ELSEVIER

Information Processing Letters 52 (1994) 201–206

Information Processing Letters

# On dynamic threshold schemes [☆]

Hung-Min Sun, Shiuh-Pyng Shieh [*]

*Department of Computer Science and Information Engineering, National Chiao Tung University, 1001 TA Hsueh Road, Hsinchu 30050, Taiwan, ROC*

Communicated by K. Ikeda; received 9 August 1993; revised 19 April 1994

**Abstract**

An $(m, n)$ threshold scheme is to decompose the master key $K$ into $n$ secret shadows in such a way that the master key $K$ cannot be reclaimed unless any $m$ shadows are collected. However, any $m-1$ or fewer shadows provide absolutely no information about $K$. In 1989, Laih et al. proposed the concept of dynamic threshold schemes which allow the master key to be updated without changing the secret shadows. However, the *perfect* dynamic threshold scheme, which provides *perfect secrecy* though the master key is allowed to be changed, has not been proposed. Nor has any paper shown the existence of perfect dynamic threshold schemes. In this paper, we prove that perfect dynamic threshold schemes do not exist when their master keys need be updated $\lfloor \log_2 |\mathscr{S}| / \log_2 |\mathscr{K}| \rfloor$ times or more without changing the secret shadows, where $\mathscr{S}$ is the secret shadow space and $\mathscr{K}$ is the master key space. Furthermore, we propose an perfect dynamic threshold scheme which allows its master key to be updated once without changing the secret shadows.

*Keywords:* Safety/security in digital systems; Cryptography; Dynamic threshold scheme; Information theory

## 1. Introduction

Because of the proliferation of computers into areas such as electronic mail, electronic fund transfers, etc., the question of protecting important information from being compromised, destroyed, or transmitted into wrong hands has received a lot of attention in recent years. While public-key and private-key cryptosystems provide ways to protect information [6,7], a different type of protection schemes, the *threshold schemes*, were introduced by Blakely and Shamir in 1979 [1,8]. The threshold schemes are mainly used to protect the master keys of a secure system from being lost, destroyed and modified. The main idea underlying an $(m, n)$ threshold scheme is to divide the top secret (master key) $K$ into $n$ shadows $S_i$'s $(1 \leqslant i \leqslant n)$ in such a way that the top secret $K$ cannot be reclaimed unless $m$ shadows are collected. However, any $m-1$ or less secret shadows provide no information about $K$. It means that the

[☆] This research was supported by the National Science Council, Taiwan under grant number NSC-RH-2243-E-009-081.

[*] Corresponding author. Email: ssp@csie.nctu.edu.tw.

*SSDI* 0020-0190(94)00143-X

prior probability $p(K=K_0)$ equals the conditional probability $p(K=K_0 \mid \text{given any } m-1 \text{ or less secret shadows})$.

By using the entropy function $H$ from [3], we can state the requirements for an $(m, n)$ threshold scheme as follows:

(1) $H(K \mid S_{i_1}, \ldots, S_{i_m}) = 0$,

(2) $H(K \mid S_{i_1}, \ldots, S_{i_{m-1}}) = H(K)$,

for an arbitrary set of $m$ indices $\{i_l, \ldots, i_m\}$ from $\{1, \ldots, n\}$.

As an example, we review the $(m, n)$ threshold scheme proposed by Shamir [8] as follows.

Let $f(x) = a_{m-1} \cdot x^{m-1} + \cdots + a_1 \cdot x + a_0 \pmod p$ be a polynomial of degree $m-1$ over the finite field GF($p$). The $n$ shadows $S_i$'s are computed from $f(x)$ as follows,

$$S_i = f(i) \pmod p, \quad i = 1, \ldots, n.$$

The master key $K$ is given by: $K = a_0 = f(0)$.

Obviously, given any $m$ secret shadows $S_{i_1}, \ldots, S_{i_m}$, $\{i_1, \ldots, i_m\} \subset \{1, \ldots, n\}$, $f(x)$ can be reconstructed from the Lagrange interpolating polynomial as follows [2],

$$f(x) = \sum_{k=1}^{m} S_{i_k} \cdot \prod_{j=1, j \neq k}^{m} \frac{(x - i_j)}{(i_k - i_j)} \pmod p.$$

Thus, the master key $K$ can be obtained by $f(0)$.

In the conventional threshold schemes, the corresponding shadows must be updated accordingly when the master key is renewed for security reasons. Obviously, it is time-consuming and inconvenient if master keys change frequently, especially when the number, $n$, of the secret shadows is large. In particular, if the possibility of the master keys being compromised is not due to the disclosure of the shadows, it is not required to change these shadows when the master key is renewed. In 1989 [5], Laih et al. proposed the concept of dynamic threshold scheme in which the master key can be renewed while the originally issued secret shadows remain intact. In their paper, they proposed a relative dynamic threshold scheme of which the secrecy decreases as the number of changes to the master key increases. However, the *perfect* dynamic threshold scheme which provides perfect secrecy has not been realized. In this paper, we will first show that the perfect dynamic threshold scheme does not exist if the master key need be updated $\lfloor \log_2 |\mathcal{S}| / \log_2 |\mathcal{K}| \rfloor$ times or more, where $\mathcal{S}$ is the secret shadows space and $\mathcal{K}$ is the master key space. It implies that there does not exist any perfect dynamic threshold scheme in which the master key can be updated for infinite times without modifying the secret shadows. Second, we will propose an perfect dynamic threshold scheme in which the master key can be updated once without changing the secret shadows. In Section 2, we will give formal definitions of the dynamic threshold scheme and the perfect dynamic threshold scheme. In Section 3, we will discuss the existence of perfect threshold schemes. In Section 4, we will demonstrate how to construct an perfect dynamic threshold scheme in which the master key can be updated once while not changing the secret shadows. Finally, we will give the conclusions in Section 5.

## 2. Dynamic threshold scheme

In this section, we define the dynamic threshold scheme and the perfect dynamic threshold scheme.

**Definition 1.** An $(m, n, T)$ dynamic threshold scheme (DTS) is an $(m, n)$ threshold scheme in which the newly created master key $K$ can be updated up to $T-1$ times without modifying any secret shadows, and satisfies the following requirements:

Let $V^t$ denote the public information distributed at $t$, $V_a^t$ denote all public information distributed till $t$, $K^t$ denote the master key used at $t$, and $K_a^t$ denote all master keys used till $t$, $1 \leqslant t \leqslant T$, where $T \in \mathbb{N}$,
(3) $H(K^t \mid S_{i_1}, \ldots, S_{i_m}, V^t) = 0$,
(4) $H(K^t \mid S_{i_1}, \ldots, S_{i_{m-1}}, V_a^u, K_a^{t-1}, \text{for } u \leqslant T) > 0$,
for an arbitrary set of $m$ indices $\{i_1, \ldots, i_m\}$ from $\{1, \ldots, n\}$.

Note that the keys of conventional $(m, n)$ threshold schemes will not be changed. Therefore conventional threshold schemes are special cases of dynamic threshold schemes and can be represented by $(m, n, l)$ DTSs. According to the security level which the DTS can provide at each updates of the master key, a *perfect* $(m, n, T)$ DTS is defined as follows.

**Definition 2.** An $(m, n, T)$ DTS is *perfect* if

$$H\left(K^t \mid S_{i_1}, \ldots, S_{i_{m-1}}, V_a^u, K_a^{t-1}, \text{for } u \leqslant T\right) = H(K^t)$$

for an arbitrary set of $m$ indices $\{i_l, \ldots, i_m\}$ from $\{1, \ldots, n\}$.

## 3. Perfect dynamic threshold scheme over finite sets

In the section, we will show that the perfect dynamic threshold scheme does not exist when the master key need be updated $\lfloor \log_2 |\mathcal{S}| / \log_2 |\mathcal{K}| \rfloor$ times or more while the secret shadows remain unchanged, where $\mathcal{S}$ is the secret shadow space and $\mathcal{K}$ is the master key space.

**Lemma 3.** *If there exists a perfect $(m, n, T)$ DTS, there exists a perfect $(m, m, T)$ DTS.*

**Proof.** The perfect $(m, n, T)$ DTS can be realized by generating the same $n$ secret shadows as those in a perfect $(m, n, T)$ DTS but distributing only $m$ of them. The remainders, $n - m$ secret shadows, are destroyed. Thus, the scheme satisfies the definition of a perfect $(m, m, T)$ DTS. □

**Theorem 4.** *There does not exist any perfect $(m, n, T)$ DTS in which the master key and the secret shadows are taken from finite sets $\mathcal{K}$ and $\mathcal{S}$, respectively, and $T > \lfloor \log_2 |\mathcal{S}| / \log_2 |\mathcal{K}| \rfloor$.*

**Proof.** From Lemma 3, it is clear that there does not exist a perfect $(m, n, T)$ DTS if there does not exist a perfect $(m, m, T)$ DTS. Hence, we need only to show the nonexistence of perfect $(m, m, T)$ DTS. We will prove the theorem by contradiction. Assume that there exists a perfect $(m, m, T)$ DTS in which the master key and the secret shadows are taken from finite sets $\mathcal{K}$ and $\mathcal{S}$, respectively, and $T > \lfloor \log_2 |\mathcal{S}| / \log_2 |\mathcal{K}| \rfloor$. It is clear that for any $t$, $1 \leqslant t \leqslant T$,
(5) $H(K^t \mid S_1, \ldots, S_m, V^t) = 0$,
(6) $H(K^t \mid S_2, \ldots, S_m, V_a^u, K_a^{t-1}, \text{for } u \leqslant T) = H(K^t)$.
Then we can create a perfect private-key cryptosystem as follows. Let the key of the private-key cryptosystem be $S_1$, the plaintext $M = \langle K^1, \ldots, K^T \rangle$, and the corresponding ciphertext $C = \langle V^1, \ldots, V^T, S_2, \ldots, S_m \rangle$. That is, $C = E_{S_1}(M)$. From (5), given $S_1$ and $C$, the plaintext $M$ can be reconstructed from the $m$ shadows in the perfect DTS. Assume that the plaintext $M$ is taken randomly

from $\mathscr{K}^T$, then $H(M)=H(K^1,\dots,K^T)=T\cdot\log_2|\mathscr{K}|$. On the other hand,

$$\begin{aligned}H(M\mid C)&=H\big(K^1,\dots,K^T\mid S_2,\dots,S_m,V^1,\dots,V^T\big)\\&=H\big(K^1\mid S_2,\dots,S_m,V^1,\dots,V^T\big)+H\big(K^2\mid S_2,\dots,S_m,V^1,\dots,V^T,K^1\big)\\&\quad+\cdots+H\big(K^T\mid S_2,\dots,S_m,V^1,\dots,V^T,K^1,\dots,K^{T-1}\big)\\&=H\big(K^1\mid S_2,\dots,S_m,V_\mathrm{a}^T\big)+H\big(K^2\mid S_2,\dots,S_m,V_\mathrm{a}^T,K^1\big)\\&\quad+\cdots+H\big(K^T\mid S_2,\dots,S_m,V_\mathrm{a}^T,K^{T-1}\big)\\&=H(K^1)+H(K^2)+\cdots+H(K^T)\quad(\text{by }(6))\\&=\log_2|\mathscr{K}|+\log_2|\mathscr{K}|+\cdots+\log_2|\mathscr{K}|\\&=T\cdot\log_2|\mathscr{K}|.\end{aligned}$$

Therefore, $H(M)=H(M\mid C)$ and $p(M=M_0)=p(M=M_0\mid C)=1/|\mathscr{K}|^T$. Hence, this private key cryptosystem is perfectly secure. In this cryptosystem, the length of the message is $T\cdot\log_2|\mathscr{K}|$ and the length of the key is $\log_2|\mathscr{S}|$. Because $T>\lfloor\log_2|\mathscr{S}|/\log_2|\mathscr{K}|\rfloor$ and $T\in\mathbb{N}$, we have $T>\lfloor\log_2|\mathscr{S}|/\log_2|\mathscr{K}|\rfloor+1$. Let $a=\log_2|\mathscr{K}|$ and $b=\log_2|\mathscr{S}|$. Then

$$\begin{aligned}T\cdot\log_2|\mathscr{K}|&\geqslant\big(\lfloor\log_2|\mathscr{S}|/\log_2|\mathscr{K}|\rfloor+1\big)\cdot\log_2|\mathscr{K}|=\big(\lfloor b/a\rfloor+1\big)\cdot a\\&>\big((b/a-1)+1\big)\cdot a=b=\log_2|\mathscr{S}|.\end{aligned}$$

So, $T\cdot\log_2|\mathscr{K}|>\log_2|\mathscr{S}|$. It means that the number of possible messages is greater than the number of possible keys. This is a contradiction to the perfect secrecy system which requires that the number of possible keys must be greater than or equal to the number of possible messages [2,9]. Therefore, perfect $(m, m, \lfloor\log_2|\mathscr{S}|/\log_2|\mathscr{K}|\rfloor+1)$ DTS does not exist. It implies perfect $(m, n, \lfloor\log_2|\mathscr{S}|/\log_2|\mathscr{K}|\rfloor+1)$ DTS does not exist. That is, the perfect dynamic threshold scheme does not exist when the master key need be updated more than or equal to $\lfloor\log_2|\mathscr{S}|/\log_2|\mathscr{K}|\rfloor$ times. □

From Theorem 4, we conclude that the necessary condition for the existence of a perfect $(m, n, T)$ DTS is that the length of the secret shadow should be at least $T$ times longer than that of the master key. In order to maintain and manage the secret shadows efficiently, the length of the secret shadow should be as short as possible. Hence, the secret shadow length of a perfect $(m, n, 2)$ DTS must be optimal if it is equal to twice of that of the master key. In the next section, we give a construction of the perfect $(m, n, 2)$ threshold scheme with the optimal length.

## 4. The design of a perfect $(m, n, 2)$ DTS

In this section, we will propose a perfect $(m, n, 2)$ DTS in which the master key can be updated once (while the secret shadows remain the same) and be still protected perfectly though up to $m-1$ secret shadows are disclosed. Other perfect $(m, n, T)$ DTSs can also be realized in the same way.

We construct the perfect $(m, n, 2)$ threshold scheme as follows. To distinguish between "times" and "exponent", we will use $x^t$ to denote $x$ at $t$, and $(x)^t$ to denote exponential operation on $x$. In addition, $f'(x)$ denotes the first-order derivation of $f(x)$. The $n$ shadows $S_i$ are selected randomly from GF$(p^2)$. $S_i=\langle s_{i,1}, s_{i,2}\rangle \pmod p$, $i=1,\dots,n$. At $t$, $1\leqslant t\leqslant 2$, let

$$f_t(x)=a_{2m-1}^t\cdot(x)^{2m-1}+\cdots+a_1^t\cdot(x)+a_0^t \pmod p$$

be a polynomial of degree $2m-1$ over the finite field GF($p$). The master key $K^t$ is given by:

$$K^t = a_0^t = f_t(0) \pmod p$$

The public information $V^t$ is given by:

$$V^t = \langle f_t(1) - s_{1,1},\ f_t(1) - s_{1,2}, \dots, f_t'(n) - s_{n,2} \rangle \pmod p.$$

Obviously, being given any m secret shadows (without loss of generality, we assume that those $m$ shadows are $S_1, \dots, S_m$), $\langle f_t(1), f_t'(1), f_t(2), f_t'(2), \dots, f_t(m), f_t'(m) \rangle$ can be obtained from $V^t$. Thus, $f_i(x)$ can be reconstructed from the Hermite interpolating polynomial [4] as follows,

$$f_t(x) = \sum_{k=1}^{m} \{1 - 2L_k'(k)(x-k)\} \cdot (L_k(x))^2 \cdot f_t(k) + \sum_{k=1}^{m} (x-k) \cdot (L_k(x))^2 \cdot f_t'(k) \pmod p,$$

where $L_k(x) = \Pi_{j=1, j=k}^{m} (x-j)/(k-j)$. Thus, the master key $K^t$ can be obtained by $f_t(0)$.

The security of the resulting dynamic threshold scheme can be analyzed as follows. At $t=1$, we assume that $m-1$ secret shadows are known (namely, $S_1, \dots, S_{m-1}$), i.e. $H(S_i) = 0$, for $1 \leqslant i \leqslant m-1$, and the public information $V^1$ and $V^2$ are also distributed. (It is clear that the knowledge of $V^2$ will not leak any information about secret shadows because $f_2(x)$ is unknown.) Then the value of $\langle f_1(1), f_1'(1), \dots, f_1(m-1), f_1(m-1) \rangle$ is known and $H(S_i)$ $(i > m-1)$ is still equal to $2 \log_2 p$. Thus, we have $2m-2$ linear equations about $f_1(x)$ and $f_1'(x)$ which have $2m$ unknown coefficients totally. So, the coefficients of $f_1(x)$ can be represented by linear functions of two variables, e.g.

$$f_1(x) = (3a + 5b + 1) \cdot (x)^{2m-1} + \cdots + (2a + 3b + 4) \cdot (x) + (6a + 2b + 5) \pmod p.$$

So, $K^1 = f_1(0)$ is also a linear function of two variables over GF($p$). It is clear that $H(K^1 \mid V^1, V^2$, any $m-1$ secret shadows$) = \log_2 p = H(K^1)$. It provides perfect secrecy at $t=1$ though up to $m-1$ secret shadows are disclosed.

At $t=2$, we assume that $m-1$ secret shadows are known (namely, $S_1, \dots, S_{m-1}$), and $K^1$ is released, i.e. $H(S_i) = 0$ and $H(K^1) = 0$, for $1 \leqslant i \leqslant m-1$. Therefore the values of $\langle f_1(1), f_1'(1), \dots, f_1(m-1), f_1'(m-1) \rangle$ and $f_1(0)$ are known. We have $2m-1$ linear equations about $f_1(x)$ and $f_1'(x)$ which have $2m$ unknown coefficients totally. So, the coefficients of $f_1(x)$ can represented by linear functions of a variable. Thus, $H(S_i)$ $(i > m-1)$ is equal to $\log_2 p$. On the other hand, the value of $\langle f_2(1), f_2'(1), \dots, f_2(m-1), f_2'(m-1) \rangle$ is also known. Also $\langle f_2(m), f_2'(m) \rangle$ can be expressed by linear functions of a variable. So we have $2m$ linear equations with $2m+1$ unknown variables totally. So, the coefficients of $f_2(x)$ can be expressed into linear functions of a variable. It is clear that $H(K^2 \mid V^1, V^2$, any $m-1$ secret shadows, $K^1) = \log_2 p = H(K^2)$. It provides perfect secrecy at $t=2$ though up to $m-1$ secret shadows are disclosed. Hence, the dynamic threshold scheme satisfies the definition of perfect dynamic threshold scheme.

Note that all secret shadows will be known if $K^1$ and $K^2$ are released, and $m-1$ secret shadows are known in the perfect ($m$, $n$, 2) DTS above. Therefore the scheme cannot provide perfect secrecy at $t=3$ when up to $m-1$ secret shadows are disclosed.

Note that the length of the secret shadow is just twice that of the master key in the resulting perfect ($m$, $n$, 2) DTS. In the same way, by including higher-order derivations of $f(x)$, it is possible to design an perfect ($m$, $n$, $T$) DTS in which the length of the secret shadows is just $T$ times that of the master key.

## 5. Conclusions

In this paper, we first show that the perfect dynamic threshold scheme does not exist when the master key need be updated $\lfloor \log_2 |\mathscr{S}| / \log_2 |\mathscr{K}| \rfloor$ times or more but the secret shadows remain the same, where $\mathscr{S}$ is the secret shadows space and $\mathscr{K}$ is the master key space. It implies that there does not exist any perfect dynamic threshold scheme in which the master key can be updated for infinite times while not modifying the secret shadows. The necessary condition for the existence of a perfect $(m, n, T)$ DTS is that the length of the secret shadow should be at least $T$ times longer than that of the master key. And then, we propose a perfect $(m, n, 2)$ dynamic threshold scheme in which the master key can be updated once without changing the secret shadows, though $m-1$ secret shadows are disclosed. Other perfect $(m, n,$ T) DTSs in which the length of the secret shadow is just $T$ times that of the master key can be realized in the same way.

## References

[1] G.R. Blakley, Safeguarding cryptographic keys, in: *Proc. NCC* **48** (AFIPS Press, Montvale, NJ, 1979) 313–317.

[2] D.E.R. Denning, *Cryptography and Data Security* (Addison-Wesley, Reading, MA, 1983).

[3] R.W. Hamming, *Coding and Information Theory* (Prentice-Hall, Englewood Cliffs, NJ, 1986).

[4] D.R. Kincaid and E.W. Cheney, *Numerical Analysis* (Brooks/Cole, 1990).

[5] C.S. Laih, L. Harn, J.Y. Lee and T. Hwang, Dynamic threshold scheme based on the definition of cross-product in an $n$-dimensional linear space, *J. Inform. Sci. Engineering* **7** (1991) 13–23; also in: *Advances in cryptology: Eurocrypt'89* (Springer, Berlin, 1990) 286–298.

[6] National Bereau of Standards, Data encryption standard, *FIPS PUB* **46**, Washington, DC, 1977.

[7] R.L. Rivest, A. Shamir and L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM* **21** (1978) 120–126.

[8] A. Shamir, How to share a secret, *Comm. ACM* **22** (11) (1979) 612–613.

[9] C.E. Shannon, Communication theory of secrecy systems, *Comput. Security J.* **VI** (2) (1990) 7–66.