# Secure password authentication schemes and their applications

## — How to achieve security with short passwords —

**Kazukuni KOBARA * and SeongHan SHIN**

**[Translation from *Synthesiology*, Vol.7, No.3, p.179-189 (2014)]**

Passwords are widely used for encrypting files, authenticating remote users on a communication network, and establishing encrypted channels for authenticated users. However, the possibility of passwords being stolen or abused raises security problems, and having to remember a number of lengthy passwords is often inconvenient. The purpose of this research is to develop new schemes to resolve these problems and make them generally available to society. In this paper, we introduce our research strategies and scenario to achieve this purpose.

*Keywords* : Authentication, key management, password, phishing, cloud

## 1 Introduction

### *1.1 Background*

Passwords are used for many wide-range purposes to identify users on the network, to perform remote user authentication for establishing an encrypted communication channel with such users, to encrypt files, and so on. However, passwords have many problems of security such as being stolen and abused or of inconvenience in remembering several long passwords. Improvements are sought for such issues.

On the other hand, there are methods other than using passwords to identify an individual, such as using biometrics or personal belongings. The biometric authentication has problems such as impersonation using artificial materials, low identification capability, and requirement of a special device to detect artificial impersonation,[1] and research to improve such issues is currently in progress. The authentication method using personal belongings should be combined with passwords to prevent abuse in case the object is stolen or lost, and it is not necessarily a complete replacement to the password method. For file encryption, there are methods of using the encryption keys instead of passwords, but the password is necessary to protect the decryption keys. Although there exist methods using information other than passwords, they are not complete replacements to the password method at this moment. Therefore, in this research, we aim to solve the problems of passwords by focusing on improvements of the methods handling the passwords.

Figure 1 shows the statistical data[2] published by the National Police Agency pertaining to the password security problems. Here, “lax setting and management of password” means that the password was cracked due to exhaustive searches because an easily guessed password was used. “Former employees, acquaintances, etc.” means that the crime was committed by individuals such as the server manager who had the right to access to the victim’s password. The former case will be explained in detail in subchapter 1.2. For the latter case, it has been a problem that a third party can know the password by using the information leaked from the server, and this problem will be explained in subchapter 1.3. As countermeasures to “heard or peeked” and “lax setting and management of password,” it is recommended to employ two-factor authentication where information other than passwords is used concurrently, in addition to alerting and educating the users. However, as the two-factor authentication becomes more prevalent, the resistance against loss and theft of client devices becomes important, and this will be explained in subchapter 1.4. Finally, the problem of phishing fraud will be discussed in subchapter 1.5.

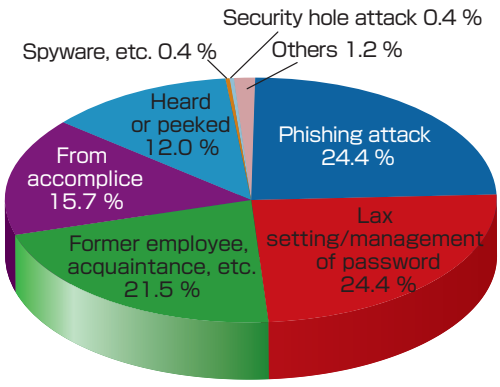


**Fig. 1 Ways of obtaining passwords**

Research Institute for Secure Systems (RISEC), AIST Tsukuba Central 2, 1-1-1 Umezono, Tsukuba 305-8568, Japan
* E-mail: kobara_conf-mlaist.go.jp

Original manuscript received October 24, 2013, Revisions received January 14, 2014, Accepted April 3, 2014

**Table 1. Comparison of remote user authentication methods using passwords**

| | Authentication methods | Security against password exhaustive searches: Against eavesdropping and impersonation | Security against password exhaustive searches: In case of stored information leakage: From client | Security against password exhaustive searches: In case of stored information leakage: From server | Security against password exhaustive searches: In case of stored information leakage: From both with time lag | Security against phishing attacks | Number of passwords |
|---|---|---|---|---|---|---|---|
| One-factor authentication | Conventional protocol using password only | × | ○ | × | × | × | Multiple |
| | PAKE | △ | ○ | × | × | ○ | Multiple |
| Two-factor authentication | PKI server authentication + PW | △ | ○ | × | × | × | Multiple |
| | PKI server authentication + PW + OTP | ○ | ○ | × | × | × | Multiple |
| | PKI (mutual authentication) | ○ | × | ○ | × | △ | One |
| | LR-AKE (this research) | ○ | ○ | ○ | ○ | ○ | One |

Table 1 is a summary of the comparison of remote user authentication methods using passwords. The column on the furthest left of the table shows the methods, and these can be roughly divided into one-factor authentication where passwords only are used and two-factor authentication where passwords and stored information are used. Note that these methods not only authenticate the user, but also have the function of establishing an encrypted communication channel between the user and the server. Briefly explaining the outline of each method, the "PKI (public key infrastructure) server authentication + PW (password)" and "PKI server authentication + PW + OTP (one-time password)" are methods where the server has a pair of public key and private key, the encrypted communication channel is established between the client device and the server using the public key, and that encrypted communication channel is used to transport the user's password or one-time password (OTP) to the server. If the public key is considered to be an authentication information that must be managed by the user, it will be two-factor authentication, while if it is considered to be information that does not have to be managed by the user, it will be one-factor authentication. In many cases, the latter form of management is taken, and this is one of the technological security holes that allow phishing fraud. This problem will be explained in subchapter 1.5. The one-factor authentication that uses passwords only can be categorized into "conventional protocol using password only" and "password authenticated key exchange (PAKE)." The former has disadvantages of being susceptible to eavesdropping on the communication channel and impersonation, but PAKE solved these issues. However, in these methods, the password or its hash value (value to which the password is processed) that is used to authenticate the user must be stored on the server, and is susceptible to leakage of information. Moreover, if the user uses the same password in multiple servers, the password that was leaked due to a problem in one server can be used to log in to a server or service that is presumed to be secure. In order to prevent this problem, the user must set different passwords for each service, and must remember multiple passwords as shown in the last column of Table 1.

The PKI mutual authentication is a method resistant against information leakage from servers. In this method, both the server and the user have a pair of public and private keys, and the user's public key (or related information) is stored on the server. Therefore, even if the information leaks from the server, the private key needed for impersonation cannot be obtained. However, since the private key is stored on the client side in this method, it is weak against the information leakage from the client. This issue will be explained in subchapter 1.4. The leakage-resilient authenticated key establishment (LR-AKE) is a method that was devised and practically applied through this research. The user uses only one short password, yet this system is resilient to eavesdropping, impersonation, leakage of stored information from either the server or the client, phishing, and others.

The aforementioned problems and the items in the remaining columns of Table 1 will be explained in the following subchapters.

### *1.2 Vulnerability against exhaustive searches of passwords*

The most basic method for increasing resilience against password exhaustive searches is to use an extremely long password that is randomly selected. However, this method substantially reduces usability and is not practical. Therefore, a way must be considered to increase resilience against exhaustive searches while using a short password that is within the range in which a person can remember it effortlessly. Although this may seem to be a paradoxical issue, the solution may arise if one can understand that the password exhaustive searches can be categorized into an offline exhaustive search, a parallel online exhaustive search, and a serial online exhaustive search, and that there are differences among these search methods.

Here, an offline exhaustive search is a method of testing the passwords using data obtained by eavesdropping

communication, without connecting to the server. For example, when a random number c and r calculated by r = h(c, pw) are transmitted through the communication channel and function h() is public while only a password pw is secret, the attacker that eavesdropped on them can verify whether pw' is the correct password or not by calculating r' = h(c, pw') using the password candidate pw' and checking whether r = r' is valid. The number of passwords that can be tested is increasing year by year in proportion to increased computational capacity, and this is an extremely powerful method of attack since it is not limited by the server's setting.

As the length of keys that is sufficiently secure against offline exhaustive searches, the National Institute of Standards and Technology (NIST) of the USA recommends the use of more than 80 bits until 2010, more than 112 bits from 2011 to 2030, and more than 128 bits or more after 2031.[3] These correspond to 14, 19, and 22 characters, respectively, when converted to the length of passwords consisting of randomly selected small and capital letters and numbers. In fact, based on this estimate, the file encryption software recommends the use of passwords with 20 characters or longer.[4] On the other hand, the length of passwords that can be memorized by a human effortlessly is about 7±2 characters,[5] and this cannot withstand an offline exhaustive search.

In contrast, the parallel and serial online exhaustive searches are methods where, in the authentication protocol executed with the server, the guessed password is validated by checking whether it is acceptable or not. The serial online exhaustive search is a method of testing the passwords one by one for a single account, while the parallel online exhaustive search is a method where parallel searches are done for multiple accounts. In either method, the password cannot be tested unless one is connected to the server, and therefore, the risk against password exhaustive searches can be controlled regardless of increase of computational power, by limiting the number of passwords that can be tested during a certain period of time on the server.

This means that depending on what type of exhaustive search can be applied to a password handling method, the length of passwords that can be used securely varies. For the column of the resilience against password exhaustive searches in Table 1, the case where the offline exhaustive search can be applied is marked ×, the case where the parallel online exhaustive search can be applied is △, and the case where neither can be applied is ○. The case where the stored information is leaked will be explained in subchapters 1.3 and 1.4. Even in the case where there is no information leakage, in the "conventional protocol using password only," the offline exhaustive search can be applied just by eavesdropping on the communication channel. Also in case of "PAKE" and "PKI server authentication + PW," parallel online exhaustive search can be executed on multiple accounts since anyone can test the password. In cases of "PKI server authentication + PW + OTP," "PKI mutual authentication," or "LR-AKE," not even online exhaustive search can be applied since the correctness of the password cannot be tested online unless authentication information other than the password from the client is available.

**Table 2. Examples of information leakage incidents from servers**

| Information leakage incidents | Outline of incident |
|---|---|
| Information leakage from Adobe Systems[6] | It was announced that there was possibility that about 2.9 million customer information was leaked due to illegal access (October 2013). |
| Information leakage from OCN[7] | It was announced that there was possibility that about 4 million OCN account information was leaked outside due to illegal access (July 2013). |
| Information leakage from Yahoo! Japan[8] | It was announced that there was high possibility that about 1.48 million user IDs and "secret information" for password resetting were leaked due to illegal access (May 2013). |
| Information leakage from Yahoo! USA[9] | About 400,000 user login authentication information was leaked outside due to cyber attack (July 2012). |
| Information leakage from Citigroup[10] | About 210,000 credit card customer information was leaked due to illegal access (Jun 2011), and the total financial damage by illegal use of the leaked card information was over 200 million yen.[11] |
| Information leakage from Sony PSN[12] | Large-scale personal information leakage occurred due to unauthorized invasion to Sony's PSN (Play Station Network, 77 million users) and Qriocity (April 2011). Due to this incident, Sony was ordered to pay a fine of about 35 million yen in the UK.[13] |

### *1.3 Vulnerability against information leakage from the server*

Generally, servers are carefully managed by specialist managers, and it has been thought that information leakage was not likely to occur. However, in recent years, incidents of information leakage from servers have occurred quite frequently, and it is becoming more difficult to assume that such information leakage does not occur. Table 2[6]-[13] shows major information leakage incidents from servers in the past 2-3 years.

With the information leakage from the server, the problem is that large amount of information is leaked at one time and many users are subject to being exposed. The average estimated compensation per person calculated by the Japan Network Security Association for the first semester of FY 2012 was 57,710 yen.[14]

For the effect on the password authentication method in the case where the information leakage occurs from the server, in the method categorized as the "PKI server authentication + PW" and "PKI server authentication + PW + OTP," the user's

password or the hash value (value to which the password is processed) is stored on the server. Therefore, if such values leak, the password can be identified by applying the offline exhaustive search. Moreover, if the identified password has been reused for other services, there may be subsequent exposure on services where the leaks have not occurred.

In the method categorized as "PKI server authentication + PW + OTP," information to generate one-time passwords is also stored on the server, and if this information is leaked, the one-time password that the user has to enter can be known.

### *1.4 Vulnerability against information leak from the client*

Figure 2 shows the number of incidents of information leakages that occurred through loss, misplacement, or theft of the devices or memory media. This figure is created from the statistical data from 2005 to 2011 published in the Japan Network Security Association's "Report on the information security incidents."[15]

The number of leakage incidents declined steadily until about 2007, and this is thought to be due to the implementation of regulations against carrying out personal computers and portable media at companies and organizations to counter the information leakage incidents that occurred earlier. However, the effect slowed down after 2007, and the cases cannot be reduced to 300 or less per year. These figures reflect only the large-scale incidents that were covered by the news media, and the number is expected to increase if the small-scale incidents that did not make the news are included. Moreover, many more people are likely to carry small and highly functional devices such as smart phones and tablets in the near future, and the numbers of loss, misplacement, or theft of such devices are expected to increase proportionally.

The client device contains the information necessary for remote user authentication such as the encryption key that

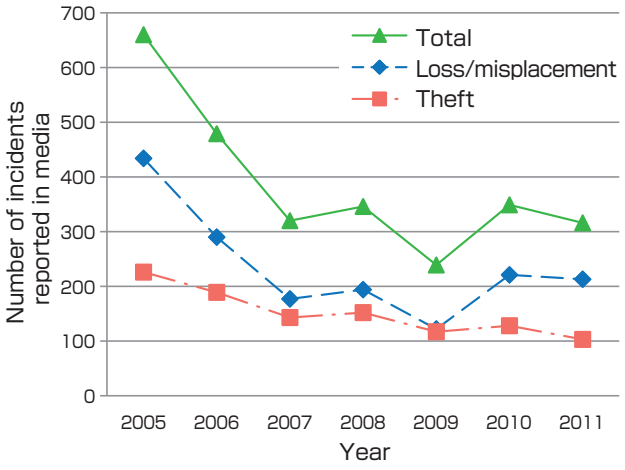


**Fig. 2 Number of information leakage incidents from clients**

was encrypted with password in the authentication method or the passwords stored on the device, and if such information leaks, impersonation of the user or identification of the user's password becomes possible. In the method categorized as "PKI mutual authentication" in Table 1, the key for user authentication is stored in the client device, and this key is generally encrypted with a password. Therefore, if an attacker acquires the device, the password and key can be found by offline exhaustive search.

### *1.5 Vulnerability against phishing*

In the methods categorized as "PKI server authentication + PW" and "PKI server authentication + PW + OTP" in Table 1, the encrypted communication channel is established between the user and the server, and then the password or one-time password entered by the user is transmitted to the server through this encrypted communication channel. The user authentication is done when the transmitted password or one-time password is decrypted and compared to the correct values in the server. Since the communication channel is encrypted, the password or OTP cannot be obtained even if eavesdropping occurs. However, the attacker may try to steal the information such as the user password by leading the user to a fake server made by the attacker. Various tactics may be used, for example, by sending spam mail that may claim: "Your passcode of your bank account has been leaked. Please change the password immediately from the following website." In the method categorized as "PKI mutual authentication," while the user's password is not transmitted to the server, the information entered after authentication (for example, credit card number and personal information) may be stolen.

In the methods using these PKIs, there are mechanisms that warn the user when the user connects to a fake server, but these may not function effectively because a non-malicious server may use a self-signed public key certificate, the user may ignore the warning when led to a fake server, or there may be fake servers that have valid certificates (without warning) generated when a leaked CA's signature key is abused. In contrast, in PAKE and LR-AKE, the password is not transmitted to the server, and the valid server does not have such a warning. Since the server authentication is conducted in the authentication protocol, the connection to the fake server is forcibly denied.

## 2 Research scenario to solve the problem

The scenario of this research is shown in Fig. 3. The goal is to devise and put into practice new methods that solve the problems of passwords shown in middle-left of the figure, and to provide this technology to society. The characteristic of this research scenario is that the practical application research is conducted only after thorough consideration of the problem solvability and the improvements of the

fundamental cryptographic theories for problem solving. This is because in a case where a fatal cryptanalytic method on the fundamental cryptographic technology is discovered after the deployment of the new technology, vast amount of cost and time will be needed to correct the basic principle and to change the method, since the problem cannot be solved with simple corrections such as patch applications. In fact, there are many examples where cryptanalytic methods were discovered for wireless LAN,[16] electronic keys for automobiles,[17] IC cards,[18] and mobile phones after their deployments,[19] and that have become major social problems.

The stages of the research scenario will be explained in the following subchapters.

### *2.1 Theoretical research for the problem solvability*

To clarify at an early stage whether a certain social problem can be solved by science and technology is very important since this knowledge aids the decision on whether to pour the research resource into that topic, and this may in turn lead to the optimal assignment of resources. Fortunately, it is possible to theoretically clarify whether the required item can be solved for the problems related to cryptographic technology, and based on the problem solvability the main stage of the research can be continued smoothly.

In this research, the theoretical decision would be made on whether the problems described in subchapters 1.2 to 1.5 can be solved by cryptographic technology. If they are unsolvable problems, the reasons why they cannot be solved are clarified theoretically, and if they are solvable, the actual instantiations are presented. If it cannot be clarified whether a problem is solvable or unsolvable, it is raised to academic societies as an open problem and the cooperation of other researchers is sought.

### *2.2 Research for improvements in theoretical aspects*

In the case where the problem solvability is theoretically not impossible, a specific solution will be presented, but the initial solution will have room for improvements in computational complexity and security. Therefore, the theoretical improvements of the solution will be conducted over some time. Such improvements may be done by the original researchers, or may be done by other research groups. Also, such improvements in the information security field will be done against offense as well as defense, and the improvements from the offensive side plays a very important role. This is because if an attacker makes improvements to the attack method after the method is deployed to society or if the defender predicts possible new attack methods beforehand, the latter will dramatically reduce the cost of correction and effect on society.

### *2.3 Research for the practical application*

A method for which no attack can be found and which has been theoretically improved advances a step closer to practical use. Research for practical use includes the followings:

- Research for additional functions needed in case of practical use,
- Research for implementation method,
- Research for coordinating with other application software.

The first is research to make the proposed method more usable or to enable multiple usages, and the second is research on how these will be implemented. The third is research on how to coordinate implemented methods with external software. The details and results of this research that was actually conducted will be described in the following chapter.

## 3 Inspection and result of the research scenario

In this chapter, research topics selected in order to realize the research goals according the aforementioned scenario, the reasons for selection, and the results will be explained.

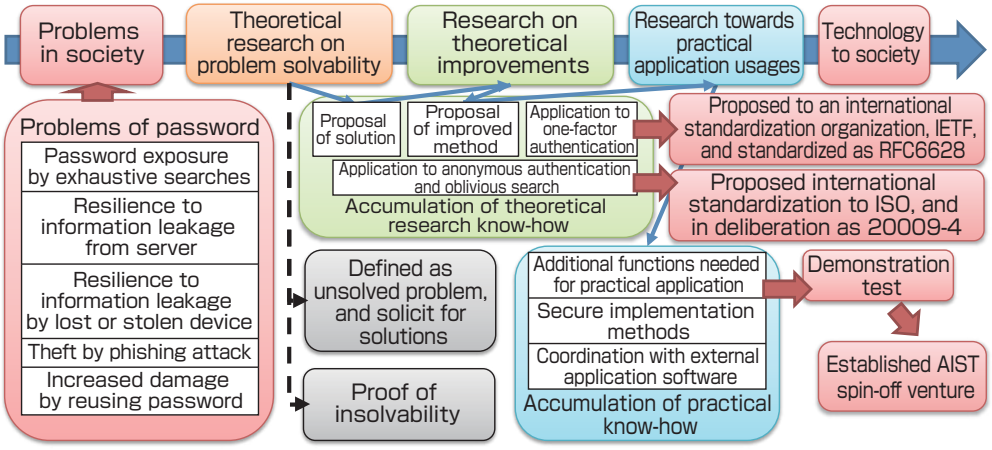


**Fig. 3 Scenario of this research**

### *3.1 Result of theoretical research on the problem solvability*

When it is found that the aforementioned problem is solvable by the research at this stage, the limiting conditions required for the solution become apparent. The main limiting conditions are described below.

- [Limiting condition 1] Assuming that the stored information is leaked totally from the server in the one-factor authentication, where the user remembers only one short password, it is impossible to protect the user's password from offline exhaustive searches no matter how the cryptographic technologies are combined.

With this condition, it is clear that all the problems in subchapters 1.2 to 1.4 cannot be solved using the one-factor authentication where the user remembers only one short password. Therefore, we decided to focus the research topic on two-factor authentication where the information other than the password is stored on the client side. However, simply employing two factors in the authentication method does not lead to a solution of the problems. In fact, the previous "PKI server authentication + PW + OTP" method that has been widely used as the two-factor authentication is vulnerable to leakage from the server, and the "PKI mutual authentication" method, as a different two-factor authentication, is weak against the leakage of information stored on the client side. There has been no proposal or case study in the research community and the industry on how short passwords, the authentication information to be stored in the client device, and the cryptographic technology can be combined to solve the problems. This was also an academically challenging issue.

On the other hand, the following condition can be derived as the limit of two-factor authentication methods.

- [Limiting condition 2] Assuming that the stored information is leaked from both the server and the client at the same time in the two-factor authentication, where the user remembers one short password and stores information, it is impossible to protect the user's password from offline exhaustive searches no matter how the cryptographic technologies are combined.

Here, "the stored information is leaked … at the same time" means that leakages of the stored information from both the server and the client occur in the same authentication transaction. However, this leaves room for problem solving in a case, for example, the server's stored information used in the *n*th authentication and the client's authentication information used in the *n+1*th authentication are not used in the same authentication transaction. Therefore, the highest-level of security for which the solvability is not denied by this limiting condition is that the user's password is protected from offline exhaustive searches even if the stored information is leaked from both the server and the client, unless the leakages occur at the same time. By the way, the parallel online password exhaustive searches are ineffective in two-factor authentication only when there is sufficient number of candidates of authentication information stored in the client device. This is because in the two-factor authentication, unless a large number of the authentication information stored on the client side can be obtained, the online password exhaustive search cannot be applied in parallel.

We had conducted the research by focusing on whether a composition that satisfies the highest-level of security for which the solvability of resilience against information leakage is not denied exists or not, and proposed a specific solution that satisfied the condition for the first time in the world. The main points of the technological composition include that, first, the independently selected secret information for each server is stored on the client side, and then, the verification data computed from the secret information stored on the client device and only one password remembered by the user are stored on each server as information to be used to authenticate the user. By doing this, it becomes difficult to retrieve the password from the verification data stored on the server. By automatically updating the information stored on the client side and the server side after the authentication is completed successfully, it also becomes difficult to find out the password even if the leakages occur from both the client and the server at different time slots. Moreover, we designed a cryptographic protocol where an attacker cannot narrow down the password candidates even if the attacker obtains the stored information and the messages that are exchanged through the communication channels.

We named this method Leakage-Resilient Authenticated Key Establishment (LR-AKE).[20]

### *3.2 Research result of the improvements in the theoretical aspect*

In this stage of the research, we have worked on how to reduce the computational costs of LR-AKE, how to strengthen security against much more sophisticated attacks, and how to prove the security of LR-AKE mathematically by showing the reduction to the computationally-hard problem. Also, we succeeded in improving the previous one-factor authentication and oblivious search methods by applying the knowledge accumulated through this research.

For computational costs, in the initially proposed method,[20] the required cryptographic processing (specifically, about 720 times of multiple-precision multiplication with 1024-bits or more) was heavy on the client, and it was not easy to conduct such heavy cryptographic processing on the thin client devices such as the mobile phones used at the time. Therefore, we proposed a method where the number of

multiple-precision multiplication could be reduced to three times, and also proved that breaking the proposed method is equivalent to solving the mathematically hard problem.[21]

For strengthened security against much more sophisticated attacks, we proposed a method where an attacker cannot retrieve the user's password and data distributed between the server and the client even if the attacker replaces authentication information stored on the client side into anything, and proved that to break the proposed method is equivalent to solving the mathematically hard problem.[22] The authentication information stored on the client side may be stored on a portable medium for carrying, but this attack assumed a case where the portable medium is stolen, rewritten, and then returned to the original place.

By applying the knowledge of the cryptographic protocol designs accumulated through research at this stage, we also succeeded in improving the PAKE, the anonymous PAKE, and the oblivious search method. However, since these protocols use only one factor as secret information, the resilience to offline exhaustive searches using the information leaked from the server cannot be guaranteed. Yet, they achieve security against eavesdropping on the communication channel and impersonation attacks (identification of search word in the oblivious search method) with the least computational costs, and we succeeded in proving that to break the proposed methods is equivalent to solving the mathematically hard problems.[23]-[25] Here, the anonymous password authentication protocol is a method to only verify that a user belongs to a certain group without making the server identify the individual user. This can be applied to the following usages:

- Anonymous whistleblowing from a member of an organization,
- Anonymous counseling service to a member (such as counseling for medical condition, bullying, or personal troubles),
- Formation of community for members with a certain attribute (such as women only),
- Anonymous communication channel restricted to the purpose of use.

The above method can also be used as an efficient core engine for conducting search while hiding the search word from the server by using the search word instead of the password, and for conducting matching while keeping each other's condition secret. The method of Reference [25] was proposed to the International Organization for Standardization (ISO), and the deliberation for standardization as 20009-4 (Anonymous entity authentication – Part 4: Mechanisms based on weak secrets) is in progress.[26] For the method of Reference [23], the specification for application to a general Internet protocol, Internet Key Exchange version 2 (IKEv2) was proposed to the Internet Engineering Task Force (IETF), an international standardization organization, and was approved and published as the international standard RFC6628.[27] In an implementation version of the LR-AKE system, the methods of References [23] and [24] are used as the subprotocols to distribute the client's authentication information to users via the network by issuing one-time passwords to the users. The methods are contributing greatly to enhance the usability of user registration.

### *3.3 Research result towards practical use*

In this subchapter, we explain the specific contents and results of the research mentioned in subchapter 2.3.

#### *3.3.1 Research result of the additional functions needed in practical use*

In order to realize both usability and security in LR-AKE, we devised several ways to maintain a high-level of security even if the user selects a short password. Specifically, even if an attacker obtains messages exchanged through the communication channel and data stored on either the server or the client side, the protocol is designed in a way that the offline and parallel online exhaustive searches of the password cannot be applied. Also, even if an attacker obtains the authentication information leaked from the client device and sequentially tests the password candidates one by one on the server, the stored authentication information is automatically updated when the regular user completes authentication successfully, and after that the leaked authentication information that the attacker obtained can no longer be used.

The attacker can test the password candidates until the stored authentication information is updated, but it is possible to lock the user's account after a fixed number of authentication failures. However, with a simple method such as the above, a low-level attacker who does not have the client's stored authentication information can disrupt the valid authentication process by locking the legitimate user's account by intentionally failing authentication, or by overloading the server with a large amount of authentication requests. Therefore, we devised and implemented a mechanism where in case such a low-level attacker connects, the authentication process is terminated without overloading the server, and in case of authentication failure, it is possible to determine whether an impersonator is testing without knowing the stored information, whether a password is being tested from a different device using the leaked stored information, or whether a legitimate user typed a wrong password.[28] This enables the detection of attacks using the leaked information while preventing the illegal lockdown of a legitimate user account and the disruption of authentication server service by the attacker who has not obtained the stored authentication information.

Moreover, if all the password authentication methods are

replaced with LR-AKE, the user just needs to remember only one password even if the user uses several independent services. However, during a transition period, the user must memorize or store several passwords, used in other services, in addition to the LR-AKE password. Therefore, we considered and implemented a function, by using the characteristic of LR-AKE that makes it resilient against information leakage, whereby important information such as passwords and encryption keys used in other methods are placed in distributed storages after being computed with the LR-AKE server, the client and the LR-AKE password, and the original information cannot be restored unless the LR-AKE authentication is completed successfully.[29] The information placed in distributed storages in LR-AKE cannot be restored from the information stored in either the server or the client side as in the case of LR-AKE password, and these information are automatically updated each time the LR-AKE authentication is successfully done.

However, by adding this distributed storage function, a new problem emerged. Our proposed method is resilient against leakage as mentioned earlier, but the stored original data cannot be retrieved if the stored information on either the server or the client side become unavailable. Also in LR-AKE, the information stored on the server and the client are updated, whenever authentication is successfully done, in order to maximize resilience against leakages. Therefore, in cases of malfunction of the server or loss of the client device, the original data in distributed storages in LR-AKE cannot be retrieved even if one of the nodes is restored to the previous state using the backup data. By using the multiple LR-AKE servers and multiple clients, the original data was made retrievable after node crashes while maintaining leakage resilience, and also the information stored on one LR-AKE client device was made retrievable from other LR-AKE client devices. Also in a case where the user mistakenly locked the account by entering wrong passwords several times surpassing the threshold number of failures, we implemented a mechanism to unlock the account from the user's effective LR-AKE account. We call such redundant configuration of the LR-AKE the cluster mode,[30] in order to distinguish it from the single mode that is the configuration of one client device and one server.

If the cluster mode is used, in addition to placing the personal data in distributed storages in the LR-AKE, a group can be formed so that the same information is shared within the group without leaking the information to the server.[31] Therefore, for example, computer administrators of a company can manage important information securely within the group, such as sharing the administrator's password for servers and devices. In such a case, the password that each user must remember can be a short one, and that password will not be known to the other group members or the server administrator.

#### *3.3.2 Research result of the implementation method*

Since the LR-AKE will be basically used in a situation where a high level of security is required, we also considered security measures during the implementation in addition to maintaining its high security level. These operations mainly followed the best practice for secure implementation, and did not yield results such as academic papers or patents for which novelty was demanded. However, the knowledge gained in these operations was greatly useful in advancing the research for cyber security of critical infrastructures and control systems in which we became involved later.

Also, some ambiguous parts of the specification became apparent only after we actually implemented it. As mentioned earlier, LR-AKE is equipped with the function to update the stored information after user's successful authentication in order to automatically invalidate the leaked authentication information, and the mechanism for determining whether the cause of authentication failure was a typing mistake by the legitimate user or whether the password was being tested using the stored information leaked from the client. Since these were assumed for cases where the protocol was completed normally, ambiguous parts remained for what would occur in a case where the communication was suddenly cut off. Therefore, we investigated a way to ensure recovery of communication at all times and to maintain the above functions and security level, even if the communication was cut off at any point in the protocol, and this was reflected in the details of the specifications and then implemented.

#### *3.3.3 Research result of the coordination with other software applications*

When precision of the implementation increased, the coordination with various application software became an issue. One method was to incorporate the LR-AKE as part of each software, but this method became problematic because it required a lot of workloads in which corrections were necessary at each update of LR-AKE in addition to the initial corrections to the software. Moreover, since the boundaries of responsibility were ambiguous, it became difficult to obtain cooperation of the application developers. Therefore, the Application Programming Interface (API), an interface to call up the LR-AKE function from the application software side, was defined, and an attempt was made to eliminate the correction in coordinating the software during the LR-AKE update. That is, the interface was not changed when the LR-AKE was updated or a new interface was added while the old one was left intact. Moreover, we investigated and implemented the coordination mechanism without correcting the program on the application side. Specifically, a one-time password is created on the LR-AKE client side and the server side after the LR-AKE authentication, the server uses the password registration protocol of the application, the one-time password is registered as the user password to be

used in the application, and finally the client uses the one-time password to obtain authentication using the password authentication protocol provided by the application. At the same time, the server authentication is done by delivering the information about the server to the client via a secure communication channel set up between the LR-AKE server and the LR-AKE client. With this coordination mechanism, the user can receive various services linked with LR-AKE just by performing the LR-AKE authentication, and the source code of the linked application does not have to be changed.

In fact, this mechanism was used in the demonstration test at AIST. In this test, the LR-AKE and the Virtual Private Network (VPN) that allows the authenticated users over external networks to be connected to the intra network were coordinated, and the users could use some services of the AIST network by performing the LR-AKE authentication. Of course, since the VPN software is a product of a different company, we could not change its source code. Therefore, we enabled the coordination without changing the VPN source code using the aforementioned mechanism. As the demonstration test, the system went into operation on March 13, 2010 to check that there were no problems, and from July 27, 2010 we asked participation of the Research Center for Information Security and the Tsukuba Advanced Computing Center to respond immediately in case any problem occurred, and had them use the system in place of the regular VPN connection. Since it was confirmed that there were no problems in the operation, we had prepared to have more people participate in 2011. However, the Tsukuba area was hit by the earthquake on March 11, 2011 and the servers of AIST Tsukuba including the LR-AKE server were shut down temporarily. Fortunately, the LR-AKE in the demonstration test was operated in the aforementioned cluster mode where the secondary server was set up in AIST Chugoku. So, we were able to continuously maintain the function of retrieving the data that were distributed in the LR-AKE cluster mode even after the coordination with VPN and the LR-AKE server at Tsukuba were shut down.

## 4 Conclusions

We discussed the basic theoretical researches and their practical application researches on the cryptographic construction that makes the exhaustive searches against the user's password impossible, even if the stored information is leaked from either the server or the client. Later, the practical application technology was offered as a commercial Software Development Kit (SDK) to call up the LR-AKE function from a software that requires user authentication and key management, as a commercial server, and as technical support, by setting up a spin-off AIST venture company. Moreover, part of the function was proposed to IETF and was published as an international standard RFC6628.

Currently, this technology is in an stage of being offered to society and being employed by innovators (innovative users according to the studies of innovation diffusion[32]). In April 2013, we received the Encouragement Award of the Excellent New Technology/Product Award for small and medium-sized enterprises and the Special Award for industrial-academic-government cooperation sponsored by the Resona Group and Nikkan Kogyo Shimbun, and this was an opportunity to be known to some of industry.

However, from the fact that in the past it took about 20~30 years for the public key technology to be prevalent in society, it is expected that the same amount of time might be necessary for the prevalence of LR-AKE. Therefore, until LR-AKE is taken up by early adopters (users who are responsive to new items) or early majorities (users who take in new items earlier than average people), and reaches the critical mass of diffusion of about 16 % at which point the technology is said to start to spread rapidly, it is necessary to steadily accumulate achievements and to continue to work on activities to raise its awareness.

Also, we hope that this paper would be a reference for the practical use of research results and for offering such results to society.

## References


[1] M. Suzuki and M. Une: Seitai ninsho shisutemu no zeijakusei no bunseki to seitai kenchi gijutsu no kenkyu doko (Analysis of vulnerabilities of biometric authentication system and research trends in the biometric detection technology), *Kin'yu Kenkyu*, 28 (3), 69-106 (2009) (in Japanese).

[2] National Police Agency: Heisei 23 nen chu no fusei akusesu koi no hasseijokyo-to no kohyo nitsuite (On the release of information for the occurrence of unauthorized access and others in 2011), http://www.npa.go.jp/cyber/statics/h23/pdf040.pdf, (2012) (in Japanese).

[3] E. Barker, W. Barker, W. Burr. W. Polk and M. Smid: Recommendation for key management - Part 1: General (revision 3), *NIST Special Publication*, 800-57, (2012).

[4] TrueCrypt Foundation: TrueCrypt Beginner's Tutorial Part 2, http://www.truecrypt.org/docs/tutorial2, accessed in August 2013.

[5] G. A. Miller: The magical number seven, plus or minus two: Some limits on our capacity for processing information, *Psychological Review*, 63 (2), 81-97 (1956).

[6] http://headlines.yahoo.co.jp/hl?a=20131004-00000005-rbb-sci, accessed in October 2013.

[7] http://www.ntt.com/release/monthNEWS/detail/20130724.html, accessed in October 2013.

[8] http://itpro.nikkeibp.co.jp/article/NEWS/20130523/479201/, accessed in October 2013.

[9] http://jp.reuters.com/article/technologyNews/idJPTJE86B02120120712, accessed in October 2013.

[10] http://www.bloomberg.co.jp/news/123-LMJIFD1A1I4H01.html, accessed in October 2013.

[11] http://www.zaikei.co.jp/article/20110627/74852.html, accessed in October 2013.

[12] http://www.nikkei.com/article/DGXZZO27529030X20C11A4000000/, accessed in October 2013.
[13] http://japanese.engadget.com/2013/01/24/psn-3500/, accessed in October 2013.
[14] Japan Network Security Association: 2012 Joho sekyuriti inshidento ni kansuru chosa hokokusho [Kamihanki sokuhoban] (Report on information security incidents in 2012 [Prompt report for the first semester]), http://www.jnsa.org/result/incident/2012.html, (2013) (in Japanese).
[15] Japan Network Security Association: Joho sekyuriti inshidento ni kansuru chosa hokokusho (Report on information security incidents), http://www.jnsa.org/result/2013.html, (2009-2012) (in Japanese).
[16] AIST: Musen LAN no sekyuriti ni kakawaru zeijakusei no hokoku ni kansuru kaisetsu (Explanation on the report of vulnerabilities of wireless LAN security), https://www.rcis.aist.go.jp/TR/TN2009-01/wpa-compromise-summary.html, (2009) (in Japanese).
[17] K. Zetter: Researchers crack KeeLoq code for car keys, *WIRED*, http://www.wired.com/threatlevel/2007/08/researchers-cra/, (2007).
[18] E. Phillips: Mifare crypto1 RFID completely broken, http://hackaday.com/2008/01/01/24c3-mifare-crypto1-rfid-completely-broken/, (2008).
[19] H. Horesh: Technion team cracks GSM cellular phone encryption, http://www.cs.technion.ac.il/~barkan/GSM-Media/HaaretzInternetEnglish.pdf, (2003).
[20] SH. Shin, K. Kobara and H. Imai: Leakage-resilient authenticated key establishment protocols, *ASIACRYPT 2003*, LNCS 2894, 155-172 (2003).
[21] SH. Shin, K. Kobara and H. Imai: An efficient and leakage-resilient RSA-based authenticated key exchange protocol with tight security reduction, *IEICE Transactions*, E90-A (2), 474-490 (2007).
[22] SH. Shin, K. Kobara and H. Imai: An RSA-based leakage-resilient authenticated key exchange protocol secure against replacement attacks, and its extensions, *IEICE Transactions*, E93-A (6), 1086-1101 (2010).
[23] SH. Shin, K. Kobara and H. Imai: Secure PAKE/LR-AKE protocols against key-compromise impersonation attacks, *SITA 2008*, 965-970 (2008).
[24] SH. Shin, K. Kobara and H. Imai: RSA-based password-authenticated key exchange, revisited, *IEICE Transactions*, E91-D (5), 1424-1438 (2008).
[25] SH. Shin, K. Kobara and H. Imai: Anonymous password-authenticated key exchange: New construction and its extensions, *IEICE Transactions*, E93-A (1), 102-115 (2010).
[26] ISO: Anonymous entity authentication - Part 4: Mechanisms based on weak secrets, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=64288, accessed in October 2013.
[27] SH. Shin and K. Kobara: Efficient augmented password-only authentication and key exchange for IKEv2, *IETF, RFC 6628*, 1-20 (2012).
[28] Y. Onda, SH. Shin, K. Kobara and H. Imai: How to distinguish on-line dictionary attacks and password mis-typing in two-factor authentication, *ISITA2010*, 571-576 (2010).
[29] SH. Shin, K. Kobara and H. Imai: Joho roei ni kenro na ninsho deta kanri shisutemu no gaiyo (shinguru modo) [Outline of leakage-resilient authentication and data management system (single mode)], *Computer Security Symposium 2007*, 2007 (10), 673-678 (2007) (in Japanese).
[30] SH. Shin, K. Kobara and H. Imai: Joho roei ni kenro na ninsho deta kanri shisutemu no gaiyo (kurasuta modo) [Outline of leakage-resilient authentication data management system (cluster mode)], *SITA 2007*, 790-795 (2007) (in Japanese).
[31] SH. Shin, K. Kobara and H. Imai: Grupu kan deno fairu kyoyu o junan katsu anzen ni okonau tameno shin-hoshiki kento (On flexible and secure file sharing for group members), *Computer Security Symposium 2011*, 2011 (3), 803-808 (2011) (in Japanese).
[32] E. M. Rogers: *Diffusion of Innovations*, 5th Edition, Free Press, New York (2003).

## Authors

**Kazukuni KOBARA**

Received M.E. degree in computer science and system engineering from the Yamaguchi University in 1994. Joined the Institute of Industrial Science (IIS), The University of Tokyo in 1994. Research associate of IIS in 2000. Received his Ph.D. degree in engineering in 2003. Joined AIST in 2006. Engaged in the research of fundamental theory and its applications of information security technologies as the Leader of the Research Team for Security Fundamentals, Research Center for Information Security (RCIS), AIST. Principal Research Scientist in July 2006. From 2012, engages in the research of security technologies for control systems and critical infrastructures as the Leader of Control System Security Research Group, Research Institute for Secure Systems (RISEC), AIST. In this paper, engaged mainly in the research scenario and description of the practical application process.

**SeongHan SHIN**

Received Ph.D. degree in information science and technology from The University of Tokyo in 2005. Joined AIST in 2006. Engaged in the research of fundamental theory for authentication and cryptographic protocol as well as its applications in the Research Team for Security Fundamentals, Research Center for Information Security (RCIS), AIST. From 2012, engages in the research of security technologies for Internet service and international standardization in the Secure Service Research Group, Research Institute for Secure Systems (RISEC), AIST. In this paper, engaged mainly in description of the theoretical researches.

## Discussions with Reviewers

### 1 Make the paper's title and abstract clearer and more structured

**Comment (Toshihiro Matsui, Research Institute for Secure System, AIST)**

The "next generation technology for …" as in your title is often seen in proposals, but it merely indicates that something may become somewhat better by an improvement that cannot be described clearly. As the abstract says, "Here, next generation is … to maintain a secure system even when a short password

is stolen either from a server or a client," if you can show the content of the next generation, you should use a specific predicate to describe it. The proposed title is vague and can include all the papers for new authentication and key management that may appear in the future so that you cannot catch the reader's attention. For *Synthesiology*, which is a technological journal that discusses the technological synthesis method for all specialties, I would like to see some indication that you are approaching a key idea of synthesis and methodology, rather than giving an introduction of a single technology. That is, from the title the reader should be able to image why such fundamental technology is necessary, and how it may change society and industry.

**Answer (Kazukuni Kobara)**

In the title, we changed the "next-generation authentication" to the more specific "secure password authentication," and condensed the "key management infrastructures" and "LR-AKE" in the latter half into "their applications."

### 2 Analysis of social and industrial problems and necessary technological development

**Comment (Toshihiro Matsui)**

The paper starts suddenly from comparison of the user authentication methods, and does not say which social problems this technological development is trying to solve. The definition of the problem and the significance of the research will become clear if you state in the beginning part of the paper the current situation of passwords, why they leak, what happens when they leak, why their protection is so difficult, and so forth. These are stated in order from subchapter 1.2 sequentially, but the order should be reversed.

**Answer (Kazukuni Kobara)**

We changed the beginning of chapter 1 to a description of the situation of passwords, and explained the way passwords are used and the causes of leakages. We also changed the structure of the paper to explaining difficulty of password protection from subchapter 1.2 to 1.5.

### 3 Characteristic as a *Synthesiology* paper

**Comment (Toshihiro Matsui)**

Reading through the paper, I understood that the characteristic of this research was not in making improvements based on feedbacks from the actual users, but in conducting R&D by preliminarily predicting all sorts of possible problems, taking measures, and conducting risk assessments in advance. In a technology like cyber security which emphasizes credibility for safety, it is not appropriate to take a common approach of offering a half-finished technology to society asking matureness and then making improvements. Therefore, it is necessary to extract and investigate all possible problems in advance and to take measures against them. I think that it is better to emphasize this point and describe it systematically.

**Answer (Kazukuni Kobara)**

As you pointed out, at the beginning of chapter 2 we described the characteristic of this research scenario, that is, "the importance to shift to practical application research only after conducting sufficient investigations and improvements on the security aspects of cryptographic technology that is the basis of the proposed method in advance."

### 4 One-factor PAKE

**Comment (Toshihiro Matsui)**

In subchapter 3.1, you write that the research will be limited to two-factor authentication because password leakages cannot be prevented with one-factor authentication. Yet in the middle of subchapter 3.2, you write that sufficient security might be obtained by improving the one-factor PAKE. As these two statements contradict, clarification is requested. After that, you also write about the search method hiding the search word as well as the development of an international standardization. If they are off the main topic, please remove these descriptions to avoid confusion.

**Answer (SeongHan Shin, Kazukuni Kobara)**

In order to avoid misunderstanding that two-factor authentication is unnecessary, we added in paragraph 4 of subchapter 3.2 that: PAKE and anonymous password authentication have security only against eavesdropping and impersonation; in oblivious search method, the search word is protected only against attacks over the network; and they are not resilient against leakage from the server.

Also, these subchapters present examples indicating that the technological knowledge accumulated in the theoretical improvement research can be applied to various applications. So, we added this explanation to the end of paragraph 1 as well as paragraph 4 of subchapter 3.2.

### 5 Explanation of offline exhaustive search and parallel online exhaustive search

**Comment (Katsuhiko Sakaue, Information and Communication Infrastructure Division, AIST)**

I understood that your proposed method is a powerful one where neither the offline nor parallel online exhaustive searches can be applied. However, since the readers from other fields may know only the familiar example of remote user authentication method, I don't think that they can grasp what exactly are offline and parallel/serial online exhaustive searches only through the brief explanation given in the text. Because this is an important point that demonstrates superiority of the proposed method, I think you should add easy-to-understand explanations.

**Answer (Kazukuni Kobara)**

We added the explanations for offline and parallel/serial online exhaustive searches in subchapter 1.2.

### 6 Explanation of why it boils down to four problems

**Comment (Katsuhiko Sakaue)**

You give four problems of the current password authentication methods in subchapters 1.2~1.5, and at the beginning of chapter 2 you state that the goal of this research is to solve these problems fundamentally. However, the non-specialists cannot understand why it boils down to these four problems. Please add some clarifying explanations.

**Answer (Kazukuni Kobara)**

We added the statistical data on the ways of obtaining passwords in subchapter 1.1, and added explanations of how these ways are related to the four problems stated in subchapters 1.2~1.5.