Scientia Iranica, Vol. 15, No. 2, pp 246–251
© Sharif University of Technology, April 2008

SCIENTIA
IRANICA

A New, Publicly Verifiable, Secret Sharing Scheme

A. Behnad[1] and T. Eghlidos[*]

A Publicly Verifiable Secret Sharing (PVSS) scheme, as introduced by Stadler, has a feature where anyone, besides the participants, can verify the validity of the shares distributed by the dealer. Schoenmakers added a new feature, by providing a proof of correctness of the shares released by the players in the reconstruction process. This protocol is claimed to be an improvement on Stadler's and Fujisaki-Okamoto's, both in efficiency and in the type of intractability assumptions. However, Young-Yung improved Schoenmakers' PVSS, using a Discrete-Log instead of a Decision Diffie-Hellman. In this paper, a new PVSS is presented, having an intrinsic difference with its predecessors, that is, the participants can prove the validity of their given shares, implicitly, proving their membership by a zero-knowledge protocol. This feature prevents cheaters from participating in the reconstruction process to gain valid shares. Hence, the new proposed PVSS is more secure than previous ones. Besides, the dealer only sends the amount of commitments limited to the threshold value, regardless of the number of shareholders; this leads to a more dynamic protocol.

INTRODUCTION

A secret sharing scheme is a method for increasing the security of cryptographic systems so that, instead of having access to the secret (key) exclusively, a secret is shared between groups of participants by a dealer in the distribution process, such that specific subgroups (access structure) of the shareholders can recover the secret by pooling their shares in the reconstruction process. Secret sharing was first introduced by Blakley [1] and Shamir [2], independently. Threshold secret sharing has more importance in applications than other kinds of secret sharing scheme and it is used in advanced protocols. In a (t, n)-threshold scheme, a secret value is shared between n participants, such that any t of them can recover the secret by pooling their shares simultaneously. Shamir's threshold secret sharing scheme is based on polynomial interpolation in a finite field. In spite of introducing other secret sharing schemes, for instance [3] and [4], Shamir's scheme has attracted more attention than the others, due to its effective applicability and the fact that it is the basis of most other secret sharing protocols.

Although Shamir's scheme is simple and efficient, it still has some security considerations, such as an inability to recognize the honesty of the dealer in sharing the secret, preventing cheating by players and detecting cheaters. Hence, several protocols have been introduced to cover the security issues mentioned above. Among these protocols, the Verifiable Secret Sharing scheme (VSS) [5-8], enables shareholders to verify their own shares and, thus, prevent them from submitting incorrect shares in the reconstruction process. Subsequently, Stadler [9] introduced the notion of Publicly Verifiable Secret Sharing (PVSS) with the objective that, not only can shareholders verify that shares are correctly distributed, but also that anyone can verify the same fact. Stadler expressed the main goal of this specification to convince each shareholder of the uniqueness of the reconstructed secret, i.e. each authorized subset of the access structure reconstructs the unique secret. Schoenmakers [10] extended this idea, such that the shareholders can provide a proof of correctness for each share released in the reconstruction process. According to [10], his approach is much simpler than Stadler's and the followed Fujisaki-Okamoto's

[1] *Department of Electrical Engineering, Sharif University of Technology, Tehran, I.R. Iran.*

[*] *Corresponding Author, Department of Electrical Engineering, Electronics Research Center, Sharif University of Technology, Tehran, I.R. Iran.*

PVSS [11], both theoretically and practically. Later, Young-Yung [12] presented an improvement on [10] and presented a PVSS for sharing discrete-logarithms that is as hard to break as the Discrete-Log problem itself, in contrast to [10], which is based on the Decision Diffie-Hellman. The scheme presented in [12] has a property that diverts from the traditional Shamir-based secret sharing.

In the previous PVSS, each participant registers a public key at the beginning of the distribution process and the dealer publishes the encrypted shares in such a way that the shareholders can decrypt and verify their own shares, but they can only verify the correctness of the other shares. Indeed, the membership of shareholders in the secret sharing protocol is recognized by their registered public key. Thus, it is necessary for their shares to be verified, regardless of their membership.

In contrast, in this paper, a new PVSS is introduced, in which the membership of the shareholders is merely related to their shares, without any need for a pre-registered key. Thus, there is no difference between the player who receives an incorrect share in the distribution process and the third party. Instead, in the new PVSS, two different processes were added to the protocol; one in the distribution process, called *disputation*, is used in case any complaint against the dealer is reported from the shareholders. By this process, similar to the previous PVSS protocols, the honest dealer can prove to anyone that the correct shares were sent to those shareholders who complained. The other one, called membership proof, is used to authenticate the membership of the shareholders. This implies that the shareholders can prove the validity of their given shares and prove their membership by a zero-knowledge protocol. This process is applied at the beginning of the secret reconstruction process to prevent unauthorized parties participating in the final step, i.e. pooling the shares.

In this way, it is only necessary for the shareholders to verify their own shares in the distribution process, because, if a participant does not receive a correct share in the distribution process, his membership will not be verified in the reconstruction process and will be discarded.

Thus, the PVSS described here has an inherent difference with that of Schoenmakers and his predecessors, but still involves the concept of PVSS. In contrast to the previous protocols, in which the dealer directly proves the correctness of the distributed shares, in the approach described in this paper, the shareholders can prove the honesty of the dealer in sharing the secret, by proving their membership to other parties (i.e. anyone).

The new protocol involves Feldman's [6] scheme, as the basis for both sharing and reconstructing the secret, although Pedersen's scheme [7] could also be made use of. As long as a threshold secret sharing is linear, one can apply secret sharing without a dealer [7,13,14] and proactive secret sharing [14-16] to the protocol. The new protocol is prepared for application of these features, but in this paper, the authors avoid mentioning the two states of the protocol explicitly.

The security of the two added processes mentioned above, i.e. *disputation* and *membership proof*, are based on the Diffie-Hellman problem, similar to the Schoenmakers' protocol, followed by a zero-knowledge proof. From a performance point of view, the new PVSS does not make use of any key for commitments, has less number of commitments and is more dynamic than the variant introduced by Shoenmakers.

The outline of this paper is, as follows. First, basic notations are presented and the new PVSS scheme is introduced. Then, the performance of the new scheme is discussed and the security of the scheme is presented. After that, the whole paper is summarized and the results are discussed. Finally, concluding remarks are presented.

PRELIMINARIES

Throughout this paper, all computations are performed in two different fields, Z_p and Z_q, where p and q are two large prime numbers, such that $q|p-1$. Let G_q denote a subgroup of prime order q in Z_p^*, such that computing discrete logarithms in this group is infeasible. Moreover, $g \in G_q$ denote a generator of the group.

Note that, all computations in the form of g^α are accomplished in Z_p^* and those of the exponents are performed in Z_q. All other computations are performed in Z_q. The module of each congruence relation is mentioned if necessary.

NEW PVSS

The new construction for a (t, n)-threshold access structure is described, however, it can be applied to any monotone access structure for which a linear secret sharing scheme exists [10]. This protocol, similar to all secret sharing protocols, consists of two processes, distribution and reconstruction. In the distribution process, a dealer shares a secret and distributes the shares among participants who, subsequently, verify their received shares. If any share is not approved by a participant, the other participants, or third party, investigate the complaint within the so-called disputation stage. In the secret reconstruction process, the players mutually verify their membership, exchange their shares and, after verifying them, reconstruct the secret.

Distribution Process

This process consists of the following three stages.

Distribution of the Shares

The dealer sets $F(x) = F_0 + F_1.x + \cdots + F_{t-1}.x^{t-1}$, where $F_0 = s$ is the secret and $F_1, \cdots, F_{t-1} \in_{\mathrm{R}} Z_q$, then publishes $C_i = g^{F_i}$ for $i = 0, 1, \cdots, t-1$. The participant, j, $j = 1, 2, \cdots, n$, registers g^{a_j} as his public key to the dealer, where $a_j \in_{\mathrm{R}} Z_q$. Also, the dealer picks $d \in_{\mathrm{R}} Z_q$, publishes g^d, then, sends the encrypted share, $E_j = s_j(g^{a_j})^d$, back to the participant, j, where $s_j = F(j)$ for simplicity is the assigned share.

Verification of the Shares

The shareholder, j, decrypts E_j by computing $s_j = E_j.[(g^d)^{a_j}]^{-1}$, then, verifies the share, s_j, by computing $g^{s_j} = \prod_{i=o}^{t-1} C_i^{j^i}$. If the relation does not hold, then, the shareholder complains against the dealer.

Disputation

In the case of any complaint, the third party, R, can vote against the dealer, D, or the shareholder, A, by the following protocol:

1. A and D choose $a, d \in_{\mathrm{R}} Z_q$, respectively, and publish g^a and g^d;
2. A and D calculate g^{ad} and publish $\lambda = g^{(g^{ad})^{-1}}$, independently;
3. R checks if $\lambda_{\mathrm{A}} = \lambda_{\mathrm{D}}$. If it holds, the protocol is continued; else R requests the values a, d from A and D. Thus, R can detect the dishonest party by calculating g^a, g^d and $g^{(g^{ad})^{-1}}$. In this case, the protocol is terminated;
4. D publishes $e_{\mathrm{A}} = s_{\mathrm{A}} g^{ad} \pmod{q}$;
5. R chooses r_1, $r_2 \in_{\mathrm{R}} Z_q$ and sends $\rho = g^{r_1 + r_2 e_{\mathrm{A}}}$ to D;
6. D calculates $\delta = \rho^{(g^{ad})^{-1}}$ and sends it back to R;
7. R checks if $[\delta(\lambda^{r_1})^{-1}]^{r_2^{-1}} = \prod_{i=0}^{t-1} C_i^{j_{\mathrm{A}}^i}$. If the equality holds, s_{A} is correct, otherwise, the share is not valid.

Note that, in the new PVSS, the registered key, g^{a_j}, by participant j, in the distribution process, is used only to receive the share securely, in contrast to the previous PVSS [9,10], where the registered key is necessary for share verification in the secret reconstruction process.

Reconstruction Process

This process consists of the following two stages.

Membership Proof of the Shareholders

When the number of participants reaches at least the threshold t, each two shareholders run the membership sub-process to verify the membership of the other party. In a case where the membership of at least t parties is verified mutually, the reconstruction process enters the next step.

Membership Proof

Here, anyone plays the role of verifier and the prover possesses the share, s_j, $j = 1, 2, \cdots, n$, as follows:

1. The verifier chooses $a \in_{\mathrm{R}} Z_q$ and sends g^a to the prover;
2. The prover chooses $b \in_{\mathrm{R}} Z_q$, then, sends $\mathrm{R}_P = (g^a)^{b+s_j}$ and g^b to the verifier;
3. The verifier computes $\mathrm{R}_V = [(g^b) \times (\prod_{i=0}^{t-1} C_i^{j^i})]^a$, then, checks whether $\mathrm{R}_V = \mathrm{R}_P$ or not. If it holds, the prover is the shareholder who assigned the share, S_j.

Along with membership proof, the conventional key, g^{ab}, can be made by each two parties, for the use of encryption.

Pooling the Shares

The shareholders send their encrypted shares, using the conventional key, g^{ab}, obtained from the membership proof stage, to the other shareholders. Each of them extracts and verifies the share, using C_i, by computing $g^{s_j} = \prod_{i=0}^{t-1} C_i^{j^i}$. The secret is reconstructed, as follows:

$$s = \sum_{i=1}^{t} \omega_i s_i,$$

where $\omega_i = \prod_{j \neq i} \frac{i}{j-1}$ is a Lagrange coefficient.

PERFORMANCE

All previous PVSS protocols (see [9-12]) follow a similar approach for improving security and performance. However, the new PVSS adds another view to the protocol.

The new PVSS has the following advantages over previous protocols:

1. It does not make use of key registration for share verification in the secret reconstruction process. The shareholders are identified by their own shares;
2. The number of commitments in the new PVSS is limited to the t elements of G_q, whereas in the previous PVSS protocols, it is more. For example in [10] one element of G_q and one element with a length of size $|q|$ are added for each shareholder. The number of commitments in [11] is significantly more than that mentioned above [10];
3. This method is more dynamic than previous ones; a new participant can join the secret sharing protocol without any need for publishing new commitments by the dealer;

4. In the reconstruction process of the new PVSS, the secret is not recovered until the membership of each player is verified by the other players. But, in the previous PVSS [9-12] there is no method for considering the membership proof of the players. Thus, unauthorized parties can participate in the secret reconstruction process.

Even though it is not mentioned explicitly in previous protocols, it is possible to verify the membership of the players using the registered public keys. For doing this, a player should be convinced that the other players are those who registered their public keys in the distribution process. But, in the new PVSS, the membership is proved directly, without any need of the registered keys. This property makes the protocol more dynamic and verifying the membership does not depend on the availability of the registered key and the commitment of one's share.

In contrast to the protocol described in [10], which is more similar to the authors' PVSS, the new protocol is interactive at both added disputation and membership proof stages. However, the disputation stage is not run, if the dealer and participants play fair. The number of times this stage might be run depends only on the number of complaints. If r complaints are reported, this stage is performed with the complexity of $O(rn)$, where n is the number of participants.

SECURITY

Two major features of the new PVSS protocol are disputation and membership proof, which are added to the distribution and reconstruction processes, respectively. Hence, the security of the protocol is based on the security of these two stages.

Publicly Verifiable Secret Sharing is mainly applicable to cases where there is a complaint against the dealer in the distribution process. In this situation, the dealer should be able to publish a mask of the share, s_{A}, given to the shareholder, A, so that:

(i) Only A is able to extract and verify s_{A} from the masked value;

(ii) The dealer is able to prove to the third party that A can calculate the correct value of s_{A} from the masked value.

These features are fulfilled within the disputation stage. In this stage, the conventional key, g^{ad}, is made by the Diffie-Hellman key agreement between A and D. Thus:

(i) Only the shareholder, A, can extract the share, s_{A}, from the published masked value, $s_{\text{A}}g^{ad}$, by the dealer, in step 4 of the disputation stage;

(ii) Because the dealer commits to g^{ad} by λ, in step 2 of the disputation stage, which is verified in step 3 of this stage by a third party, the equality in step 7 holds, if, and only if, the dealer would send the valid share in step 4.

In the disputation stage, the third party, R, is convinced that the dealer, D, publishes the encrypted correct share, e_{A}. On the other hand, the shareholder, A, obtains a correct share by decrypting e_{A}, which is stated within Lemma 1.

Lemma 1

(a) The dealer, D, cannot send an invalid share to the participant, A;

(b) The participant, A, cannot claim that the received share is invalid.

Proof

(a) By verifying $\lambda_{\text{A}} = \lambda_{\text{D}}$ in step 3 of the disputation stage, R is convinced that A and D agree on the common key. Suppose that a dishonest dealer sends the forged encrypted share, e'_{A}, in step 4 and replaces e'_{A} with e_{A}, in ρ, during step 6, to deceive R in step 7. Even if D could solve the discrete logarithm, he should compute $r_1 + r_2 e_{\text{A}}$ from $r_1 + r_2 e'_{\text{A}}$, which is impossible, due to the unknown numbers; r_1 and r_2;

(b) By verifying the equality in step 7, R is convinced that D sent an encrypted correct share, with the committed common key, to A. On the other hand, from step 3, R was convinced that A had the same common key. Therefore, A can extract the valid share from e_{A}.□

The security of the membership proof stage is based on the Diffie-Hellman assumption, which is proved by Lemma 2.

Lemma 2

Under the Diffie-Hellman assumption, it is infeasible for an unauthorized party to pretend to be a shareholder.

Proof

In order to impersonate a shareholder possessing, s_i, the unauthorized party should be able to compute g^{as_i} from the inputs g^a and $g^K, g^{a_1}, g^{a_2}, \cdots, g^{a_{t-1}}$ to an algorithm $\mathcal{A}$ with some probability of success. Using the same algorithm, one could obtain $g^{\alpha\beta}$ from g^α and g^β with the same probability, by setting $a = \alpha$ and simulating a secret sharing scheme, in which β corresponds to the share of the shareholder, i, i.e. $\beta = K' + a'_1 i + \cdots + a'_{t-1} i^{t-1}$ and feed g^α and $g^{K'}, g^{a'_1}, g^{a'_2}, \cdots, g^{a'_{t-1}}$ to A. By doing this, the party should first choose the coefficients,$K', a'_1, a'_2, \cdots, a'_{t-1}$, such that the relation, $g^{\beta} = g^{K'} g^{a'_1 i} \cdots g^{a'_{t-1} i^{t-1}}$ holds. This implies solving the Diffie-Hellman problem.□

Note that proof of the correctness of the shares to the third party in Lemma 1 and the membership proof in Lemma 2 are both realized by zero-knowledge proofs. However, the security of both stages, i.e., disputation and membership proof, are based on the intractability of the Diffie-Hellman problem.

RESULTS AND DISCUSSION

The main goal in verifying the validity of a share by other players, as stated by Stadler [9], is the assurance of the uniqueness of the reconstructed secret (key) by each subset of the access structure. However, this property of publicly verifiable secret sharing has a more important application than that Stadler observed. Using this property, the dealer can prove to the other parties that a correct share has been sent to a specified player. Thus, this player cannot claim that an incorrect share has been received. A similar approach was employed in [10-12]. In [10], Schoenmakers extended the PVSS by adding a new property to the reconstruction process, such that the participants could provide proof of the correctness of their released share.

In the new scheme, by establishing a new stage as membership proof, the assurance of the correctness of each share by other parties is considered a part of reconstruction and not a part of the distribution process. In this way, after the shares have been verified by the shareholders, each one can be assured of the correctness of the shares possessed by the other shareholders, for, if a party did not receive a correct share in the distribution process, his membership could not be proved in the reconstruction process. So, the protocol does not distinguish between this party and a third party.

Membership proof has the capability of gathering authorized shareholders for the secret reconstruction. Suppose that a number of authorized shareholders, less than the threshold, intend to recover the secret. For this purpose, they should gather the remaining shareholders up to the threshold. If there were not any criterion to verify membership, even in the presence of only one cheat among the players, he would not be detected until the secret reconstruction process. Thus, the cheater could interfere and postpone the process. Hence, this additional process separates the shareholders from other players.

Note that this method results in a more dynamic protocol, as publication of a new key commitment by the dealer would no longer be required.

Moreover, the new PVSS provides the participants with the possibility of complaint against the dealer, if they were to receive an invalid share in the disputation phase, added to the distribution process.

CONCLUSION

Two important characteristics of PVSS, which have already been stated, are proving the correctness of distributed shares to anyone in the distribution process and verifying shares pooled in the secret reconstruction process. In this paper, by adding a new phase, called membership proof, each shareholder is able to prove the holding of a valid share without revealing it, which implies the membership proof of the shareholder. Within this phase, everyone can be convinced of the authorization of those players who have participated in the reconstruction process.

The new method has the advantage of limiting the number of commitments to the threshold used in the protocol, regardless of the number of shareholders.

It seems that the new PVSS is consistent in situations where communication between dealer and shareholder, after the distribution process, is not possible; also, in situations where saving the commitments by each shareholder is impossible, due to security concerns or memory limitation. Considering the properties of Ad-Hoc networks, it appears that the new PVSS is also suitable for application in these networks.

ACKNOWLEDGMENT

The authors are grateful to the anonymous referee for his/her valuable comments.

REFERENCES

1. Blakley, G.R. “Safeguarding cryptographic keys”, *Proc. of the 1979 AFIPS National Computer Conference*, **48**, pp 313-317 (1979).
2. Shamir, A. “How to share a secret”, *Communications of the ACM*, **22**(11), pp 612-613 (1979).
3. Asmuth, C. and Bloom, J. “A modular approach to key safeguarding”, *IEEE Transactions on Information Theory*, *IT*-**29**, pp 208-211 (1983).
4. Karnin, E.D., Greene, J.W. and Hellman, M.E. “On secret sharing systems”, *IEEE Transactions on Information Theory*, *IT*-**29**(1), pp 35-41 (1983).
5. Chor, B., Goldwasser, S., Micali, S. and Awerbuch, B. “Verifiable secret sharing and achieving simultaneity in presence of faults”, *Proc. of the 26th Annual IEEE Symp. on the Foundations of Computer Science (FOCS)*, pp 383-395 (1985).
6. Feldman, P. “A practical scheme for non-interactive verifiable secret sharing”, *Proc. of the 28th IEEE Symp. on the Foundations of Computer Science*, pp 427-437 (1987).
7. Pedersen, T. “Non-interactive and information-theoretic secure verifiable secret sharing”, *Crypto’91*, LNCS 576, pp 129-140 (1992).

8. Rabin, T. “Robust sharing of secrets when the dealer is honest or faulty”, *J. of the ACM*, **41**(6), pp 1089-1109 (1994).
9. Stadler, M. “Publicly verifiable secret sharing”, *Eurocrypt’96*, LNCS 1070, pp 190-199 (1996).
10. Schoenmakers, B. “A simple publicly verifiable secret sharing scheme and its application to electronic voting”, *Crypto’99*, LNCS 1666, pp 148-164 (1999).
11. Fujisaki, E. and Okamoto, T. “A practical and provably secure scheme for publicly verifiable secret sharing and its applications”, *Eurocrypt’98*, LNCS 1403, pp 32-46 (1998).
12. Young, A. and Yung, M. “A PVSS as hard as Discrete Log and shareholder separability”, *PKC 2001*, LNCS 1992, pp 287-299 (2001).
13. Ingemarsson, I. and Simmons, G.J. “A protocol to set up shared secret schemes without the assistance of a mutually trusted party”, *Eurocrypt’90*, LNCS 473, pp 266-282 (1991).
14. Stinson, D.R. and Wei, R. “Unconditionally secure proactive secret sharing scheme with combinatorial structures”, *Proc. of the 6th Annual Workshop on Selected Areas in Cryptography*, SAC’99, LNCS 1758, pp 200-214 (1999).
15. Herzberg, A., Jarecki, S., Krawczyk, H. and Yung, M. “Proactive secret sharing or: How to cope with perpetual leakage”, *Crypto’95*, pp 339-352 (1995).
16. Jarecki, S. “Proactive secret sharing and public key Cryptosystems”, M.Sc. Thesis, MIT (1995).