Toward Research-Promotion Infrastructure for Multi-Modal Imaging

Matsuura K, Imai H

Institute of Industrial Science, the University of Tokyo, Tokyo, Japan

Introduction

Biomagnetic imaging usually works well when combined with other measurements. Currently common way is MRI superposition; estimated biomagnetic signal sources are superposed on magnetic-resonance images which provide anatomical information of the subject. Future directions, however, will very probably include multi-modal imaging [1]–[3]; wide variety of different measurements or estimated results will get together onto the same platform aiming at revealing more and more complicated neural activities as a whole. Looking ahead at such a situation, we consider how to provide a "research-promotion" infrastructure in the following two senses. First, we wish to encourage researchers with different scientific or technological backgrounds to cooperate together as openly as possible. Second, we wish to protect privacy of subjects.

Basically, the infrastructure should

- ensure data integrity hopefully even over an open and insecure network,
- control access structure and data linkage, and
- be efficient enough to be applied to medical data of a large size.

Conforming to these points, our framework is both at the level or layer of cryptographic primitives and at protocol design and integration. In this paper, we are devoted to the first issue and propose an extended use of "signcryption" which provides both the functions of public-key encryption and digital signature [4].

In writing a letter with ensured confidentiality and no forgery, for centuries it has been a common practice for the originator of the letter to sign his/her name on it and then seal it in an envelope. This two-step "signature-then-seal" process is not inconvenient to most originators since the time and cost involved is usually regarded as being marginal. Likewise, electronic message-delivery services often use digital signature and encryption technologies consecutively. Although the sum of the cost for signature and the cost for encryption are computationally expensive, this two-step "signature-then-encryption" process has been a standard method for a secure and authenticated delivery. Originating from questioning whether it is absolutely necessary for one to spend the sum of the costs to achieve both confidentiality and authenticity, the author of [4] proposes a new cryptographic primitive called signcryption.

Intuitively, a digital signcryption is a cryptographic method that fulfills both the functions of secure encryption and digital signature, but with a cost smaller than that required by signature-then-encryption. For details, the readers can consult [4]. We here note that three important properties can be efficiently adopted: confidentiality of contents, unforgeability, and non-repudiation. In the following, we show how to extend this primitive for digitized multi-modal data $(M_1, M_2, \cdots, M_n; m_1, m_2, \cdots, m_{n'})$ where $M_1, M_2, \cdots, M_n$ are materials which require both secrecy and integrity while $m_1, m_2, \cdots, m_{n'}$ need only integrity.

Methods

We use system parameters and functions as follows:

p:	a large prime (1024bit, for example)
q:	a large prime factor of $p-1$
g:	an integer with order q modulo p
$hash()$:	a one-way hash function whose output has at least 128bit
$KH()$:	a keyed one-way hash function
(E, D):	encryption and decryption algorithms of a private-key cipher
$\|$:	concatenation
x_a:	sender's private key chosen from $[1, 2, \cdots, q-1]$
y_a:	sender's public key such that $y_a = g^{x_a} \bmod p$
x_b:	recipient's private key chosen from $[1, 2, \cdots, q-1]$
y_b:	recipient's public key such that $y_b = g^{x_b} \bmod p$.

At the first step, the sender (say, Alice) chooses an integer u randomly from $[1, 2, \cdots, q-1]$. She then computes

$$
\begin{aligned}
(k_1, k_2) &= hash\,(y_b^u \bmod p) && (1)\\
r &= KH_{k_2}\,(M_1 \| M_2 \| \cdots \| M_n \| m_1 \| m_2 \| \cdots \| m_{n'}) && (2)\\
s &= (u + r \cdot x_a) \bmod q && (3)\\
c &= E_{k_1}\,(M_1 \| M_2 \| \cdots \| M_n) && (4)
\end{aligned}
$$

and sends r, s, c, m_1, m_2, $\cdots$, m_n to the recipient (say, Bob). On receiving this message set, Bob first recovers (k_1, k_2) as

$$(k_1, k_2) = hash\left(\left(g^s \cdot y_a^{-r}\right)^{x_b} \bmod p\right). \tag{5}$$

He then decrypts the secret materials by

$$(M_1 \| M_2 \| \cdots \| M_n) = D_{k_1}(c). \tag{6}$$

Finally, the data integrity and the linkage between the encrypted and the plain materials are verified by the following criterion:

$$
\begin{array}{ll}
\text{Valid} & \text{if } r = KH_{k_2}\,(M_1 \| M_2 \| \cdots \| M_n \| m_1 \| m_2 \| \cdots \| m_{n'})\\
\text{Invalid} & \text{otherwise.}
\end{array}
$$

If an attacker modifies some of the plain materials, the keyed hash value is changed and no longer equivalent to r. The attacker cannot adjust r to the message set with modified materials since he has no knowledge of the recipients secret key x_b and thus can get neither k_1 nor k_2. The concept of the proposed scheme is outlined in Fig. 1 We call this scheme "multi-modal signcryption".

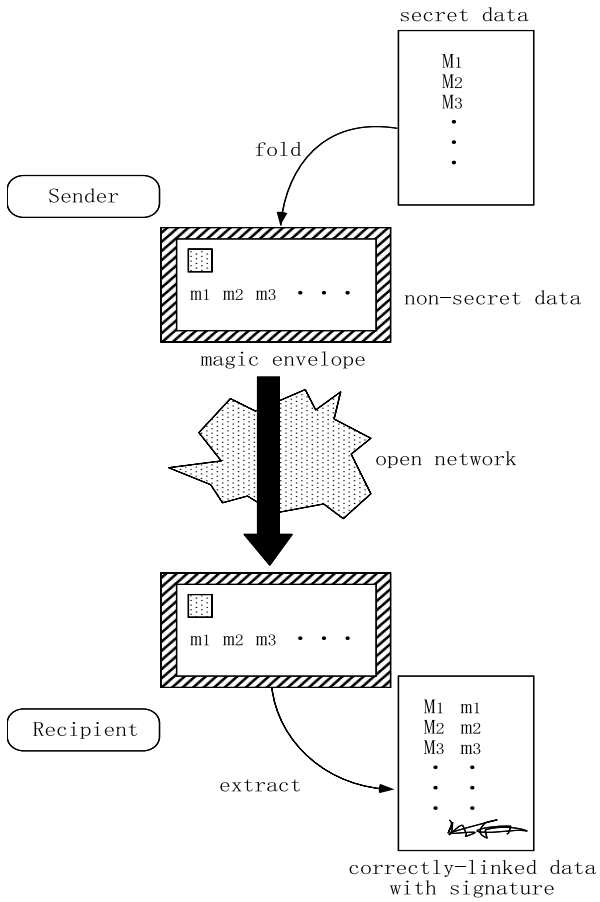

Figure 1: Concept of multi-modal signcryption.

We evaluate the performance of multi-modal signcryption by comparing computational cost and communication overhead with those of conventional signature-then-encryption approach based on RSA scheme, where the sender Alice

1. computes the authenticator S by using her secret key with the input of $(M_1 \| M_2 \| \cdots \| M_n \| \ m_1 \| \ m_2 \| \cdots \| m_{n'})$,
2. encrypts $(M_1 \| M_2 \| \cdots \| M_n \| S)$ with the public key of the recipient, and
3. sends the encrypted result together with $(m_1, m_2, \cdots, m_n)$

and the recipient Bob

1. decrypts the encrypted materials with his secret key, and
2. verifies the sender's authenticator S is valid by using her public key.

The RSA encryption/decryption considered is a version designed for inputs of arbitrary length.

Specific numeric comparison requires the knowledge of up-to-date implementation technique. Regarding conventional schemes, a high-quality survey of cryptographic software implementation in [5] is helpful. We follow [6] regarding the techniques and the assumptions for estimating the performance of multi-modal signcryption.

Results

The performance analysis was carried out for different levels of security including the currently standard one. The result is summarized in Table 1 where the size of the RSA composite determines the level of security. The larger the composite gets, the more secure the system is. The security level currently recommended by research community of information security is about 1024 bits. At this level, multi-modal signcryption saves computational cost and communication overhead by 32.3[%] and by 88.3[%], respectively.

Table 1 also shows that these advantages will get more significant in the future; larger sizes of RSA composite bring larger cost reduction both in computation and in communication. Although not included in this paper, a comparison with ElGamal scheme [7] gives similar characteristics.

Discussion

This paper shows how to adapt a relatively new cryptographic primitive called signcryption to multi-modal imaging data. The proposed scheme, called multi-modal signcryption, maintains three important security properties of the original signcryption: confidentiality of contents, unforgeability, and non-repudiation. In addition, we can verify the linkage between different imaging data, especially between encrypted materials and non-encrypted materials.

Table 1: Advantage of multi-modal signcryption in comparison with signature-then-encryption based on RSA. The larger the size of RSA composite, the higher the security level. Currently recommended level is 1024 bits or so.

size of RSA composite in bits	Reduction in computational cost [%]	Reduction in communication overhead [%]
768	14.2	84.9
1024	32.3	88.3
1280	43.1	90.0
1536	50.3	91.4
2048	59.4	93.0
2560	64.8	94.0
3072	68.4	94.5
4096	72.9	95.0
5120	75.6	96.0
10240	86.5	98.0

A cost evaluation tells that the computational cost is reduced by at least 32.3[%]. This reduction gets more significant if we consider future situation with higher level of security. Likewise, the communication overhead is reduced by at least 88.3[%]. This reduction also becomes more significant in future situation. Since biomedical imaging data are in general of a large size, the efficiency of multi-modal signcryption will contribute a lot to a practical system.

We can find an approach to use a global network for medical imaging [8] and expect that networked research-promotion infrastructure would enhance the progress of brain science with higher speed. One feasible scenario is a commitment of the inverse analysis.

Non-invasive measurements play an important role in biomedical research. A very common research flow is composed of setup, data acquisition, inverse analysis, interpretation of the inverse solutions, and update of the setup and the inverse-analysis algorithm. In an advanced research such that physiologists and signal-processing engineers work separately, the research tends to make a progress very slowly. Two main reasons for this slow progress are (i) slow experiments and (ii) slow data-circulation. That is, (i) we have to be careful in dealing with the subjects (very probably human beings) and (ii) it takes quite a long time to make contracts between the researchers. It is difficult to solve the first problem. By contrast, the second problem could be solved by using information-security technologies to build research-promotion infrastructure which allows the commitment of inverse analysis over an open and global network.

In search of faster flows in biomedical researches based on non-invasive measurements, our framework should cover not only signal processing but also information security technologies.

References

[1] Garnero L, Baillet S, Lachaux J-P, Renault B: Data operating in a PET/EEG/MRI fusion experience. Human Brain Mapping Suppl. 1: 84, 1995

[2] Hochman DW, Whitaker HA, Haglund M, Ojemann GA: Is there concordance between functional brain mapping techniques? Human Brain Mapping Suppl. 1: 85, 1995

[3] Takanashi Y, Yoshikawa K, Iwamoto K, et al: Comparison of functional localization in human visual cortices using MEG and fMRI: a preliminary report, Hashimoto I, Okada YC, Ogawa S (eds): Visualization of Information Processing in the Human Brain: Recent Advances in MEG and Functional MRI (EEG Suppl. 47). Amsterdam: Elsevier, 1996, pp. 59–63

[4] Zheng Y: Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption), Advances in Cryptology — Crypto'97, Lecture Notes in Computer Science 1294, Berlin: Springer-Verlag, 1997, pp. 165–179

[5] Menezes A, van Oorschot P, Vanstone S: Handbook of Applied Cryptography. Boca Raton, Florida: CRC Press, Inc., 1996

[6] Matsuura K, Zheng Y, Imai H: Compact and flexible resolution of CBT multicast key-distribution, Proc. of Worldwide Computing and Its Applications '98 (WWCA'98), Lecture Notes in Computer Science 1368, Berlin: Springer-Verlag, 1998, pp. 190–205

[7] ElGamal T: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Information Theory: IT-31, 4, 469–472, 1985

[8] Wong STC, Huang HK: Networked multimedia for medical imaging. IEEE Multimedia: 4, 2, 24–35, 1997

Acknowledgments

The authors would like to thank Prof. Zheng at Monash University for his motivating us to extend signcryption for next-generation applications.