A Secure Business Chat System that Prevents Leakage and Eavesdropping from the Server by Advanced Encryption Technology

Reo Yoshida, Yuki Okano, Hironobu Okuyama, and Tetsutaro Kobayashi

Abstract

In business-oriented chat applications, end-to-end encryption is needed to prevent governments and service providers from eavesdropping or leaking information. At NTT Secure Platform Laboratories, we are working on a prototype secure business chat system that not only prevents leakage from terminals by not leaving any data on the terminals, but also makes it possible to exchange and search messages without disclosing any secrets to the server. This article introduces the encryption technology used in this prototype system.

Keywords: multi-cast key distribution, proxy re-encryption, searchable symmetric encryption

1. Introduction

Prominent consumer-oriented messaging applications include LINE in Japan and Asia, and Facebook Messenger and WhatsApp in Europe and the US. Each application claims to have several million users. Following accusations of communication insecurities made by the former Central Intelligence Agency employee Edward Snowden [1] and by WikiLeaks [2], people have started to suspect that these chat room applications may be subject to eavesdropping and data theft by governments and messaging service providers. Furthermore, according to a safety assessment of typical messaging applications carried out by the Electronic Frontier Foundation [3], users are becoming much more interested in the specific security measures of each application and in how these measures are implemented. To address these growing concerns, LINE, Facebook Messenger, and WhatsApp are taking steps to improve the security of their chat applications by implementing measures such as end-to-end encryption, whereby messages are encrypted and decrypted in the user terminals so as to guarantee that service operators cannot eavesdrop on their messages.

Business-oriented chat applications include ChatWork and TopicRoom in Japan, and Skype for Business and Slack in Europe and the US. Unlike consumer-oriented applications, the chat data in these applications belong to the business, so most applications do not leave chat data on the terminals but instead keep this information on servers such as cloud services for each login. In this way, they can prevent leakage of data even if a terminal is lost or stolen.

2. Issues involving end-to-end confidentiality in business chat applications

In business chat applications, data are saved in a cloud service or some other form of server to prevent the chat data from being leaked when a device is lost or stolen. However, for business-oriented applications,

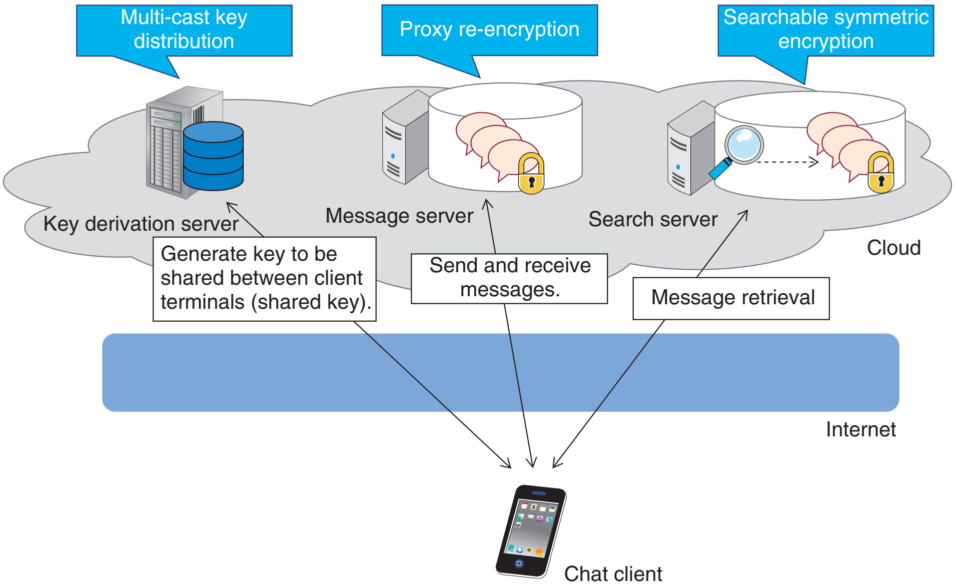

Multi-cast key distribution
Proxy re-encryption
Searchable symmetric encryption
Key derivation server
Message server
Search server
Cloud
Generate key to be shared between client terminals (shared key).
Send and receive messages.
Message retrieval
Internet
Chat client

Fig. 1. System overview and technical features of encrypted business chat system.

it is assumed that there will be many users. Consequently, there will probably be frequent changes to the members of the chat rooms and messaging services as people move to new positions, new employees arrive, and older employees leave. With conventional encryption methods, it is therefore technically difficult to implement end-to-end encryption while preserving data on a server, and in fact, no applications have yet achieved this. Furthermore, although there are many server-side applications that can implement full-text searching of chat messages at higher processing speeds, it is technically difficult to search messages without disclosing information to the server, and this is another feature that is not yet supported by any applications.

In summary, there are three confidentiality issues that need to be addressed in business chat systems.

- Implementing multi-user chat functions with end-to-end encryption
- Storing encrypted chat data on a server and enabling the members authorized to view the data to be modified and updated as the chat room members are modified and updated
- Allowing full-text searching of chat messages on the server while maintaining the secrecy of chat information on the server

3. Approach of NTT Secure Platform Laboratories

At NTT Secure Platform Laboratories, we have been developing encryption technology for many years, and we are studying how it can be used to solve the abovementioned issues and implement a secure business chat system that prevents eavesdropping and leakage of chat contents from the server. As a result, we have developed the following three techniques:

- Multi-cast key distribution [4]
- Proxy re-encryption
- Searchable symmetric encryption

An overview of a business chat system to which these techniques have been applied is shown in **Fig. 1**.

4. Three techniques for implementing secure business chats

The three techniques developed to ensure that business chats remain secure are described in more detail in this section.

4.1 Multi-cast key distribution

A key sharing protocol is a protocol that allows keys used for the encryption and decryption of messages to be shared between clients by communicating over a non-secure communication path that may be subject to eavesdropping. These shared keys can then

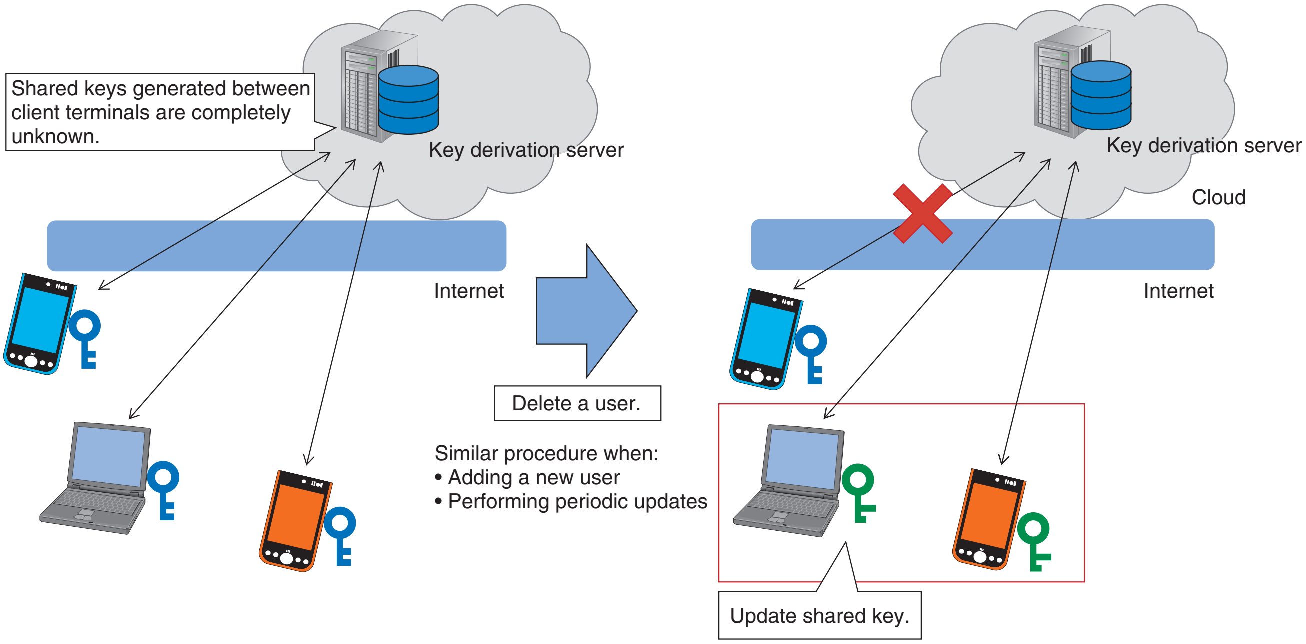


Fig. 2. Multi-cast key distribution.

be used to keep the communication secret. An example of a key sharing protocol that operates between two clients is the Diffie-Hellman key exchange, which is the protocol used by most existing business chat systems. However, when keys are shared among large numbers of clients, this two-user key sharing protocol must be performed repeatedly, which is inefficient. This can lead to technical issues when sharing keys among large numbers of users and may lead to capping the number of participants in a chat room.

With NTT's multi-cast key distribution technique, a key derivation server is placed in the center, and the keys are shared among multiple users via this server (**Fig. 2**). This is much more efficient than sharing keys among users directly. Since the shared key is generated by performing advanced calculations from secret information held by each user and the key derivation server, the shared key itself is not sent between the user and the key derivation server, and there is no way that the shared key can be known by the key derivation server. It is also possible to add new users and delete existing users, and the system includes a mechanism that updates the keys every time such an event occurs. This makes it possible to communicate information that is kept secret from the server and is only accessible to the users (however many) who are communicating at that time.

4.2 Proxy re-encryption

Proxy re-encryption is a technique whereby, instead of decrypting a ciphertext that can be decrypted with a key K1, a so-called re-encryption key RK is used to transform the ciphertext so that it can be decrypted with a different key K2. For example, a ciphertext addressed to user A on message server S could be transformed (re-encrypted) by server S using a re-encryption key so that it can be decrypted by user B. The plaintext of the original message is not made available to server S at any point.

In the business chat system introduced here, the shared key is updated by multi-cast key distribution when changes are made to the chat room members, for example, organization changes or changes of personnel. When this takes place, the data stored on the message server must be capable of being decrypted with the updated shared key. With NTT's proxy re-encryption technique, the data are re-encrypted and then decrypted using the updated shared key, without it being possible to decrypt any messages on the server (**Fig. 3**). Thus, even if a chat room member update occurs, the messages are never disclosed to the server and can only be decrypted by current chat room participants. With conventional proxy re-encryption techniques, the computer processing needed to re-encrypt all the encrypted chat data would be too slow to be of practical use for a business

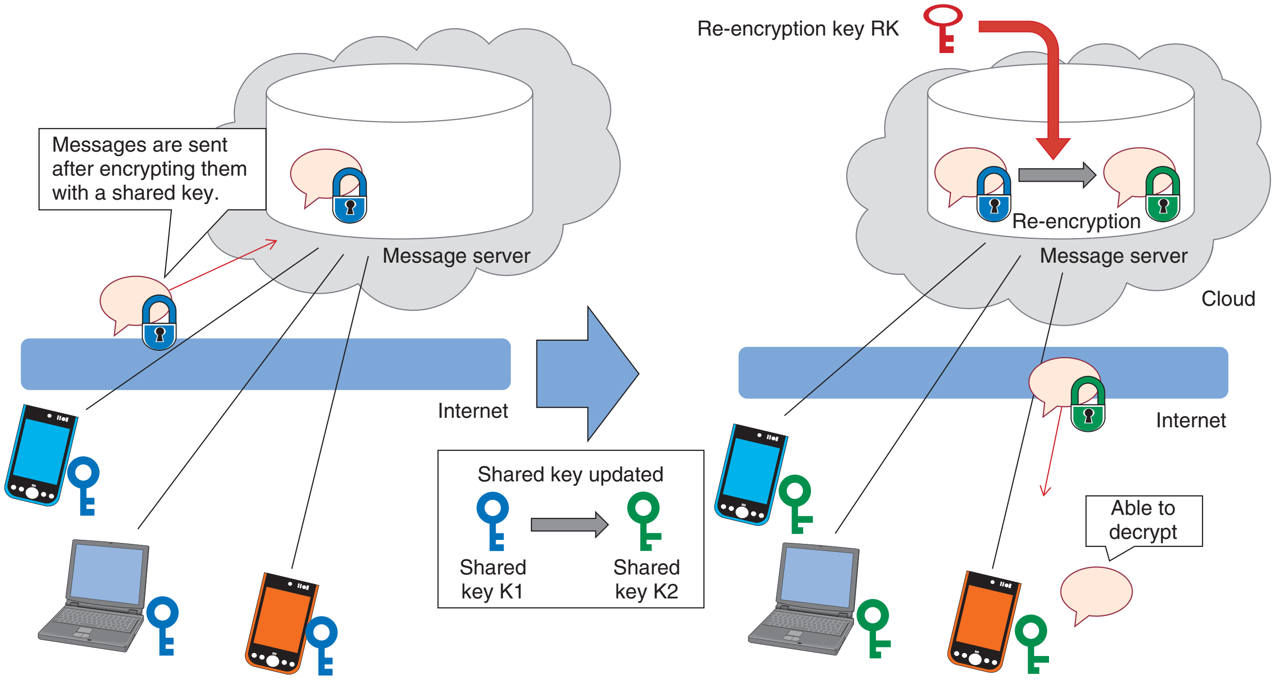


Fig. 3. Proxy re-encryption.

chat system. In NTT's proxy re-encryption technique, the processing is limited to only those parts of the data that need to be processed while keeping the data secure. In this way, we can perform re-encryption more efficiently than conventional proxy re-encryption techniques.

4.3 Searchable symmetric encryption

Searchable symmetric encryption is a technique that makes it possible to search for keywords in a set of data while the data and keywords remain encrypted. In a searchable symmetric encryption, the user generates a key (search key) and uses it to make a secret index to the data that are not disclosed to the search server. The server stores the user's secret index on the search server together with the encrypted data. The user uses the search key to send secret queries, and the server uses the secret queries and concealed index to search for the corresponding data without decrypting any of the data, and then sends the results back to the user (**Fig. 4**). In the keyword search function of a business chat system, it must be possible to retrieve the required information quickly from previous messages. NTT's searchable symmetric encryption technique can perform secret searches that are fast enough for business chat systems where real-time performance is needed. Even if new users are added, these users can also generate secret keywords and carry out searches using them.

5. Evaluation

We applied the above techniques to an existing business chat application in order to evaluate them. The client application's user interface was left unchanged, while the above encryption techniques were applied to add a new key derivation server and search server and to add re-encryption functions to the message server. We analyzed the operation of the client application and the data stored on the message server and search server, and we confirmed that the following functions were operating correctly (**Fig. 5**).

- Adding/removing users and updating shared keys (multi-cast key distribution)
- Re-encrypting messages when shared keys are updated (proxy re-encryption)
- Performing keyword searches using secret indexes and secret keywords (searchable symmetric encryption)

Table 1 compares the average processing times needed for logging in, exchanging messages, and performing keyword searches in a conventional chat system and in a chat system with the addition of the above three functions.

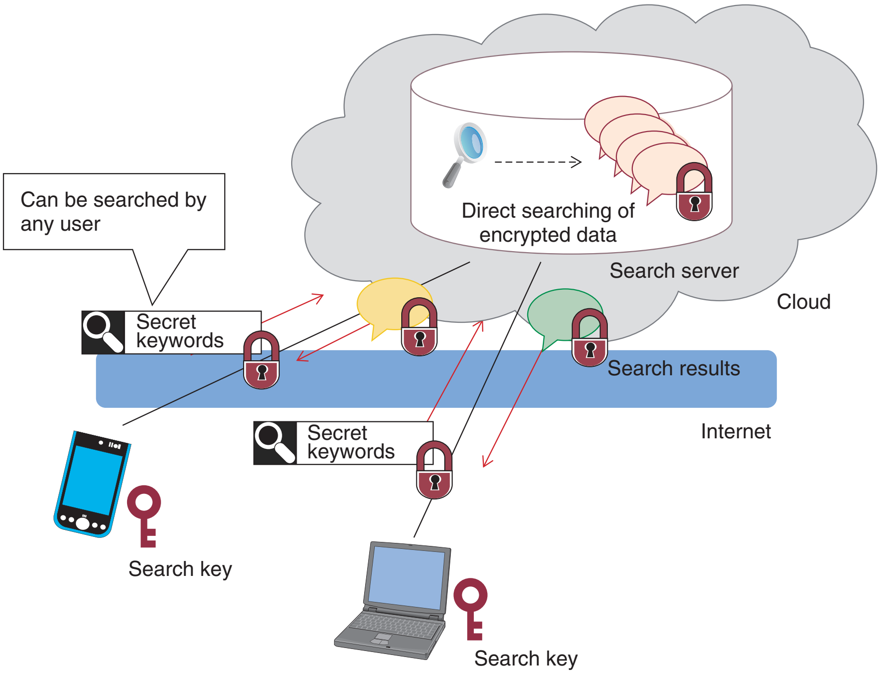
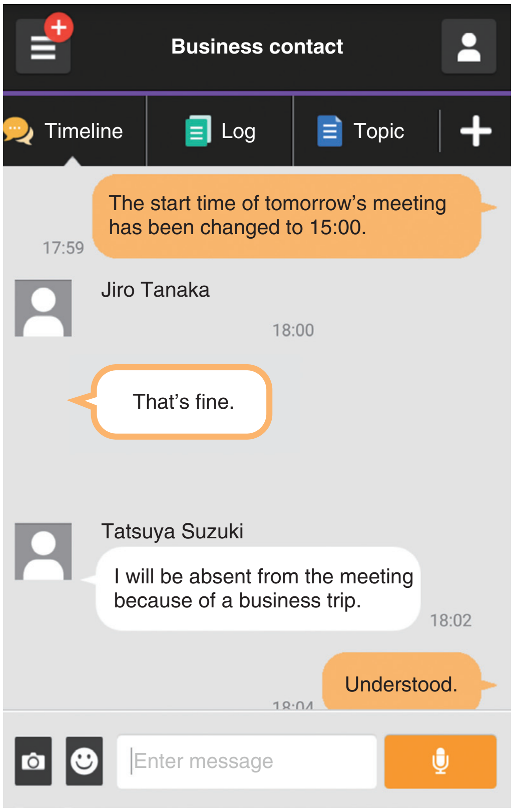


Fig. 4. Searchable symmetric encryption.



17:59 The start time of tomorrow's meeting has been changed to 15:00.

Jiro Tanaka

18:00 That's fine.

Tatsuya Suzuki

I will be absent from the meeting because of a business trip. 18:02

18:04 Understood.

Fig. 5. Screen shot of an existing business chat application after applying the three functions.

Table 1. Comparison of average processing times in an existing business chat application.

Item	Ordinary processing time	Processing time with three additional functions
Enter chat room	3–4 seconds	3–4 seconds
Sending & receiving messages	≤1 second	1–2 seconds
Keyword search	≤1 second	≤1 second

6. Future prospects

We have devised encryption schemes for secure business chat systems that prevent eavesdropping and leakage of information from the server. We have also developed and tested a prototype business chat system that implements these encryption schemes and confirmed that its performance is sufficient to withstand practical use.

We plan to make this business chat system commercially available in the future. We will also publish the details of these encryption systems at conferences and in technical journals. We are also considering the possible application of this technology to other areas such as virtual private networks or email systems and are working to put it to practical use.

References

[1] G. Greenwald, "No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State," Picador USA (Reprint edition), 2015.

[2] WikiLeaks, https://wikileaks.org/nsa-japan/

[3] A Project of the Electronic Frontier Foundation, https://www.eff.org/secure-messaging-scorecard

[4] K. Yoneyama, R. Yoshida, Y. Kawahara, T. Kobayashi, H. Fuji, and T. Yamamoto, "Multi-cast Key Distribution: Scalable, Dynamic and Provably Secure Construction," Proc. of Prov. Sec. 2016, pp. 207–226, Nanjing, China, Nov. 2016.

Trademark notes

Reo Yoshida

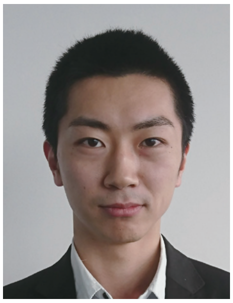
Researcher, Data Security Project, NTT Secure Platform Laboratories.

He received a B.S. in mathematics from Nagoya University, Aichi, in 2007 and an M.I. in informatics from Kyoto University in 2009. He is presently researching cryptography and information security at NTT Secure Platform Laboratories.

Hironobu Okuyama

Senior Research Engineer, Data Security Project, NTT Secure Platform Laboratories.

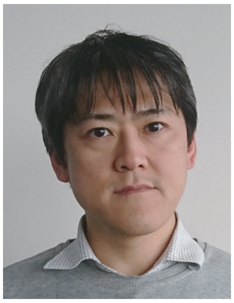
He received a B.S. in mathematical sciences from Tohoku University, Miyagi, in 1990 and an M.S. in mathematical sciences from Chiba University in 1992. He is presently engaged in research on information security.



Yuki Okano

Researcher, Data Security Project, NTT Secure Platform Laboratories.

He received a B.S. and M.S. in mathematical sciences from Keio University, Kanagawa, in 2012 and 2014. He is presently researching information security.



Tetsutaro Kobayashi

Senior Research Engineer, Data Security Project, NTT Secure Platform Laboratories.

He received a B.Eng. and M.Eng. in electrical and electronic engineering from Tokyo Institute of Technology in 1993 and 1995, and a Ph.D. in information and communication engineering from the University of Tokyo in 2005. He is currently conducting research on information security. He was awarded the SCIS (Symposium on Cryptography and Information Security) 2000 paper prize.