due to the enormous increase in both inter-machine communication and processing required. Over the past few years, however, improvements in algorithms and increases in the speeds of processors and networks have turned SMPC from theoretical possibility to practical reality.

2.2 NEC's High-speed SMPC

NEC has succeeded in the development of a high-speed SMPC system using three machines. Even if an attacker seizes control of one of the machines, it is still impossible to leak any information.

In SMPC, data processing is expressed in logical expressions of "XOR" and "AND" gates. NEC has achieved a dramatic increase in speed[2)] by improving the "AND" gate operation by redesigning the secret sharing method and maximizing the amount of processing that can be computed within each machine without communications, as well as by optimizing the processing itself.

Table below shows the throughput in the case where

Table Processing performance of SMPC.

(No. of blocks/second for AES)

Year	System	Throughput
2013	Company C (1)	3,450
2016	Company C (2)	25,000
2016	Company C (3)	90,000
2016	NEC	1,324,117

SMPC is applied to Advanced Encryption Standard (AES), which is used for a standard performance benchmark of SMPC. In this case, encryption is performed while the secret key and data continue to be secret shared. As shown in Table, Company C's system boasted the highest performance as of December 2016. Since then, NEC's system has blasted through that benchmark, achieving throughput 400 times faster than Company C's system achieved in 2013 and 14 times faster than their 2016 results.

In order to evaluate the usefulness of the performance, we applied it to a Kerberos authentication server, which is widely used for directory services. The result showed that it achieved authentication processing at 35,000 queries per second[3], far exceeding the criterion for use of Kerberos authentication at large corporations, which is 10,000 per second.

Meanwhile, security issues of SMP include the problem of malicious operation in the event that a machine is taken over by an attacker. For example, using the machine under control of the attacker, it should be still possible to perform the secure processing and detect the anomaly. The ability of the detection is crucial if the system is to be put into a practical use. NEC is also developing a high-speed and safe system capable of detecting malicious servers in SMPC[2].

NEC's approach to the increased speed cannot only be applied to SMPC based on the logical operations, but also to those based on the sum and multiplication of arithmetic operations based on secret sharing in the integer or the decimal. For biometric authentication and data analysis, increased speed can be achieved by applying SMPC based on the arithmetic operations. Detailed design and evaluation of algorithms is currently underway.

3. Applications of SMPC in FinTech

3.1 Protection of Authentication Information

User and device authentication is the starting point for security in most FinTech services including mobile payment. SMPC provides extremely robust protection for authentication data.

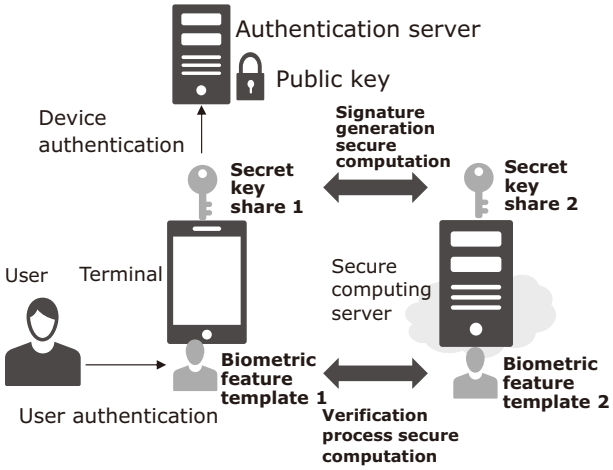

Fig.4 Protection of FIDO-based authentication information using SMPC.

In this section, we will look at two use cases in which authentication data is protected by SMPC. The first case is concerned with the protection of data in FIDO-based authentication. FIDO-based authentication uses biometric data to authenticate users. When the authentication is successful, the user terminal generates a digital signature in the terminal and the authentication server verifies the signature. **Fig. 4** shows an example for protecting the template of user's biometric information and a secret key of the device. In this example, the template and the secret key are securely distributed to the user's terminal and the secure computation server. When authentication is executed, the user's terminal and the secure computation server communicate to perform SMPC. This process makes it possible to verify the biometric authentication and to generate a signature for device authentication without restoring the biometric template and the secret key.

When RSA is used in device authentication as shown in Fig. 4, simple SMPC can be applied using the characteristics of RSA (**Fig. 5**). The two shares, $d[1]$ and $d[2]$, which are generated from the RSA secret key d so that they satisfy $d = d[1] - d[2]$. While the user's device and the server work together, the user's device generates signature σ for data M that has been made by adding information such as time to RSA authentication challenge m send from the authentication server.

$$\sigma = H(M)^d \bmod N = H(M)^{d[1]} / H(M)^{d[2]} \bmod N$$

Here, N is a public key of RSA, and H is the hash function used in signature generation. Thanks to SMPC, the signature σ can be generated without restoring the se-

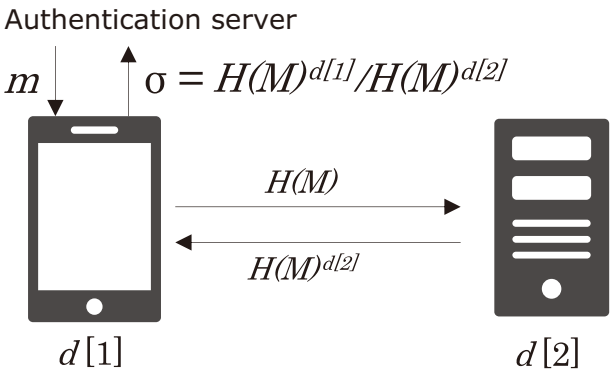

Fig.5 Multi-party computation of FIDO-based RSA signature.

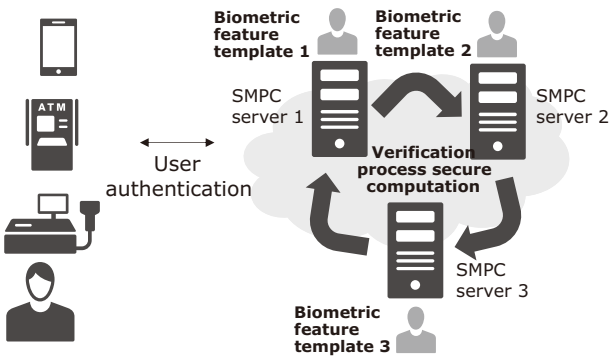

Fig.6 Application example of SMPC in user authentication platform.

cret key *d*.

The second case concerns protection of authentication information in the user authentication platform in the cloud. In this case, the authentication platform is assumed to offer user authentication functions to various terminals and services such as POS. With such a massive amount of authentication information registered, the authentication platform requires extremely robust protection. Secure distribution of such a huge quantity of authentication data through multiple servers to perform SMPC makes it possible to prevent information leakage even if one of the servers comes under the control of an attacker.

Fig. 6 shows an example of biometric authentication. Upon authentication, the terminals securely distribute the biometric template for verification. These shares are separately encoded and transmitted between the terminals and servers. The registered shares for the biometric template are used by the servers to execute SMPC verification processing. In this usage configuration, it is assumed that high-volume authentication is implemented on the cloud side; therefore, the SMPC used here requires high throughput. In 2.2 above, we discussed the practicality of NEC's high-speed SMPC in the Kerberos authentication. We are also working to achieve practical performance in verification processing of biometric authentication.

3.2 Protection of Customer Information

FinTech companies provide consumers with an ever-expanding range of services including their purchase histories, collection of relevant information on the Internet via SNSs, bank account information using APIs, and advanced loan and asset management. As these services rely on the collection and processing of massive amounts of customer data, providing enhanced security measures that reliably prevent leakage of collected customer data is critical. SMPC is a proven solution that makes it possible to process data and prevent information leakage from administrators, as well as providing unprecedentedly secure protection of customer information.

Customer data collected by FinTech companies is the key to competitiveness and innovation. That information can also be used to build even more advanced and sophisticated services by collaborating with other companies to perform combined analysis of data without mutually disclosing confidential information. For example, collaborative analysis could improve the accuracy of customer creditworthiness. SMPC not only makes it possible to analyze combined data without disclosing the data to the concerned parties, but it also prevents third parties from accessing it. In this way, SMPC can provide the security FinTech companies need to leverage their data and utilize it in collaboration with other companies.

4. Conclusion

In this paper, we introduced the concept of Secure Multi-Party Computation (SMPC) which securely distributes data across multiple servers and processes it while keeping it encrypted. We also showed its use cases in FinTech applications where NEC's high-speed SMPC could be used to prevent leakage of authentication information. In the future, we will continue to improve SMPC performance, while developing its initiative applications with a view to achieving a reliable, efficient security platform that will eliminate the risk of information leakage in FinTech applications.

Reference

1) About Macromill:
http://www.macromill.com/honote/20160405/report.html
2) T. Araki, J. Furukawa, Y. Lindell, A. Nof, and K. Ohara, High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority. ACM CCS, 2016.
3) J. Furukawa, Y. Lindell, A. Nof, and O. Weinstein, High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority, to appear in Eurocrypt2017

Authors' Profiles

OKAMURA Toshihiko
Principal Researcher
Security Research Laboratories

TERANISHI Isamu
Assistant Manager
Cyber Security Strategy Division

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.11 No.2 FinTech That Accelerates Digital Transformation

Papers for Special Issue

NEC Information

Vol.11 No.2
June 2017

Special Issue TOP