A Multi-stage Secret Sharing Scheme Using All-or-Nothing Transform Approach

Mitra Fatemi*, Taraneh Eghlidos, and Mohammadreza Aref

Sharif University of Technology,
Information and System Security Laboratory(ISSL)
Azadi Ave., Tehran, Iran
m.fatemi@ee.sharif.edu
{teghlidos,aref}@sharif.edu

Abstract. A multi-stage secret sharing (MSS) scheme is a method of sharing a number of secrets among a set of participants, such that any authorized subset of participants could recover one secret in every stage. The first MSS scheme was proposed by He and Dawson in 1994, based on Shamir's well-known secret sharing scheme and one-way functions. Several other schemes based on different methods have been proposed since then. In this paper, the authors propose an MSS scheme using All-Or-Nothing Transform (AONT) approach. An AONT is an invertible map with the property that having "almost all" bits of its output, one could not obtain any information about the input. This characteristic is employed in the proposed MSS scheme in order to reduce the total size of secret shadows, assigned to each participant. The resulted MSS scheme is computationally secure. Furthermore, it does not impose any constraint on the order of secret reconstructions. A comparison between the proposed MSS scheme and that of He and Dawson indicates that the new scheme provides more security features, while preserving the order of public values and the computational complexity.

Keywords: Multi-stage secret sharing, All-or-nothing transforms, Resilient functions.

1 Introduction

In order to provide both security and availability for a given secret, one way is to distribute it among a number of shareholders (participants). The distribution should be accomplished in such a way that any subset of participants, the size of which is at least equal to a given number, be able to reconstruct the secret, using their shares (shadows). More specifically, a (t, n)-threshold secret sharing scheme refers to the procedure of assigning each of the n participants a private share, such that every subset of at least t participants could recover the secret. This concept was introduced by Shamir [1] and Blakley [2] in 1979, independently.

[*] This work is partially supported by ITRC under the contraction no. T500/20961 and supported by cryptography chair of Iran NSF.

S. Qing, C.J. Mitchell, and G. Wang (Eds.): ICICS 2009, LNCS 5927, pp. 449–458, 2009.

Later, various features like verifiability of the shares [3], resistance against the presence of a number of cheaters [4], dynamic change of the threshold and the number of participants [5] were added to the threshold secret sharing scheme.

A (t, n)-threshold secret sharing scheme is called *perfect* if less than t participants neither could reconstruct the secret, nor obtain any information about it. It has been shown that in a perfect secret sharing scheme, the size of the shares should at least be the same as the size of the secret [6]; in the case of equality, the scheme is referred to as *ideal.* Now, suppose that there are more than one secret to be shared among a group of participants. The dealer may run a perfect threshold secret sharing scheme for each of the secrets and send the related shares to each of the participants via a secure channel. In this way, even though the problem is solved, the difficulty of managing the possible large number of shadows arises. That is, each participant needs to keep multiple shadows to participate in each run of the secret sharing. Besides, protecting shares from an unauthorized access becomes more difficult, due to the increase in the number of shares assigned to each shareholder.

The concept of multi-stage secret sharing (MSS) was introduced by He and Dawson in 1994 [7] to solve the above mentioned problem. An MSS scheme is a method of distributing many secrets among a set of participants, while each of them gets only one master shadow. In an MSS scheme, the secrets are recovered one by one in different stages, possibly according to a pre-specified order. MSS schemes usually need a number of public values. The shareholders, who wish to participate in a secret reconstruction stage, derive the corresponding sub-shadow from their master-shadow and these public values.

The MSS scheme in [7] was based on the Shamir's polynomial secret sharing, a one-way (hash) function and the concept of "shift values". Later, various MSS schemes were presented based on different methods such as coding approach [8], congruence relations and Chinese Reminder Theorem [10] and linear equations [9]. The computational complexity and number of public values are two important factors for comparing the efficiency of MSS schemes and a number of publications appeared to reduce the value of these parameters [11] and [12].

In this paper, the authors employ *All-or-Nothing Transforms(AONT)* to realize the concept of an MSS scheme . An AONT is an invertible and randomized transformation $\mathbb{T}$, which reveals no information about x even if *almost all* the bits of $\mathbb{T}(x)$ are known. This concept was first introduced by Rivest [13] and further improved by Canetti et al. [14]. In the proposed MSS scheme, AONT is utilized so as to dramatically reduce the size of secret shadows corresponding to a particular secret. Therefore, one could share more secrets among the participants by assigning each of them several private values (shadows), the total size of which is equal to the size of each secret. Regarding the information theoretic lower bound of shares proposed in [15] and [6], an unconditionally secure MSS scheme is impossible. More Precisely, to achieve an unconditionally secure (perfect) secret sharing scheme, the size of each shadow should be at least equal to the sum of the sizes of different secrets. This contradicts the definition of the MSS schemes, which are proposed to reduce the size of the shares. Hence, the proposed scheme aims to provide the computational security. The authors compare the new MSS scheme with that of He and Dawson. This comparison shows that the new scheme provides more security features, while the computational complexity and number of public values remain almost the same. Moreover, the secrets should be reconstructed according to a pre-specified order in [7], while they can be recovered with an arbitrary order in the proposed scheme.

The rest of the paper is organized as follows. In section 2, we briefly review the MSS scheme proposed by He and Dawson. In section 3, the concept of AONT is described and some of its features are illuminated. The authors propose the new MSS scheme in section 4. A thorough analysis of the new scheme together with a comparison between the proposed scheme and that of He and Dawson is presented in the subsequent section. Finally, a summary of the whole paper is given in section 6.

2 He and Dawson's MSS Scheme

In this section, we briefly explain the earliest MSS scheme proposed by He and Dawson.

Let p be an odd large prime number. All the values in this scheme are chosen from the field $GF(p)$. Let $s_1, s_2, \ldots, s_m$ denote m secrets to be shared according to (t, n)-threshold schemes among n participants. Suppose that $f : GF(p) \rightarrow GF(p)$ is a one-way function. For any x and any nonnegative integer k, $f^k(x)$ resembles k successive application of f to x. Let $x_1, x_2, \ldots, x_n$ be the public identities of the n participants. The dealer performs the following steps.

1. Choose n random values $y_1, y_2, \ldots, y_n$ and privately send $y_i, i = 1, \ldots, n$, to the ith participant as his/her shadow.
2. For $j = 1, \ldots, m$, choose a random polynomial of degree $t - 1$ with the constant value equal to s_j:

$$g_j(x) = s_j + a_{1,j}x + a_{2,j}x^2 + \ldots + a_{t-1,j}x^{t-1} \tag{1}$$

   and compute $g_j(x_i)$ and $d_{i,j} = g(x_i) - f^{j-1}(y_i)$ for every $1 \leq i \leq n$. The values $d_{i,j}$ are called shift values. Publish all shift values.

The secrets reconstruction process should be conducted in m successive stages with jth secret s_j reconstructed at the (*m-j+1*)th stage. When a shareholder p_i wants to participate in the jth secret reconstruction stage, he/she should submit the value $g_{m-j+1}(x_i)$ which can be calculated by adding the sub-shadow $f^{m-j}(y_i)$ to the public value $d_{i,m-j+1}$. Having t points on the function $g_{m-j+1}(x)$, one could obtain s_{m-j+1}. The pre-specified order of secret reconstruction in this scheme is needed to guarantee that no information leaks about the shadows corresponding to the undisclosed secrets from the revealed ones.

A security analysis of this scheme is given in section 5.2.

3 All-or-Nothing Transforms

The concept of AONT was first introduced in [13]. However, more general descriptions of it and its applications are presented in [14].

Definition 1. *An l-AONT is a randomized polynomial time computable transformation* $\mathbb{T} : \{0,1\}^k \rightarrow \{0,1\}^s \times \{0,1\}^p$ *such that [14]:*

- *For any string x, given (all the bits of) $\mathbb{T}(x)$, one can efficiently recover x.*
- *Any polynomial time adversary that learns all but l bits of the secret part of $\mathbb{T}(x)$, obtains "no information" about x, where the first s bits of the output indicates the secret part and the last p bits of it represents the public part.*

Indeed, all-or-nothing transforms allow to encode any x in such a way that the encoding is easily invertible, and still, an adversary who learns all but l bits of the secret part of the encoded data, cannot extract any useful information about x. Therefore, using AONT, we can protect an arbitrary secret x by storing $\mathbb{T}(x)$ in an "exposure-resilient" way. That is, even if almost all the bits of $\mathbb{T}(x)$ are exposed, no information can be revealed about x.

AONT could be categorized into three classes: AONT with perfect security, AONT with statistical security and AONT with computational security (for an exact definition, see [14]). However, the last class of AONT involves parameters taken from a wider range of values. In addition, in an MSS scheme, we look for computational security rather than perfect security. Hence, this class of AONT is taken into consideration hereafter.

There are many approaches towards devising AONT, some of which are applying a hash function to the message, using a scheme based on an FFT-like arrangement of randomized multi-permutations and an approach based on secret sharing schemes [13]. Another construction for an AONT $\mathbb{T} : \{0,1\}^k \rightarrow \{0,1\}^s \times \{0,1\}^k$ is presented in [14] in which the process of creating an l-AONT is seen as that of a one-time-pad encryption. Here, the encryption of $x \in \{0,1\}^k$ is just $x \bigoplus R$, where R is a random string of length k derived by inserting an l-exposure resilient function $f : \{0,1\}^s \rightarrow \{0,1\}^k$ on a secret value r, that is $R = f(r)$. An l-exposure resilient function is a concept tightly related to l-AONT, which means that knowing all but l bits of the input, no one could gain any information about the output[16],[14]. The l-AONT output is the pair $(r, x \bigoplus f(r))$. The following theorem [14] has been obtained from this construction and it will be used in the design of the proposed MSS scheme.

Theorem 1. *Assume $l \leq s \leq poly(l)$ where $m = poly(k)$ indicates that m is polynomialy bounded in k. There exist functions $\mathbb{T} : \{0,1\}^k \rightarrow \{0,1\}^s \times \{0,1\}^k$ (with secret output of length s and public output of length k), such that $\mathbb{T}$ is a computationally secure l-AONT with $l < k \leq poly(s)$.*

A reasonable setting seems to be $s = O(k)$ (that is just slightly smaller than k) and $l = \lfloor s^{\epsilon} \rfloor$ to have excellent exposure-resilience [14].

4 The Proposed AONT Approach to Multi-Stage Secret Sharing

In this section, we propose an MSS scheme based on l-AONT with computational security. The value of parameters in the new scheme are derived from the results of theorem 1.

4.1 Reducing the Share Size in a Secret Sharing Scheme

Before considering the special case of an MSS scheme, here we explain how one could reduce the size of shares in a secret sharing scheme, using an AONT. To clarify the technique, the well-known Shamir's threshold secret sharing scheme is utilized. However, it could be implemented on any other perfect secret sharing scheme. The security level of the resulted scheme depends on the secrecy of the AONT; that is, the scheme would have statistical or computational security if an AONT with the same level of security is used. As stated before, we just focus on computationally secure ones.

All secret sharing protocols consist of two processes: distribution and reconstruction. In the distribution process, a dealer shares a secret and distributes the shares among participants. In the secret reconstruction process, the shareholders exchange their shares and reconstruct the secret. In the following, we describe each process for the secret sharing scheme with reduced share size.

:Let S denotes a secret that the dealer wishes to share among a set $\{p_1, \ldots, p_n\}$ of n participants according to a (t, n)-threshold secret sharing scheme. Let p be a large prime number such that $S \in GF(p)$. The dealer first chooses $t-1$ arbitrary random coefficients $a_1, a_2, \ldots, a_{t-1}$, uniformly distributed over $GF(p)$, and constructs the following polynomial:

$$f(x) = S + a_1x + a_2x^2 + \ldots + a_{t-1}x^{t-1} \tag{2}$$

Next, he/she chooses n distinct nonzero values $x_1, \ldots, x_n \in GF(p)$ as the identities corresponding to the n participants and calculates $y_1 = f(x_1), \ldots, y_n = f(x_n)$, which are values in $GF(p)$. Suppose that all elements in $GF(p)$ have size k, that is, they could be represented by k bits, where $k = \lceil log_2 p \rceil$. The dealer chooses a computationally secure l-AONT $\mathbb{T} : \{0,1\}^k \rightarrow \{0,1\}^s \times \{0,1\}^k$ with $s = O(k)$ and $l = s^{\epsilon}$ for some small $0 < \epsilon < 1$. Then he/she computes the values $\mathbb{T}(y_1), \mathbb{T}(y_2), \ldots, \mathbb{T}(y_n)$ and publishes the $k + s - l$ least significant bits of each (least significant $s - l$ bits of the secret part and all k bits of the public part). Finally, the dealer sends the l most significant private bits of $\mathbb{T}(y_1), \mathbb{T}(y_2), \ldots, \mathbb{T}(y_n)$ to the n participants as their secret shadows and publishes the map $\mathbb{T}$ and its inverse.

: Let a subset of t participants $\{p_{i_1}, \ldots, p_{i_t}\}$ come together in order to reconstruct the secret. By appending the corresponding $(k + s - l)$-bit public values to their l-bit shadows, the shareholders could obtain the whole bits of $\mathbb{T}(y_{i_1}), \mathbb{T}(y_{i_2}), \ldots, \mathbb{T}(y_{i_t})$. Next, they could efficiently recover $y_{i_1}, \ldots, y_{i_t}$, using the inverse transform $\mathbb{T}^{-1}$. Having t points on the secret polynomial of degree

$t-1$, the participants are able to calculate the polynomial and recover the constant coefficient S.

Note that in the above scheme, the size of each share is l/k times of the secret size which is a small fraction, due to the choice of l-AONT parameters. Indeed, $l/k \lessapprox s^{\epsilon}/s$ for some small $0 < \epsilon < 1$. Below, a multi-stage secret sharing scheme for m secrets is represented where m denotes $\lfloor k/l \rfloor$.

4.2 Sharing Multi Secrets

Let $S_1, \ldots, S_m \in GF(p)$ denote the m secrets to be shared among the participants $p_1, \ldots, p_n$, according to (t, n)-threshold secret sharing schemes. The dealer performs all steps mentioned in the distribution process of section 4.1 for each secret. Let $y_{i,j} = f_j(x_i)$ for $1 \leq i \leq n$ and $1 \leq j \leq m$, where $f_j(x)$ is the polynomial used for sharing the jth secret. In this case, the shadow of the ith shareholder is the concatenation of the first l bits taken from each of $\mathbb{T}(y_{i,1}), \mathbb{T}(y_{i,2}), \ldots, \mathbb{T}(y_{i,m})$. Likewise, the public values are comprised of the last $k+s-l$ bits of each $\mathbb{T}(y_{i,j})$, for $1 \leq i \leq n$ and $1 \leq j \leq m$.

Now, let a group of t participants $\{p_{i_1}, \ldots, p_{i_t}\}$ wish to collaborate on reconstructing the secret S_j in a stage. Each of them first attaches those l private bits from his/her shadow, which are related to the jth secret, to the corresponding $k+s-l$ bits of the public values. In this way, they could recover the values $\mathbb{T}(y_{i_1,j}), \mathbb{T}(y_{i_2,j}), \ldots, \mathbb{T}(y_{i_t,j})$. Then, using the inverse map, the cooperating participants are able to derive the values $y_{i_1,j}, y_{i_2,j}, \ldots, y_{i_t,j}$. Finally, using the Lagrange interpolation, the participants could recover the secret S_j.

$$f_j(x) = \sum_{u=1}^{t} y_{i_u,j} \prod_{v=1, v\neq u}^{t} \frac{x - x_{i_v}}{x_{i_u} - x_{i_v}} = S_j + a_{1,j}x + a_{2,j}x^2 + \ldots + a_{t-1,j}x^{t-1} \quad (3)$$

In the proposed scheme, the total size of each shadow assigned to a participant is $m \times l$ bits which is $m \times l/k$ times of the secret size. Regarding that $m = \lfloor k/l \rfloor$, we have $m \times l/k = \lfloor k/l \rfloor \times l/k \lessapprox 1$. This implies that the share size does not exceed the secret size. Also, the total size of public values in this scheme is $m \times (k+s-l) \times n$ bits, which is $\lfloor k/l \rfloor \times (k+s-l)/k \times n \lessapprox \lfloor k/l \rfloor \times (2k-l)/k \times n = \lfloor k/l \rfloor \times (2-l/k) \times n \lessapprox (2m-1) \times n$ times of the secret size.

It is easy to check that in the proposed scheme, there is not any constraint on the order of secret reconstruction and the participants could disclose the secrets at any order they wish. Moreover, the threshold corresponding to the various secrets could be different. Indeed, it suffices to make use of secret polynomials with different degrees. A comprehensive analysis of the proposed MSS scheme and a comparison with that of He and Dawson is presented in the next section.

5 Investigation of the Proposed Scheme

In this section, we discuss about the security and performance of the proposed scheme in two parts. In the first part, it is shown that the scheme provides computational security. In the subsequent part, efficiency of the scheme is investigated and a comparison with some of other MSS schemes, especially that of He and Dawson's scheme is made. The reason behind this choice of the reference scheme is due to the simplicity of its structure. Moreover, it is the first scheme which introduced the concept of multi-stage secret sharing [7]. The comparison results show that the proposed scheme achieves two additional security features, while preserving the same order of computational complexity and public values.

5.1 Security Analysis

So as to demonstrate that the proposed scheme provides computational security, we state the following two theorems.

Theorem 2. *In the proposed scheme, a group of participants whose number is less than the threshold t, do not gain any information about any of the secrets $S_j, 1 \leq j \leq m$.*

Proof. To prove this assertion, we assume that there are at most $t-1$ participants who conspire to discover the secret S_j in one stage. To achieve this goal, the collaborating participants need to recover t points of $f_j(x)$ (as defined in 3). However, they have at most $t-1$ points of it. Since the secret polynomial coefficients are randomly chosen from $GF(p)$ with a uniform distribution, the secret takes all the values in $GF(p)$ with the same probability when the unknown point of $f_j(x)$ varies over $GF(p)$ (p is a large prime number). Hence, the cheaters (collaborating participants) obtain no information about the secret. From the other side, since $\mathbb{T}(x)$ is a computationally secure l-AONT, knowing at most $k+s-l$ bits from $\mathbb{T}(x)$, makes it computationally infeasible to gain any information about x. Hence, the public values do not leak any information about the shares of non-attendant participants.

Theorem 3. *In the proposed scheme, there is no information leakage from reconstructed secrets to the non-disclosed ones.*

Proof. Since all coefficients of every secret polynomial (including the secrets) are chosen uniformly at random from $GF(p)$, the shares generated by one of them are independent from those generated by the others. Hence, there is no information leakage from the reconstructed secret(s) and the revealed shares to the non-disclosed ones. The two above theorems ensure that the proposed scheme offers the desired level of security.

5.2 Comparative Results

Here, we compare the proposed MSS scheme with that of He and Dawson from the following points of view: Number of public values and share size, the computational complexity of the scheme, and security features.

Before investigating the special case of He and Dawson's scheme [7], we should remark that the schemes in [8] and [12] focus on reconstructing the secrets simultaneously. However, the scheme proposed in [7] and that of this paper have the privilege of recovering the secrets in different stages. Hence, it does not seem reasonable to compare these two types of multi-secret sharing schemes. In addition, in [10] there is an increase in the share size as a consequence of applying the Chinese Reminder Theorem on different sub-shadows. Indeed, in this scheme, the share size is equal to the sum of the secret sizes.

The comparison results between the proposed MSS scheme and [7] are presented in Table 1. It could be inferred from the results that the share size in both schemes is nearly the same as the secret size. Note that if the number of shared secrets in the proposed scheme be less than $m = \lfloor k/l \rfloor$, the share size would be smaller than the secret size. Besides, the number of public values of the proposed scheme has the same order as in [7]. Precisely speaking, it is two times of the number of public values in the scheme presented in [7].

The scheme proposed by He and Dawson employs a one-way function in addition to the Shamir's threshold secret sharing scheme. However, the proposed MSS scheme based on l-AONT approach utilizes an all-or-nothing transform together with the Shamir's secret sharing scheme. The construction of the applied AONT is based on a one-time pad encryption and a resilient function. Also, resilient functions have structures based on one-way functions [14]. As a consequence, both schemes make use of similar structures with the same number of times (Tabel 1).

Table 1. Comparison of the proposed scheme with that of He & Dawson

	He-Dawson's scheme	Prposed scheme
share size to secret size ratio	1	$m \times l/k \lessapprox 1$
No. of public values	$m \times n$	$(2m-1) \times n$
Computational complexity	$m\times$ Shamir's scheme $(m-1) \times n$ one-way function	$m\times$ Shamir's scheme $m \times n$ AONT
Shadow memory	$m \times n$	n

In the MSS schemes proposed in [7] and [17], once a number of bits of a participant's master-shadow reveals, the security of all of his her sub-shadows gets compromised. This is a consequence of deriving different sub-shadows from a master-shadow. This problem is inhibited in our scheme by deriving different sub-shadows independently.

As a final point, we indicate that in the He and Dawson's scheme, once a participant receives his/her master shadow y_i, he/she has to compute all sub-shadows $f(y_i), f^2(y_i), \dots, f^{m-2}(y_i), f^{m-1}(y_i)$ since $f^{m-1}(y_i)$ is supposed to be the first sub-shadow he/she would use. This is implicitly equivalent to an increase in the share size. That is, each shareholder needs $m \times k$ bits of memory (shadow memory) to store m units of k-bit sub-shadow. The larger the share size, the more susceptible shares to the information leakage. On the other side, once a sub-shadow is exposed, all of the subsequent sub-shadows, derived from it, get revealed. This is resulted from applying a one-way function to the participants master shadows in order to derive their different sub-shadows. The proposed scheme brings this problem to an end by independently generating the sub-shadows.

6 Conclusions

In this paper, the authors have considered secret sharing schemes with several secrets and proposed a new approach, based on l-AONT, for multi-stage secret sharing schemes. Under these functions, any bit string is converted to an exposure-resilient one, that is, having "almost all" bits of the output, one could not obtain any information about the input. Using this property, the authors have reduced the share size such that the total size of sub-shadows assigned to a participant for reconstructing different secrets has become as small as a secret size. To the best of author's knowledge, this is the first time that l-AONTs (resilient functions) are used to realize secret sharing schemes. The proposed MSS scheme is compared with that of He and Dawson. The results indicate that the new scheme has removed the security drawbacks in their scheme, which are resulted from deriving different sub-shadows by applying a one-way function on the previous sub-shadow. Still, the number of public values and the computational complexity of the scheme have the same order as those of [7].

References

1. Shamir, A.: How to Share a Secret. Commun. ACM 22(11), 612–613 (1979)
2. Blakley, G.R.: Safeguarding Cryptographic Keys. In: AFIPS, National Computer Conference, vol. 48, pp. 313–317 (1979)
3. Stadler, M.: Publicley Verifiable Secret Sharing. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 190–199. Springer, Heidelberg (1996)
4. Ogata, W., Kurosawa, K.: Optimum Secret Sharing Scheme Secure against Cheating. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 200–211. Springer, Heidelberg (1996)
5. Barwick, S.G., Jackson, W.A., Martin, K.M.: Updating the Parameters of a Threshold Scheme by Minimal Broadcast. IEEE Transactions on Information Theory 51(2), 620–633 (2005)
6. Stinson, D.R.: An Explication of Secret Sharing Schemes. Des., Codes, Cryptogr. 2, 357–390 (1992)
7. He, J., Dawson, E.: Multi-Stage Secret Sharing Scheme Based on One-way Function. Electronic Letters 30(19), 1591–1592 (1994)
8. Chien, H.Y., Jan, J.K., Tseng, Y.M.: A Practical (t, n) Multi-Secret Sharing Scheme. IEICE Transactions on Fundamentals E83-A(12), 2762–2765 (2000)
9. Runhua, S., Liusheng, H., Yonglong, L., Hong, Z.: A Threshold Multi-Secret Sharing Scheme. In: IEEE International Conference on Networking, Sensing and Control, ICNSC 2008, pp. 1705–1707 (2008)
10. Chan, C.W., Chang, C.C.: A Scheme for Threshold Multi-Secret Sharing. Applied Mathematics and Computation 166, 1–14 (2006)

11. Harn, L.: Comment: Multistage Secret Sharing based on One-way Function. Electronics Letters 31(4), 262 (1995)
12. Yang, C.C., Chang, C.C., Hwang, M.S.: A (t, n) multi-secret sharing scheme. Applied Mathematics and Computation 151(2), 483–490 (2004)
13. Rivest, R.: All-or-Nothing Encryption and the Package Transform. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 210–218. Springer, Heidelberg (1997)
14. Canetti, R., Dodis, Y., Halevi, S., Kushilevitz, E., Sahai, A.: Exposure-Resilient Functions and All-or-Nothing Transforms. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 453–469. Springer, Heidelberg (2000)
15. Karnin, E.D., Greene, J.W., Hellman, M.E.: On Secret Sharing System. IEEE Transaction on Information Theory 29(1), 35–41 (1983)
16. Chor, B., Friedman, J., Goldreich, O., Hastad, J., Rudich, S., Smolensky, R.: The Bit Extraction Problem or t-resilient Functions. In: FOCS, pp. 396–407 (1985)
17. He, J., Dawson, E.: Multisecret-Sharing Scheme Based on One-way Function. Electronic Letters 31(2), 93–95 (1995)