3-11 Hysteresis Signature and Its Related Technologies to Maintain the Digital Evidence for Network Activities in Future Society

TOYOSHIMA Hisashi and MIYAZAKI Kunihiko

Security Requirements are varied with rapid growth of Internet and mobile network in digitization progress of information. The necessity for reexamination of the security technological strategy is increasing. For example, the systematic security countermeasures which can prove having dealt with information appropriately are required in addition to direct security countermeasure such as encryption and access control. The problem of digital evidence occurs as a view which takes the lead for that. NICT started a research project "research and development about next-generation evidence based technologies" in 2001, and Hitachi tackled this. This paper reports overview of results of the research project and related topics which contain hysteresis signature for long-tem documents and its verification technologies.

Keywords
Digital evidence, Digital signature, Hysteresis signature, Log chain crossing, Accountability

1 Introduction

Recently growing emphasis has been placed on the human aspects of IT security issues, as seen in an increasing focus on information management. Accordingly, demand has grown for the development of measures to respond to these problems.

However, compared to access control for specific confidential information, security measures against problems such as information leakage must cover a wider range of phenomena, particularly when an information system is used directly in business activities involving many people. Consequently, these broader measures incur vast costs and are never perfect.

Societal activities not restricted to information systems generally do not aim for comprehensive prevention; instead, after implementation of certain basic measures, they primarily rely on judicial and other after-the-fact systems as a safety net.

On the other hand, traditional security technology for information systems has mainly covered proactive measures against individual events such as unauthorized access.

Information distribution will continue to proliferate, with a corresponding increase in the value of information. Follow-up measures will be required in addition to the proactive measures in place if we are to construct a balanced security system.

So-called "digital evidence" technology can provide a basis for future follow-up measures. In particular, digital signature technology is among the most important techniques of post-analysis, as indicated by the current enactment of the Law Concerning Electronic Signatures and Certification Services.

The Law Concerning Electronic Signatures and Certification Services assumes a Public Key Infrastructure (PKI) and aims at establishing “presumption of authenticity of an electromagnetic record”. Thus, one of the main purposes of the law is the establishment of digital evidence.

However, the Public Key Infrastructure is only partially developed. While some systems use authentication to identify another party, few apply digital signatures to establish digital evidence, which is among the main purposes of the law, as stated above. Several reasons may be proposed; for example, some have noted that the value of digital evidence has yet to be confirmed, given the scarcity of legal precedents regarding electromagnetic recordings. Nevertheless, a proper technical base must be established before implementation of any societal system to address these issues.

In this context, one technical challenge arises when considering a method of securing the long-term effectiveness of digital signature technology.

For example, digital signature technology uses keys. Each key has an expiration date specified by the PKI, which is relatively short in terms of digital evidence. After the expiration date, the digital evidence cannot be verified, even for digital documents signed before the expiration date. Another problem is seen in that the key itself consists of digital data and thus can be more easily copied and distributed than non-digital signature methods such as seals. Accordingly, it may remain difficult to restrict the extent of damage, including damage to digital evidence of earlier digital documents, once the key has been leaked.

Given this background, this study has devoted efforts to engineering development aimed at resolving problems in digital signature technology and establishing digital evidence using digital signatures.

2 Hysteresis signature technique

2.1 Problems in long-term use of signatures

With the increase in Internet use, a wide range of documents is currently produced in digital format. Digital signature technology, designed to ensure authenticity and permit identification of digital documents, is thus becoming more and more important. Use of this technology will undoubtedly expand to guarantee the authenticity and maintain the evidential power of documents used over long periods.

For example, the Electronic Document Law was enacted in April 2005, which allows for the digitization of paper documents for storage. The authenticity of a digitized document relies on the digital signature and the corresponding time stamp. This type of archived document must be retained for a relatively long period (seven years for tax documents, for example). The authenticity of these documents may require verification even after long periods.

When documents such as claims, bills, or wills—which may be converted into cash or become effective after a certain period—are digitized, authenticity will require similar verification after long periods.

If conventional digital signature technology is used to maintain digital evidence for a long period, it should be noted that the technical environment is likely to change between the time the signature is generated and later verification. For example, discovery of the private key, though difficult at the time the signature is generated, may become possible later with drastic progress in cryptanalysis techniques and computers. Human error may also occur, including key leakage due to inadequate handling of the key by the authorized user. Cases such as these, in which the private key loses its secrecy, are referred to as “cryptosystem collapses”.

Once a cryptosystem collapse occurs and the attacker obtains the private key for the signature, the attacker can easily generate any number of authorized signatures (or signatures that appear authorized) later (upon verification of the signature). Consequently, a signature rightfully generated in the past cannot be distinguished from one forged later by the attacker, even if the signature is verified correctly. The digital evidence has been lost.

This paper presents an overview and discusses the security of the hysteresis signature technique[1]-[4], which makes it possible to guarantee digital evidence based on digital signatures even when a cryptosystem collapse takes place. The paper also presents evaluation results of an implementation of the hysteresis signature technique.

2.2 Related techniques

In addition to the hysteresis signature technique, digital signature techniques for long-term use include (a) the forward secure signature method[5], (b) the key insulated signature method[6][7], (c) use of an electronic notary service[4][8], (d) use of time stamps[4], (e) use of signature extension servers[8], (f) use of digital evidence through MAC (Message Authentication Code)[9], and (g) signature methods featuring execution hardware authentication tags[10].

These are roughly divided into the two approaches indicated below. The hysteresis signature technique is classified in the latter approach.

(1) The key is updated regularly (e.g., daily) to limit damage even if the key is leaked ... (a), (b)

(2) In addition to an ordinary signature verification procedure, other means of verification are prepared to distinguish an authorized signature from a forged signature, even if the key is leaked ... (c)-(g)

The former approach updates the key relatively frequently, and is thus considered highly effective against key leakage. However, it is relatively ineffective if the key is at risk of being discovered through progress in cryptanalysis techniques or computers. On the other hand, the latter approach is effective independent of the cause of the cryptosystem collapse. However, it should be noted that these techniques are based on a variety of assumptions, including those of the different third-party organizations required Reference[11] shows the results of classification of these techniques based on dependence on a third-party organization. In this respect the hysteresis signature technique is relatively independent.

2.3 Overview of the hysteresis signature technique

The hysteresis signature technique generates a signature while acquiring a log list of past signatures. In this way, a chain structure is constructed among the signatures, rendering it difficult to forge the signature in a cryptosystem collapse.

A hysteresis signature uses the hash value of the (n-1)-th signature datum when generating the n-th signature. (The initial value for the initial generation is IV.) Thus, the value of the resultant signature data at a certain point is influenced by all elements of the signature log list that have been included since inception of the signature system.

In an ordinary signature system, the message for which the signature is generated and the digital signature are transmitted to the recipient (i.e., the verifying party) together. With a hysteresis signature, the hash value of the previous signature must also be transmitted.

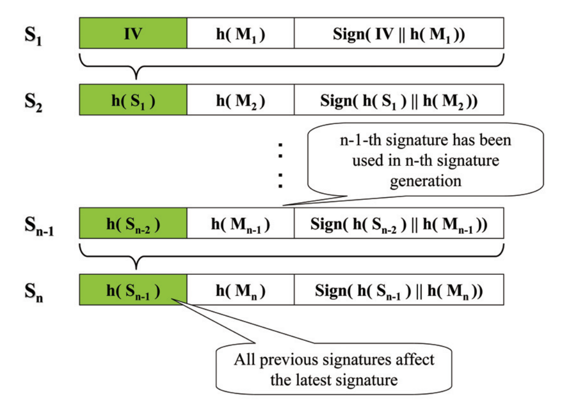
S_1
IV
h(M_1)
Sign(IV || h(M_1))
S_2
h(S_1)
h(M_2)
Sign(h(S_1) || h(M_2))
n-1-th signature has been used in n-th signature generation
S_{n-1}
h(S_{n-2})
h(M_{n-1})
Sign(h(S_{n-2}) || h(M_{n-1}))
S_n
h(S_{n-1})
h(M_n)
Sign(h(S_{n-1}) || h(M_n))
All previous signatures affect the latest signature

Fig. 1 Generation of hysteresis signature (Overview)

[Generation of hysteresis signature]

[Input (external)] Message M_n

[Input (internal)] Private key, signature record S_{n-1}

[Output (external)] Signature $H(S_{n-1})$, Sign $(H(s_{n-1}) || H(M_n))$

[Output (internal)] Signature record S_n

Step 1:

Calculate the hash value, $H(S_{n-1})$, for the previous signature record, S_{n-1}, stored as the log data in advance. Use as the chain data.

Step 2:

Link the chain data, $H(s_{n-1})$, calculated in Step 1 and the hash value $H(M_n)$ of the message, M_n, to which the signature is generated, to form $H(S_{n-1}) || H(M_n)$. Generate a signature for $H(S_{n-1}) || H(M_n)$ using the private key.

Step 3:

Transmit $H(S_{n-1})$ and $Sign(H(S_{n-1}) || H(M_n))$ as the signature with the message M_n.

Step 4:

Store $S_{n-1} || H(M_n) || Sign(H(S_{n-1}) || H(M_n))$ as the new signature record, S_n.

The recipient of the message bearing a hysteresis signature verifies the signature as follows (for ordinary transactions).

[Verification of hysteresis signature]

[Input] message M_n, signature $H(S_{n-1})$, $Sign(H(S_{n-1}) || H(M_n))$, public key

[Output] YES or NO

Step 1:

Link the hash value $H(M_n)$ of M_n and the $H(S_{n-1})$ received as the signature and calculate $H(S_{n-1}) || H(M_n)$.

Step 2:

Using $H(S_{n-1}) || H(M_n)$ and $Sign(H(S_{n-1}) || H(M_n))$ as the input, perform normal signature verification using the public key.

Step 3: Output YES or NO

When verifying a past hysteresis signature generated after the cryptosystem collapse, the above verification procedures are insufficient. This is because a person other than the authorized signer can generate signatures resulting in YES results in the above procedures, as the cryptosystem collapse has already occurred. In such a case, in addition to the above procedures, the message recipient or the arbitrator (assigned to judge the validity of the signature) verifies that the signer's stored signature records include the signature record S_n corresponding to the signature in question. Further, the recipient or the arbitrator verifies the validity of the signature record, S_n, as below. Here, S_m (referred to as the reliability point) is a signature record whose validity is guaranteed in some way, by establishing that it is the most recent signature or through reference to past newspaper publication, for example.

[Verification of signature log list]

[Input] Signature record, S_n, to be verified, public key, signature record $S_{n+1},,, S_m$

[Output] YES or NO

Step 1:

Input $H(S_{n-1}) || H(M_n)$ and $Sign(H(S_{n-1}) || H(M_n))$ contained in S_n, and perform normal signature verification based on a public key (single signature log list verification).

Step 2:

Verify that the hash value of S_n agrees with $H(S_n)$ contained in the signature record, S_{n+1}. (Verify consistency with the subsequent log list.)

Step 3:

Perform $n:=n+1$. Return to Step 2 if $n<m$.

Step 4:

Output NO if verification fails in any of Steps 1 to 3. Output YES if the signature passes verification.

Below we discuss basic considerations related to the security of a hysteresis signature as described above. To evaluate security in this case, we consider the possibility of future cryptosystem collapses and assume the following.

(Premise 1)

The cipher was not broken when the signature was generated (at the start of the transaction). Thus, the recipient of the message with the signature accepts the message at the time of transaction if the signature is verified via an ordinary method.

(Premise 2)

It is possible that the attacker will discover the signer's private key information and will forge the signature before the expiration of the signed message.

(Premise 3)

The onewayness of the hash function (more precisely, the second-preimage resistance; simply referred to as onewayness below) will not be broken over time.

With these premises, the following proposition concerning the above verification procedures holds.

Proposition 1:

Assume that S_n is verified through the above signature log list verification procedure using the signature record S_{n+1}. Then, if S_{n+1} is not forged, S_n is not forged. Here, "S_i is forged" means that S_i is verified according to the above signature log list verification procedures; here, the hash value, $H(M'_i)$, of the message contained in S_i differs from the hash value of the message, M_i, originally generated by the signer.

Proof:

Assume that S_{n+1} is not forged, and that S_n is forged. Let M'_n denote the message for which the signer originally generated the signature, and S'_n, the message's signature record. Then, as $S_n(=H(S_{n-1}) || H(M_n) || Sign(H(s_{n-1}) || H(M_n)))$ is forged, $H(M_n) \neq H(M'_n)$. Thus, $S_n \neq S'_n$. On the other hand, $H(S'_n)$ satisfies Step 2 of the signature log list verification procedures and thus must agree with $H(S_n)$ contained in the signature record, S_{n+1}, which is not forged (i.e., it corresponds to the (n+1)-th signature generated by the signer). This contradicts the onewayness of the hash function, H. Therefore, if S_{n+1} is not forged, S_n is not forged.

Corollary 2:

If S_m is not forged for any n (> m) and if the output from the signature log list verification procedures is YES for all i that satisfy $n \leq i < m$ when input with the signature record to be verified, S_i, the public key, and the signature log list S_{i+1}, then S_n is not forged.

Proof: Obvious. (Repeat applying Proposition 1.)

From Corollary 2, it is proved that the signatures that correspond to signature records in the past traceable range along the chain—beginning at the signature record corresponding to a signature undoubtedly generated by the signer—are all undoubtedly generated by the signer.

Thus, the signer can demonstrate that the signatures in the signature log list are all generated by the signer by storing the complete signature record without deletion and providing proof that the latest signature has undoubtedly been generated by the signer.

More specifically, we considered an example using a 1,024-bit RSA signature for the signature method and SHA-1 (160-bit output) for the cryptographic hash function as components of the hysteresis signature.

Table 1 shows the currently known security details (the computational complexity required for an attack) for these components.

Table 1 *Security details for components of hysteresis signature*

Component	Type of attack	Order of computational complexity required for attack
1,024-bit RSA signature	Calculates the private key from the public key	2^{80}
SHA-1 (160-bit output)	Finds two different input values that give the same output value [Attack against collision resistance of the hash function]	2^{80} *1
	Finds a single input value (different from the original value) based on the given output value [Attack against onewayness of the hash function]	2^{160}

*1 In February 2005, news reports indicated that the collision resistance of SHA-1 may be attacked with a computational complexity of approximately 2^{69}. The details have not been disclosed at the time of writing of this article. However, if this is true, the 2^{80} computational complexity with respect to collision resistance in subsequent discussions should be replaced with a cost of 2^{69}. Nevertheless, the security of the hysteresis signature is based on the onewayness of the hash function (the second-preimage resistance) as discussed in this article, so that vulnerability related to collisions will not affect the final security of the hysteresis signature. In other words, the genuineness of a hysteresis signature generated in the past using SHA-1 can be verified even after collision resistance is broken.

Thus, when the hysteresis signature is generated using a 1,024-bit RSA signature and the SHA-1 hash function, the above premises can be restated as follows if only the computational complexity is considered:

(Premise 1)

When the signature is generated (at the start of the transaction), the computational complexity on the order of 2^{80} or greater cannot be met by the attacker.

(Premise 2)

Before the expiration of the signed message, the computational complexity on the order of 2^{80} or greater can be met by the attacker.

(Premise 3)

Before the expiration of the signed message, the computational complexity on the order of 2^{160} or greater cannot be met by the attacker.

In other words, Proposition 1 holds as long as the computational complexity on the order of 2^{160} or greater cannot be met by the attacker before the expiration of signed message. While the 1,024-bit RSA signature currently in wide use can be forged with a calculation cost on the order of 2^{80}, the computational complexity required to forge a hysteresis signature is on the order of 2^{160}, a significantly greater level of security. This increased security is due to the onewayness of the hash function and does not depend on the secrecy of the information, as is the case in ordinary digital signature techniques.

To summarize the basic considerations concerning security discussed above, compared to conventional digital signatures the security of the hysteresis signature:

(1) entails greater computational complexity (for example, approximately 2^{80} times greater for the 1,024-bit RSA signature and the SHA-1 hash function); and

(2) offers security based on factors other than the secrecy of specific secret information, enabling response to future key leakage.

The validity of the premise that the onewayness of the hash function will not be broken over time is arguable. Some may say that it is unreasonable to assume security of the hash function when the digital signature is assumed to be broken. However, this study assumes that the onewayness of the hash function will not be broken when the digital signature is broken, based on the following:

[Reason 1]

The computational complexity required to attack the hash function is greater than that required to attack the digital signature. As shown in Table 1, the computational complexity required to break the onewayness of the hash function is in the order of 2^{160}, which is much greater than the computational complexity considered necessary to discover the private key for the signature based on the public key (on the order of 2^{80}) with the best attack method currently known. The threat to a hysteresis signature is that of the attacker forging the signature and the signature log list in such a way that these are consistent with the signature log list previously generated by the signer. It should be noted that it is not sufficient to break the collision resistance of the hash function; it is also necessary to break the onewayness of the hash function for this forgery to be successful.

[Reason 2]

In digital signatures that do not depend on the secrecy of specific information, once the private key for the signature is leaked, an unlimited number of authorized signatures (or signatures that appear authorized) can easily be generated. However, the hash function does not feature such secrecy. Thus, the assertion that onewayness can be broken given certain known information does not apply. Even if the attacker could break onewayness once, (i.e., if the attacker could find an input value that yields the given output value once) the attacker must exert the same effort as in the first round to break onewayness again. (In other words, in order to obtain the input value for another given output value, the same computational complexity is required as in the first round).

[Reason 3]

Quantum computers, based on an architecture completely different from that of current computers, are currently under study.

Although practical application of these computers remains in the future, it is already known that present public key cryptography (including digital signatures) will be rapidly decodable with such computers. On the other hand, there are currently no known effective attack methods against the hash function that take advantage of the features of quantum computers. Thus, the hash function is considered also to be highly resistant against attacks using new quantum computer technology.

Based on the reasons discussed above, if current digital signature technology is compromised for some reason in the future, it is nevertheless assumed that a significantly greater amount of time will be required to break the onewayness of the hash function. Thus, this study assumes the validity of the premise that the onewayness of the hash function will not be broken over time.

2.4 Evaluation of implementation

This section discusses the evaluation results for an implemented prototype hysteresis signature system.

The prototype system developed was a mail client with the hysteresis signature function installed as a plug-in. A 160-bit ECDSA signature algorithm with the SHA-1 hash function was used as the basic algorithm in constructing the hysteresis signature.

The program was executed on a machine with an Intel ®Pentium® III 650 MHz processor and the execution time was measured. The processing time required for the signature generation function was approximately 5.35 ms. Compared to the 5.17 ms of processing time in conventional public key signature generation, this result corresponds to an increase of approximately 3.5%.

The time required to verify a signature was approximately 9.54 ms. This represents an increase of less than 1% over the 9.46-ms required processing time with conventional signature verification. However, after the cryptosystem collapse, signature log list verification is also required. The time required for this process is approximately 1.7 s to track 10,000 histories. This is considered a practical processing time.

The above evaluation with an actual model has confirmed that the hysteresis signature technique offers improved security with little increase in processing time.

3 Activities for ensuring digital evidence in a network environment

3.1 Problems in a network environment

As discussed in the previous section, hysteresis signatures are effective as a means to ensure digital evidence for each user. In the future, it will also be important to determine how digital evidence will be ensured over entire networks if we are to ensure the smooth operation of the activities that rely on these networks.

In hysteresis signature and other techniques for long-term use, third-party organizations play an important role. However, given the aim of ensuring digital evidence over entire networks, the following problems are posed in any approach relying simply on a central organization.

(1) Both today and in the future, all data related to digital evidence must be sent to the central organization if the data is subject to its authority. Thus, the load and responsibilities of the central organization will be extremely large.

(2) If the credibility of the central organization is compromised, the societal damage will be immense.

(3) Users may feel uncertain about privacy protection under such a system.

This paper thus discusses a technique to secure digital evidence dispersed between the central organization and general users as well as among general users, using a chain structure for the signature records constructed using the hysteresis signature technique.

3.2 Overview of signature log chain crossing

The hysteresis signature technique constructs a chain structure in the signature log list for each user. The signature log chain crossing technique expands this chain-type relationship to other users.

Let us consider, for example, applying the hysteresis signature technique to a common transaction between users A and B, in which user B signs an agreement that user A has already signed. As the signature of user A contains information concerning other signatures that user A has generated in the past, when user B adds his or her signature to the data containing the user A signature, the signature log list of user A is added to the signature log list of user B. Further, after users A and B have signed the agreement, user A can sign this agreement again to confirm receipt and then store it. The signature log list of user B is then added to the signature log list of user A.

In this way, through the repeated exchange of signatures in normal transactions, consistency with the signature log lists of other users must be maintained in any effort to tamper with the signature log list of a given user. This is the principle of signature log chain crossing.

As shown in Fig.2, repeated crossing between users as such generates relationships among the signature log lists of various users, and is expected to increase digital evidence throughout entire networks.

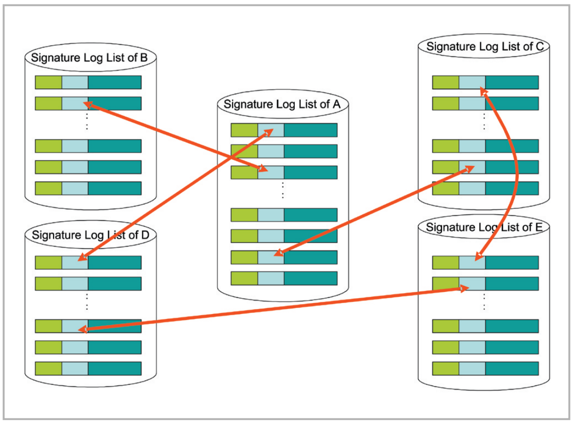

Fig.2 Signature log chain crossing

3.3 Contents of development

This section discusses the results of implementing the signature log chain crossing technique discussed in the previous section.

Although in the previous section we stated that the repeated exchange of signatures between users constitutes log chain crossing, in practice this exchange is insufficient, as it is not easy to determine in a search whose and which signature record is related to another, rendering verification difficult.

Thus, we decided to manage this information as a user search file. As any information regarding a given user's relationship with another entails issues of privacy, this information is to be managed independently from the signature log list.

In terms of security, the more frequent the signature log chain crossing, the better. However, general users are not always able to exchange signatures repeatedly with other users. In such a case, the user may deposit the signature with a central organization. However, simple concentration in a central organization raises the problems already discussed.

Thus, as shown in Fig.3, the developed prototype system established a hierarchical structure within the central organization, consisting of two layers: a web disclosure organization, which responds to a request instantaneously, and a newspaper disclosure organization, which secures long-term digital evidence. Separating these two functions into layers levels the load distribution and also improves security.

Specifically, the system functions as follows. First, the user regularly deposits the latest signature log list to the web disclosure organization. The web disclosure organization adds its own signature (hysteresis signature) and opens the log list to the public on a website to guarantee that the signature exists for anyone to verify. In other words, the web disclosure organization functions as the direct trust anchor supporting the digital evidence of each user.

On the other hand, the web disclosure organization regularly sends its own current signature log list to the newspaper disclosure organization, and the latter publicizes the log list in newspapers and other media.

Information placed in a newspaper is mass-printed and stored in numerous libraries, so that it is much more difficult to tamper with this data after the fact than it is to tamper with digital data.

In this way, the newspaper disclosure organization functions as the direct trust anchor to support the digital evidence of the web disclosure organization. Indirectly, it also serves as a trust anchor supporting the digital evidence of general users.

It is not practical for a general user to rely directly on the newspaper disclosure organization, in light of both data amounts and cost. However, implementation with the hierarchical structure described above is effectively equivalent to such direct use.

This hierarchical structure can be further extended to involve more layers. In the future, such a system is expected to serve as a needed safety net for digital evidence throughout a networked society.

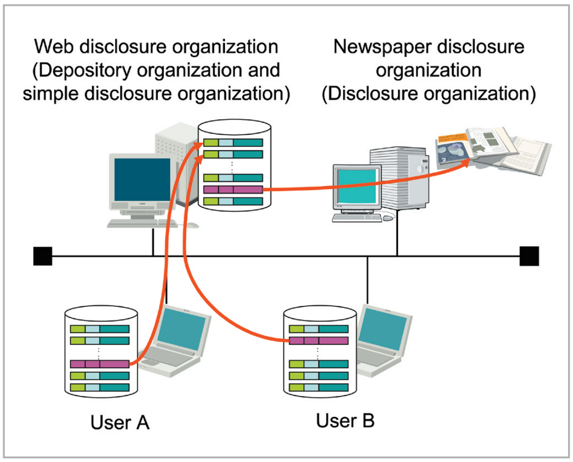
Web disclosure organization
(Depository organization and
simple disclosure organization)
Newspaper disclosure
organization
(Disclosure organization)
User A
User B

Fig.3 Hierarchical structure of the central organization

3.4 Future problems

As discussed above, the dispersive approach with signature log chain crossing can secure digital evidence throughout entire networks.

In addition to the construction of a more extensive safety net as discussed above, future problems include developing a means to provide general users with appropriate verification of signatures based on secured digital evidence.

We have also verified signatures using the prototype system developed to date. However, this verification requires collection of data secured dispersively, entailing a load too high for general users. Further, although this technique can sometimes maintain reliability even when the reliability of the third-party organization is partially lost, it is not easy to judge the extent of remaining reliability.

One solution is to provide verification agency services. This approach is also considered effective when using signature techniques other than the hysteresis signature method. We hope that these services will soon be provided as part of the societal infrastructure.

4 Summary and future development

As stated at the beginning of this article, security technology must evolve in step with advanced security needs. The growing use of the term “forensics” indicates the extent to which security technology is beginning to reflect broader societal concepts, against the backdrop of continued growth in network use.

The approach to digital evidence discussed in this article is important even before we consider the implications of terms such as “forensics” and “accountability”.

Implementing response models based on these broader societal considerations will allow for an effective response to advanced security demands, including the pressing need to protect against information leakage.

The above approach to security will also develop with growing attention to corporate accountability in relation to digital activities. Nevertheless, the ultimate aims of the measures discussed here will not be achieved within a closed system or corporation, but instead will require a wide range of societal mechanisms. Multiple layers of protections must be established—among industry trade groups, for example, or within regional economic areas. Finally, establishment of a broad safety net will be required to form the backbone of these layers, such as a national authentication network.

Today, we are at a stage in which legality is beginning to be discussed in terms of individual digital activities. In this respect we must wait as legal precedents become established.

Meanwhile, analytical applications based on log analysis are becoming more popular. Appropriate security criteria must be established for these applications as well.

It can be argued that it ought to be a national strategy to review the use of digital signatures as the foundation of digital evidence and to develop and improve the field. In line with such strategy, it goes without saying that digital evidence should also feature sufficient transparency to allow users to verify digital evidence at any time as necessary.

Given the anticipated developments discussed above, the usefulness and desirability of implementing the network-based dispersive approach is clear. We regard that the current technical development along these lines—further research into the hysteresis signature technique, for example, can provide a certain level of technical measures to respond to new security demands.

In the future, we will demonstrate the necessity of a digital-evidence-based approach using the techniques developed in this study. We will also need to pursue further research and development of the hysteresis signature—for example, as it may be applied within authentication networks.

Acknowledgments

We would like to express our sincere gratitude to Prof. Mitsuru Iwamura of Waseda University, Prof. Tsutomu Matsumoto of Yokohama National University, Prof. Ryoichi Sasaki of Tokyo Denki University, Prof. Hiroshi Yoshiura of the University of Electro-Communications, and Prof. Takato Natsui of Meiji University, all of whom provided us a great deal of valuable advice and guidance.

References

1 Tsutomu Matsumoto, Mitsuru Iwamura, Ryoichi Sasaki, and Takeshi Matsuki, “Alibi Establishment for Electronic Signatures: How to prove that you did not make the electronic signature in question even when the base cryptosystem was collapsed Part 1. Concepts and Basic Schemes”, IPSJ SIG Technical Reports Vol.2000 No.030, 1999-CSEC-008, (2000). (in Japanese)

2 Seiichi Susaki, Kunihiko Miyazaki, Kazuo Takaragi, and Tsutomu Matsumoto, “Alibi Establishment for Electronic Signatures: How to prove that you did not make the electronic signature in question even when the base cryptosystem was collapsed Part 2. Concrete Schemes and Evaluation”, IPSJ SIG Technical Reports Vol.2000 No.030, 1999-CSEC-008, (2000). (in Japanese)

3 Mitsuru Iwamura, Kunihiko Miyazaki, Tsutomu Matsumoto, Ryoichi Sasaki, and Takeshi Matsuki, “Alibi establishment and passage of time proof on digital signature -- Hysteresis signature and digital ancient documents --”, Computer Science Magazine Bit, Vol.32, No.11, pp. 42-48, Kyoritsu-shuppan, (2000). (in Japanese)

4 Seiichi Susaki and Tsutomu Matsumoto, “Alibi Establishment for Electronic Signatures”, IPSJ Journal, Vol.43, No.8, pp. 2381-2393 (2002). (in Japanese)

5 Mihir Bellare and Sara K.Miner, “A Forward-Secure Digital Signature Scheme”, In Proc. of Crypto, pp.431-448, 1999.

6 Yevgeniy Dodis, Jonathan Katz, Shouhuai Xi, and Moti Yung, “Key-Insulated Public Key Cryptosystems”, EUROCRYPY 2002, Lecture Notes in Computer Science, Vol.2332, pp.65-82, Springer-Verlag, 2002.

7 Yevgeniy Dodis, Jonathan Katz, Shouhuai Xi, and Moti Yung, “Strong Key-Insulated Signature Schemes”, International Workshop on Practice and Theory in Public key Cryptography (PKC2003), Lecture Notes in Computer Science, Vol.2567, pp.130-144, Springer-Verlag, 2003.

8 Electronic Commerce Promotion Council of Japan Certification/Notary WG, “Interim report on long-term storage of digital documents”, H12-Certification/NotaryWG-3 (2001). (in Japanese)

9 Akira Komori, Kanta Matsuura, and Osamu Sudo, “Analysis of Digital Evidence for Financial Dispute Settlement”, In proceddings of SCIS2002, IEICE, pp.627-632 (2002). (in Japanese)

10 Masashi Une and Tsutomu Matsumoto, “A Digital Signature Scheme that can erify Signing Hardware”, IPSJ SIG Technical Reports, 2002-CSEC-18, pp.245-252 (2002). (in Japanese)

11 Kunihiko Miyazaki, Hiroshi Yoshiura, Mitsuru Iwamura, and Tsutomu Matsumoto, Ryoichi Sasaki, “Evaluation Method for Digital Signature Schemes for Long-term Documents Based on Dependency to Third Parties”, IPSJ Journal, Vol.44, No.08, (2003). (in Japanese)

TOYOSHIMA Hisashi

Senior Manager, Public Business Planning Operation, Government&Public Corporation Information Systems Sales Management Division, Hitachi Ltd.

Public Information System, Information Security

MIYAZAKI Kunihiko

Researcher, 7th Research Department, Systems Development Laboratory, Hitachi Ltd.

Cryptography, Information Security