Cheating Immune Secret Sharing

Xian-Mo Zhang[1] and Josef Pieprzyk[2]

[1] School of IT and CS, University of Wollongong
Wollongong, NSW 2522, AUSTRALIA, xianmo@cs.uow.edu.au
[2] Algorithms and Cryptography Centre, Department of Computing
Macquarie University, Sydney , NSW 2109, AUSTRALIA, josef@ics.mq.edu.au

Abstract We consider secret sharing with binary shares. This model allows us to use the well developed theory of cryptographically strong boolean functions. We prove that for given secret sharing, the average cheating probability over all cheating and original vectors, i.e., $\overline{\rho} = \frac{1}{n} \cdot 2^{-n} \sum_{c=1}^{n} \sum_{\alpha \in V_n} \rho_{c,\alpha}$, satisfies $\overline{\rho} \geq \frac{1}{2}$, and the equality holds $\Longleftrightarrow$ $\rho_{c,\alpha}$ satisfies $\rho_{c,\alpha} = \frac{1}{2}$ for every cheating vector δ_c and every original vector α. In this case the secret sharing is said to be cheating immune. We further establish a relationship between cheating-immune secret sharing and cryptographic criteria of boolean functions. This enables us to construct cheating-immune secret sharing.

1 Introduction and Background

Since its invention in 1978 by Blakley [2] and Shamir [9], secret sharing has evolved dramatically. Initially, it was designed to facilitate a distributed storage for a secret in an unreliable or insecure environment. Later, however, secret sharing has been incorporated into public key cryptography giving rise to the well-known concept of group or society oriented cryptography (see [5]). Now secret sharing is one of the basic cryptographic tools with variety of very interesting schemes based on algebraic or geometric structures. Tompa and Woll [11] observed that Shamir secret sharing can be subject to cheating by dishonest participants. The cheater is able to recover the valid secret from the invalid one passed by the combiner. As the result, the honest participants are left with invalid secret while the cheater holds the valid one. This observation is true for all linear secret sharing. The cheating attack can also be extended for geometrical secret sharing. Cheating prevention can be considered in the context of conditionally and unconditionally secure secret sharing. We focus our attention on unconditionally secure secret sharing. In this setting, cheating can be thwarted by (1) share verification by the combiner – all invalid shares are identified and discarded, where the key recovery goes ahead only if there are enough valid shares to recover the valid secret (see $[3, 4, 6]$), and (2) discouraging cheaters from sending invalid shares to the combiner – this argument works if the cheater gains no advantage over honest participants. In other words, sending invalid share will result with recovery of an invalid secret which gives no clues to the cheater as to the value of the valid secret. We intend to consider a class of secret sharing for which, a cheating participant is no better off than a participant who tries simply to guess a secret. Ideally, the probability of successful cheating should be equal to the probability of guessing the secret by a participant. To make our considerations explicit, we assume that secret and shares are binary.

For this case we prove that there is a secret sharing, further in the work called *cheating immune*, that gives no advantage to a cheater making it, in a sense, immune against cheating.

Secret sharing allows a group of participants $\mathcal{P} = \{P_1, \ldots, P_n\}$ to collectively hold a secret $K \in \mathcal{K}$, where $\mathcal{K}$ is a set of elements from which the secret is drawn. Secret sharing is created by a trusted algorithm called a *dealer* who for a given secret, generates a collection of shares $s_i \in \mathcal{S}$, where $\mathcal{S}$ is a set of shares. Note that s_i is given to P_i, $i = 1, \ldots, n$. The collective ownership of the secret is defined by the access structure of secret sharing. The access structure Γ is a collection of subgroups of $\mathcal{P}$ that are authorized to recover the secret. An authorized group of participants $\mathcal{A} \in \Gamma$ is able to reconstruct the secret by invoking a trusted algorithm called *combiner.* The combiner always returns the valid secret if the group $\mathcal{A}$ submits their valid shares. If the group, however, is too small, i.e. $\mathcal{A} \notin \Gamma$, then the algorithm returns a value which is not the valid secret (with an overwhelming probability). In this work, we describe a secret sharing by a set of *distribution rules* [10], where a distribution rule is a function $f : \mathcal{P} \to \mathcal{S}$ that represents possible distribution of shares to the participants. In other words, secret sharing is a set $\mathcal{F} = \bigcup_{K \in \mathcal{K}} \mathcal{F}_K$ where $\mathcal{F}_K$ is a distribution rule corresponding to the secret K. Equivalently, $\mathcal{F}$ can be presented in the form of *distribution table* $\mathcal{T}$. The table has $(n + 1)$ columns – the first one includes secrets and the other n ones list shares assigned to participants $(P_1, \ldots, P_n)$, respectively. Each row of the distribution table specifies the secret for a collection of shares held by $\mathcal{P}$. Note that $\mathcal{F}_K$ can be seen as a part of the distribution table with rows whose first entry is K. This table is denoted by $\mathcal{T}_K$. Most of practical secret sharing schemes are linear and therefore subject to an attack observed by Tompa and Woll [11]. The attack permits a dishonest participant who at the pooling stage submits an invalid share, to recover the valid secret from an invalid one returned by the combiner.

2 Model of Cheating

We introduce the following notations. Set $\alpha = (s_1, \ldots, s_n)$, the sequence of shares held by $\mathcal{P}$ and the secret $K = f(\alpha)$, and $\alpha^* = (s_1, \ldots, s_{c-1}, 1 \oplus s_c, s_{c+1}, \ldots, s_n)$, the sequence of shares submitted to the combiner where P_c modified her share. Set $\delta_c = (0, \ldots, 0, 1, 0, \ldots, 0)$ where all zero except the c-th position. δ_c represents modification done by the cheater and $K^* = f(\alpha^*)$ is the invalid secret returned by combiner. Let $\Omega^*_\alpha = \{(x_1, \ldots, x_{c-1}, s_c, x_{c+1}, \ldots, x_n) | \; f(x_1, \ldots, x_{c-1}, 1 \oplus s_c, x_{c+1}, \ldots, x_n) = K^*\}$, the set of all shares taken from rows of $\mathcal{T}$ containing α and K which are consistent with the invalid secret returned by the combiner. The set Ω^*_α determines the view of the cheater after getting back K^* from the combiner. Let $\Omega_\alpha = \{(x_1, \ldots, x_{c-1}, s_c, x_{c+1}, \ldots, x_n) | \; f(x_1, \ldots, x_{c-1}, s_c, x_{c+1}, \ldots, x_n) = K\}$, the set of rows which contain the current share of P_c and the valid secret K. The function f is called *defining function.* The nonzero vector $\delta_c = (0, \ldots, 0, 1, 0, \ldots, 0)$, where only the c-th coordinate is nonzero, is called the *cheating vector.* $\alpha = (s_1, \ldots, s_n)$ is called the *original vector.* The value of $\rho_\alpha = \#(\Omega^*_\alpha \cap \Omega_\alpha)/\#\Omega^*_\alpha$, where $\#X$ denotes the the number of elements in the set

X, expresses the probability of cheater success with respect to $\alpha = (s_1, \ldots, s_n)$. As the original vector $\alpha = (s_1, \ldots, s_n)$ is always in $\Omega_\alpha^* \cap \Omega_\alpha$, the probability of successful cheating is always nonzero or $\rho_{c,\alpha} > 0$. Given secret sharing with its defining function f on V_n. The value of $\rho_c = 2^{-n} \sum_{\alpha \in V_n} \rho_{c,\alpha}$ is the average cheating probability over all original vectors in V_n for a fixed cheating vector. The value of $\overline{\rho} = \frac{1}{n} \sum_{c=1}^{n} \rho_c = \frac{1}{n} \cdot 2^{-n} \sum_{c=1}^{n} \sum_{\alpha \in V_n} \rho_{c,\alpha}$ is the average cheating probability over all cheating vectors (with Hamming weight one) and all original vectors in V_n. Of course $\overline{\rho}$ depends on particular f.

Theorem 1. *Given secret sharing with its defining function f on V_n. Then for each fixed integer c with $1 \leq c \leq n$, we have $\rho_c \geq \frac{1}{2}$ where the equality holds $\Longleftrightarrow$ $\rho_{c,\alpha} = \frac{1}{2}$ for each $\alpha \in V_n$.*

Proof. Write $y = (x_1, \ldots, x_{c-1})$ and $z = (x_{c+1}, \ldots, x_n)$. Set $R_1 = \{(y,z) | f(y, 1, z) = 1,\ f(y, 0, z) = 1\}$, $R_2 = \{(y,z) | f(y,1,z) = 1,\ f(y,0,\ z) = 0\}$, $R_3 = \{(y,z) | f(y,1,z) = 0,\ f(y,0,\ z) = 1\}$, $R_4 = \{(y,z) | f(y,1,z) = 0,\ f(y,0,\ z) = 0\}$, and $\# R_i = r_i$, $i = 1,2,3,4$. Obviously $r_1 + r_2 + r_3 + r_4 = 2^{n-1}$. Let $\beta_1 \in V_{c-1}$, $\beta_2 \in V_{n-c}$ and $\alpha = (\beta_1, 0, \beta_2)$ or $\alpha = (\beta_1, 1, \beta_2)$. By definition, $\rho_{c,\alpha}$ can be expressed as follows: (1) $\frac{r_1}{r_1+r_2}$ when $\alpha = (\beta_1, 0, \beta_2)$ with $(\beta_1, \beta_2) \in R_1$, (2) $\frac{r_2}{r_1+r_2}$ when $\alpha = (\beta_1, 0, \beta_2)$ with $(\beta_1, \beta_2) \in R_2$, (3) $\frac{r_3}{r_3+r_4}$ when $\alpha = (\beta_1, 0, \beta_2)$ with $(\beta_1, \beta_2) \in R_3$, (4) $\frac{r_4}{r_3+r_4}$ when $\alpha = (\beta_1, 0, \beta_2)$ with $(\beta_1, \beta_2) \in R_4$, (5) $\frac{r_1}{r_1+r_3}$ when $\alpha = (\beta_1, 1, \beta_2)$ with $(\beta_1, \beta_2) \in R_1$, (6) $\frac{r_3}{r_1+r_3}$ when $\alpha = (\beta_1, 1, \beta_2)$ with $(\beta_1, \beta_2) \in R_3$, (7) $\frac{r_2}{r_2+r_4}$ when $\alpha = (\beta_1, 1, \beta_2)$ with $(\beta_1, \beta_2) \in R_2$, (8) $\frac{r_4}{r_2+r_4}$ when $\alpha = (\beta_1, 1, \beta_2)$ with $(\beta_1, \beta_2) \in R_4$. There exist following two cases to be considered:

Case 1: $R_j \cup R_i \neq \emptyset$ for each $(j,i) \in \{(1,2),(3,4),(1,3),(2,4)\}$. In this case $r_j + r_i \neq 0$ for each $(j,i) \in \{(1,2),(3,4),(1,3),(2,4)\}$. Therefore $\rho_c = 2^{-n} \sum_{\alpha \in V_n} \rho_{c,\alpha} = 2^{-n}(\frac{r_1^2}{r_1+r_2} + \frac{r_2^2}{r_1+r_2} + \frac{r_3^2}{r_3+r_4} + \frac{r_4^2}{r_3+r_4} + \frac{r_1^2}{r_1+r_3} + \frac{r_3^2}{r_1+r_3} + \frac{r_2^2}{r_2+r_4} + \frac{r_4^2}{r_2+r_4})$. It is easy to see that $\frac{a^2+b^2}{a+b} \geq \frac{1}{2}(a+b)$ for any two real numbers $a, b \geq 0$ with $a + b > 0$ where the equality holds $\Longleftrightarrow$ $a = b$. Therefore $\rho_c \geq 2^{-n}(\frac{1}{2}(r_1+r_2) + \frac{1}{2}(r_3+r_4) + \frac{1}{2}(r_1+r_3) + \frac{1}{2}(r_2+r_4)) = 2^{-n}(r_1+r_2+r_3+r_4) = \frac{1}{2}$ where the equality holds $\Longleftrightarrow$ $r_1 = r_2 = r_3 = r_4$ $\Longleftrightarrow$ $\rho_{c,\alpha} = \frac{1}{2}$ for each $\alpha \in V_n$.

Case 2: $R_{j_0} \cup R_{i_0} = \emptyset$ for some $(j_0, i_0) \in \{(1,2), (3,4), (1,3), (2,4)\}$. Without loss of generality let $R_1 \cup R_2 = \emptyset$. Thus $r_1 = r_2 = 0$ and thus $r_3 + r_4 = 2^{n-1}$. There exist following two cases to be considered:

Case 2.1: $R_j \cup R_i \neq \emptyset$ for each $(j,i) \in \{(3,4),(1,3),(2,4)\}$. In this case $r_j + r_i \neq 0$ for each $(j,i) \in \{(3,4),(1,3),(2,4)\}$. Thus $\rho_c = 2^{-n} \sum_{\alpha \in V_n} \rho_{c,\alpha} = 2^{-n}(\frac{r_3^2}{r_3+r_4} + \frac{r_4^2}{r_3+r_4} + \frac{r_3^2}{r_1+r_3} + \frac{r_4^2}{r_2+r_4})$. Since $r_1 = r_2 = 0$, we have $\rho_c = 2^{-n} \sum_{\alpha \in V_n} \rho_{c,\alpha} = 2^{-n}(\frac{r_3^2+r_4^2}{r_3+r_4} + r_3 + r_4) \geq 2^{-n}(\frac{1}{2}(r_3+r_4) + r_3 + r_4) = \frac{3}{4}$.

Case 2.2: $R_{j_1} \cup R_{i_1} = \emptyset$ for some $(j_1, i_1) \in \{(3,4),(1,3),(2,4)\}$. Recall that $r_3 + r_4 = 2^{n-1}$. Thus $(j_1, i_1) \neq (3,4)$. Without loss of generality let $R_1 \cup R_3 = \emptyset$. Thus $r_3 = 0$ and $r_4 = 2^{n-1}$. Therefore $\rho_c = 2^{-n} \sum_{\alpha \in V_n} \rho_{c,\alpha} = 2^{-n}(\frac{r_4^2}{r_3+r_4} + \frac{r_4^2}{r_2+r_4})$. Since $r_2 = r_3 = 0$, we have $\rho_c = 2^{-n}(r_4 + r_4) = 1$.

Summarizing Cases 1 and 2, we have proved that $\rho_c \geq \frac{1}{2}$ where the equality holds $\Longleftrightarrow$ $\rho_{c,\alpha} = \frac{1}{2}$ for each $\alpha \in V_n$. $\square$

Theorem 2. *Given secret sharing with its defining function f on V_n. Then $\overline{\rho} \geq \frac{1}{2}$ where the equality holds $\Longleftrightarrow$ $\rho_{c,\alpha} = \frac{1}{2}$ for each integer c with $1 \leq c \leq n$ and each $\alpha \in V_n$.*

Proof. By using Theorem 1, we have $\overline{\rho} = \frac{1}{n}\sum_{c=1}^{n} \rho_c \geq \frac{1}{2}$. Assume $\overline{\rho} = \frac{1}{2}$. Since $\overline{\rho} = \frac{1}{2}$ and $\rho_c \geq \frac{1}{2}$, $c = 1, \ldots, n$, $\rho_c = \frac{1}{2}$, $c = 1, \ldots, n$. Due to Theorem 1, $\rho_{c,\alpha} = \frac{1}{2}$ for each integer c with $1 \leq c \leq n$ and each $\alpha \in V_n$. We have proved the necessity. The sufficiency is obvious. □

3 Cheating Immune Secret Sharing and Its Construction

Due to Theorem 2, if $\min\{\rho_{c,\alpha} | \alpha \in V_n,\ 1 \leq c \leq n\} < \frac{1}{2}$ then $\max\{\rho_{c,\alpha} | \alpha \in V_n,\ 1 \leq c \leq n\} > \frac{1}{2}$. Naturally it is desirable that $\rho_{c,\alpha} = \frac{1}{2}$ for each integer c with $1 \leq c \leq n$ and each $\alpha \in V_n$. In this case the secret sharing is said to be *cheating immune*. Due to Theorems 1 and 2, we conclude

Corollary 1. *Given secret sharing with its defining function f on V_n. Then the following statements are equivalent: (i) $\overline{\rho} = \frac{1}{2}$, (ii) $\rho_c = \frac{1}{2}$ for each integer c with $1 \leq c \leq n$, (iii) $\rho_{c,\alpha} = \frac{1}{2}$ for each integer c with $1 \leq c \leq n$ and each $\alpha \in V_n$.*

Cheating immunity of secret sharing can be investigated in the context of well-known characteristics of the defining function f such as resiliency (see [14]) and the SAC (see [12, 13]).

Theorem 3. *Given secret sharing with its defining function f on V_n. Then the secret sharing is cheating immune $\Longleftrightarrow$ f is 1-resilient and satisfies the SAC.*

Proof. We keep using the notations in the proof of Theorem 1. It is easy to verify that $f(x_1, \ldots, x_n)|_{x_c=1}$ is balanced (1-resiliency) $\Longleftrightarrow$ $r_1 + r_2 = r_3 + r_4$, while $f(x_1, \ldots, x_n)|_{x_c=0}$ is balanced (1-resiliency) $\Longleftrightarrow$ $r_1 + r_3 = r_2 + r_4$. From the proof of Theorem 1, $f(x) \oplus f(x \oplus \delta_c) = \begin{cases} 0 \text{ if } (y,z) \in R_1 \cup R_4 \\ 1 \text{ if } (y,z) \in R_2 \cup R_3 \end{cases}$. Thus $f(x) \oplus f(x \oplus \delta_c)$ is balanced (SAC) $\Longleftrightarrow$ $r_1 + r_4 = r_2 + r_3$. Note that $r_1 + r_2 = r_3 + r_4$, $r_1 + r_3 = r_2 + r_4$ and $r_1 + r_4 = r_2 + r_3$ together $\Longleftrightarrow$ $r_1 = r_2 = r_3 = r_4$. From the proof of Theorem 1, $r_1 = r_2 = r_3 = r_4$ $\Longleftrightarrow$ $\rho_{c,\alpha} = \frac{1}{2}$ for each $\alpha \in V_n$. Due to the arbitrariness of the integer c with $1 \leq c \leq n$, the proof is completed. □

Based on Theorem 3, to construct an cheating immune secret sharing scheme, we need a 1-resilient function on V_n satisfying the SAC.

Theorem 4. *Let $n > 0$ be an even integer. Then there exists a secret sharing with its defining function f on V_n such that (i) this secret sharing is cheating immune, (ii) the nonlinearity (see [14]) of f is equal to $2^{n-1} - 2^{\frac{1}{2}n}$.*

Proof. Let h be a bent function [7] on V_{n-2} (n is even). Set $g(x_1, \ldots, x_{n-1}) = (1 \oplus x_{n-1})h(x_1, \ldots, x_{n-2}) \oplus x_{n-1}(1 \oplus h(x_1 \oplus a_1, \ldots, x_{n-2} \oplus a_{n-2}))$ where the Hamming weight of $(a_1, \ldots, a_{n-2})$ is $\frac{1}{2}n - 1$. Set $f(x_1, \ldots, x_n) = (1 \oplus x_n)g(x_1, \ldots, x_{n-1}) \oplus x_n g(x_1 \oplus 1, \ldots, x_{n-1} \oplus 1)$. From the proof of Theorem 17 of the reference [8], f is 1-resilient, satisfies the SAC and has a nonliearty $2^{n-1} - 2^{\frac{1}{2}n}$. Due to Theorem 3, the secret sharing with defining function f is cheating immune. □

4 Conclusions

For given secret sharing, the average cheating probability $\overline{\rho}$ over all cheating and original vectors, satisfies $\overline{\rho} \geq \frac{1}{2}$, and the equality holds $\Longleftrightarrow$ the cheating probability $\rho_{c,\alpha}$ satisfies $\rho_{c,\alpha} = \frac{1}{2}$ for every cheating vector δ_c and every original vector α. In this case the secret sharing is said to be cheating immune. We further have found a relationship between cheating immune secret sharing and cryptographic criteria of boolean functions, and then we have successfully constructed cheating immune secret sharing with a highly nonlinear defining function.

Acknowledgement

The first author was supported by a Queen Elizabeth II Fellowship (227 23 1002).

References

1. E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, Vol. 4, No. 1:3–72, 1991.
2. G. R. Blakley. Safeguarding cryptographic keys. In *Proc. AFIPS 1979 National Computer Conference*, pages 313–317. AFIPS, 1979.
3. M. Carpentieri. A perfect threshold secret sharing scheme to identify cheaters. *Designs, Codes and Cryptography*, 5(3):183–187, 1995.
4. M. Carpentieri, A. De Santis, and U. Vaccaro. Size of shares and probability of cheating in threshold schemes. *Advances in Cryptology - EUROCRYPT'93*, LNCS No. 765, pages 118–125. Springer-Verlag, 1993.
5. Y. Desmedt. Society and group oriented cryptography: A new concept. *Advances in Cryptology - CRYPTO'87*, LNCS No. 293 pages 120–127. Springer-Verlag, 1988.
6. T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In *Proceedings of 21st ACM Symposium on Theory of Computing*, pages 73–85, 1989.
7. O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory (A)*, 20:300–305, 1976.
8. P. Sarkar and S. Maitra. Highly nonlinear balanced boolean functions with important cryptographic properties. *Advances in Cryptology - EUROCRYPT2000*, LNCS No. 1807, pages 485–506. Springer-Verlag, 2000.
9. A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, November 1979.
10. D.R. Stinson. *Cryptography: Theory and Practice.* CRC Press, 1995.
11. M. Tompa and H. Woll. How to share a secret with cheaters. *Journal of Cryptology*, 1(2):133–138, 1988.
12. A. F. Webster. Plaintext/ciphertext bit dependencies in cryptographic system. Master's Thesis, Department of Electrical Engineering, Queen's University, Ontario, 1985.
13. A.F. Webster and S.E. Tavares. On the design of S-boxes. *Advances in Cryptology – CRYPTO'85*, pages 523–534. Springer-Verlag, 1986.
14. X. M. Zhang and Y. Zheng. Cryptographically resilient functions. *IEEE Transactions on Information Theory*, 43(5):1740–1747, 1997.