A NEW SECRET SHARING SCHEME ADVERSARY FUZZY STRUCTURE BASED ON AUTOMATA

A. SAEIDI RASHKOLIA, M. M. ZAHEDI AND M. H. DEHKORDI

Abstract. In this paper, we introduce a new verifiable multi-use multi-secret sharing scheme based on automata and one-way hash function. The scheme has the adversary fuzzy structure and satisfy the following properties: 1) The dealer can change the participants and the adversary fuzzy structure without refreshing any participants' real-shadow. 2) The scheme is based on the inversion of weakly invertible finite automata and its security depends on the properties of the one-way hash functions. 3) The scheme does not encounter time-consuming computations like discrete logarithm problem. 4) The validity of the transmitted data can be verified by the combiner and participants. 5) Every participant has only one reusable real-shadow, whereas the most of other existing schemes have more than one shadow. In addition, the proposed scheme which is based on automata has all the properties of a perfect scheme. Finally, the comparisons among other schemes and our scheme prove the efficiency of our scheme.

1. Introduction

Automata theory, a natural model of cryptosystems, is a mathematical theory, which investigates behaviour and structure, and their relationship with discrete and digital systems. In studying cryptosystems, e.g. the FAPKC4 [16], on the basis of automata, the invertibility of finite automata has a major role. The security of all cryptosystems based on the invertibility theory of finite automaton depends on the difficulties of inversion of nonlinear finite automata [17].

A secret sharing scheme allows to divide the secret S into different pieces or shares given to a set of participants C so that only certain qualified subsets of participants are able to recover the secret using their respective shares. The set of all qualified subsets of participants is called the access structure which corresponds to S. In addition, secret sharing schemes are designed to protect secret information from getting lost or destroyed, or from falling into wrong hands [2, 4, 5, 18]. In 1979, Blakley [1] and Shamir [13] independently suggested a scheme, which is known as the (t, n)-threshold secret sharing scheme. Secret sharing schemes have recently found a variety of applications in areas like e-voting schemes, access control systems, digital cash protocols, etc. These applications can be usefully carried out using a secret sharing scheme realizing adversary structure. This method comprises sharing

Received: April 2017; Revised: June 2017; Accepted: September 2017

Key words and phrases: Secret sharing, Adversary fuzzy structure, One-way hash function, Finite automaton, Weakly invertible.

a secret among a finite set of participants so that only certain pre-specified subsets of participants are not able to recover the secret. A number of secret sharing schemes based on adversary structure have been put forward; for instance, Sun and Shieh [14, 15] have proposed a graph-based secret sharing scheme realizing adversary structure and Guo and Ma [6] have proposed one called GM scheme. In addition, Qin et al have suggested QDW scheme, a secret sharing scheme combining threshold and adversary structure [12]. There are a number of problems in most secret sharing schemes adversary structure are as follows [3, 7, 9, 8, 10]:

(1) In the previous secret sharing adversary structure schemes there is not any algorithm for identifying access and adversary structure.
(2) Because of efficiency, security and the cost of communications over secure channel, each participant should keep more than one real-shadow with small size in a practical secret sharing scheme.
(3) In each secret sharing session, only one secret can be shared; therefore, they are not multi-secret sharing schemes.
(4) Since the schemes are not multi-use, when one secret is reconstructed, the dealer must re-distribute fresh real-shadows to every participant over channel.
(5) Cheating by dealer and participant cannot be detected; therefore, the participants cannot verify recovering a unique secret; in other words, the schemes are not verifiable secret sharing schemes.
(6) Without updating any participants' real-shadow, the dealer cannot dynamically change the participants' set or adversary structure.
(7) A secret sharing scheme with adversary fuzzy structure, which can solve all these problems, was not previously available.

In this paper, a fuzzy set specifies the access and adversary structure of scheme. In fact, a new verifiable multi-secret sharing scheme adversary fuzzy structure is presented based on the one-way hash function and automata, in which every participant must keep only one real-shadow which its size is the same as the size of secret. In this scheme, based on automata, new secrets can be shared; and the participant set and the adversary structure can be dynamically changed without refreshing any participants' real-shadow. This scheme is a multi-use secret sharing one with the advantage of better verifiability and fewer real-shadows preserved by every participant compared to other schemes with adversary structures.

The rest of the paper is organized as follows. In Section 2, some preliminaries and basic definitions will be provided. The proposed secret sharing scheme based on fuzzy structure will be presented in Section 3. The analysis and discussions of the proposed scheme will be presented in Section 4, and some conclusions are given in Section 5.

2. **Preliminaries**

2.1. **Automata** [17]**.** For a finite set X, we show X^n the set of words of length n, with $n \in N_0$, and $X^0 = \{\varepsilon\}$, where ε shows the empty word. We will also use $X^* = \cup_{n\geq 0} X^n$, the set of all finite words and X^ω will denote the set of infinite words.

Definition 2.1. A finite automaton is a quintuple $(X, Y, S, \delta, \lambda)$, where:

(1) X is a nonempty finite set called the input alphabet of the finite automaton;
(2) Y is a nonempty finite set called the output alphabet of the finite automaton;
(3) S is a nonempty finite set called the set of states of the finite automaton;
(4) δ is a function from $S \times X$ to S called the state transition function of the finite automaton;
(5) λ is a function from $S \times X$ to Y called the output function.

Let $M = (X, Y, S, \delta, \lambda)$ be a finite automaton. we expand the domain of δ to $S \times X^*$ as follows. For any state s_0 in S and any $n(> 0)$ input letters $x_0, x_1, \ldots, x_{n-1}$ in X, we compute recurrently states $s_1, \ldots, s_n$ in S by $s_{i+1} = \delta(s_i, x_i), i = 0, 1, \ldots, n-1$, and define $\delta(s_0, x_0x_1 \ldots x_{n-1}) = s_n$. In the case of $n = 0$, we define $\delta(s_0, \varepsilon) = s_0$. We expand the domain of λ to $S \times (X^* \cup X^\omega)$ and the range of λ to $Y^* \cup Y^\omega$ as follows. For any state s_0 in S and any $n(> 0)$ input letters $x_0, x_1, \ldots, x_{n-1}$ in X, we define $\lambda(s_0, x_0x_1 \ldots x_{n-1}) = y_0y_1 \ldots y_{n-1}$. In the case of $n = 0$, we define $\lambda(s_0, \varepsilon) = \varepsilon$. For any state s_0 in S and any infinite input letters $x_0, x_1, \ldots$ in X, we define $\lambda(s_0, x_0x_1 \ldots) = y_0y_1 \ldots$, where $y_i = \lambda(\delta(s_0, x_0x_1 \ldots x_{i-1}), x_i), i = 0, 1, \ldots$. In addition, suppose that $m, n(m < n)$ are two integer numbers. To simplify the notions we use $\|_{i=m}^{n} x_i$ instead of the word $x_mx_{m+1} \ldots x_n$.

Definition 2.2. Let $M = (X, Y, S, \delta, \lambda)$ and $M' = (Y, X, S', \delta', \lambda')$ be two finite automaton. For any states s in S and s' in S', if for any $\alpha \in X^\omega$ there exists $\alpha_0 \in X^*$ such that $\lambda'(s', \lambda(s, \alpha)) = \alpha_0\alpha$ and $\mid \alpha_0 \mid = \tau$, where τ is a non-negative integer and (s', s) is called a match pair with delay τ.

Definition 2.3. A finite automaton $M = (X, Y, S, \delta, \lambda)$ is said to be weakly invertible with delay τ, if $\lambda(s, \|_{i=0}^{\tau} x_i)) = \lambda(s, \|_{i=0}^{\tau} x_i{}')$ then $x_0 = x_0'$, for all $s \in S$, for all $\|_{i=0}^{\tau} x_i$ and $\|_{i=0}^{\tau} x_i{}' \in X^{\tau+1}$,

Definition 2.4. Let $M = (X, Y, S, \delta, \lambda)$ and $M' = (Y, X, S', \delta', \lambda')$ be two finite automaton. M' is called a weak inverse with delay τ of M, if for any s in S there exists s' in S' such that (s', s) is a match pair with delay τ.

Theorem 2.5. *If $M = (X, Y, S, \delta, \lambda)$ is weakly invertible with delay τ, then there exists $M' = (Y, X, S', \delta', \lambda')$ such that M' is a weak inverse with delay τ of M, i.e., for any $x_0, x_1, \ldots, \in X$ and given any state $s_0 \in S$ there exists $s_0' \in S_0'$ and $\lambda'(s_0', \lambda(s_0, x_0x_1 \ldots)) = x_0'x_1' \ldots x_{\tau-1}'x_0x_1 \ldots$* [17].

2.2. **Secret Sharing Scheme** [6]**.** Let $C = \{C_i\}_{i=1}^{n}$ be a set of n participants. The dealer (D) shares the secret S between participants of C. The set $E \subseteq C$ is called a qualified subset of participants if the shared secret can be reconstructed by combining the real-shadows of participants of E. The set $E \subseteq C$ is called an unqualified subset of participants if the shared secret cannot be reconstructed by combining the real-shadows of participants of E. The set of all qualified subsets of participants is called the access structure which corresponds to S.

2.3. **Fuzzy Sets** [20]**.**

Definition 2.6. A fuzzy subset of set M is a function from M into $[0, 1]$.

Definition 2.7. Let μ be a fuzzy subset of a set M. For $t \in [0, 1]$, the set

$$\mu_t = \{E \in M \mid \mu(E) \geq t\}$$

is called a level subset of M.

3. The Proposed Scheme

In this section, a new Multi-secret Sharing Scheme Adversary Fuzzy Structure is presented using inversion of automaton and a one-way hash function.

Definition 3.1. Let C be a set of n participants and μ be a fuzzy subset of the set 2^C where 2^C is the power set of C. A fuzzy access structure Ψ_t is a subset of μ_t where $t \in [0, 1]$, with the following property: If $E \in \Psi_t$ and $E \subset F \subseteq C$, $E \neq F$, then $\mu(E) < \mu(F)$.

Using the above definition, the access structure Ψ_t should satisfy the monotone increasing property. Thus, it has minimal subsets and the access structure Ψ_t can be uniquely determined by the family of its minimal subsets.

Definition 3.2. For a given fuzzy access structure Ψ_t on the set of participants C, the corresponding minimal access structure is denoted by

$$(\Psi_t)_{min} = \{E \in \Psi_t \mid F \nsubseteq E, \text{ for all } F \in \Psi_t - \{E\}\}.$$

Definition 3.3. An adversary fuzzy structure Υ_t is a subset of $(\mu_t)^c$ where $t \in [0, 1]$ and $(\mu_t)^c = 2^C - \mu_t$, with the following property: If $E \in \Upsilon_t$ and $F \subset E \subseteq C, E \neq F$, then $\mu(F) < \mu(E)$.

Using the above definition, the adversary fuzzy structure Υ_t should satisfy the monotone decreasing property. Thus, it has maximal subsets and the adversary fuzzy structure Υ_t can be uniquely determined by the family of its maximal subsets.

Definition 3.4. For a given adversary fuzzy structure Υ_t on the participants set C, the corresponding maximal adversary structure is denoted by

$$(\Upsilon_t)_{max} = \{E \in \Upsilon_t \mid E \nsubseteq F, \text{ for all } F \in \Upsilon_t - \{E\}\}.$$

Definition 3.5. Υ_t is a secret sharing scheme adversary fuzzy structure if it satisfies the following two properties:

(1) Reconstruction property: any subset of participants belongs to $(\Upsilon_t)^c = 2^C - \Upsilon_t$ can recover the secret.

(2) Privacy property: any subset of participants belongs to Υ_t cannot recover the secret.

In the case $t = 1$, secret sharing scheme adversary fuzzy structure Υ_t can be trivially constructed. In this scheme, no participant will receive a real-shadow from dealer and the secret will be kept secret. Further, if $t = 0$, then the secret would not be completely secret. Therefore, a nontrivial adversary fuzzy structure Υ_t is an adversary fuzzy structure for which $t \neq 1$ and $t \neq 0$. In this paper, we suppose that Υ_t is a non-trivial adversary fuzzy structure on C.

3.1. **Starting Phase.** Suppose that X, Y are two vector spaces over the finite field $GF(q)$ of dimension l whose vectors are represented by column vectors. Let Υ_t be a adversary fuzzy structure on the set $C = \{C_1, C_2, \dots, C_n\}$ of participants. Let $S = \{S_1, S_2, \dots, S_R\}$ be a set of R secrets to be shared among n participants where each S_i is a column vector in Y. The dealer D, randomly chooses n distinct vectors, $\{d_1, d_2, \dots, d_n\}$ from vector spaces over $GF(q)$ of dimension l, and sends d_i to C_i as her/his real-shadow over secure channel. The dealer D creates a notice board (NB) used to store necessary public values, and it is openly readable to all participants, but only D can modify or update the contents of the board. Then, D Publishes a suitable secure one-way hash function H, which maps an input vector x from the vector spaces over $GF(q)$ of arbitrary finite dimension to an output vector $H(x)$ from the vector spaces over $GF(q)$ of a fixed dimension l. Finally, D considers the operation "$\bowtie$" such that

$$x = [x_1\ x_2\ \dots\ x_m]^t,\ y = [y_1\ y_2\ \dots\ y_n]^t,$$

$$x \bowtie y = [x_1\ x_2\ \dots\ x_m\ \ y_1\ y_2\ \dots\ y_n]^t.$$

3.2. **Construction Phase.** The dealer, D, performs the following steps:

(1) Using the Theorem 2.5 construct i) a finite weakly invertible automaton $A = (X, Y, Q, \zeta, \lambda)$ with delay τ; ii) the weak inverse $A' = (Y, X, Q', \zeta', \lambda')$ with delay τ of A'; iii) the generating states $q_0 \in Q$ and $q_0' \in Q'$ such that $\lambda'(q_0', \lambda(q_0, x_0x_1 \dots)) = x_{-\tau}x_{-\tau+1} \dots x_{-1}x_0x_1 \dots$ for any $x_0, x_1 \dots \in X$.

(2) Compute $(\Upsilon_t)_{max}$ the maximal adversary fuzzy structure which corresponds to the adversary fuzzy structure Υ_t.
Without loss of generality, let $(\Upsilon_t)_{max} = \{F_1, ..., F_{\tau'}\}$.

(3) Using the Theorem 2.5 construct i) a finite weakly invertible automaton $B = (Y, X, P, \eta, \kappa)$ with delay $\tau'(\tau < \tau')$; ii) the weak inverse $B' = (X, Y, P', \eta', \kappa')$ with delay τ' of B; iii) the generating states $p_0 \in P$ and $p_0' \in P'$ such that $\kappa'(p_0', \kappa(p_0, y_0y_1 \dots)) = y_{-\tau'}y_{-\tau'+1} \dots y_{-1}y_0y_1 \dots$ for any $y_0, y_1 \dots \in Y$.

(4) Generate random different vectors $\{y_k\}_{k=1}^{\tau'}$ of Y and $\{z_j\}_{j=0}^{\tau'}$, $\{x_k^i\}_{k=0}^{\tau'}$, $i = 1, 2, \dots, R$ of X such that

$$\kappa(p_0, S_i\|_{k=1}^{\tau'} y_k) = \|_{j=0}^{\tau'} H(z_j \bowtie x_j^i),\ i = 1, 2, \dots, R.$$

where

$$\|_{j=0}^{\tau'} x_j'^i = \|_{j=0}^{\tau'} H(z_j \bowtie x_j^i),\ i = 1, 2, \dots, R.$$

(5) Compute $DS_i = H(S_i \bowtie x_i^i)$ and publish $(\Upsilon_t)_{max}$, $\{H(z_j)\}_{j=1}^{\tau'}$ and DS_i on the NB.

(6) Generate a public vector z of X and publish it on the NB. Note that the dealer uses it to create the pseudo-shadows of all participants from their real-shadows.

(7) Compute the pseudo-shadow $H(d_i \bowtie z)$ of C_i, $i = 1, \dots, n$.

(8) Generate n random distinct vectors $\{e_k^i\}_{k=1}^n$,$i = 1, 2, \dots, n$ of X and $\{b_k^{ij}\}_{k=1}^n$, $j = 1, 2, \dots, \tau'$ of Y such that

$$\lambda(q_0, z_j\|_{k=1}^n e_k^i) = H(d_i \bowtie z)\|_{k=1}^n b_k^{ij},\ i = 1, 2, \dots, n,\ j = 1, 2, \dots, \tau',$$

where

$\|_{k=0}^{n} b_k^{\prime ij} = H(d_i \bowtie z)\|_{k=1}^{n} b_k^{ij},\ i = 1, 2, \ldots, n,\ j = 1, 2, \ldots, \tau'.$

(9) Constructs the table $T = (T_1, T_2, \ldots, T_n)^t$ such that the row $T_i = (a_{i1}, a_{i2}, \ldots, a_{i\tau'})$, for $i = 1, 2, \ldots, n$ and $\tau' = | (\Upsilon_t)_{max} |$, contains the information the dealer intends to distribute to participant C_i. Then compute a_{ij} as follows: if $C_i \in F_j$, then $a_{ij} = \emptyset$, otherwise, $a_{ij} = \|_{k=1}^{n} b_k^{ij}$. Finally publish $T_i = (a_{i1}, a_{i2}, \ldots, a_{i\tau'})$ on the NB for $i = 1, 2, \ldots, n$.

(10) Set the transition functions

$$\zeta'(q'_k, b_k^{\prime ij}) = q'_{k+1},\ k = 0, 1, \ldots, n-1$$

and

$$\eta'(p'_k, x_k^{\prime i}) = p'_{k+1},\ k = 0, 1, \ldots, \tau' - 1.$$

(11) Publish $\{q'_k\}_{k=0}^{n}$, $\{p'_k\}_{k=0}^{\tau'}$, $\{x_k^{\prime i}\}_{k=0}^{\tau'}$, $\{b_k^{ij}\}_{k=1}^{n}$ and output functions λ', κ' on the NB.

3.3. **Reconstruction Phase.** Let $\nu_t \subset \mu_t$, and suppose that its participants want to reconstruct the shared secrets. The participants of ν_t can use their pseudo-shadows and public information on the NB in order to reconstruct the secrets. In the reconstruction process, the participants of ν_t do not need to use their real-shadows; they only use their pseudo-shadows generated from their real-shadows. The combiner and participants of ν_t for reconstructing the secret $S_i, i = 1, 2, \ldots, R$ perform the following steps:

(1) Each participant $C_i \in \nu_t$ obtains z from NB, and uses his/her real-shadow d_i to compute pseudo-shadow $H(d_i \bowtie z)$. Then, C_i sends his/her pseudo-shadow to the combiner, who can be any participant of ν_t or somebody else.

(2) For each $C_i \in \nu_t$, he/she downloads $\{q'_k\}_{k=0}^{n}$, $\{b_k^{ij}\}_{k=1}^{n}$ and T_i from the NB and uses pseudo-shadow of C_i to compute z_j's corresponding to all non empty entities of T_i. Then, the combiner by calculating $\lambda'(q_0{}', \|_{k=0}^{n} b_k^{\prime ij}) = \|_{k=0}^{n} b_k^{''ij}$, obtains (according to step (1) of construction phase) $z_j = b_\tau^{''ij}$. Subsequently, he/she reconstructs each secret $S_i \in S$ by downloading $\{p'_k\}_{k=0}^{\tau'}$ and $\{x_k^{\prime i}\}_{k=0}^{\tau'}$ from NB, computes $\kappa'(p'_0, \|_{k=0}^{\tau'} x_k^{\prime i})) = \|_{k=0}^{\tau'} x_k^{''i}$ and obtains (according to step (3) of construction phase) $S_i = x_{\tau'}^{''i}$.

3.4. **Verification Phase.**

3.4.1. *Dealer Verification.* By downloading the row T_i from the NB and performing the following two steps:the participant C_i can verify that the dealer is a cheater or not

(1) Check which entities of T_i must be non empty according to adversary fuzzy structure Υ_t using the maximal adversary fuzzy structure $(\Upsilon_t)_{max}$. If the results are the same, go to the next step; otherwise, the dealer is a cheater.

(2) Calculate $\lambda'(q_0{}', \|_{k=0}^{n} b_k^{\prime ij}) = \|_{k=0}^{n} b_k^{''ij}$ by computing $H(d_i \bowtie z)$ from his/her real-shadow d_i and by downloading each non empty entity of T_i such as a_{ij}, and $\{q'_k\}_{k=0}^{n}$ from the NB. Now if $H(z_j) = H(b_\tau^{''ij})$, $(H(z_j)$ is published by

dealer in Step (5) of construction phase) then hash function H is valid. Because $z_j = b_{\tau}^{''ij}$. Otherwise, the dealer is a cheater.

Note that when participant C_i passes this step (2) for all non empty entities of T_i, then he/she can ensure that his/her pseudo-shadow $H(d_i \bowtie z)$ is valid. Now if the dealer wants to cheat in the non empty entity a_{ij} of C_i for the purpose that C_i recovers $b_{\tau}^{''ij}$ instead of z_j from it, he/she can replace $a_{ij} = \|_{k=1}^{n} b_k^{ij}$ with a fake value a'_{ij} in equation

$$\|_{k=0}^{n} b_k^{'ij} = H(d_i \bowtie z) \|_{k=1}^{n} b_k^{ij} = \lambda(q_0, z_j \|_{k=1}^{n} e_k^{i})$$

such that C_i computes $b_{\tau}^{''ij}$ from equation $\lambda'({q_0}', \|_{k=0}^{n} b_k^{'ij}) = \|_{k=0}^{n} b_k^{''ij}$ and equation $H(z_j) = H(b_{\tau}^{''ij})$ holds. Therefore, the dealer needs to find $b_{\tau}^{''ij}$ such that $b_{\tau}^{''ij} \neq z_j$ and $H(z_j) = H(b_{\tau}^{''ij})$, but it is computationally hard because H is a secure one-way hash function. Thus, for the purpose that $H(z_j) = H(b_{\tau}^{''ij})$ is verified by C_i, the dealer must replace the value $H(z_j)$ on the NB with the hashing fake value $H(b_{\tau}^{''ij})$ so that C_i cannot identify the fake value. But, the dealer can present only one value $H(z_j)$ on the NB in Step (5) of construction phase for each $j = 1, \ldots, \tau'$ and all participants can read this unique value from the NB, and use it to check the correctness of their non empty entities. Hence, all participants that have a non empty value in the jth entity of their related rows, can verify that they can recover the same z_j by using hash value $H(z_j)$ for each $j = 1, \ldots, \tau'$. Therefore, if all participants ensure that their pseudo-shadows are valid in the Step (2) of the above procedure, the dealer cannot be a cheater.

3.4.2. *Participants Verification.* The combiner can verify the validity of the pseudo-shadow $H(d_i \bowtie z)$ when he/she receives $H(d_i \bowtie z)$ from the C_i. The combiner downloads row T_i from the NB and only for one non empty value of T_i such as a_{ij} computes $b_{\tau}^{''ij}$ from equation $\lambda'({q_0}', \|_{k=0}^{n} b_k^{'ij}) = \|_{k=0}^{n} b_k^{''ij}$. Then, he/she compares $H(z_j)$ with $H(b_{\tau}^{''ij})$, if these two values are equal, the combiner can make sure from the properties of the one-way hash function that the pseudo-shadow $H(d_i \bowtie u)$ is valid and the participant C_i cannot be a cheater.

3.4.3. *Combiner Verification.* When each participant of ν_t receives the secret S_i from the combiner, he/she can verify the validity of S_i by checking the equation $DS_i = H(S_i \bowtie x_i^i)$, where DS_i has published in Step (5) of construction phase.

4. Scheme Analysis

4.1. **Security of the Scheme.** The security of the proposed scheme depends on the properties of the secure one-way hash function. Since the output vector of H has the same dimension as each secret, according to the properties of H, the following attacks are computationally hard.

(1) An adversary participant cannot compute z_j from the public values $H(z_j)$ and thus he/she cannot compute the secret S_i from $\kappa'(p'_0, \|_{j=0}^{m} H(z_j \bowtie x_j^i))$, and $H(S_i \bowtie x_i^i)$.

(2) Since the output and transition functions λ, ζ of automaton A and κ, η of automaton B are kept secretly by dealer, thus a adversary cannot access to z_j, $H(d_i \bowtie z)$ and S_i.

(3) The combiner cannot recover the real-shadow d_i of C_i from the submitted pseudo-shadow $H(d_i \bowtie z)$, because the hash function H is chosen secure. Therefore, any information cannot leak from one-way hash function H.

4.2. **Correctness of the Scheme.** The following theorem shows that the proposed scheme is a secret sharing scheme with adversary fuzzy structure.

Theorem 4.1. *Let Υ_t be a non-trivial adversary fuzzy structure on a set C of participants. Then, the scheme described in Section 3 is a secret sharing scheme with adversary fuzzy structure Υ_t.*

Proof. The theorem will be proved using Definition 3.5 by the following two properties:

(1) (Reconstruction property) Let $M \subseteq C$ and $M \notin \Upsilon_t$. We show that the participants of M can reconstruct all shared secrets. To prove this property, we require to show that the participants of M can reconstruct $z_1, z_2, \ldots, z_{\tau'}$ using their pseudo-shadows. Since, $M \notin \Upsilon_t$ and $(\Upsilon_t)_{max} = \{F_1, \ldots, F_{\tau'}\}$, we have $M \nsubseteq F_j$ for each $j = 1, \ldots, \tau'$. Hence, for each $j = 1, \ldots, \tau'$ there exists at least a $r_j (1 \leq r_j \leq n)$ such that $C_{r_j} \in M$ and $C_{r_j} \notin F_j$. Therefore according to Step (9) of the construction phase, for each $j = 1, \ldots, \tau'$ the entity $a_{r_j j}$ of the row T_{r_j} of the public table T is equal to

$$a_{r_j j} = \|_{k=1}^{n} b_k^{r_j j}.$$

Therefore, according to the Step (8) of the construction phase we have

$$\|_{k=0}^{n} b_k^{\prime r_j j} = H(d_{r_j} \bowtie z) \|_{k=1}^{n} b_k^{r_j j} = \lambda(q_0, z_j \|_{k=1}^{n} e_k^{r_j})$$

and so

$$\lambda'(q_0', \|_{k=0}^{n} b_k^{\prime r_j j}) = \|_{k=0}^{n} b_k^{''r_j j}$$

Now, using Theorem 2.5, and the Steps (1) and (8) of the construction phase, we have $z_j = b_\tau^{''r_j j}$, $j = 1, ..., \tau'$. Therefore, for each $j = 1, ..., \tau'$, there exists at least one participant of M such that z_j can be computed by his/her pseudo-shadow. Thus, the participants of $M \in (\Upsilon_t)^c$ can collect all partitions $z_1, z_2, \ldots, z_{\tau'}$ using their pseudo-shadows. Consequently, the participants of M, can reconstruct all secrets from eqution $\kappa'(p_0', \|_{j=0}^{\tau'} H(z_j \bowtie x_j^i)) = \|_{j=0}^{\tau'} x_j^{''i}$ and $S_i = x_{\tau'}^{''i}$, $i = 1, 2, \ldots, R$ using Theorem 2.5, and according to the Steps (3), (4) of the reconstruction phase.

(2) (Privacy property) Let $M \subseteq C$ and $M \in \Upsilon_t$,. We show that the participants of M cannot recover any secret. Since $M \in \Upsilon_t$, there exists a subset $F_j \in (\Upsilon_t)_{max}$ such that $M \subseteq F_j$. By Step (9) of the construction phase, for each participant $C_i \in F_j$ the entity a_{ij} of the row T_i of table T is empty. Hence according to Step (8) of the construction phase we have

$\lambda(q_0, z_j\|_{k=1}^n e_k^i) = H(d_i \bowtie z)$ which is a contradiction, because the length of words in both sides of equation is not equal.

Thus, no participant of F_j can reconstruct z_j using his/her pseudo-shadow. Therefore, the participants of $M \subseteq F_j$ cannot compute z_j, and so the participants of M cannot recover the secret. □

4.3. **Discussion.** Now, some important properties of the proposed scheme are discussed.

- The proposed scheme uses automaton and vector space such that every participant keeps only one real-shadow.
- The secret space has the same size as the shadow space, because each secret and each shadow belongs to vector spaces over $GF(q)$ of dimension l. In the special case $q = 2$, real and pseudo shadows and secrets are corresponds to some binary strings from $\{0, 1\}^l$.
- Our scheme is a multi-secret sharing scheme, because in each secret sharing session, several secrets can be shared.
- In this scheme, for every set of secrets and its related adversary fuzzy structure, the dealer randomly generates a public vector, which is used in the generation of pseudo-shadow of each participant $(H(d_i \bowtie z), i = 1, \ldots, n)$, and in sharing process, therefore the pseudo-shadow $H(d_i \bowtie z)$ of each participant C_i depends on the public parameter z and his/her real-shadow d_i. On the other hand, the real-shadow d_i cannot be revealed from $H(d_i \bowtie z)$ by the properties of the one-way hash function$H$. Thus, to share a new set of secrets, the dealer merely needs to generate a new vector z randomly, and will refresh some public information on the NB, while the participants do not need to refresh their real-shadows which shows that this scheme is multi-use.
- In our secret sharing scheme, adversary fuzzy structure Υ_t can be changed without updating the real-shadow of participants. Therefore, the dealer generates a new random vector z and he/she updates $(\Upsilon_t)_{max}$ and other information on the NB without refreshing the real-shadows of participants. In addition, if the dealer intends to add a new participant C_{new}, he/she can generate a random real-shadow d_{new} and send it to C_{new} over the secure channel. Old participants' real-shadows can remain unchanged. Therefore, in our scheme, the participants set and adversary fuzzy structure can be changed by updating public information on the NB without refreshing any participants' real-shadow.
- Since each participant in our scheme can verify the validity of other participants' pseudo-shadows as well as his/her own in the verification phase, cheating by the dealer or any participant can be detected. Therefore, it is a verifiable secret sharing scheme and the participants can verify that they can recover unique secrets.
- The high computational complexity of our scheme is based on the hash function and automaton.

Capability	GM [6]	QDW [12]	DY [5]	DA [3]	PLW [11]	WZX [19]	Our scheme
It has adversary fuzzy structure.	No	No	No	No	No	No	Yes
It uses Automata and vector spaces.	No	No	No	No	No	No	Yes
Each participant holds only one real-shadow.	No	No	Yes	Yes	Yes	Yes	Yes
The scheme is multi-use.	No	Yes	Yes	Yes	Yes	No	Yes
It can prevent the participants from cheating.	No	Yes	Yes	Yes	No	No	Yes
It is impossible for the dealer to cheating.	No	No	Yes	Yes	No	No	Yes
The real-shadow is reusable when participants are joining/quitting the group.	No	No	Yes	Yes	Yes	Yes	Yes

Table 1. The Comparison Among Some Secret Sharing and Our Scheme

- Tables 1 gives the results of comparison among the GM [6], QDW [12] , DY [5], DA [3], PLW [11], WZX [19] and our scheme. It shows that
  1. The scheme has the adversary fuzzy structures.
  2. It uses automata and vector spaces.
  3. Each participant holds only one real-shadow.
  4. The scheme is multi-use.
  5. It can prevent the participants from cheating.
  6. It is impossible for the dealer to cheating.
  7. The real-shadow is reusable when participants are joining/quitting the group.

5. Conclusion

In this paper, a new multi-use multi-secret sharing scheme with adversary fuzzy structure was proposed. The proposed scheme was based on the automaton and one-way hash function in which each participant has to keep only one real-shadow to share many sets of secrets. In this scheme, in order to reconstruct secrets, each involved participant only submits a pseudo-shadow computed from the real-shadow instead of the real-shadow. The length of each shadow is as short as that of each shared secret. Analysis shows that our scheme is computationally secure, efficient and verifiable scheme.

References

[1] G. R. Blakley, *Safeguarding cryptographic keys*, Proc. of the National Computer Conference, **48** (1979), 313–317.

[2] Y. F. Chen, Y. K. Chan, C. C. Huang, M. H. Tsai and Y. P. Chu, *A multiple-level visual secret-sharing scheme without image size expansion*, Inform. Sciences., **177(21)** (2007), 4696–4710.

[3] A. Das and A. Adhikari, *An efficientmulti-usemulti-secret sharing scheme based on hash function*, Appl. Math. Lett., **23(9)** (2010), 993–996.

[4] M. H. Dehkordi and S. Mashhadi, *An efficient threshold verifiable multi-secret sharing*, Comp. Stand. Inter., **30(3)** (2008), 187–190.

[5] M. H. Dehkordi and Y. Farzaneh, *A New Verifiable Multi-secret Sharing Scheme Realizing Adversary Structure*, Wireless. Pers. Commun., **82(3)** (2015), 1749–1758.

[6] Y. B. Guo and J. F. Ma, *Practical secret sharing scheme realizing generalized adversary structure*, J Comput. Sci Technol., **19(4)** (2004), 564–569.

[7] L. Harn, *Efficient sharing (broadcasting) of multiple secrets*, IEE. P-Comput. Dig. T., **142(3)** (1995), 237–240.

[8] J. He and E. Dawson, *Multi secret-sharing scheme based on one-way function*, Electron. Lett., **31(2)** (1995), 93–95.

[9] J. He and E. Dawson, *Multistage secret sharing based on one-way function*, Electron. Lett., **30(19)** (1994), 1591–1592.

[10] W. Jackson, K. Martin and C. O'Keefe, *On sharing many secrets*, Advances in Cryptology–Asiacrypt'94, (1995), 42–54.

[11] L. J. Pang, H. Li And Y. Wang, *An efficient and secure multi-secret sharing scheme scheme with general access structure*, Wuhan Univ. J. Nat. Sci., **11(6)** (2006), 1649–1652.

[12] H. Qin, Y. Dai and Z. Wang, *A secret sharing scheme based on (t, n) threshold and adversary structure*, Int. J. Inf. Secur., **8(5)** (2009), 379–385.

[13] A. Shamir, *How to share a secret*, Commun. Acm., **22(11)** (1979), 612–613.

[14] H. M. Sun and S. P. Shieh, *An efficient construction of perfect secret sharing schemes for graph-based structures*, Comput. Math. Appl., **31(7)** (1996), 129–135.

[15] H. M. Sun and S. P. Shieh, *Secret sharing schemes for graph-based prohibited structures*, Comput. Math. Appl., **36(7)** (1998), 131–140.

[16] R. Tao and S. Chen, *The generalization of public key cryptosystem FAPKC4*, Chinese. Sci. Bull., **44(9)** (1999), 784–790.

[17] R. Tao, Finite Automata and Application to Cryptography, Tsinghua University Press, Springer, 2008.

[18] M. Van Dijk, W. A. Jackson and K. M. Martin, *A general decomposition construction for incomplete secret sharing schemes*, Design. Code. Cryptogr., **15(3)** (1998), 301–321.

[19] Y. Wei, P. Zhong and G. Xiong, *A Multi-stage Secret Sharing Scheme with General Access Structures*, In 4th International Conference on Wireless Communications, Networking and Mobile Computing, IEEE, (2008), 1–4.

[20] L. A. Zadeh, *Fuzzy sets*, Inform. Control, **8(3)** (1965), 338–353.

Ali Saeidi Rashkolia, Department of Mathematics, Graduate University of Advanced Technology, Kerman, Iran
E-mail address: `a-saeidi@kgut.ac.ir`

Mohammad Mahdi Zahedi*, Department of Mathematics, Graduate University of Advanced Technology, Kerman, Iran
E-mail address: `zahedi_mm@kgut.ac.ir`

Masoud Hadian Dehkordi, School of Mathematics, Iran University of Science and Technology, Tehran, Iran
E-mail address: `mhadian@iust.ac.ir`

*Corresponding author