57

A new copyright protection scheme using the multiple RSA cryptosystems in personal cards for network shopping

Shinji Ishii
NTT Human Interface Laboratories
1-2356 Take, Yokosuka-shi, Kanagawa-ken, 238-03 JAPAN
telephone 81 468 59 4579
facsimile 81 468 59 8212
e-mail address ishii@mistral.hil.ntt.jp

Abstract

A major problem in circulating copyrighted digital content through a computer network is how to protect against the illegal copying of the content. As a means of addressing this problem, we propose a new copyright protection scheme which features the use of a personal card (e.g. PCMCIA Card, PC Card) and the dividing between various parties of a customer's card private key for a RSA public key cryptosystems (Rivest, 1978). Our proposed scheme has many advantages in key management.

The scheme promises to facilitate rapid growth in the market of copyrighted digital content by protecting the rights and assuaging the anxieties of both *content* owners and customers.

Keywords

security, copyright protection, RSA cryptosystems, network shopping, Internet, Multiple key, key management

1 INTRODUCTION

Recently, the Internet has expanded dramatically and shifted from an academic network to a commercial network. The Internet crime has changed too as a result. Crime aimed at obtaining profit illegally is a particular problem in a commercial network. In such crimes, the scale and damage caused are larger than before. Commercial business on the Internet will not mature as a real market if there are no means to prevent the criminal pursuit of illegal profit.

The motivation behind this work was the need for a mechanism to protect the rights of both owner and customer in the commercial circulation of copyrighted *digital content* on a

N. Terashima et al. (eds.), *Advanced IT Tools*

computer network. The need for such a mechanism has grown out of the widespread increase in circulation of copyrighted information over computer networks in recent years.

There are two kinds of methods for guaranteeing payment for copyrighted digital contents:

- prohibiting copying even by the purchase customer.
- free copying and distribution of copyrighted digital contents, but on systems where the customer is charged when the content is used (*superdistribution*) (Mori, 1990).

These two kinds have both merits and drawbacks. With current technology, the latter is better but a lot of technical problems are still to be overcome. Our proposed scheme is of the former kind.

2 ONLINE COPYRIGHT PROTECTION SYSTEM

2. 1 Our previous work

Digital content (e.g. computer programs, digital audio, digital video) can be easily copied. Copyright holders' rights should be protected by devising the scheme to not allow illegal copying, to stimulate the market for trading in copyrighted content.

Figure 1 is a copyright protection system (Yamanaka, 1996) using a Type II PCMCIA Card. The card has an RSA Processor (Ishii, 1994), which can perform RSA decryption in 0.1 seconds using 1,024-bit key. The system can protect against eavesdropping, customer illegal copying, etc., and can be done by letting the provider encrypt and send content to customers, and having customers decrypt it in a tamper-resistant unit.

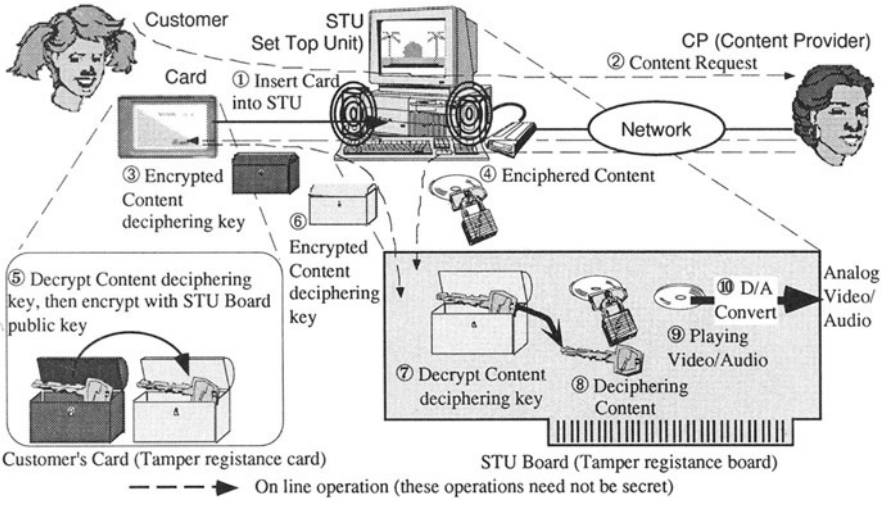

Figure 1 A copyright protection system

2. 2 Key generation problem

However, we notice a problem when the above system is strictly analyzed, i.e. the system can

not handle digital signatures *perfectly*.

A satisfactory system must include functions not only for **(1) customer (user) authentication** and **delivery confirmation**, but also for **(2) protection against illegal digital copying**.

(1) is possible in a public key encryption system using a pair of self-generated keys. However **(1)** and **(2)** can not be achieved simultaneously, because of the following *inconsistency*:

- *No one except the key owner should* ***have*** *the private key - a fact known to all other parties as well* **(1)**.
- *Even key owners themselves should* ***not know*** *what their private keys are* **(2)**.

These conditions are summarized in Table 1.

Table 1 Conditions for a private key in a personal card

Operation	*Customer*	*Other party*
Digital signature	Only uses key	Does not know key
Decryption of purchased digital content	Does not know key	Does not know key

These conditions concern key generation in the personal card. If the customer generates the key for the personal card, the digital signature is effective, but because this key can be known, copyright protection cannot be achieved in content encryption.

To overcome the above inconsistency, we propose a new copyright protection scheme using RSA, the defacto standard of public key encryption algorithms. The scheme involves the use of a personal card containing multiple secret keys and makes it possible to satisfy requirements **(1)** and **(2)** simultaneously.

The proposed scheme has two principal features:

- All parties are aware that nobody has a customer's private key except the personal card owner.
- The owner of a personal card (i.e. customer) does not know the value of his/her own private key because the key is locked in the device.

The key itself is generated in the personal card and it cannot be read from the device in any way.

As a result, a customer buying copyrighted digital information can not illegally copy it. Moreover, the proposed scheme has several other advantages in key management applications and it can be easily adopted in the present RSA cryptosystems.

3 PROPOSED SCHEME

3. 1 Security policy

The proposed scheme must be adopted in a practical system. So, aspects of the security policy are as follows:

- Mutual trust is not necessary between parties.
- Copying digital content should be as difficult as breaking the current public key encryption or secret key encryption algorithms.
- The protocol for our proposed scheme must be legally valid, because if a lawsuit ensues, it may eventually be judged in court.

- Customer should not have to remember a lot of secret keys or parameters.
- Content providers should hold all relevant copyright rights.
- A customer should need only one personal card.

3. 2 Multiple RSA cryptosystems

We found that requirements **(1)** and **(2)** (see section 2.2) could be satisfied by secretly dividing the customer's private key embedded in a personal card among a number of interested parties. A multiple public key cipher for cipher communication between more than three parties, each with a similar role (Boyd, 1988), is a suitable method for dividing the key in our proposed scheme. The main reason is that the cryptographic strength of a multiple cipher is equivalent to that of RSA.

However, our goal is quite different from that described in (Boyd, 1988). Therefore, our key generation procedure and key management method are also quite different.

3.3 Proposed scheme system configuration

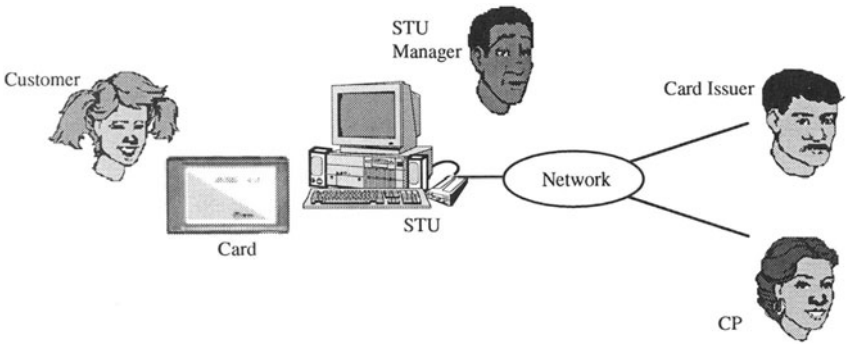

Figure 2 System configuration

The proposed scheme has the following advantages:
- Even a customer who has bought copyrighted digital content can not copy it.
- If customers lose their access privileges (e.g. by forgetting their passwords) to their own personal cards, they can revive them by applying through a defined reissue procedure.
- If any party forgets their secret parameter, it can be changed by applying through the above reissue procedure.
- A private key can be changed.
- The number of parties is changeable after key generation.
- Unless all secret keys are stolen, no private keys for public key encryption in a personal card will be exposed.
- Even if any number of parties is involved, none of them have any advantage over the others.

There must be four key generating parties for a personal card: "Customer", "STU" (Set Top Unit), "CP" (Content Provider) and "Card Issuer" (customer personal card issuer), who have a financial relationship.

The shape of the personal card is not a critical problem, but the device must have:
- an interface with the STU (described later)

• enough capacity to have a different key written into it for each party, as well as assurance that only public keys can be read out
• an RSA function, and
• a tamper resistant shell

With today's technology, the most suitable card for a personal portable device is the PC Card for PCs. In the following, it is assumed the device is a PC Card, referred to as the "Card" for brevity.

3.4 Multiple RSA key generation

The STU is the end-user's terminal equipment unit, such as a multimedia PC, which receives digital content from the CP and has an interface with the Card. The STU can be set up in a Customer's home, public place, etc.; there are no restrictions on its location. Thus, it is assumed that the STU ownership is not unique. In addition, the STU is tamper resistant and has functions for deciphering encrypted digital content and for the digital decoding-playing of voice and video (see Figure 1). This party can be made, for example, by taking a single PC expansion board and sealing its surface completely by coating it with a plastic mold.

The CP is the party that provides the copyrighted digital content to the STU over the network.

Both the STU and the CP have a function for secret key encryption [e. g. DES (NBS, 1977), FEAL (Miyaguchi, 1990), IDEA (Lai, 1991)] and a function for public key encryption RSA.

The customer's Card key is generated as follows (and see Figure 3)

• Card Issuer

The Card Issuer inputs a seed for the multiple key r_1 into the Card. Using r_1, the Card generates a public Card ID and secret random number d_1 (part of a multiple key) and calculates a public exponentiation e and a public modulus n for RSA, where e and n are a public key of RSA. All e, n and Card ID are installed into a readable register in the Card. d_1 is stored in a register in the Card, too, but this register becomes unreadable after it is read once. The Card Issuer then secretly makes a card issuing list. The list contains the Card ID and d_1.

Next, the Card is sent to the CP.

• CP

The CP inputs a seed for the multiple key r_2 into the Card. Using r_2, the Card generates a random number d_2 which is stored in another register in the Card. The register becomes unreadable after it is read once. The CP reads out the Card ID, e and d_2 from the Card register. Then, the CP secretly makes a card issuing list containing the Card ID and d_2.

Then, the Card is sent to the STU Manager.

• STU Manager

The STU Manager inputs a seed for the multiple key r_3 into the Card. Using r_3, the Card generates a secret random number d_3 (instead of d_2) but otherwise operates in the same way as the CP. Finally, the Card is sent to the Customer.

• Customer

The customer inputs a seed for the multiple key r_0 into the Card. The Card then secretly calculates d_0 and generates RSA key private key d using. d_1, d_2, d_3 and r_0, where d is a private key of RSA. The n, e, d_1 and the Card ID can be read from the Card. Next, the customer changes the permission to read d_1 Card from "readable" to "not readable". Of course d cannot be read from the Card. Finally, the Customer makes his/her own private card parameter list that

contains the Card ID and d_1.

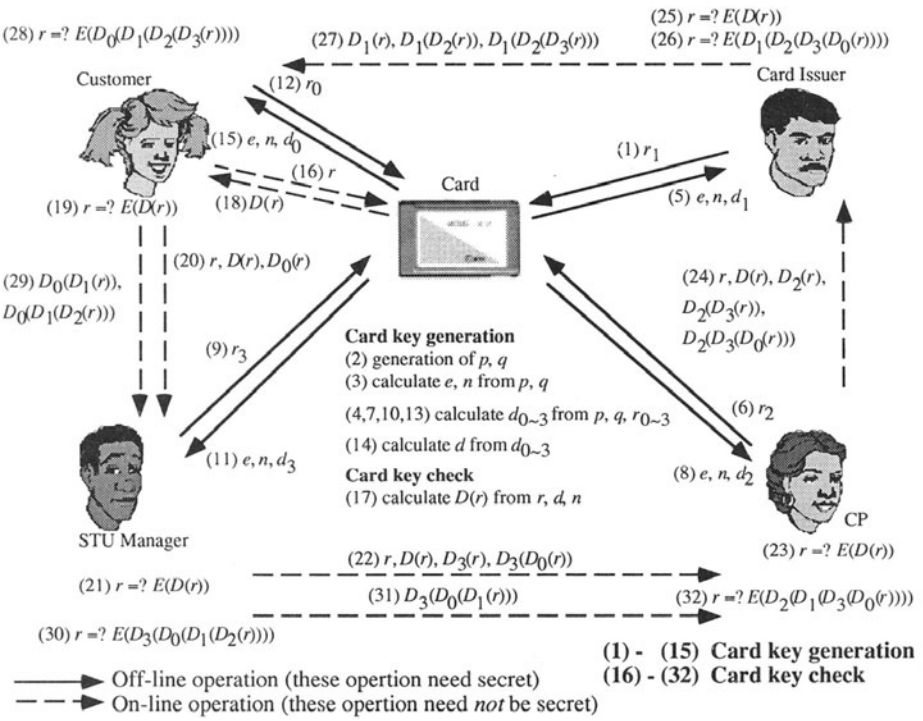

Figure 3 Card key generation and Card key check protocol

Table 2 Multiple key generation step

	Public key	*Private key*			
		Card Issuer	*CP*	*STU*	*Customer*
Random seed		r_1	r_2	r_3	r_0
Multiple key	e, n	d_1	d_2	d_3	d_0
RSA key	e, n		d		

We suggest that all parties submit to a key generation check to ensure that Customer, STU Manager, CP and Card Issuer recognize and agree that the Card key d was generated using their random numbers. The checking procedure can be easily done on the network.

It is possible to confirm by checking whether the key was made illegally. The Customer generates a random number r as the *challenge code*. The Card calculates $D(r)$ form r using private key d and public key n. The Card sends $D(r)$ back to the Customer, and the Customer calculates $E(D(r))$ using public key e and n. Then, he/she verifies that $E(D(r)) = r$. (If the verification fails, the Card key generation protocol is not successful). Then, the Customer generates $D_0(r)$ and sends r, $D(r)$ and $D_0(r)$ to the other party. Finally, all parties can make verifications using the parameters received (Figure 3 (20) - (32)).

3.5 Card reissue and key update

The Card key reissue procedure is shown in Figure 4. When the Card is lost, destroyed or stolen, the Customer the follows the following procedure. The customer makes a "Card reissue request form: f " in digital form. The items on the form are decided beforehand, so it can be made easily with a word processor, etc.

The reissue procedure begins when all parties acknowledge the reissue. The processing procedure is mostly the same as with a new issue. f and all parameter in this procedure are recorded for evidence when reissuing.

If the parameters from all parties are the same in the reissue, the same key can be generated. And if any party uses a different parameter, the key for the newly issued Card is different from the former one. Thus, this method can be applied to key updating.

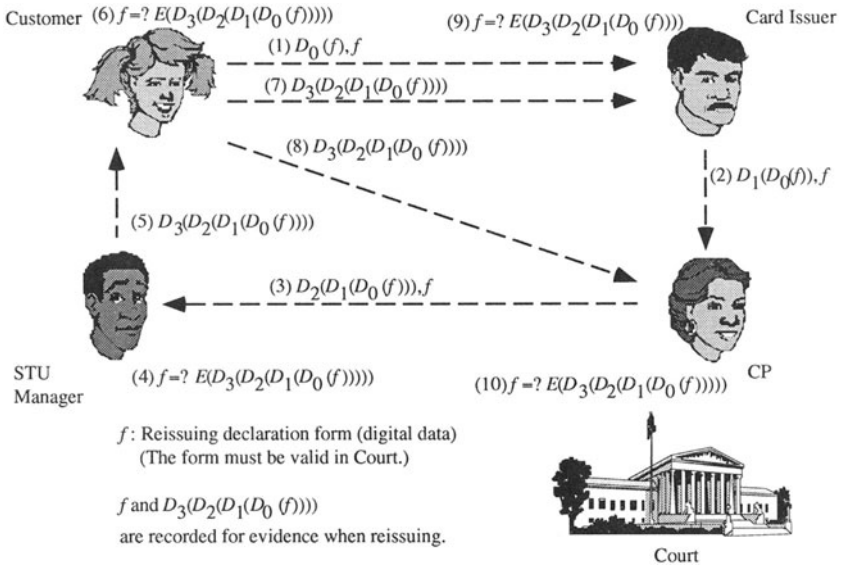

Figure 4 Card reassuring protocol

4 DISCUSSION OF SECURITY STRENGTH

Let's discuss the cryptographic strength of this proposed scheme. To break RSA, it is necessary to decompose two big prime factors. It is the same when searching for the one remaining key when all others are known. Because each party uses his/her own secret information, the remaining secret information must be guessed. The security of the public key proposed here is exactly the same as that of the original RSA.

The only difference is that here, the RSA key is divided between the parties who take part in its generation. Thus, the method of attack on this proposed scheme is the same as that on RSA. When all parties each bring a part of the key, it is not a conspiracy but mutual agreement. Thus, the cryptographic strength of this proposed scheme is the same as that of original RSA.

5 CONCLUSION

In using the Card discussed above, no one can copy any copyrighted digital content, not even the Card owner. Moreover, all parties have legally valid evidence to protect themselves against any dishonest parties. Owners of copyrighted digital content can protect their rights by using our proposed scheme. This should lead to further rapid growth of *content business* on computer networks and ensure that owners of copyrighted digital content can circulate copyrighted information on computer networks without any danger of their rights being compromised.

6 ACKNOWLEDGMENTS

The author would like to extend special thanks to Mr. Masanori Obata of NTT Human Interface Laboratories, for his useful discussion of Multiple RSA key. Thanks are also due to Mr. Kiyoshi Yamanaka, Project Term Leader, NTT Human Interface Laboratories for helpful advice on this work.

7 REFERENCES

Boyd, C. (1988) Some applications of multiple key ciphers: *Advances in Cryptology - EUROCRYPT '88 Proceedings*: Springer-Verlag, 455-467.

Ishii, S. Ohyama, K. and Yamanaka, K. (1994) A single-chip RSA processor implemented in a 0.5-μm rule gate array, *IEEE ASIC'94*, Rochester, NY. 433-436.

Lai, X. and Massey, J. (1991) A Proposal for a new block encryption standard, *Advances in Cryptology -EUROCRYPT '90 Proceedings*: Springer-Verlag, 55-70.

Miyaguchi, S. (1990) Extension of the FEAL cipher, *NTT Review*, Vol. 2, No. 6, 37-42.

Mori, R. and Kawahara, M. (1990) Superdistribution: The concept and the architecture, transaction *IEICE*, E73, No. 7, 1133-1146.

Federal information processing standards publication, National Bureau of Standard, 46

Rivest, R. L., Shamir, A. and Adleman, L. (1978) A method for obtaining digital signatures and public-key cryptosystems, *Communications of ACM*, 120-126.

Yamanaka, K. Takashima, Y. and Oyaizu, I. (1996) Security technologies for multimedia-on-demand services - copyright protection system -, *NTT Review*, Vol. 8, No. 2, 37-42.

8 BIOGRAPHY

Shinji Ishii is a research engineer at NTT Human Interface Laboratories. He joined NTT's laboratories in 1989, and is currently engaged in research and development of data security for multimedia network application services.

Mr. Ishii received his Masters in electrical engineering from Saitama University in 1989. He is a member of The Information Processing Society of Japan, and of the Institute of Electronics, Information and Communication Engineers.