A generalization of Secret Sharing Scheme on the Basis of Recovering Algorithm, K-RA

Masao KASAHARA
the Faculty of Informatics, Osaka Gakuin University Kishibe-Minami,
Suita-Shi, Osaka 564-8511 JAPAN
E-mail: kasahara@utc.osaka-gu.ac.jp

Abstract

Extensive studies have been made of the Secret Sharing Scheme(SSS). In this paper new classes of SSS, referred to as K-SSS, $K_{\rm I}$-SSS, $K_{\rm II}$-SSS and $\tilde{K}$-SSS are presented on the basis of recovering algorithm, K-RA. As an application, we shall also present a method for the recovering of secret informations learned only by heart, based on a particular class of K-SSS, $K_{\rm I}$-SSS.

1 Introduction

Extensive studies have been made of the Secret Sharing Scheme(SSS)[1, 2, 3, 4, 5, 6, 7]. The idea of SSS was independently proposed by Shamir [1] and Blakely [2]. Shamir constructed SSS based on a polynomial by letting the constant term of the polynomial be the secret and remaining coefficients, random numbers. McEliece and Sarwate generalized the Shamir's Scheme, referred to as S-SSS, in terms of Reed-Solomon codes [3, 4]. We shall refer to this scheme due to McEliece and Sarwate as MS-SSS.

In this paper, we present a method of applying the recovering algorithm referred to as K-RA[7, 8] to MS-SSS. We then propose a generalized version of MS-SSS using the recovering algorithm, K-RA. We shall refer to the generalized version as K-SSS for short and present 4 classes of K-SSS, i.e. general K-SSS, $K_{\rm I}$-SSS, $K_{\rm II}$-SSS and $\tilde{K}$-SSS. We shall also present a method for the recovering of secret informations learned only by heart, based on $K_{\rm I}$-SSS.

2 Preliminaries

Let us define the following symbols:

$\{s_i\}$: Set of secrets over F_{2^m}.

$\{r_i\}$: Set of random numbers over F_{2^m}.

$\{g_i\}$: Set of check symbols of (n,k)RS code over F_{2^m}.

$D(s_i)$: Dealer who wants to share secret s_i.

$U(r_i)$: User who holds share r_i.

$U(g_i)$: User who holds share g_i.

$H(s_i)$: Size of secret s_i (in bits), entropy of s_i.

$H(r_i)$: Size of random number r_i (in bits), entropy of r_i.

$\#A$: Order of set A.

In this paper, we first assume that the number of secret $\{s_i\}$,$\#\{s_i\}$, is only one. A method of a generalization of our scheme so that $\#\{s_i\}$ may take on a larger value than one will be described in Sections 4 and 5.

Based on MS-SSS, let us define the following vector $\boldsymbol{f}$ and the polynomial $f(X)$:

$$\begin{aligned} \boldsymbol{f} &= (s_1, r_1, \cdots, r_{k-1}). \quad (1) \\ f(X) &= s_1 + r_1 X + \cdots + r_{k-1} X^{k-1}. \quad (2) \end{aligned}$$

Regarding $f(X)$ as if it were a message vector, we construct a codeword of (n,k)RS code where the generator polynomial $G(X)$ is given by the polynomial of degree d over F_{2^m}.

Let us denote the constructed codeword by the following vector $\boldsymbol{v}$ and $v(X)$:

$$\begin{aligned} \boldsymbol{v} &= (g_1, g_2, \cdots, g_d, s_1, r_1, r_2, \cdots, r_{k-1}). \quad (3) \\ v(X) &= g(X) + f(X)X^d. \quad (4) \end{aligned}$$

We shall refer to $\boldsymbol{v}$ as characteristic vector.

The check symbols $g_1, g_2, \cdots, g_d$ of the codeword for the given $f(X)$ is given as

$$f(X)X^d \equiv g(X) \bmod G(X), \quad (5)$$

where $g(X)$ is given by

$$g(X) = g_1 + g_2 X + \cdots + g_d X^{d-1}. \quad (6)$$

Remark 1: As we have shown in Eq.(3), the codeword $\boldsymbol{v}$ is given by a systematic form in a sharp contrast with the codeword in a nonsystematic form given by Refs.[3] and [4]. It is evident that the generator polynomials cannot be kept secure even if the codeword if RS code is given by the nonsystematic form.□

3 Secret Recovering Algorithm[7, 8]

3.1 Distributing of Shares

In the following, we shall describe a method for the distributing of the shares in a form of the describing of an algorithm, for an easy understanding.

[Algorithm 1]

Step 1: Dealer $D(s_1)$ constructs the following codeword (the characteristic vector) of (n,k)RS code given by Eq.(3) :
$\boldsymbol{v} = (g_1, g_2, \cdots, g_d, s_1, r_1, r_2, \cdots, r_{k-1})$

Step 2: Dealer $D(s_1)$ secretly distributes r_i to User $U(r_i), i = 1, \cdots, k-1$ and g_i to User $U(g_i), i = 1, \cdots, d$, secretly. □

We now assume the followings :

S1: Dealer $D(s_1)$ deletes the secret s_1 completely.

S2: Dealer $D(s_1)$ keeps the set of locations $\{i, j\}$ of $\{r_i, g_j\}$ and the generator polynomial $G(x)$ of (n,k)RS code, in an appropriate method so that they may not be lost.

S3: Dealer $D(s_1)$ asks frequently for the users $\{U(r_i)\}$ and $\{U(g_i)\}$ to cooperate for the recovering of the secret s_1, while the users keep shares unaltered for a long period, unless something should happen in their shares. □

3.2 Secret Recovering Algorithm(K-RA)

The following algorithm is due to the method given in Refs.[7] and [8]. We shall refer to this algorithm as K-Recovering Algorithm or K-RA for short. We also assume for simplicity, that $D(s_i)$ wishes to recover his secret s_1.

In the following algorithm, Steps 7 through 10, the sendings of y_i and $\tilde{g}_i$ to $D(s_1)$ are not required to be performed in a secure manner. In order to clearly show this advantage, we shall describe that Steps 7 through 10 are performed in a public.

[Algorithm 2(K-RA)]

Step 1: Because $D(s_1)$ deleted the secret s_1, and remembers nothing. $D(s_1)$ estimates the value of $s_1, \hat{s_1}$, in a totally random manner.

Step 2: Dealer $D(s_1)$ calculates

$$\begin{aligned}(\hat{s_1} + x_1)X^d &\equiv s_{11} + s_{12}X + \cdots + s_{1d}X^{d-1} \\ &\quad \mathrm{mod} G(X),\end{aligned} \tag{7}$$

where x_1 is a random number to keep $\hat{s_i}$ be secret.

Step 3: Dealer $D(s_1)$ secretly sends s_{1j} to $U(g_j), j = 1, \cdots, d$.

Step 4: User $U(r_i)$ calculates

$$\begin{aligned}(r_i + y_i)X^{d+i} &\equiv r_{i1} + r_{i2}X + \cdots + r_{id}X^{d-1} \\ &\quad \mathrm{mod} G(X),\end{aligned} \tag{8}$$

where y_i is a random number to keep r_i be secret.

Step 5: User $U(r_i)$ secretly sends r_{ij} to User $U(g_j), j = 1, \cdots, d$.

Step 6: User $U(g_j)$ calculates

$$g'_j = s_{1j} + r_{1j} + r_{2j} + \cdots + r_{k-1,j}. \tag{9}$$

Step 7: Dealer $D(s_1)$ publicizes x_1.

Step 8: User $U(r_i)$ publicizes y_i.

Step 9: User $U(g_i)$ publicizes $g_i + g'_i = \tilde{g}_i$.

Step 10: The following vector $\boldsymbol{v'}$ is publicized :

$$\boldsymbol{v'} = (\tilde{g_1}, \tilde{g_2}, \cdots, \tilde{g_d}, x_1, y_1, \cdots, y_{k-1}). \tag{10}$$

Step 11: Based on the publicized $\boldsymbol{v'}$, Dealer $D(s_1)$ is able to know the error value of $e_1 = s_1 + \hat{s_1}$ on the symbol x_1. With this knowledge, the secret s_1 can be recovered as follows :

$$s_1 = \hat{s_1} + e_1. \tag{11}$$

□

From the above-mentioned steps it is evident that any person is able to recover secret s_i if and only if the person is given more than $k-1$ shares from the cooperative users among $k+d-1$ users.

Remark 2: No information on $\hat{s_1}$ or any element of $\{r_i\}$ is disclosed, because the random number x_1 and $\{y_i\}$ are added on $\hat{s_1}$ and on the elements of $\{r_i\}$. However it should be reminded that the coefficients $s_{1j}, r_{1j}, r_{2j}, \cdots, r_{k-1,j}$ are required to be kept secret in order to let g'_j be secret. □

Remark 3(Point of K-RA): The most important point regarding to K-RA can be summarized as follows. Namely, it takes advantage of the fact that the following vector $\boldsymbol{v''}$ is a codeword of (n,k)RS code when there exist no errors in $\{r_i\}$ and $\{g_i\}$:

$$\begin{aligned} \boldsymbol{v''} &= (\tilde{g_1}, \tilde{g_2}, \cdots, \tilde{g_d}, s_1 + \hat{s_1} + x_1, y_1, \cdots, \\ & \quad y_{k-1}). \end{aligned} \tag{12}$$

Thus one cannot know any secret from the publicized vector $\boldsymbol{v'}$ given by Eq(10).

The idea of K-RA seems very simple. However the present author believes that the idea is solely originated in careful investigations on the decoding mechanism of error correcting code. □

Theorem 1: When there exist τ errors in shares $\{r_i\}$ and check symbols $\{g_i\}$, it is posible to correct these erroneous symbols provided that the following relation holds :

$$1 + 2\tau \leq d. \tag{13}$$

□

Theorem 2: No information on s_1, $\{r_i\}$ or $\{g_i\}$ is disclosed when using Algorithm 2(K-RA). □

From Theorems 1 and 2, we see that, using K-RA, it is possible to recover s_1 without disclosing not only s_1 but also $\{r_i\}$ and $\{g_i\}$, based on the vector $\boldsymbol{v'}$ that can be publicized without deteriorating any security level, even if some of the shares have errors.

Remark 4: In our proposed secret recovering algorithm, K-RA, each cooperative user publicizes only a random data for the recovering of the secret s_1, whenever asked to cooperate for the recovering. Dealer $D(s_1)$ is able to recover his or her secret only from the public data, v'. Dealer is also able to know exactly that some of the shares are erroneous and is able to replace them by the correct shares. □

4 A Generalized Scheme of MS-SSS

In this section, we shall present a generalized scheme of MS-SSS, K-SSS, assuming that we shall use K-RA.

In K-SSS, we assume the existence of a group of λ independent dealers $\{D(s_i)\}$. We assume that no dealer conspire with any other dealers in order to disclose the secrets $\{s_i\}$. We also assume the existence of a group $\{U(r_i)\}$ of μ cooperative users. Our scheme is very general in a sense that $D(s_i)$ can take the role of several $U(r_i)$'s.

In K-SSS, the characteristic vector $\boldsymbol{v}$ of Eq.(3) is generalized to vector $\tilde{\boldsymbol{v}}$ as

$$\tilde{\boldsymbol{v}} = (\boldsymbol{g}_d; \boldsymbol{s}_\lambda; \boldsymbol{r}_\mu), \tag{14}$$

where g_λ, s_λ and r_μ are

$$\boldsymbol{g}_d = (g_1, g_2, \cdots, g_d), \tag{15}$$

$$\boldsymbol{s}_\lambda = (s_1, s_2, \cdots, s_\lambda), \tag{16}$$

and

$$\boldsymbol{r}_\mu = (r_1, r_2, \cdots, r_\mu), \tag{17}$$

respectively.

By deleting $n - \varepsilon$ components of $\boldsymbol{v} = (v_1, v_2, \cdots, v_n)$, let us construct the following punctured vector $\bar{v_\varepsilon}$:

$$\bar{v_\varepsilon} = (\bar{v_1}, \bar{v_2}, \cdots, \bar{v_\varepsilon}), \tag{18}$$

where $\bar{v_i}$ is a component of $\boldsymbol{v}$.

Let us assume the followings :

Assumption 1: Entropy of $s_i \in F_{2^m}, H(s_i)$, takes on the same value of $H(s_i) = m$ (bits). □

Assumption 2: Conditional entropy of $H(s_i|s_j)$ satisfies $H(s_i|s_j) = H(s_i)$, for $i \neq j$. □

Theorem 3: It is possible to recover λ secrets correctly even if there exists τ erroneous shares in the set of shares $\{r_i\}$ and $\{g_i\}$, provided that the following relation holds:

$$\lambda + 2\tau \leq d. \tag{19}$$

□

Theorem 4: By assuming that $\lambda = \mu = d$ and letting $\{r_i\} \cup \{g_i\}$ be denoted by $\{t_i\}$, we have

$$H(\boldsymbol{s}_\lambda|\boldsymbol{t}_{\lambda+\varepsilon}) = (\lambda - \varepsilon)H(s) \text{ for } \varepsilon \leq \lambda. \tag{20}$$

□

From Theorem 4, we see that our scheme is a ramped scheme [9].

A different scheme of K-SSS where r_i is generated not by $D(s_i)$ but by User $U(r_i)$ would prove to be another interesting SSS. A different new scheme will be referred to as K̃-SSS for short. In K̃-SSS, user $U(r_i)$ sends coefficients $\{r_{ij}\}$ of $r_i X^{d+i}$ mod $G(X)$ to User $U(g_j)$in a similar manner as in Step 5 of Algorithm 2.

5 Particular Scheme of K-SSS

5.1 Preliminaries

In this section we shall present the following two particular classes of K-SSS where no $\boldsymbol{r}$ is used.

K$_{\mathrm{I}}$-SSS: K-SSS where $d < \lambda$ holds.

K$_{\mathrm{II}}$-SSS: K-SSS where $d \geq \lambda$ holds.

We shall show that these classes yield interesting new classes of SSS.

5.2 K$_{\mathrm{I}}$-SSS

In K$_{\mathrm{I}}$-SSS, the charactristic vector $\boldsymbol{v}_{\mathrm{I}}$ is given by

$$\boldsymbol{v}_{\mathrm{I}} = (g_1, g_2, \cdots, g_d, s_1, s_2, \cdots, s_\lambda), d < \lambda. \tag{21}$$

Theorem 5: In $\boldsymbol{v}_{\mathrm{I}}$, the following relations hold :

$$H(\boldsymbol{s}_\lambda|\boldsymbol{g}_d) = (\lambda - d)H(s). \tag{22}$$

$$H(s_i|\boldsymbol{g}_d) = H(s). \tag{23}$$

□

Remark 5: From the information theoretic view point, in this paper, it would be desirable to assume the using of an ideal error correcting codes that is not only the maximum distance separable(MDS) code but also the perfect code. When using such ideal error correcting code for any value of m and $\lambda - d \geq 2$, $\boldsymbol{g}_d$ can be publicized without deterioroting any security level on individual secret s_i, under Assumptions A1 and A2. However the perfect code over F_{2^m} has been left unconstructed. Thus the using of RS code, the maximum distance separable code, would be reasonable. Besides for $m \gtrsim 160$, RS code can be used in a sufficiently secure manner as the perfect code[10, 11]. □

Let us denote the probability of estimiting s_λ correctly when $\boldsymbol{g}_\lambda$ is given, by $P_c(\boldsymbol{s}_\lambda|\boldsymbol{g}_d)$.

Theorem 6: In K$_{\mathrm{I}}$-SSS over F_{2^m}, the probability $P_c(\boldsymbol{s}_\lambda|\boldsymbol{g}_d)$ is given by

$$P_c(\boldsymbol{s}_\lambda|\boldsymbol{g}_d) = 2^{-m(\lambda-d)}. \tag{24}$$

□

Corollary 1: For any dealer, the probability $P_c(\boldsymbol{s}_\lambda|\boldsymbol{g}_d)$ is given by

$$P_c(\boldsymbol{s}_\lambda|\boldsymbol{g}_d) = 2^{-m(\lambda-d-1)}. \tag{25}$$

□

From Theorem 6, we see that estimating $\boldsymbol{s}_\lambda$ correctly based on the publicized $\boldsymbol{g}_d$ can be disregarded for $m \gtrsim 160$ from the practical point of view. We also see that for $m = 160, \lambda - d = 2$ the estimating any secret from the publicized data is impractical.

We shall show that K_I-SSS over F_{2^m} has an interesting application referred to as Forgotten Secret Recovering Problem(FSRP), which will be defined below.

Definition 1: FSRP(Forgotten Secret Recovering Pr-oblem) : Each member of $\{D(s_i)\}$ keeps secrets $\{s_i\}$ in a completely secret manner. Therefore in such case, one of the ideal method would be to learn s only by heart without storing s in any form of physical memories. When by any chance, certain number of members of $\{D(s_i)\}, \{\tilde{D}(s_i)\}$, are not able to recall forgotten secrets, $\{\tilde{s}_i\}$, then other members, $\{D(s_i)\}$, assist for $\{\tilde{D}(s_i)\}$ to recover the forgotten secrets, $\{\tilde{s}_i\}$. In this cooperative work of the recovering of secrets, $\{\tilde{s}_i\}$, it is strictly required that no information on the secrets of all the members of Group $\{D(s_i)\}$ be disclosed even among the members of Group $\{D(s_i)\}$. □

In usual daily life we remember several passwords, several phone-numbers whose total size itself exceeds 160 bits. Thus K_I-SSS over $F_{2^{160}}$ described above can be successfully used as one of the solutions for FSRP.

The proposed solution on FSRP yields the following advantages:

A1: K_I-SSS used for the solving of FSRP is optimum in a sense that the size of the public data $\boldsymbol{g}_d$ takes on the theoretical minimum value of $m\tau$ (bits) for the recovering of any set of forgotten secrets of total size of $m\tau$ (bits).

A2: In our solution of using K_I-SSS with K-RA, public data, $\boldsymbol{g}_d$, is used unchanged no matter how often the recovering of forgotten secrets are performed without disclosing any information on the secrets $\{s_i\}$.

A3: K_I-SSS is asymptotically optimum in a sense that the probability of the estimating $\{s_i\}$ correctly from the publicized data of the theoretically minimum size approaches rapidly to zero, in an exponential manner, as $m(\lambda - d)$ increases.

□

5.3 K_{II}-SSS

In K_{II}-SSS where $\lambda \leq d$ holds, the set $\{g_i\}$ is kept secret. Namely at least $d - \lambda + 2$ share holders of $\{U(g_i)\}$ should keep their secrets in a secret manner. We have the following theorem.

Theorem 7: In K_{II}-SSS, λ secrets can be recovered correctly even when τ erroneous shares exist among d shares, provided that the following relation holds :

$$\lambda + 2\tau \leq d. \tag{26}$$

□

Remark 6: In K_{II}-SSS, by cooperations of independent dealers $\{D(s_i)\}$, each dealer is able to construct more efficient SSS, provided that no dealer colludes with any other members for the disclosing of the secrets $\{s_i\}$. □

Example 1: K_{II}-SSS over $F_{2^{160}}, d = 12, \lambda = 6$, using K-RA:
Secrets $s_1, s_2, \cdots, s_6$ can be recovered successfully without disclosing any informaiton on $\{s_i\}$ even if 3 erroneous shares exist among the collected 12 shares. □

In Example 1, even if 5 dealers among 6 dealers $\{D(s_i)\}$, collude, the remaing secret can be kept secret provided that shares $\{g_i\}$ are kept secret. The probability of estimating the only one remaining share by 5 dealers in collusion is given by $2^{-160} = 10^{-48}$, extremely small value.

We also see that in Example 1 on an average each dealer has two shares from which the dealer get no information on other dealer's secrets. On the other hand, if the dealer $D(s_i)$ independently constructs $\mathrm{K_{II}}$-SSS with the characteristic vector (s_i, g_{i1}, g_{i2}), then in such scheme it becomes impossible to recover the secret correctly even when only one erroneous share exists.

6 Concluding Remark

We have presented a new class of Secret Sharing Scheme, K-SSS, $\mathrm{K_I}$-SSS, $\mathrm{K_{II}}$-SSS and $\tilde{\mathrm{K}}$-SSS along with the recovering algoritm, K-RA. We have also presented a theoretically optimum method for the recovering of secret informations learned only by heart, based on $\mathrm{K_I}$-SSS.

A new class of SSS referred to as $\tilde{\mathrm{K}}$-SSS where the users $\{U(r_i)\}$ generate their random numbers by themselves independently from the secret holders, is also suggested. Various interesting problems have been left for the future.

References

[1] A. Shamir, "How to share a secret", Communications of the ACM, Vol.22, pp612-613 (1979).

[2] G. Blakley, "Safeguarding cryptographic keys", Proceedings of AFIPS National Computer Conference, pp.313-317 (1979).

[3] J.L. Massey, "Minimal codewords and secret sharing", Proc. 6th Joint Swedish-Russian Int. Workshop on Info. Theory, pp.276-279 (1993-08).

[4] R.J. McEliece and D.V. Sarwate, "On sharing secrets and Reed-Solomon codes", Comm. ACM, Vol.24, pp.583-584 (1981-09).

[5] Ito,M.,A.Saito, and T.Nishizeki "Multiple assignment scheme for sharing secret", Journal of Cryptology, 6, pp.15-20 (1993).

[6] Kurosawa, K., K.Okada, K.Sakano, W.Ogata, and S.Tsujii, "Nonperfect secret sharing schemes and matroids", Advances in Cryptolog–EUROCRYPT'93, Lecture Notes in Computer Science, vol.765, ed.T.Helleseth.Springer-Verlag, Berlin, pp.126-141 (1993).

[7] M.Kasahara, "A new class of product-sum cryptosystem – appending a solution of problem related to password –", SCIS 2001, pp.535-540, Oiso, Japan (2001-01).

[8] M.Kasahara, "How to recover the forgotten secrets", SCIS 2002, Shirahama, Japan, pp.13-18 (2002-01).

[9] G.R.Blakley and C.Meadows, "Security of ramp scheme", Proc. of Crypto'84, Lecture Note on Computer Science, 196, pp.242-268 (1984).

[10] T.Hada, M. Morii and M. Kasahara, "On error detecting capability of Reed-Solomon codes", Tech.Report of IEICEJ, IT89-12(1989-07).

[11] M.Morii, "On Error-Correcting Capability for Reed-Solomon Codes", IEICE Trans. Fundamentals, A, Vol. J74-A, No.1, pp.96-103 (1991-01)