A New Class of Biometrics on the Basis of Forgotten Secret Recovering Scheme, KSS(I)

Masao KASAHARA
Faculty of Informatics, Osaka Gakuin University, Suita-shi, 564-8511 Japan.
kasahara@ogu.ac.jp

Abstract

In this paper, we present a new secret sharing scheme, referred to as KSS(I) on the basis of systematic Reed-Solomon code[2]. We show that KSS(I) can be successfully applied to biometrics.

Keyword

Secret Sharing Scheme, Biometrics, Reed Solomon code.

1 Introduction

In 1979, Shamir proposed an interesting scheme, Secret Sharing Scheme (SSS)[1]. Rightafter Shamir's proposal, McEliece and Sarwate proposed SSS using non-systematic Reed-Solomon (RS) code.

In Aug. 2000, the present author submitted a challenge problem "How to prevent a user from forgetting about password?" in the news-letter of IEICE Japan [3]. Regretably we got no mathematical solution from the readers of approximately $10,000$ copies. Accordingly the present author published the solution in Ref. [4] in 2001 and Ref. [5] in 2004.

We shall refer to the proposed scheme in Refs. [4] and [5], "Forgotten Secret Recovering Scheme for k Users" where each user has a secret as FSRS(k). In Ref. [6] we discussed on a particular class of FSRS(k), FSRS(1), where only one user has k secrets.

In 1999, Juels and Wattenberg presented an interesting fuzzy commitment scheme [7], where they combined the techniques from the fields of error-correcting code and cryptography. In 2002, Juels and Sudan also proposed an interesting problem referred to as "Movie Lover's Problem, MLP" [8]. They presented a Fuzzy Vault Scheme(FVS) based on non-systematic Reed-Solomon code(RS code), on this matter.

In this paper, we present a new secret sharing scheme based on systematic RS code, referred to as KSS(I). We show that KSS(I) can be successfully applied to a biometric scheme[9-13].

2 KSS(I)

2.1 Preliminaries

Let us define several symbols.

$G(x)$	:	Generator polynomial of Reed-Solomon (RS) code over $\mathbb{F}_{2^m}$.
g	:	Degree of $G(x)$.
x_i	:	Secret variable, $i = 1, 2, \cdots, k$.
$\boldsymbol{x}$	:	$(x_1, x_2, \cdots, x_k)$.
$HF_i(\boldsymbol{x})$,	:	Hash function of $\boldsymbol{x}$ published by Center, $i = 1, 2, \cdots, J$.
$hF_i(y_i)$,	:	Hash function in the variable y_i published by Center, $i = 1, 2, \cdots, J$.
S_i	:	Alice's biometric secret when being registered at Center, $i = 1, 2, \cdots, k$.
$\widehat{S}_i$	:	Alice's biometric secret when being authenticated at Center, $i = 1, 2, \cdots, k$.
$\boldsymbol{S}$	:	$(S_1, S_2, \cdots, S_k)$.
$\hat{\boldsymbol{S}}$	:	$(\hat{S}_1, \hat{S}_2, \cdots, \hat{S}_k)$.
$\|A\|$	:	Size of A (in bit).
$H_D(\boldsymbol{u}, \boldsymbol{v})$	:	Hamming distance between $\boldsymbol{u}$ and $\boldsymbol{v}$.

In the followings, biometric secrets will be simpliy referred to as secrets.

2.2 Construction of code word

Let the Alice's biometric secret polynomial over $\mathbb{F}_{2^m}$ be denoted by

$$S(x) = S_1 x^{(S_1)} + S_2 x^{(S_2)} + \cdots + S_k x^{(S_k)}, \tag{1}$$

where $(S_i) \geq g$; $i = 1, 2, \cdots, k$.

In $S(x)$, the location (S_i) is uniquely determined from S_i. Let us explain the one to one correspondence relation between S_i and (S_i) by a toy example, for simplicity.

In Table 1, we show the correspondence between S_i and $\hat{S}_i$ over $\mathbb{F}_{2^3}$ where we assume that $g = 3$, namely $(S_i) \geq 3$, $i = 1, 2, 3, 4$.

For example, when $S_i = \alpha^4 = \alpha + \alpha^2$, then the correspond-

ing binary number is

$$0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 = 6. \tag{2}$$

It should be noted that, due to the above-mentioned one to one correspondence, the order is effectively imposed on secrets. This feature is particularly desirable in biometrics.

Let the remainder $u(x)$ be obtained by

$$S(x)x^g \equiv u(x) \mod G(x), \tag{3}$$

where $G(x)$ is the generator polynomial of RS code over $\mathbb{F}_{2^m}$. The code word $W(x)$ is then constructed by

$$W(x) = S(x)x^g + u(x). \tag{4}$$

Let $u(x)$ be represented by

$$u(x) = u_1 + u_2 x + \cdots + u_g x^{g-1}. \tag{5}$$

The code word in a vector form can be represented by

$$\boldsymbol{W} = (u_1, u_2, \cdots, u_g, S_1, S_2, \cdots, S_k). \tag{6}$$

2.3 Error correction procedure

Let the Alice's secret polynomial obtained when being authenticated at Center be denoted by

$$\hat{S}(x) = \hat{S}_1 x^{(\hat{S}_1)} + \hat{S}_2 x^{(\hat{S}_2)} + \cdots + \hat{S}_k x^{(\hat{S}_k)}. \tag{7}$$

It should be noted that the relation

$$S_i x^{S_i} \neq \hat{S}_i x^{\hat{S}_i} \tag{8}$$

may hold for some i's.

At the authentication process, with Alice's request, Center presents $\boldsymbol{u} = (, u_1, u_2, \cdots, u_g)$ to Alice. Alice constructs the following word:

$$\begin{aligned}\hat{W}(x) = {} & u_1 + u_2 x + \cdots + u_g x^{g-1} \\ & + \hat{S}_1 x^{(\hat{S}_1)} + \hat{S}_2 x^{(\hat{S}_2)} + \cdots + \hat{S}_k x^{(\hat{S}_k)}.\end{aligned} \tag{9}$$

Table 1: Correspondence between S_i and (S_i)

S_i	α^0	α^1	α^2	(S_i)
α^0	1	0	0	-
α^1	0	1	0	-
α^2	0	0	1	-
α^3	1	1	0	3
α^4	0	1	1	6
α^5	1	1	1	7
α^6	1	0	1	5
α^i	2^0	2^1	2^2	
	Natural Binary Number			Location

Let us assume that without losing generality, the relation:

$$\hat{S}_1 \neq S_1, \hat{S}_2 \neq S_2, \cdots, \hat{S}_t \neq S_t \tag{10}$$

and

$$\hat{S}_{t+1} = S_{t+1}, \hat{S}_{t+2} = S_{t+2}, \cdots, \hat{S}_k = S_k \tag{11}$$

holds.

Theorem 1: The secrets $\hat{S}_1$, $\hat{S}_2$, $\cdots$, $\hat{S}_t$ can be corrected to S_1, S_2, $\cdots$, S_t respectively if and only if

$$4t \leq g \tag{12}$$

holds. □

Proof: $\hat{S}_i \neq S_i$ results in double error, $\hat{S}_i x^{\hat{S}_i} + S_i x^{S_i}$, in the code word $W(x)$, yielding the proof. □

2.4 Registration process

The registration process at Center is performed by the following steps.

Step1 : Alice constructs the code word $\boldsymbol{W}$ by $\boldsymbol{W} = (u_1, u_2, \cdots, u_g, S_1, S_2, \cdots, S_k)$.
Step2 : Alice sends $\boldsymbol{u} = (u_1, u_2, \cdots, u_g)$ to Center.
Step3 : Alice deletes $\boldsymbol{u}$.
Step4 : Center keeps $\boldsymbol{u}$.
Step5 : Alice calculates the hashed values, H_1, H_2, $\cdots$, H_J, based on her secrets $S_1, S_2, \cdots, S_k$ using hash function $HF_i(S_1, S_2, \cdots, S_k)$.
Step6 : Alice calculates the hashed values h_1, h_2, $\cdots$, h_J based on H_i using hash function $hF_i(H_i)$, $i = 1, \cdots, J$.
Step7 : Alice sends $\boldsymbol{h} = (h_1, h_2, \cdots, h_J)$ to Center.
Step8 : Center keeps $\boldsymbol{h}$.
Step9 : Alice deletes $\{H_i\}$ and $\boldsymbol{h}$.

2.5 Authentication process

The process at the i-th authentication opportunity at Center, after the registration is completed, is given by the following steps.

Step10 : Center presents $\boldsymbol{u} = (u_1, u_2, \cdots, u_g)$ to Alice.
Step11 : Alice constructs the word $\widehat{\boldsymbol{W}}$ by $\boldsymbol{W} = (u_1, u_2, \cdots, u_g, \widehat{S}_1, \widehat{S}_2, \cdots, \widehat{S}_k)$.
Step12 : When the Hamming distance between $\boldsymbol{S} = (S_1, S_2, \cdots, S_k)$ and $\widehat{\boldsymbol{S}} = (\widehat{S}_1, \widehat{S}_2, \cdots, \widehat{S}_k)$, $H_D(\boldsymbol{S}, \widehat{\boldsymbol{S}})$, satisfies $4H_D(\boldsymbol{S}, \widehat{\boldsymbol{S}}) \leq g$, Alice successfully recovers $\widehat{\boldsymbol{S}} = \boldsymbol{S}$.
Step13 : Alice recovers $\widehat{H_i} = H_i$.
Step14 : Alice sends $\widehat{H_i}$ to Center.
Step15 : When Center is able to confirm that $hF(\widehat{H_i}) = \widehat{h_i} = h_i$. Center accepts Alice.

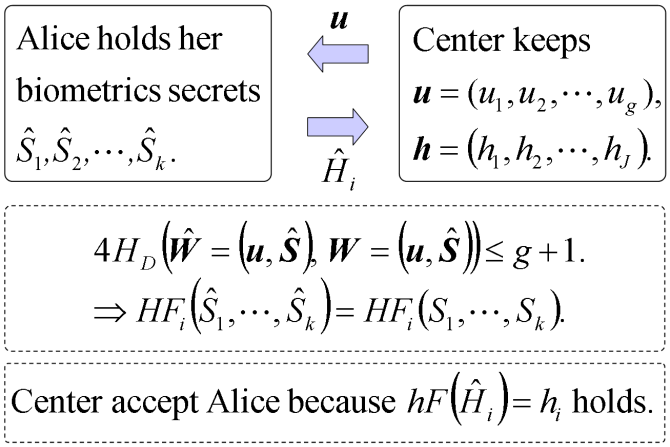

Figure 1: The i-th successful authentication process

Remark 1: Center keeps $h_1, h_2, \cdots, h_J$ for Alice. We assume that $J = 100 \sim 1000$ and $|h_i| = 100$ bit. As a result the memory size required for storing $h_1, h_2, \cdots, h_J$ is $10 \sim 100$ Kbit, a sufficiently small value. We also assume that every J times of authentication process, $\boldsymbol{h} = (h_1, h_2, \cdots, h_J)$ is renewed. □

3 Security considerations

3.1 Preliminaries

In this Section, we compare KSS(I) scheme with Juels and Sudan's scheme (JS scheme) from the standpoint of security. In the followings, S_i implies Alice's secret as in the previous sections.

3.2 JS scheme

In JS scheme, Center keeps the following set:

$$S_{ST} = \{(S_i, P(S_i))\} \bigcup \{(T_i, Z_i)\} \tag{13}$$

where Z_i is an element of $\mathbb{F}_{2^m} - \{P(S_i)\}$, T_i, an element of $\mathbb{F}_{2^m}$, and $P(x)$, a secret polynomial.

In S_{ST}, the elements $(S_i, P(S_i))$'s and (T_i, Z_i)'s are randomly scrambled. In this sub-section, we assume that the orders of these elements satisfy

$$\sharp\{S_i, P(S_i)\} = \sharp\{T_i, Z_i\}. \tag{14}$$

Let the probability that Betty chooses sufficiently large number of $(S_i, P(S_i))$'s that exceeds the acceptance threshold be denoted by $P_F(A)$. Let us assume the followings:

A1: The order of S_{ST}, $\sharp S_{ST}$, is 128.

A2: Betty choose 64 different elements of S_{ST} in a random manner.

A3: When Betty is succesful to obtain more than 56 S_i's among 64 choices, Betty is accepted as Alice.

Under above mentioned assumptions, the probability that Betty is accepted as Alice, P_{FA}, is given by

$$P_{FA} = 2.77 \times 10^{-10}. \tag{15}$$

3.3 KSS(I) Scheme

Center keeps only hashed values $\boldsymbol{u}$ and $\boldsymbol{h}$. The conditional entropy on $\{S_i\}$ when $\{u_i\}$ is disclosed is given by

$$H(S_1, S_2, \cdots, S_k | u_1, u_2, \cdots, u_g) = (k-t)m, \text{ (bit)}. \tag{16}$$

Throughout this paper we assume that this value takes on

$$(k-t)m \geq 256 \text{ (bit)}, \tag{17}$$

an extremely large value from the information theoretic point of view. For example, $(k-t)m$ takes on a large value of $(k-t)m = 448$, for $k = 64$, $t = 8$, $m = 8$.

In this example, we see that the probability P_{FA} is given by

$$P_{FA} = 2^{-448} \approx 1.38 \times 10^{-135}, \tag{18}$$

an extremely small value.

We also see that the following relations hold as we assume the using of ideal hash functions $HF_i(\boldsymbol{x})$'s and $hF_i(y_i)$'s:

$$H(S_1, S_2, \cdots, S_k | H_1, H_2, \cdots, H_J) = H(S_1, S_2, \cdots, S_k) \tag{19}$$

and

$$H(H_1, H_2, \cdots, H_J | h_1, h_2, \cdots, h_J) = H(H_1, H_2, \cdots, H_J) \tag{20}$$

respectively.

Thus, the probability that estimating $\{S_i\}$ correctly is very small. We conclude that KSS(I) scheme would be sufficiently secure.

4 Conclusion

We have presented a new class of the secret sharing schemes, KSS(I). We have shown that the proposed secret sharing schemes KSS(I) can be successfully applied to biometric scheme. It should be noted that no biometrics secret is stored in Center.

The present author is deeply thankful to Prof.Komatsu at Waseda Univ. for his kind and timely guidance to the research on biometric authentication scheme and his fruitful discussions on KSS(I). The present author greatly appreciates the fruitful discussions with Dr.Ohki and Mr.Satomura at Waseda Univ.

References

[1] A. Shamir : "How to share a secret", Communications of the ACM, vol. 22, pp.612-613, 1979.

[2] R. J. McEliece and D. V. Sarwate : "On Sharing secrets and Reed-Solomon codes", Comm. ACM, vol.24, pp.583-584, 1981.

[3] M.Kasahara : "How to recover forgotten password (Challenge Problem)", Newsletter, 29, p29, 2000-08.

[4] M.Kasahara : "A New Class of Product-Sum Cryptosystem – Appending a Solution of Problems Related to Passwords –", SCIS2001, 535-540, Oiso, Japan, 2001-01.

[5] M.Kasahara : "How to recover the forgotten secrets information", IEEE, ISIT, 2004.

[6] M.Kasahara : "New Classes of Product-Sum Type Public Key cryptosystem and Fuzzy Vault Scheme Constructed Based on Error-Correcting Codes", IEICE Technical Report, ISEC 2009, 2009-05.

[7] A.Juels and M.Wattenberg : "A Fuzzy Commitment Scheme", ACM CCS, 1999.

[8] A.Juels and M.Sudan : "A Fuzzy Vault Scheme", IEEE ISIT, 2002.

[9] A. K. Jain, R. Bolle and S. Pankanti (Eds.): "BIOMETRICS, Personal Identification in Networked society", Kluwer Academic Publishers, 1999.

[10] T.Ohki, S.Akatsuka, N.Komatsu and M.Kasahara : "Safety of template in biometric person authentication using error-correcting code", Proc. of the 18th Annual IS&T/SPIE Sympo. on Electronic Imaging (EI), 6072-20 2006-01.

[11] N. Komatsu, K. Uchida, S. Ikeno and H. Sakano: "Ohanasi (Story) on Biometrics", Nihon Kikaku Kyokai, 2008.

[12] T. Ohki, S. Hidano, N. Komatsu, M. Kasahara: "A Locked-Data Generating Method for Biometric Cryptosystem using Fuzzy Fingerprint Vault Scheme", IPSJ Journal. vol. 50, no. 9, 2009-09.

[13] K. Shukuzawa, T. Ohki, Y. Yamazaki, N. Komatsu: "A Study on the framework of Biometric Cryptosystem using a Common Template", ITE Technical Report, ME2009-226, pp.49-52, 2009-12.