A Secure and Efficient General VSS Protocol*

ZHANG Fu-tai [1,2], ZHANG Fang-guo [1], WANG Yu-min [2]

[1](*School of Computer Science, Shanxi Normal University, Xi'an* 710062, *China*);

[2](*Key Laboratory on ISN, Xidian University, Xi'an* 710071, *China*)

E-mail: zhangfutai@263.net; ffttzhang@hotmail.com

Received July 5, 2001; accepted January 7, 2002

Abstract: Verifiable secret sharing (VSS) is a very important tool in cryptography and information security. Many threshold VSS schemes are available in the literature, but only a little attention has been paid to general VSS. In this paper, the problem of general verifiable secret sharing is considered. Based on a general secret sharing scheme, Feldman's VSS scheme is extended to the case of arbitrary monotone access structures. A secure and efficient general VSS protocol is proposed. The newly proposed protocol is non-interactive, and has the best information rate. It may have practical applications in many areas, such as key escrow, group oriented cryptography, and fault-tolerant secure computation etc.

Key words: secret sharing; verifiable secret sharing; access structure; Lagrange interpolation formula; discrete logarithm

Secret Sharing[1,2] is a fundamental notion for secure cryptographic design. In a Secret Sharing protocol, the dealer shares a secret among n participants such that only specified subsets of the whole participants' can later recover the secret. In the so called (k,n) threshold model, the sharing is done so that subsets of k or more participants can later reconstruct the secret, while subsets of at most $k-1$ participants have no information about it. In practical applications, ordinary secret sharing schemes have two common drawbacks. One is they cannot withstand cheating by a participant. A malicious participant may supply a fake share during secret reconstruction so that the other cooperators cannot recover the true secret. The other is they cannot withstand cheating by the dealer. The dealer may give false shares to some participants so that these participants will never recover the true secret. Verifiable Secret sharing (VSS) was first proposed by Chor *et al*.[3] to prevent cheating by the dealer. It was later farther studied in Refs.[4~7], and several secure and efficient VSS schemes were proposed. VSS schemes allow each participant to verify that his share is consistent with the other shares, and hence allow the honest participants to ensure that the secret to be reconstructed is unique. In Ref.[6], an efficient non-interactive verifiable secret sharing scheme was proposed (Feldman's VSS scheme). Pedersen presented a non-interactive and information-theoretic secure VSS scheme in Ref.[4]. Almost all solutions to verifiable secret sharing are threshold schemes. Gennaro pointed out in Ref.[5] the significance of finding non-threshold solutions to this problem. On one hand, the security of threshold schemes is based on the implicit assumption that all nodes of the network participating in the protocol have the same level of security. It implies that the corruption of one particular node is as likely as the corruption of

* Supported by the National Natural Science Foundation of China under Grant No.60073052 (国家自然科学基金); the National Research Foundation for the Doctoral Program of Higher Education of China under Grant No.2000070101 (国家教育部博士点基金)

ZHANG Fu-tai was born in 1965. He is a Ph.D. candidate in Xidian University. His research interests are cryptography and information security. **ZHANG Fang-guo** was born in 1972. He is a Ph.D. candidate in Xidian University. His research interests are cryptography and information security. **WANG Yu-min** was born in 1936. He is a professor and doctoral supervisor in Xidian University. His current research areas include information theory, communication and cryptography.

any other nodes in the network. This is not necessarily true. On the other hand, by initiating a theory of VSS over general access structures, the study of fault-tolerant secure computation can be generalized to more practical situations. In Ref.[5] he gave the first general verifiable secret sharing protocol. But the protocol has the following drawbacks: (1) it depends on the technique of cut and choose; (2) the verification algorithm needs interaction; (3) the number of secret shares a player H_j holds is $(Kn+1)n_j$, where K is the security parameter and n_j is the number of minimal authorized subset H_j belongs to. So the amount of secret information should be stored by each participant is very large, and the protocol is not suitable for practical use. In this paper, we will concentrate on the construction of secure and efficient general verifiable secret sharing protocol applicable to arbitrary access structures. Our solution will overcome the above drawbacks.

We organize the rest of the paper as follows. Section 1 gives Feldman's VSS protocol and a general secret sharing scheme as our building blocks. Our new general VSS protocol applicable to arbitrary access structures is presented in Section 2. The security and performance analysis of our new protocol appears in Section 3. At last, Section 4 is the conclusion.

1 Building Blocks

We will use Feldman's VSS scheme and a general secret sharing scheme as basic tools.

1.1 Feldman's VSS scheme

Feldman's VSS scheme is the first non-interactive VSS scheme without a trusted authority. Up to now it is the most efficient VSS scheme available.

The parameters are as follows: p is a prime number of length $l\geq 512$; q is a 160-bit prime divisor of $p-1$; g is an element of order q in $Z^{*}{}_{p}$. The triple (p,q,g) is public. k is the threshold, and n is the number of participants.

Distribution phase: the dealer D selects at random a polynomial $f(x)=\sum_{j=0}^{k-1}a_j x^j$ over Z_q such that $a_0=S$ is the secret that will be shared among n participants $P_1,P_2,\ldots,P_n$. He sends to each participant P_j a share $\sigma_j=f(j)\bmod q$ secretly, and then broadcasts the values $\alpha_j=g^{a_j}$ mod p for $j=0,1,2,\ldots,k-1$.

Verification phase: For $j=1,2,\ldots,n$, each participant P_j checks if $g^{\sigma_j}=\prod_{i=0}^{k-1}\alpha_i^{j^i}$ mod p. If not, the share σ_j is false.

Reconstruction phase: when k participants $P_1,P_2,\ldots,P_k$ cooperate to reconstruct the secret, each P_j broadcasts his share σ_j to the other cooperators, each cooperator can verify the validity of σ_j by checking $g^{\sigma_j}=\prod_{i=0}^{k-1}\alpha_i^{j^i}$ mod p. If all shares σ_j, $j=1,2,\ldots,k$, are valid, each cooperator can reconstruct the secret using the method of Lagrange interpolation.

This scheme can tolerate up to $(n-1)/2$ malicious faults including the dealer, and the secret is only computationally secure since the value $g^s=g^{a_0}$ mod p is leaked.

1.2 A general secret sharing scheme applicable to arbitrary monotone access structures

We give a general secret sharing scheme applicable to arbitrary access structures. The scheme is the foundation of our new general verifiable secret sharing scheme.

Let $GF(q)$ be an finite field of q elements with q a large prime. $S=GF(q)$ is the secret space. The participants of the system are a dealer D who holds secrets selected uniformly at random from $S=GF(q)$, a set of share-holders $H=\{H_{1,}H_{2,\ldots,}H_n\}$ who receive shares of a secret from the dealer, and a monotone access structure Γ on H who gives out which subsets of H can effectively reconstruct the shared secret. We denote by $\Gamma_0=\{A_{1,}A_{2,\ldots,}A_t\}$ the basis of Γ, that is the set of minimal elements of Γ under inclusion.

Before sharing a secret, the dealer *D* broadcasts to all participants the set *H* and the basis $\Gamma_0=\{A_1, A_2, \ldots, A_t\}$ of the access structure Γ.

Algorithm of sharing: the dealer *D* selects at random a polynomial $f(x)=a_0+a_1x+\ldots+a_nx^n$ of degree *n* over $GF(q)$, where *n* is the number of share-holders and $a_0=s$ is the secret to be shared among players $H_1, H_2, \ldots, H_n$. Next, *D* finds out a polynomial $f_i(x)$ of degree less than k+1 for minimal authorized subset $A_i=\{H_{i1}, H_{i2}, \ldots, H_{ik}\}\in\Gamma_0$ using the k+1 points $(i_1, f(i_1)), (i_2, f(i_2)), \ldots, (i_k, f(i_k))$ and $(0,s)$ according to Lagrange interpolation formula, and computes $f_i(n+1)$ for each $i=1,2,\ldots,t$. At last, *D* sends $f(j)$ to player H_j secretly for $j=1,2,\ldots,n$, and broadcasts to all players the values $f_1(n+1)$, $f_2(n+1)$,…, and …, $f_t(n+1)$. Here $f(j)$ is the share of H_j with respect to secret *s*.

Algorithm of reconstruction: let *A* be any authorized subset of *H* and $A_j=\{H_{j1},, H_{j2}, \ldots, H_{jk}\}$ be the minimal authorized subset contained in *A*. Each player H_{jm} broadcasts his share $f(j_m)$ to all the other players in *A*. When all shares of players in A_j are collected, the secret *s* can then be reconstructed using the k+1 points $(j_1, f(j_1)), (i_2, f(j_2)), \ldots, (j_k, f(j_k))$ and $(n+1, f_j(n+1))$according to Lagrange interpolation formula. But for any unauthorized subset *B* of *H*, it is impossible to reconstruct the secret since the players in *B* cannot collect all shares of any minimal authorized subset.

This general secret sharing scheme has three obvious advantages over the others. Firstly, it is applicable to any access structures. Secondly, it has a high information rate. Finally, it has a simple algebraic structure similar to Shamir's threshold scheme.

2 A New General VSS Protocol Applicable to Arbitrary Monotone Access Structures

2.1 Parameters

As in Section 1.1, *p*, *q* are large primes such that $q|(p-1)$. *g* is a generator of the unique subgroup of Z_p^* with order *q*.

The secret space is $S=Z_q$(or $GF(q)$). The share space is also Z_q .The participants of the system are a dealer *D* and a set of *n* players (share-holders) $H=\{H_1, H_2, \ldots, H_n\}$. Γ is an arbitrary monotone access structure on *H* and $\Gamma_0=\{A_1, A_2, \ldots, A_t\}$ is its basis.

Based on the two schemes described in Section 1, we will present a new general verifiable secret sharing scheme applicable to arbitrary access structures.

2.2 Algorithm of sharing

There are two phases in this algorithm. One is share distribution and the other is share verification.

share distribution phase: In this phase, the dealer acts as in the sharing phase of the general secret sharing scheme in Section 1.2 except that he publishes the values $c_j=g^{a_j}$ (mod *p*), $j=0,1,\ldots,n$, and $d_j=g^{s_j}$ (mod *p*), $j=1,\ldots,n$, where $s_j=f(j)$ is the secret share of player H_j.

share verification phase: every one can check if

$$d_j=\prod_{k=0}^{n}(c_k)^{j^k} \text{ (mod } p\text{)}, j=1,\ldots,n, \text{ and } \quad g^{f_i(n+1)}=(c_0)^{\frac{\prod_{m=1}^{k}(n+1-i_m)}{\prod_{m=1}^{k}(-i_m)}}\prod_{j=1}^{k}(d_{i_j})^{\frac{(n+1)\prod_{m=1,m\neq j}^{k}(n+1-i_m)}{i_j\prod_{m=1,m\neq j}^{k}(i_j-i_m)}} \text{ (mod } p\text{)}$$

for any minimal authorized subset $A_i=\{H_{i1}, H_{i2}, .., H_{ik}\}\in\Gamma_0$, $i=1,\ldots,t$. Since these verification can be executed by any one who knows the public information of the sharing scheme, we may call this procedure the public verification. Each player H_j can verify the validity of his share by checking $d_j=g^{s_j}$ (mod *p*), $j=1,\ldots,n$. We call this procedure the private verification.

If the public verification fails (that is some of the equations in public verification do not hold.), the dealer is considered disqualified, and the players will abort from the sharing protocol. Otherwise, we say the public verification is successful. If the private verification for some player H_j fails, H_j should broadcast a complaint to the dealer as well as his false share received from the dealer. In response to H_j's complaint, the dealer broadcast to all players the correct share s_j such that $d_j = g^{s_j}$ (mod p). If the subset of players who complain the dealer contains a minimal authorized subset, the dealer is also considered disqualified, and the protocol stops. Otherwise we say the private verification is successful. The verification is said successful if both the public and private verifications are successful. It is believed that a secret s has been shared among the n players over the access structure Γ when the verification is successful.

2.3 Algorithm of reconstruction

If the verification phase proves the dealer is not disqualified, there must be a unique secret which has been shared among the n players based on the monotone access structure Γ.

To reconstruct the shared secret, each player H_j broadcast his secret share s_j to all the other players. Every one can verify the validity of s_j by checking $d_j = g^{s_j}$ (mod p). If the equation fails to hold, then cheating by player H_j is detected. When the correct shares of all players in a minimal authorized subset are collected, the shared secret s can be determined using Lagrange interpolation formula as in Section 1.2.

2.4 Correctness

The correctness of share distribution and secret reconstruction is obvious. We only need to prove the correctness of share verification.

Lemma 1. Verification is successful if and only if the dealer follows the protocol correctly.

Proof. Suppose the dealer follows the protocol properly, then there is a polynomial $f(x)$ of degree n such that $s_j=f(j)$, $j=1,\ldots,n$, and the point $(n+1,f_i(n+1))$ is on the polynomial determined by the $k+1$ points $(i_1,f(i_1)),(i_2,f(i_2)),\ldots,(i_k,f(i_k))$ and $(0,s)$ using Lagrange interpolation formula, $i=1,\ldots,t$, where $A_i=\{H_{i1},H_{i2},\ldots,H_{ik}\}\in\Gamma_0$ is a minimal authorized subset. This implies that

$$s_j = f(j) = \sum_{k=0}^{n} a_k j^k, \quad f_i(n+1) = s\frac{\prod_{m=1}^{k}(n+1-i_m)}{\prod_{m=1}^{k}(-i_m)} + \sum_{j=1}^{k}(f(i_j)\frac{(n+1)\prod_{m=1,m\neq j}^{k}(n+1-i_m)}{i_j\prod_{m=1,m\neq j}^{k}(i_j-i_m)}.$$

So we have $d_j = g^{s_j} = g^{f(j)} = \prod_{k=0}^{n} g^{a_k j^k} = \prod_{k=0}^{n}(c_k)^{j^k}$ (mod p), $j=1,\ldots,n$, and

$$g^{f_i(n+1)} = (c_0)^{\frac{\prod_{m=1}^{k}(n+1-i_m)}{\prod_{m=1}^{k}(-i_m)}} \prod_{j=1}^{k}(d_{i_j})^{\frac{(n+1)\prod_{m=1,m\neq j}^{k}(n+1-i_m)}{i_j\prod_{m=1,m\neq j}^{k}(i_j-i_m)}} \text{ (mod } p\text{)}, \ i=1,\ldots,t.$$

On the other hand, if $d_j = g^{s_j} = \prod_{k=0}^{n}(c_k)^{j^k}$ (mod p) for each $j=1,\ldots,n$, we have $s_j = \sum_{k=0}^{n} a_k j^k = f(j)$ (in Z_q). The equation $g^{f_i(n+1)}=(c_0)^{\frac{\prod_{m=1}^{k}(n+1-i_m)}{\prod_{m=1}^{k}(-i_m)}}\prod_{j=1}^{k}(d_{i_j})^{\frac{(n+1)\prod_{m=1,m\neq j}^{k}(n+1-i_m)}{i_j\prod_{m=1,m\neq j}^{k}(i_j-i_m)}}$ (mod p), implys that

$$f_i(n+1)=s\frac{\prod_{m=1}^{k}(n+1-i_m)}{\prod_{m=1}^{k}(-i_m)}+\sum_{j=1}^{k}(s_j\frac{(n+1)\prod_{m=1,m\neq j}^{k}(n+1-i_m)}{i_j\prod_{m=1,m\neq j}^{k}(i_j-i_m)}\quad \text{(in } Z_q\text{)}.$$

Hence the point (n+1, $f_i(n+1)$) is on the polynomial determined by the k+1 points ($i_1,f(i_1)$),($i_2,f(i_2)$),…,($i_k,f(i_k)$), and (0,s) using Lagrange interpolation formula. This proves that the dealer follows the protocol properly.

3 Security and Performance Analysis

3.1 Security analysis

We suppose a strong admissible adversary[5]. That means the adversary can corrupt all but one player in each authorized subset. The only constraint on this adversary is that at least one authorized subset must remain pure i.e. composed of all uncorrupted players. Such adversary is the strongest possible.

Theorem 1. If the verification is successful, the dishonest players who supply fake shares in reconstruction phase can be effectively detected.(This is obvious.)

Theorem 2. The proposed general VSS protocol is secure against a strong admissible adversary under the assumption that computing discrete logarithm in $GF(p)$ with respect to base g is infeasible.

Proof. If the verification is successful, there must be a unique secret s which has been shared among the n players over the access structure Γ. According to the definition of strong admissible adversary, for each minimal authorized subset A_j, there must be some shares of players in A_j that are unknown to the adversary. Since computing discrete logarithm in $GF(p)$ with respect to the base g is infeasible, the adversary cannot compute these unknown shares. So the adversary cannot use the reconstruction algorithm to recover the secret. Hence he gets no information about the shared secret except the public information. Furthermore, the shared secret can be effectively reconstructed by the pure authorized subsets since players in such authorized subsets are all honest and hold correct shares of the shared secret.

Similar to Feldman's VSS scheme, the shared secret s is computational secure since the value g^s(mod p) is revealed as part of the public information.

There is a drawback in the security aspect of our newly proposed general VSS protocol: the polynomial $f_i(x)$ determined for minimal authorized subset $A_i=\{H_{i1},H_{i2},\ldots,H_{ik}\}$ may have a degree less than k. In this case, less than k correct shares of A_i will be enough for reconstruct the shared secret. How to overcome this drawback is a problem remains to be solved.

3.2 Performance

First, notice that our new general VSS protocol is applicable to arbitrary monotone access structures. In practice, the degree of the polynomial $f(x)$ can be decreased to m–1, where m is the largest cardinality of minimal authorized subsets. If Γ is a threshold access structure with threshold k, the degree of $f(x)$ will be k–1. In this case, all $f_i(x)$ will be the same as $f(x)$, and there is no need for the dealer to compute $f_i(n+1)$. This will exactly result in Feldman's VSS scheme. So Feldman's VSS scheme can be looked as a special case of our new general VSS protocol.

Compared with Genarro's general VSS scheme[5], our new protocol has the following advantages. (1) It has a simpler structure. The structure of our new protocol is similar to that of Feldman's VSS scheme. It is based on Lagrange interpolation of polynomials over finite field. (2) It does not rely on the technique of cut and choose which is very inefficient. (3) The amount of data that must be kept secret for each player is greatly decreased. In our protocol, each player just needs to hold one secret share of the same length as the shared secret. So its information rate is the best. (4) The verification phase of our new protocol does not need any interaction. Therefor our new protocol overcomes all the drawbacks of Gennaro's general VSS scheme[5]. Our new protocol has a low computational cost since it is similar in structure with Feldman's VSS scheme which is one of the most efficient VSS schemes available.

4 Conclusions

We have presented a non-interactive general verifiable secret sharing protocol applicable to arbitrary monotone access structures. The structure of our new protocol is similar to that of Feldman's VSS scheme. The information rate of our new protocol is optimal since each player holds only one secret share of the same size as the shared secret. The new protocol can withstand a strong admissible adversary under the assumption that computing discrete logarithm is infeasible. The new protocol may have practical applications in many areas such as key escrow[8], group oriented cryptography[9,10], fault-tolerant secure computation[5] etc.

Since our new protocol is only computational secure, our further study will be on finding an efficient and information-theoretic secure general VSS protocol applicable to arbitrary monotone access structures.

References:

[1] Shamir, A. How to share a secret. Communications of the ACM, 1979,24(11):612~613.

[2] Blakley, G.R. safeguarding cryptographic keys. In: Proceedings of the National Computer Conference. New York: AFIPS Press, 1979,48:242~268.

[3] Chor, B., Goldwasser, S., Micali, S., *et al*. Verifiable secret sharing and achieving simultaneity in the presence of faults. In: Proceedings of the 26th IEEE Symposium on Foundations of Computer Science. Washington: IEEE Computer Society Press, 1985. 251~160.

[4] Pedersen, T. Non-Interactive and information-theoretic secure verifiable secret sharing. In: Feigenbaum, J., ed. Advances in Cryptology Crypto'91. Berlin: Springer-Verlag, 1991. 129~140.

[5] Gennaro, R. Theory and practice of verifiable secret sharing [Ph.D. Thesis]. Massachusetts Institute of Technology (MIT), 1996.

[6] Feldman, P. A practical scheme for non-interactive verifiable secret sharing. In: Proceedings of the 28th IEEE Symposium on Foundations of Computer Science. Washington: IEEE Computer Society Press, 1987. 427~437.

[7] Gennaro, R., Rabin, M., Rabin, T. Simplified VSS and fast-track multiparty computations with applications to threshold cryptography. In: Proceedings of the 1998 ACM Symposium on Principles of Distributed Computing, 1998. 101~111. http://www.research.ibm.com/ security/grr.ps.

[8] Fujisaki, E., Okamoto, T. A practical and provably secure scheme for publicly verifiable secret sharing and its applications, In: Nyberg, K, ed. Advances in Cryptology, EUROCRYPTO'98. Berlin: Springer-Verlag, 1998. 32~47.

[9] Gennaro, R., Jarecki, S., Krawczyk, H., *et al*. Robust threshold DSS signatures. Information and Computation, 2001,164:54~84.

[10] Shoup, V. Practical threshold signature. In: Preneel, B. ed. Advances in Cryptology, EUROCRYPT'2000, Berlin: Springer-Verlag, 2000. 207~220.

一个安全、高效的广义可验证秘密分享协议

张福泰[1,2]， 张方国[1]， 王育民[2]

[1](陕西师范大学 计算机科学学院,陕西 西安 710062);

[2](西安电子科技大学 ISN 国家重点实验室,陕西 西安 710071)

摘要: 可验证秘密分享是密码学和信息安全中的一个重要工具.在现有的文献中可见到许多门限可验证秘密分享方案,但对广义可验证秘密分享的研究却很少.研究了广义可验证秘密分享问题.基于一个广义秘密分享方案,把 Feldman 的门限可验证秘密分享方案推广到了任意单调接入结构上.提出了一个安全高效的广义可验证秘密分享协议.协议是非交互式的,并且具有最优的信息速率,它在诸如密钥托管、面向群体的密码学及容错安全计算等方面会有实际应用.

关键词: 秘密分享;可验证秘密分享;接入结构;拉格朗日插值公式;离散对数

中图法分类号: TP309 文献标识码: A