LIFETIMES OF KEYS IN CRYPTOGRAPHIC KEY MANAGEMENT SYSTEMS

E. Okamoto and K. Nakamura
C&C Systems Research Raboratories
NEC Corporation
Miyamae-ku, Kawasaki 213 Japan

1. INTRODUCTION

Network architectures, such as System Network Architecture (SNA)[1], have an encryption function including key management at a functional layer. SNA uses Data Encryption Standard (DES)[2] to encrypt data and keys. A data encrypting key is encrypted with a master key and transmitted before every session. However, "the lifetime of the master key", namely, the time when the master key should be changed, is not prescribed. If the same key is used for a long time, it is probable that this secret key will be exposed.

This paper describes the lifetimes of keys. The lifetimes are the optimal key change periods, because they represent the optimal time intervals between key changes. We investigate the lifetimes of keys in two types of key distrbution schemes. One scheme is the usual scheme where the data encrypting key to be used in the next session is encrypted with an upper-level key encrypting key and transmitted to the receiving side. In the other scheme this encrypted data encrypting key is encrypted again with the data encrypting key being used at the present session and transmitted to the receiving side. In both schemes, the key encrypting key may be encrypted with more upper-level key encrypting keys. In this paper, the former scheme and the latter scheme are called SCHEME 1 and SCHEME 2, respectively. The keys lifetime in SCHEME 2 is shown to be much longer than that in SCHEME 1.

In the discussion, we assume that the cryptattack is based on the simplest method, namely the exhaustive key search. It may be possible to cryptanalyze in a shorter time, using statistical characteristics of encrypted data sequences, though there has

H.C. Williams (Ed.): Advances in Cryptology - CRYPTO '85, LNCS 218, pp. 246-259, 1986.

been no such DES cryptanalysis reported so far. Hence, the lifetimes of keys described in this paper show one of the upper bounds.

Moreover, this paper deals with DES as an example. However, it utilizes only the fact that the effective key length is 56 bits, hence the discussion can be applied to other encryption algorithms.

2. KEY DISTRIBUTION SCHEMES AND THEIR CRYPTANALYSIS METHODS

Figure 1 shows two types of key distribution schemes, SCHEME 1 and SCHEME 2. In Fig. 1, E and D show the encryption transformation and the decryption transformation, respectively. M shows a message and R a register. The lowest level key, K_1, is a data encrypting key which is called a work key. The second level key, K_2, is used to encrypt K_1 for distribution, and so on. The highest level key, K_L, is not encrypted. It is sent via a secure channel or by a courier. Key K_L is called a master key. Every key is generated randomly at the sending side.

In SCHEME 2, when K_i is changed to K_i', selectors SEL_{i-1}, SEL_{i-2}, ..., SEL_0 select upper lines and switches SW_{i-1}, SW_{i-2},...,SW_0 connect each decryptor output to upper lines in the figure. Hence $E_K(K'_i)$ is multi-encrypted with K_{i-1}, K_{i-2}, ...,K_1.

We assume that the cryptanalysis method is based on an exhaustive key search described below.

Cryptanalysis method for SCHEME 1

1) Obtain $C_1=E_{K_1}(M)$, $C_2=E_{K_2}(K_1)$, - - -, $C_L=E_{K_L}(K_{L-1})$, where $E_{K_i}(M)$ shows an encrypted message M with key K_i and C_i a cipher text.
2) Select a master key candidate KC_L.
3) Calculate lower level key encrypting key candidates $KC_{L-1}=D_{KC_L}(C_L)$, $KC_{L-2}=D_{KC_{L-1}}(C_{L-1})$, - - -, $KC_1=D_{KC_2}(C_2)$ and message candidate $MC=D_{KC_1}(C_1)$.
4) If MC is the right message M, then let $K_L=KC_L$ and decode cipher texts, otherwise select another master key candidate

and go to 3)

Cryptanalysis method for SCHEME 2

1) Search for key K_1 from $E_{K_1}(M)$ and (partial) M. If K_1 is found, decode cipher texts until K_1 is changed.
2) Search for key K_2 from $E_{K_2}(K_1)$ and K_1. If K_2 is found, decode cipher texts until K_2 is changed.

.
.
.

L) Search for key K_L from $E_{K_L}(K_{L-1})$ and K_{L-1}. If K_L is found, decode cipher texts until K_L is changed.

There may be many Ks satisfying $E_K(M)=C$ when message text M and cipher C are given. Hence, it is necessary to check $E_K(M')=C'$ with other M' and C'. If $E_K(M')\neq C'$, continue to search for K. In this paper, searching for K from $E_K(M)$ and M means to find the real K.

If a cryptanalyst stores all cipher texts into a memory, they can all be decoded after finding the keys. However, the texts are usually quite old when the keys are cryptanalyzed, because cryptanalysis requres much time. Hence, we assume that the cryptanalyst tries to obtain online real-time messages.

Disclosure rate ξ_L is defined as

$$\xi_L = \frac{\text{mean interval in which messages are disclosed}}{\text{interval in which } K_L \text{ is used}} \qquad (1)$$

In general, rate ξ_L increases according to increase in the K_L length.

3. LIFETIMES OF KEYS

This section represents the lifetimes of keys as function of the number of key levels and the disclosure rate. First, the disclosure rates are derived.

.1 Disclosure rate

(1) Disclosure rate for SCHEME 1

Let t_L be the time when K_L is disclosed, and T_L be the time hen K_L is changed. Time t_L is a random variable. Probablity ensity function p(t) of disclosure of K_L can be expressed as,

$$p(t)=\begin{cases}\dfrac{1}{LA} & ;(0\leq t\leq LA)\\ 0 & ;\text{ otherwise },\end{cases} \tag{2}$$

here A is the total time in which all keys need to be nvestigated. In DES case, for example,

$$A=2^{56}\cdot\tau \ , \tag{3}$$

here τ is the time for encrypting one block.

Messages are exposed in the period from time t_L to T_L, hence isclosure rate ξ_L is given by

$$\xi_L=\frac{1}{T_L}\int_0^{T_L} p(t)\ (T_L-t_L)dt_L$$

$$=\frac{c_L}{2L} \tag{4}$$

where c_L is the normalized lifetime of a master key K_L, i.e.,

$$c_L=T_L/A. \tag{5}$$

(2) Disclosure rate for SCHEME 2

Let t_i be the time when the i-th level key, K_i, is exposed and let T_i be the time when K_i is changed. Times t_i and T_i distributions are shown in Fig. 2. All t_i are considered as random variables.

The probability density function of disclosure of a key is

$$p(t)=\begin{cases}\dfrac{1}{A}\ ;\ 0 \le t < A\\[2ex] 0\ ;\ \text{otherwise}\end{cases} \tag{6}$$

Disclosure rate ξ_L is given as

$$\begin{aligned}\xi_L = \frac{1}{T_L}\{&E[I(T_1-t_1)\\ &+ E[I(T_2-t_2)]-E[I(T_1-t_2)]\\ &+ E[I(T_3-t_3)]-E[I(T_2-t_3)]\\ &+ .....\\ &+ E[I(T_L-t_L)]-E[I(T_{L-1}-t_L)]\}\end{aligned} \tag{7}$$

where E shows expectation and I is the function defined as below.

$$I(t)=\begin{cases} t\ ;\ t \ge 0\\ 0\ ;\ t < 0\end{cases} \tag{8}$$

The minus terms in Eq. (7) come from the cases where the intervals (t_i, T_i)'s are crossed each other.

$E[I(T-t_i)]$ is calculated as,

$$E[I(T-t_i)]=\int_0^T p(t_1)dt_1\int_{t_1}^T p(t_2-t_1)dt_2 \cdots \int_{t_{i-1}}^T P(t_i-t_{i-1})(T-t_i)dt_i$$

$$= \frac{1}{A^i} \int_0^{\min(T,A)} dt_1 \int_{t_1}^{\min(T,t_1+A)} dt_2 \cdots \int_{t_{i-1}}^{\min(T,t_{i-1}+A)} (T-t_i)dt_i \qquad (9)$$

As A is usually large, we assume that

$$T_i \leq A \qquad (i = 1,2, \ldots, L). \qquad (10)$$

Under this condition, $E[I(T-t_i)]$ is given as

$$E[I(T-t_i)] = \frac{1}{A^i} \int_0^T dt_1 \int_{t_1}^T dt_2 \cdots \int_{t_{i-1}}^T (T-t_i)dt_i$$

$$= \frac{1}{A^i} \int_0^T dx_1 \int_0^{x_1} dx_2 \cdots \int_0^{x_{i-1}} x_i dx_i \ , \quad (x_i = T-t_i) \qquad (11)$$

$$= \frac{T^{i+1}}{(i+1)!\ A^i}$$

and ξ_L is given as,

$$\xi_L = \frac{1}{c_L} \sum_{i=1}^{L} \frac{c_i^{i+1} - c_{i-1}^{i+1}}{(i+1)!} \ , \qquad (12)$$

where

$$c_i = T_i/A \qquad (i=1,2,\ldots L) \qquad (13)$$

$$c_o = 0 \qquad (14)$$

Equations (4) and (12) relate disclosure rate ξ_L to the number of key levels L and the normalized keys lifetimes c_i. In SCHEME 2, it is desired that c_L be maximum, because K_L must be changed manually. It can be derived that c_L is maximized at

$$c_1 = c_2 = \ldots = c_{L-1} = 0 \qquad (15)$$

and the maximum c_L is given by

$$c_L=((L+1)!\cdot\varepsilon_L)^{1/L} , \tag{16}$$

where ε_L is considered as a parameter (See Appendix).

The c_1 . . . ,c_{L-1} influence on c_L will be investigated when L=2 in detail.

Figure 3 shows the relation between ε_L and c_L, and Figure 4 shows the effectiveness of increase of L on the lifetime of key. We can see that SCHEME 2 is much stronger than SCHEME 1 for cryptanalysis.

3.2 Lifetimes of keys for the two level key cryptosystems

Lifetimes c_1 and c_2 in the two level key cryptosystems are investigated. These types of cryptosystems are fairly often used. From Eq.(12), the disclosure rate ε_2 for SCHEME 2 is represented as

$$\varepsilon_2 = \frac{c_1^2}{2c_2} + \frac{c_2^3-c_1^3}{6c_2} \tag{17}$$

Figure 5 shows the relations between c_1 and c_2 for some values of a parameter ε_2.

Normalized lifetimes of keys c_2 and c_1 for SCHEME 2 are optimized by the rules below.

1) c_2 is maximized.
2) c_1 is maximized under the condition that c_2 nearly equals its maximum,i.e.,

$$c_2 = \sqrt{6\cdot\varepsilon_2} \tag{18}$$

Equation (18) comes from Eq.(16). In Figure 5, the maximum points of c_1 are given as the cross points on the graph where $c_2\doteqdot\sqrt{6\cdot\varepsilon_2}$. The line connecting these points is given by the equation,

$$\log c_1 - \log 10^{-1} = 3/2(\log c_2 - \log\sqrt{6\times10^{-1}}), \quad (19)$$

namely,

$$c_1 = 0.56\cdot\varepsilon_2^{0.75}. \quad (20)$$

Equation (19) is given from Fig. 5 by rule of thumb.

The lifetimes of master keys T_2 are shown in Table 1, when DES is employed.

For example, when $\tau=10^{-6}$ second, the master key for SCHEME 1 must be changed every year, though the master key for SCHEME 2 has only to be changed every 56 years to estalish $\varepsilon\leq10^{-4}$ (1 hour/year). When $\tau=10^{-7}$ second, SCHEME 1 must change the master key every month , whereas SCHEME 2 has only to change the master key every 5 years. Therefore SCHEME 2 is superor to SCHEME 1 on the keys lifetime.

4. CONCLUDING REMARKS

The keys lifetimes necessary to attain a certain low disclosure rate have been investigated for two types of schemes. DES is employed as an encryption algorithm example. This paper employs the poorest attack, namely the exhaustive attack as a cryptanalysis. There may be a more effective attack. As results, we recommend to adopt SCHEME 2 and to change the master key 'at least' within a few years.

ACKNOWLEDGEMENT

The authors wish to thank Mr. Kato, Mr. Ishiguro and Mr. Goto of NEC Corporation for helpful suggetions.

REFERENCES

[1] Lennon, R.E., "Cryptography Architecture for Information

Security", IBM System J., vol.17, no.2, pp.138-150, 1978

[2] Federal Information Processing Standards Publication No.46, National Burean of Standards, 1977.

[3] Okamoto,E. and Nakamura,K., "Key change Periods in Cryptographic Key Management Systems", The proceedings of the 7-th Symposium on Information Theory and Its Applications (in Japanese), pp.169-173, 1984.

APPENDIX

The aim here is to show that the maximum of c_L is given by Eq.(16) at $c_1=c_2=\ldots=c_{L-1}=0$. From Eq. (12),

$$\frac{c_L^{L+1}}{(L+1)!} - \xi_L c_L = -\sum_{i=2}^{L} \frac{c_{i-1}^{i}}{i!}\left(1-\frac{c_{i-1}}{i+1}\right) \tag{A1}$$

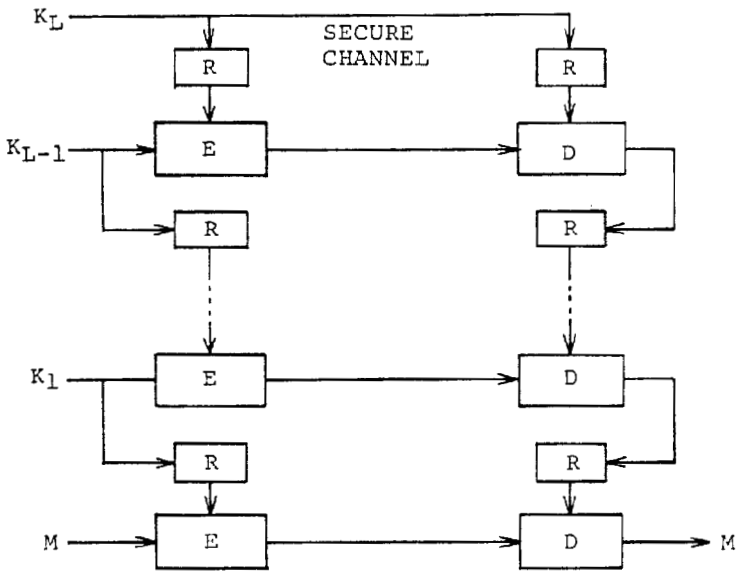
The right-hand side of Eq.(A1) is nonnegative from Eq.(10) and Eq.(13), while the left-hand side of Eq.(A1) is nonnegative if and only if

$$0 \leq c_L \leq ((L+1)!\cdot\xi_L)^{1/L} \tag{A2}$$

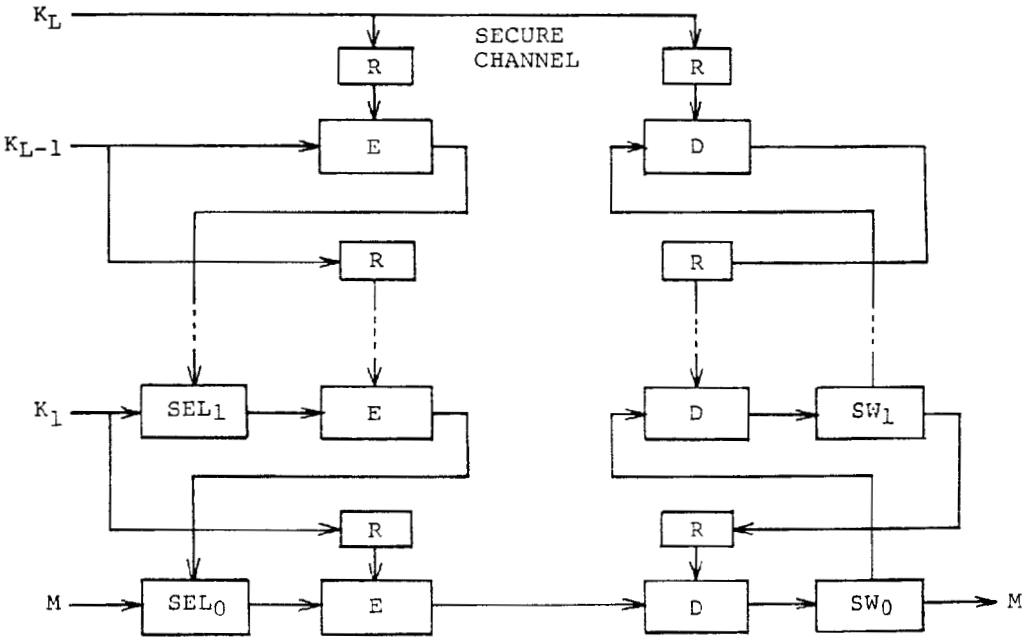
Hence the maximum of c_L is $((L+1)!\cdot\xi_L)^{1/L}$. When c_L is the maximum,

$$c_L=((L+1)!\cdot\xi_L)^{1/L}\ , \tag{A3}$$

$c_1, c_2, \ldots, c_{L-1}$ are all zero, because the right-hand side of Eq.(A1) is zero and c_{i-1} does not equal i+1 from Eq.(10) and (13).



(a) SCHEME 1



(b) SCHEME 2

Figure 1. Key distribution schemes

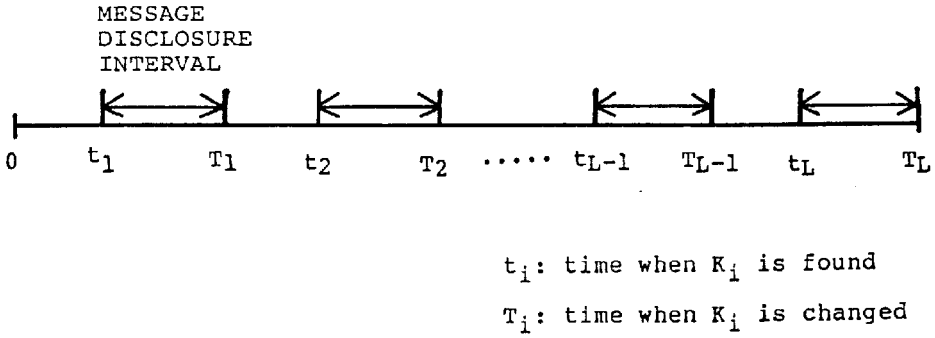


Figure 2. Times t_i and T_i distribution

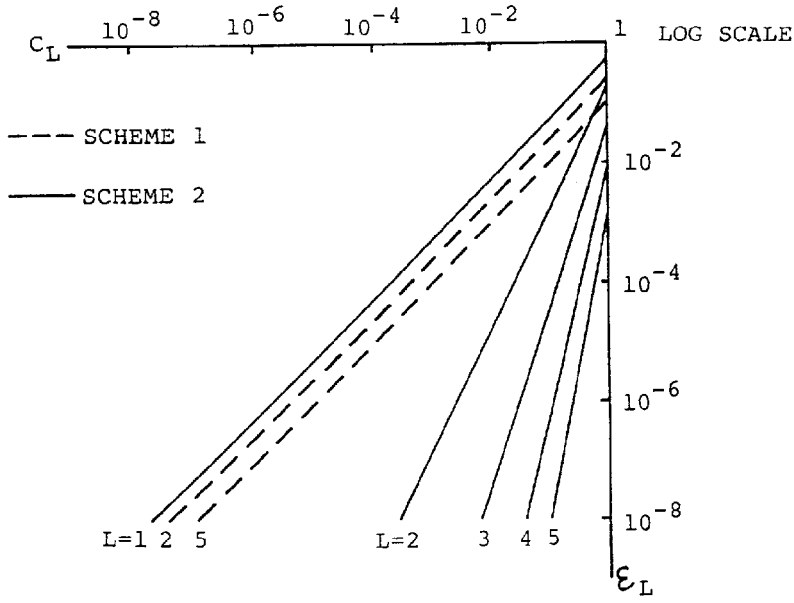


Figure 3. Relation between C_L and ε_L

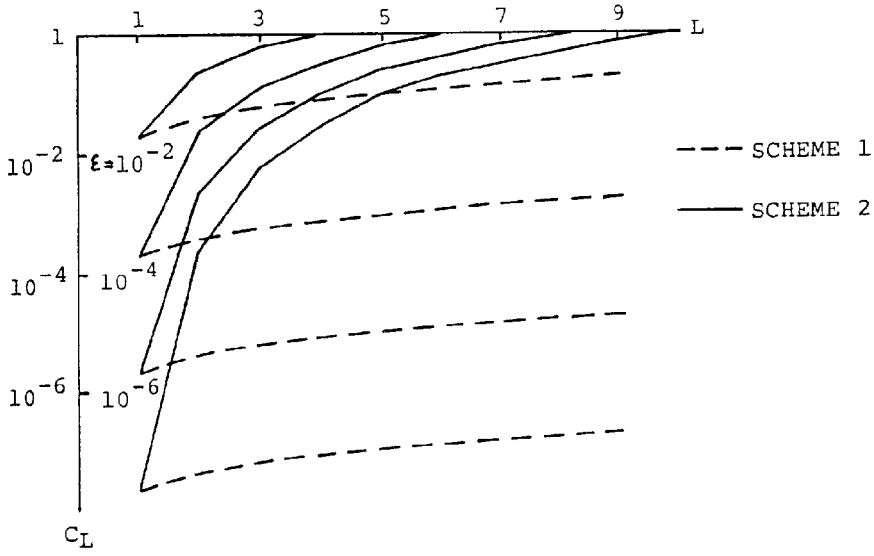


Figure 4. Relation between C_L and L

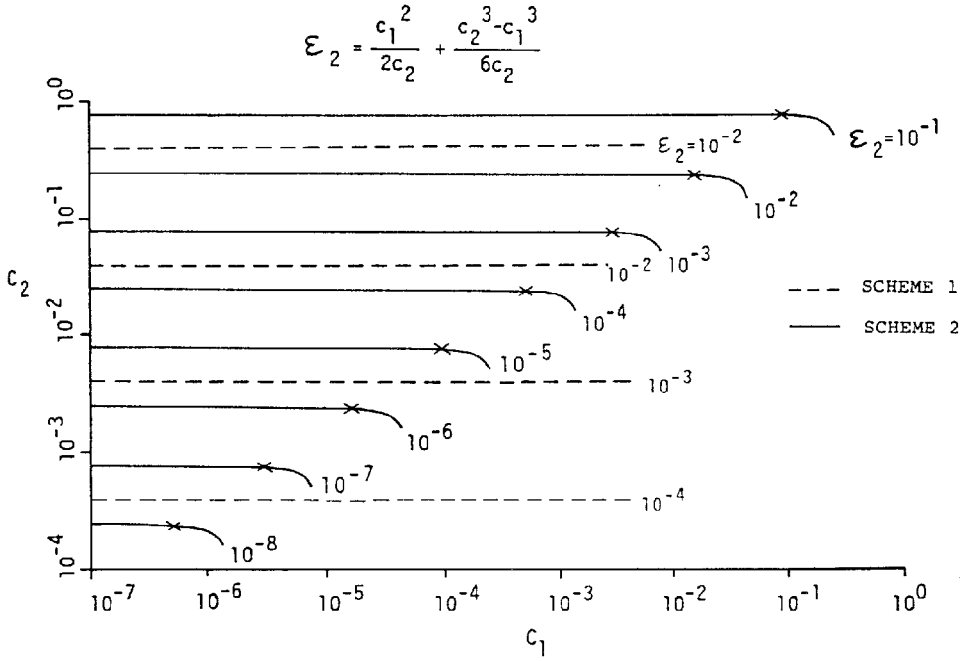


Figure 5. Relation between C_1 and C_2 with parameter ε_2

Table 1. Lifetimes of master keys for 2-level key cryptosystems

a) Lifetime of master key T_2 for SCHEME 1

Disclosure Rate ε \ Encrypting Time τ	10^{-6}(s)	10^{-7}(s)	10^{-8}(s)
10^{-1}	914 (y)	91.4 (y)	9.14 (y)
10^{-2}	91.4	9.14	334 (d)
10^{-3}	9.14	334 (d)	33.4
10^{-4}	334 (d)	33.4	3.34
10^{-5}	33.4	3.34	8.01 (h)
10^{-6}	3.34	8.01 (h)	48.0 (m)
10^{-7}	8.01(h)	48.0 (m)	4.80 (m)

b) Lifetime of master key T_2 for SCHEME 2

Cryptanalysis Ratio ε \ Encrypting Time τ	10^{-6}(s)	10^{-7}(s)	10^{-8}(s)
10^{-1}	1770 (y)	178 (y)	17.8 (y)
10^{-2}	560	56	5.6
10^{-3}	178	17.8	1.78
10^{-4}	56	5.6	204 (d)
10^{-5}	17.8	1.78	64
10^{-6}	5.6	204 (d)	20.4
10^{-7}	1.78	64	6.4
10^{-8}	204 (d)	20	2