Designs, Codes and Cryptography, 5, 183–187 (1995)

A Perfect Threshold Secret Sharing Scheme to Identify Cheaters

MARCO CARPENTIERI
Istituto per la Ricerca sui Sistemi Informatici Paralleli, Consiglio Nazionale delle Ricerche, Via Pietro Castellino 111, 80123 *Napoli (Na), Italy*

Editor: D. Jungnickel

Received December 20, 1993; Revised June 22, 1994

Abstract. In this paper we consider the problem of identifying cheaters in secret sharing schemes. Rabin and Ben-Or presented a perfect and unconditionally secure secret sharing scheme in which the honest participants are able to identify the cheaters. We present a similar scheme, but one in which the information distributed to each participant is smaller.

1. Introduction

In 1979 Blakley [2] and Shamir [10] gave protocols to solve the following problem: divide a secret s in n shares in such a way that:

i) the knowledge of k or more shares makes s computable,

ii) the knowledge of $k-1$ or less shares leaves s *completely* indeterminate.

This problem, known in the literature as "(k, n) Threshold Secret Sharing", has received considerably attention in the last few years because of its many applications to several fields, as data security, secure computation and others [6]. For an extensive bibliography and illustration of the main results in the area the reader is referred to [12] and [13]. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a finite set of n participants. Informally, a (k, n) threshold secret sharing scheme is a method to distribute shares of a secret s to the participants in $\mathcal{P}$ in such a way that any k participants can calculate s, but no subset of fewer than k participants can do so. A (k, n) threshold secret sharing scheme is said to be "perfect" if no subset of fewer than k participants can determine any partial information regarding the secret s (in an information theoretic sense), even with infinite computational resources.

In the last decade various researchers have considered the problem of guarding against the presence of cheaters in threshold secret sharing schemes [1], [3], [5], [9], [11], [15]. It is conceivable that a subset of the participants may attempt to cheat, that is, to deceive any of the other participants by lying about the shares they possess. A threshold secret sharing scheme is said to be unconditionally secure (against cheating) if the probability of successful cheating is limited to a specify probability even if the cheaters are assumed to have infinite computational resources.

The first researchers to address the problem of cheaters in threshold secret sharing schemes were McEliece and Sarwate [9]. They use an error-correcting code to construct a threshold secret sharing scheme in which any group of $k + 2e$ participants which includes at most e cheaters can correctly calculate the secret.

Tompa and Woll [15] considered the following scenario: let us suppose that $k - 1$ participants want to cheat a k-th honest one. Let s be the correct secret, that is, the secret the participants would reconstruct if they pooled together their shares. The $k - 1$ cheaters, not knowing the share of the honest participant, could return forged shares in an attempt to force the honest participant to reconstruct a secret $s' \neq s$. Tompa and Woll showed that Shamir's scheme [10] is insecure against this attack in the sense that even a single participant, with high probability, can deceive other $k - 1$ honest participants. However, they also modified Shamir's scheme to make it secure against such cheating. Briefly, they proposed a sharing algorithm that specifies a subset S_{legal} of the set S of possible secrets. A secret will be accepted as authentic only if it is an element of S_{legal}. If a set of k participants calculate the secret to be an element of $S_{illegal} = S - S_{legal}$, then they realize that at least one of them is cheating. In Tompa and Woll's scheme the probability that the $k - 1$ cheaters cheat successfully is at most $1 - k\frac{|S_{legal}|}{S}$. However, even though participants can detect when cheating has occurred, they cannot determine who is cheating.

Brickell and Stinson [3] proposed a modified version of the Blakley's construction [2] in which honest participants are able to identify cheaters. Brickell and Stinson considered a somewhat different scenario from Tompa and Woll's: there is an honest participant and the remaining $n - 1$ participants form a coalition in order to deceive him. If s is the correct secret, some $k - 1$ participants of the $n - 1$ cheaters could return forged shares in an attempt to force the n-th honest one to reconstruct a secret $s' \neq s$. Suppose that the honest participant can somehow check the shares in such a way that he is able to identify which shares are falsified. As the honest participant would like to reconstruct the correct secret, each time he identifies a forged share, he asks the remaining participants for another share. Then the $n - 1$ cheaters can return forged shares untill at most $n - k + 1$ participants are identified as cheaters. In Brickell and Stinson's construction even if there is only one honest participant and the remaining $n - 1$ participants form a coalition in order to deceive him (as described) the probability of cheating successfully is $\frac{n-k+1}{|S|-1}$, where S is the set of secrets.

Independently and simultaneously, Rabin and Ben-Or [1] developed a threshold secret sharing scheme, based on [10], having properties very similar to Brickell and Stinson's construction. In Rabin and Ben-Or's scheme, every participant in $\mathcal{P}$ receives extra information along with his share, over a finite field, to guard against cheating. Indeed, each participant P_i in $\mathcal{P}$ receives his share d_i and $n - 1$ random elements $v_{i,j}$, for $j = 1, \ldots, n$ and $j \neq i$. Moreover, each participant P_j in $\mathcal{P} - \{P_i\}$ receives $n - 1$ pairs $(w_{j,i}, z_{j,i})$, for $i = 1, \ldots, n$ and $i \neq j$, where $w_{j,i} \neq 0$ is a random element and $z_{j,i}$ is calculated as $z_{j,i} = d_i + v_{i,j}w_{j,i}$. When the participant P_i wants to let P_j know his share, he returns the pair $(d_i, v_{i,j})$. Then P_j can calculate $d_i + v_{i,j}w_{j,i}$ and he accepts d_i only if the result is $z_{j,i}$. In Rabin and Ben-Or's scheme the probability that a coalition of $n - 1$ participants cheat successfully the remaining honest participant is $1 - (1 - \frac{1}{|S|-1})^{n-k+1} \leq \frac{n-k+1}{|S|-1}$, where S is the set of secrets.

An important issue in the implementation of secret sharing schemes is the information distributed to participants since the security of the system degrades as the amount of the information that must be kept secret increases. Even though in Brickell and Stinson's construction the secret information given to each participant ($n + 2k - 3$ elements of a finite field) is smaller than the information given in Rabin and Ben-Or's scheme ($3n - 2$ elements of the field), their scheme is not perfect and is not computationally efficient if k and n are large. Conversely, Rabin and Ben-Or's scheme is perfect and can be implemented in polynomial time. In this paper we present a perfect and unconditionally secure (k, n) threshold secret sharing scheme having the same properties of Rabin and Ben-Or's scheme, but in which the information given to each participant is smaller ($k + 2(n - 1)$ elements of a finite field).

2. The Construction

Let $GF(q)$ be a finite field with q elements, where q is a prime power such that $q > n$. Assume that the secret s is chosen in the finite field $GF(q)$ by a special participant called the Dealer. The Dealer is denoted by Dl and assume $Dl \not\in \mathcal{P}$. The construction is based on Shamir's threshold secret sharing scheme [10]. When Dl wants to share the secret s among the participants in $\mathcal{P}$, he gives a k-dimensional vector $\underline{d}_i \equiv (d_{i,0}, \ldots, d_{i,k-1})$, where $k \leq n$, over $GF(q)$ as a share to participant P_i, for $i = 1, \ldots, n$. The Dealer chooses the shares as follows. Let $a_1, \ldots, a_{k-1}$ be elements chosen uniformly at random in $GF(q)$ and unknown to all the participants. Let $\alpha_1, \ldots, \alpha_n$ be distinct and non null elements in $GF(q)$ known by all the participants. If $q(x)$ is the polynomial $s + a_1x + a_2x^2 + \cdots + a_{k-1}x^{k-1}$, then $d_{i,0} = q(\alpha_i)$ and $d_{i,1}, \ldots, d_{i,k-1}$ are elements chosen uniformly at random in $GF(q)$, for $i = 1, \ldots, n$. To guard against cheating, Dl distributes extra information to the participants along with their shares. The extra information consists of $n - 1$ pairs of elements in $GF(q)$ for each participant P_j in $\mathcal{P}$. Let $g_{j,i}$ be non null elements chosen uniformly at random in $GF(q)$, for $i = 1, \ldots, n$ and $i \neq j$. Dl calculates $b_{j,i} = g_{j,i}d_{i,0} + \alpha_j d_{i,1} + \cdots + \alpha_j^{k-1} d_{i,k-1}$ and, then, he gives the participant P_j the pair $(g_{j,i}, b_{j,i})$, for $i = 1, \ldots, n$ and $i \neq j$. Thus, when the participant P_i returns his share $\underline{d}_i$, P_j can check the authenticity of $\underline{d}_i$ by verifying that it is a solution vector of the equation $g_{j,i}y_0 + \alpha_j y_1 + \cdots + \alpha_j^{k-1} y_{k-1} = b_{j,i}$, where $y_0, \ldots, y_{k-1}$ are the unknowns, $g_{j,i}, \alpha_j, \ldots, \alpha_j^{k-1}$ are the coefficients and $b_{j,i}$ is the constant, for $i = 1, \ldots, n$ and $i \neq j$.

3. Properties

The properties of the construction described in Section 2 can be summarized as follows.

LEMMA 1 *Any k participants can calculate the secret s, but no subset of fewer than k participants can determine any partial information regarding s.*

Proof. Since Shamir's scheme [10] is a perfect threshold secret sharing scheme, any k participants can calculate the secret s by interpolation [6],[8], but no subset $\mathcal{R} \subset \mathcal{P}$ of $r < k$ participants, pooling their own shares, can determine any partial information regarding s. Consider the system of r equations $g_{j,i}y_0 + \alpha_j y_1 + \cdots + \alpha_j^{k-1} y_{k-1} = b_{j,i}$, for all $P_j \in \mathcal{R}$ and where $P_i \in \mathcal{P} - \mathcal{R}$. Since α_j, for all $P_j \in \mathcal{R}$, are non null and distinct elements in $GF(q)$, the determinant of the coefficient matrix of such a system, where the first $k - r$ columns are discarded, is a non null multiple of a Vandermonde determinant. Then the r

equations are linearly independent and for each possible unknown $y_0 \in GF(q)$ there are q^{k-r-1} possible solutions. Then the participants in $\mathcal{R}$ can determine no partial information regarding $d_{i,0}$, if $P_i \in \mathcal{P} - \mathcal{R}$, and therefore the secret s. ■

LEMMA 2 *Any participant who attempts to cheat will be identified by any honest participant with probability* $1 - \frac{1}{q-1}$.

Proof. Suppose the participant P_i tells participant P_j that his share is $\underline{d}_i'$ instead of $\underline{d}_i$. Since P_i wants to force P_j to reconstruct a secret $s' \neq s$, $\underline{d}_i'$ is such that $d_{i,0}' \neq d_{i,0}$. Depending on the element $g_{j,i} \in GF(q) - \{0\}$ given by the Dealer, the participant P_j could have $q - 1$ equations to check the share of P_i. Consider the equations $g_{j,i}y_0 + \alpha_j y_1 + \cdots + \alpha_j^{k-1} y_{k-1} = b_{j,i}$ and $g_{j,i}'y_0 + \alpha_j y_1 + \cdots + \alpha_j^{k-1} y_{k-1} = b_{j,i}'$, such that $g_{j,i} \neq g_{j,i}'$. If $\underline{d}_i'$ and $\underline{d}_i$ were solution of both the equations we would have that, subtracting the members of the equations, $(g_{j,i} - g_{j,i}')d_{i,0} = b_{j,i} - b_{j,i}'$ and $(g_{j,i} - g_{j,i}')d_{i,0}' = b_{j,i} - b_{j,i}'$. Since it is $g_{j,i}' \neq g_{j,i}$ this contradicts $d_{i,0}' \neq d_{i,0}$. It follows that $\underline{d}_i'$, where $d_{i,0}' \neq d_{i,0}$, satisfies only one of the possible equations that the participant P_j could have to check the share of P_i. Then the probability that participant P_i cheats successfully participant P_j is at most $\frac{1}{q-1}$ and therefore P_i is identified by P_j with probability not lower than $1 - \frac{1}{q-1}$. ■

LEMMA 3 *Even if there is only one honest participant and the remaining $n - 1$ participants form a coalition in order to deceive him, their probability of cheating successfully is only* $1 - (1 - \frac{1}{q-1})^{n-k+1} \leq \frac{n-k+1}{q-1}$.

Proof. Let C be some subset of $n - 1$ participants in $\mathcal{P}$. Suppose that the participants in C form a coalition in order to try to convince $P_j \in \mathcal{P} - C$ that the secret is $s' \neq s$. The participants in C conspire, that is, they pool any information in cheating the participant P_j. Recall from [3] that the best strategy the $n - 1$ cheaters can follow is to leave $k - 2$ of their shares unchanged and lie about the remaining $n - k + 1$ shares. Let $\underline{d}_i'$ be the forged share given by some participant $P_i \in C$, instead of $\underline{d}_i$. Even if the $n - 1$ cheaters conspire, they only know that P_j has one of $q - 1$ equations $g_{j,i}y_0 + \alpha_j y_1 + \cdots + \alpha_j^{k-1} y_{k-1} = b_{j,i}$, for $g_{j,i} \in GF(q) - \{0\}$, to check the share of P_i. By the same argument used to prove Lemma 2, we have that $\underline{d'}_i$, where $d_{i,0}' \neq d_{i,0}$, satisfies only one of such equations. It follows that the probability that participant P_i is identified as a cheater by P_j is $1 - \frac{1}{q-1}$. Since the elements $g_{j,i}$ of the equations of P_j are chosen uniformly at random, the $n - 1$ cheaters have probability $1 - (1 - \frac{1}{q-1})^{n-k+1}$ of cheating the participant P_j. ■

LEMMA 4 *The secret information given to each participant consists of $k + 2(n - 1)$ elements of the finite field $GF(q)$.*

Proof. This follows from the construction, since each participant receives k elements of $GF(q)$ as his share and $2(n - 1)$ elements of extra information to calculate his equations. ■

LEMMA 5 *The construction can be implemented in polynomial time.*

Proof. We shall briefly review only how much time is taken by the Dealer to calculate the constants $b_{j,i}$ of the $n-1$ equations for each participant P_j. First Dl calculates the powers of α_j in $\frac{k(k-1)}{2}$ multiplications. Then the constants $b_{j,i}$ are calculated in $k(n-1)$ multiplications. Therefore Dl needs $\frac{k(k-1)}{2}+k(n-1)$ multiplications. ■

Remark. It is conceivable that the Dealer gives every participant P_j the pairs $(g_{j,i}, b_{j,i})$, where $g_{j,i}$ is the same element chosen uniformly at random in $GF(q)$, for $i=1,\dots,n$ and $i \neq j$. In this case, all the lemmas still hold, except Lemmas 3 and 4. Indeed, even if the information distributed to each participant consists of $k+n$ elements of $GF(q)$, the probability that a coalition of $n-1$ participants cheat successfully the remaining honest participant is $\sum_{j=1}^{n-k+1}\frac{1}{q-j}$.

Acknowledgements

The author thanks Professors Ugo Vaccaro, Alfredo De Santis, Roberto Vaccaro and Pasquale Lucio Scandizzo for their helpful observations and comments.

References

1. M. Ben-Or and T. Rabin, Verifiable secret sharing and multiparty protocols with honest majority, *Proc. 21st ACM Symposium on Theory of Computing*, (1989) pp. 73–85.
2. G. R. Blakley, Safeguarding cryptographic keys, *Proceedings AFIPS 1979 National Computer Conference*, (1979) pp. 313–317.
3. E. F. Brickell and D. R. Stinson, The detection of cheaters in threshold schemes, *SIAM J. Disc. Math.*, Vol. 4 (1991) pp. 502–510.
4. R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, On the size of shares for secret sharing schemes, *Advances in Cryptology—CRYPTO '91* (J. Feigenbaum, ed.), Lectures Notes in Computer Science, Springer-Verlag, New York, 576 (1992) pp. 101–113. Also to appear in *Journal of Cryptology*.
5. M. Carpentieri, A. De Santis, and U. Vaccaro, Size of shares and probability of cheating in threshold schemes, *Advances in Cryptology—EUROCRYPT 93* (T. Helleseth, ed.), Lecture Notes in Computer Science, Springer-Verlag, New York, to appear.
6. D. Denning, *Cryptography and Data Security*, Addison–Wesley, Reading, MA (1983).
7. E. D. Karnin, J. W. Greene, and M. E. Hellman, On secret sharing systems, *IEEE Trans. on Inform. Theory*, Vol. IT-29 (1983) pp. 35–41.
8. J. D. Lipson, *Elements of Algebra and Algebraic Computing*, Addison-Wesley, Reading, MA (1981).
9. R. J. McEliece and D. V. Sarwate, On sharing secrets and Reed-Solomon codes, *Communications of the ACM*, Vol. 24 (1981) pp. 583–584.
10. A. Shamir, How to share a secret, *Communication of the ACM*, Vol. 22 (1979) pp. 612–613.
11. G. Simmons, Robust shared secret schemes or "How to be sure you have the right answer even though you do not know the question", *Congr. Numer.*, Vol. 68 (1989) pp. 215–248.
12. G. J. Simmons, An introduction to shared secret and/or shared control schemes and their application, *Contemporary Cryptology*, IEEE Press (1991) pp. 441–497.
13. D. R. Stinson, An explication of secret sharing schemes, *Designs, Codes and Cryptography*, Vol. 2 (1992) pp. 357–390.
14. D. R. Stinson, *Decomposition Constructions for Secret Sharing Schemes*, Technical Report UNL-CSE-92-020, Department of Computer Science and Engineering, University of Nebraska, September 1992.
15. M. Tompa and H. Woll, How to share a secret with cheaters, *Journal of Cryptology*, Vol. 1 (1988) pp. 133–139.