ON CHEATING IMMUNE SECRET SHARING

An Braeken, Svetla Nikova
Department Electrical Engineering, ESAT/COSIC,
Katholieke Universiteit Leuven, Kasteelpark Arenberg 10,
B-3001 Heverlee-Leuven, Belgium
an.braeken,svetla.nikova@kuleuven.ac.be
Ventzislav Nikov
Department of Mathematics and Computing Science,
Eindhoven University of Technology
P.O. Box 513, 5600 MB, Eindhoven, the Netherlands
v.nikov@tue.nl

This work addresses the problem of cheating prevention in secret sharing. The scheme is said to be k-cheating immune if any group of k cheaters has no advantage over honest participants. In this paper we study the constraints of cheating immune secret sharing schemes. We give a necessary and sufficient condition for SSSs to be cheating immune. Then, we improve the upper bound of D'Arco et. al on the number of cheaters tolerated in such scheme. Our proof is much simpler than the proof of D'Arco et. al and relies on certain properties of cryptographic Boolean functions. As a result of independent interest we provide a condition given function to be t-resilient and to satisfy the propagation criterion of degree ℓ over any finite field.

INTRODUCTION

Secret sharing is widely used to produce group-oriented cryptographic algorithms, systems and protocols. Informally, a secret sharing scheme (SSS) is a method of sharing a secret K among a finite set of participants in such a way that certain specified subsets of participants can compute the secret K by pooling together. Cheating prevention is an important problem in SSS. As proven by Tompa and Woll [9], dishonest players can cheat in any linear SSS. The cheaters are able to recover the valid secret from the invalid one passed by the combiner. Recently Pieprzyk and Zhang [4] have proposed an approach to deal with cheaters, namely by discouraging them from sending invalid shares to the combiner. This means that dishonest participants have no advantage in submitting uncorrect shares compared to honest participants.

Let the secret be defined by the image of a function with inputs the shares of the participants: $f : \mathbb{F}_q^n \to \mathbb{F}_q$ where $\mathbb{F}_q$ is the finite field of q elements and $q = p^s$ with p prime. Let us call this function a *defining function* of the SSS. We also assume that we are dealing with (n, n) threshold scheme where only all n participants together are able to determine the secret.

In this paper we derive a necessary and sufficient condition for the defining function to produce SSSs that are cheating immune and strictly cheating immune. Then we improve the known upper bound for the number of cheaters based on a relation between the required properties of the defining function. This relation was known for Boolean functions, but now it is proven that it halds also for functions over any finite field.

MODEL OF CHEATING

We consider (n, n) threshold schemes, i.e. schemes for which only all n participants together are able to determine the secret. These schemes are represented by a set of distribution rules combined in a table. The secret K is computed by the defining function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ where $\mathbb{F}_q$ is the finite field of $q = p^s$ elements with p prime and $s \geq 1$. Denote the sequence of shares held by the participants $\mathcal{P} = \{P_1, \dots, P_n\}$ by the vector α and the secret $K = f(\alpha)$. Represent the cheaters by the vector $\delta \in \mathbb{F}_q^n$, also called cheating vector, in which the non-zero elements denote the deviations of the exact values. For any two vectors x, δ, the vector x_δ^+ satisfies $x_j^+ = x_j$ if $\delta_j \neq 0$ and $x_j^+ = 0$ otherwise. Conversely, the vector x_δ^- satisfies $x_j^- = x_j$ if $\delta_j = 0$ and $x_j^- = 0$ otherwise. Denote the weight of a vector v by $wt(v)$. The number of cheaters is equal to $wt(\delta)$. We are following the model and the notations from [1, 2, 4, 5, 6]. Let define the following sets:

$$
\begin{aligned}
R(\delta, \alpha_\delta^+, K) &= \{x_{\delta^-} | f(x_\delta^- + \alpha_\delta^+) = K\}; \\
R(\delta, \alpha_\delta^+ + \delta, K^*) &= \{x_{\delta^-} | f(x_\delta^- + \alpha_\delta^+ + \delta) = K^*\}.
\end{aligned}
$$

The first set represents the collection of rows of the table with the correct K and valid shares held by the cheaters. The second set represents the view of the cheater after getting back K^* from the combiner. As a consequence, the probability of successful cheating with respect to α and cheating vector δ is given by

$$
\varrho_{\delta,\alpha} = \frac{|R(\delta, \alpha_\delta^+ + \delta, K^*) \cap R(\delta, \alpha_\delta^+, K)|}{|R(\delta, \alpha_\delta^+ + \delta, K^*)|}.
$$

Definition 1 *[4, 5, 6] A secret sharing scheme (SSS) is said to be k-cheating immune if $\varrho_{\delta,\alpha} = q^{-1}$ for every $\alpha \in \mathbb{F}_q^n$ and $\delta \in \mathbb{F}_q^n$ where $1 \leq wt(\delta) \leq k$.*

In the above definition, all cheaters are assumed to submit invalid shares. This can be generalized in a model where cheaters may submit a mixture of valid and invalid shares. To write out this definition, a vector $\tau \in \mathbb{F}_q^n$ is used to specify the cheating values and a binary vector δ to denote the cheaters. For any $\tau \preceq \delta$ ($\tau_j \neq 0$ if $\delta_j \neq 0$), we consider the following probability with respect to δ, τ, α:

$$\varrho_{\delta,\tau,\alpha} = \frac{|R(\delta, \alpha_\delta^+ + \tau, K^*) \cap R(\delta, \alpha_\delta^+, K)|}{|R(\delta, \alpha_\delta^+ + \tau, K^*)|}.$$

Definition 2 *[5, 6] An SSS is called k-strictly cheating immune if $\varrho_{\delta,\tau,\alpha} = q^{-1}$ for every $\alpha, \tau, \delta \in \mathbb{F}_q^n$ such that $\tau \preceq \delta$, and $1 \leq wt(\tau) \leq wt(\delta) \leq k$.*

PROPERTIES OF THE DEFINING FUNCTION

As it has been proven in [6], the following equivalence can be derived for k-cheating immune SSS.

Theorem 3 *[6] An SSS with defining function f is k-cheating immune if and only if for any integer l with $1 \leq l \leq k$, for any vectors $\delta, \tau \in \mathbb{F}_q^n$ with $wt(\delta) = l$ and $\tau \preceq \delta$, and for any $u, v \in \mathbb{F}_q$ simultaneously holds that*

$$\begin{aligned} |R(\delta, \tau, v)| &= q^{n-l-1}; \\ |R(\delta, \tau, v) \cap R(\delta, \tau + \delta, u)| &= q^{n-l-2}. \end{aligned}$$

We now prove that the conditions of Theorem 3 imply certain properties for the defining function f of the SSS. Therefore, we first give a formal definition of these properties.

Definition 4 *[8] A function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ is said to be t-correlation-immune if and only if for every t-subset $\{i_1, \ldots, i_t\} \subseteq \{1, \ldots, n\}$, for every choice of $z_j \in \mathbb{F}_q$ with $1 \leq j \leq t$ and for every $y \in \mathbb{F}_q$ holds that*

$$P(f(x_1, \ldots, x_n) = y \mid x_{i_j} = z_j, 1 \leq j \leq t) = q^{-1}.$$

If the function is also balanced, then the function is said to be t-resilient.

Definition 5 *[7] A function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ is said to satisfy the propagation criterion of degree ℓ if and only if for any non-zero word a, such that $wt(a) \leq \ell$, the function $f(x+a) - f(x)$ is balanced (0-resilient).*

In the context of cheating immune secret sharing schemes, the following property seems to be relevant.

Definition 6 *[4, 5, 6] A function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ is said to satisfy the strengthened propagation of degree k, denoted by $B(k)$, if $f(x_\delta^- + \tau + \delta) - f(x_\delta^- + \tau)$ is a balanced function on $\mathbb{F}_q^n$, where $\tau, \delta \in \mathbb{F}_q^n$ are as in Definition 2.*

In [5], the relation between the strengthened propagation criterion of degree k and the propagation criterion of degree k is proven for characteristic 2. It is easy to see that this relation also holds for fields of characteristic $q \geq 2$.

Theorem 7 *If $f : \mathbb{F}_q^n \to \mathbb{F}_q$ satisfies the strengthened propagation of degree k then f satisfies the propagation criterion of degree k.*

We now show how these properties can be used in order to produce a defining function for a cheating immune SSS. In [6] the authors have shown a construction, which leads to a defining function for a k-cheating immune SSS, but no general properties of the defining function were mentioned. In [5] the analogous theorem is given over $\mathbb{F}_2$.

Theorem 8 *An SSS with defining function f is k-cheating immune if and only if the function f is k-resilient and satisfies $B(k)$.*

Proof. We use the same definitions and conditions for δ and τ as in Theorem 3. From the definition of δ and τ, the function $f(x_\delta^- + \tau)$ is defined on $\mathbb{F}_q^{n-l}$ (l fixed variables). Moreover, the function is balanced by the first condition of Theorem 3. As a consequence, the defining function is k-resilient.

It can be easily seen that the second condition of Theorem 3 can also be interpreted as follows. The system of equations for all u, v, τ, δ

$$\begin{cases} f(x_\delta^- + \tau + \delta) = u \\ f(x_\delta^- + \tau) = v \end{cases}$$

has exactly q^{n-l-2} solutions for x_δ^-. This implies that $f(x_\delta^- + \tau + \delta) - f(x_\delta^- + \tau) = u - v$ for q^{n-l-2} choices of x_δ^-. Because this property holds for all q^2 possibilities of the tuple (u, v), we can conclude that the function satisfies $B(k)$. $\square$

The following relation between cheating immune and strictly cheating immune SSS is known.

Theorem 9 *[6] An SSS is strictly k-cheating immune if and only if for any integer r with $0 \leq r \leq k-1$, any subset $\{j_1, \ldots, j_r\}$ of $\{1, \ldots, n\}$ and any $a_1, \ldots, a_r \in \mathbb{F}_q$, the function $f(x_1, \ldots, x_n)_{|x_{j_1}=a_1, \ldots, x_{j_r}=a_r}$ as a function on $\mathbb{F}_q^{n-r}$ is the defining function on $\mathbb{F}_q^{n-r}$ of a $(k-r)$-cheating immune SSS.*

As a consequence, combining Theorem 8 and Theorem 9, we derive a necessary and sufficient condition on the defining function of a strictly cheating immune SSS.

Corollary 10 *An SSS with defining function f is strictly k-cheating immune if and only if all subfunctions f', which are derived from the function f by fixing at most $k-1$ variables to arbitrary values in $\mathbb{F}_q$, are k-resilient and satisfy $B(k)$.*

BOUNDS ON THE NUMBER OF CHEATERS

Recently an upper bound for the number of cheaters has been proven by D'Arco *e*t. al.

Theorem 11 *[1, 2] Let f be a function defined over $GF(q)^n$. An SSS defined by f can be k-cheating immune only if $2k < n$.*

We improve this bound for fields of characteristic 2 and find a similar result for fields of general characteristic. For characteristic 2, it suffices to combine Theorem 7 and Theorem 8, together with the following well-known theorem:

Theorem 12 *[10, Theorem 2] Let f be a Boolean function on $GF(2)^n$. If f is t-resilient and satisfies the propagation criterion of degree ℓ then $t + \ell < n$. Moreover $t + \ell = n - 1 \iff t = 0,\ \ell = n-1$ and n is odd.*

Corollary 13 *Let f be a Boolean function of n binary variables. An SSS defined by f can be k-cheating immune only if $2k \leq n-2$.*

We will prove that the first part of Theorem 12 also holds for functions defined over any finite alphabet $\mathcal{F}$ of order $q \geq 2$ endowed with the structure of an abelian group. Therefore, we need to introduce some general background on the theory of finite groups.

Recall that the homomorphisms from the abelian group $\mathcal{F}$ into the multiplicative group $\mathbb{C}$ form an abelian group $\mathcal{F}'$, called the characters group which is isomorphic with $\mathcal{F}$. For $x \in \mathcal{F}$ and $y \in \mathcal{F}'$, we denote $\langle x, y\rangle$ the complex image of x under the character y. Moreover, for all $x, y \in \mathcal{F}$, the value $\langle -x, y\rangle = \overline{\langle x, y\rangle}$, or also the element $-x$ represents the symmetric x ($x - x = 0$) and $\overline{\langle x, y\rangle}$ represents the conjugate of $\langle x, y\rangle$.

For example if $\mathcal{F}$ is the additive group $(\mathbb{F}_q, +)$ where $q = p^s$, p a prime, then $\langle x, y\rangle = \theta^{tr_{\mathbb{F}_q/\mathbb{F}_p}(xy)}$ where θ is a primitive p-th root of unity in $\mathbb{C}$. Note that for $q = 2$, $\langle x, y\rangle = (-1)^{xy}$. If $\mathcal{F}$ is the additive cyclic group $(\mathbb{Z}_q, +)$ of order q, then $\langle x, y\rangle = \theta^{xy}$ with θ a primitive q-th root of unity in $\mathbb{C}$ and the product xy is performed in the ring $\mathbb{Z}_q$.

We need the following classical lemma:

Lemma 14 *For any subspace V of any finite alphabet $\mathcal{F}$ of order $q \geq 2$ endowed with the structure of an abelian group and for all $u \in \mathcal{F}'$, it holds that*

$$\sum_{x \in V} \langle x, u\rangle = \begin{cases} |V| & \text{if } u \in V^{\perp}; \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

For the sake of simplicity, we assume that we work in the field $\mathbb{F}_q$, where $q = p^s$ with p prime. We also denote the trace function in the field by $tr(xy)$ instead of $tr_{\mathbb{F}_q/\mathbb{F}_p}(xy)$. The definitions of Walsh transform W_f and autocorrelation r_f of a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ are given by:

$$W_f(w) = \sum_x \theta^{tr(f(x) - wx)} \text{ and } r_f(w) = \sum_x \theta^{f(x+w) - f(x)}. \tag{2}$$

As it is proven in [3], a function is t-resilient if and only if $W_f(w) = 0$ for all w with $wt(w) \leq t$. Analogously, a function satisfies the propagation criterion of degree l if and only if $r_f(w) = 0$ for all w with $wt(w) \leq l$.

We now generalize the Wiener-Klitchine theorem for finite fields.

Lemma 15 *For any function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ where $q = p^s$ with p prime, the following relations between the Walsh spectrum and the autocorrelation spectrum of the function f hold:*

$$W_{r_f}(s) = W_f(s)\overline{W_f(s)} \text{ and } r_f(k) = q^{-n} \sum_{s \in \mathbb{F}_q^n} W_f(s)\overline{W_f(s)}\theta^{tr(sk)}. \tag{3}$$

Proof. We start with the first equality by using (2).

$$\begin{aligned} W_{r_f}(s) &= \sum_{w\in\mathbb{F}_q^n} r_f(w)\theta^{tr(-ws)} = \sum_{w\in\mathbb{F}_q^n}\sum_{x\in\mathbb{F}_q^n} \theta^{tr(f(x+w)-f(x)-ws)} \\ &= \sum_{k\in\mathbb{F}_q^n}\sum_{x\in\mathbb{F}_q^n} \theta^{tr(f(k)-f(x)-ks+xs)} = \sum_{k\in\mathbb{F}_q^n} \theta^{tr(f(k)-ks)} \sum_{x\in\mathbb{F}_q^n} \theta^{tr(-f(x)+xs)} \\ &= W_f(s)\overline{W_f(s)}. \end{aligned}$$

Using this equality, we derive:

$$\begin{aligned} \sum_{s\in\mathbb{F}_q^n} W_f(s)\overline{W_f(s)}\theta^{tr(sk)} &= \sum_{s\in\mathbb{F}_q^n}\sum_{w\in\mathbb{F}_q^n} r_f(w)\theta^{tr(-ws)}\theta^{tr(sk)} \\ &= \sum_{w\in\mathbb{F}_q^n} r_f(w) \sum_{s\in\mathbb{F}_q^n} \theta^{tr((-w+k)s)} = r_f(k)\, q^n. \end{aligned}$$

In the last step of the the proof, we used Lemma 14. $\square$

Lemma 16 *For any affine subspace $V \subseteq \mathbb{F}_q^n$ and any function from $\mathbb{F}_q^n$ into $\mathbb{F}_q$ where $q = p^s$ with p prime:*

$$\sum_{k\in V} r_f(k) = \frac{1}{|V^\perp|}\sum_{s\in V^\perp} W_f(s)\overline{W_f(s)}. \tag{4}$$

Proof. Using (3) and Lemma 14 we have:

$$\begin{aligned} &\sum_{k\in V} r_f(k) = \sum_{k\in V} q^{-n} \sum_{s\in\mathbb{F}_q^n} W_f(s)\overline{W_f(s)}\theta^{tr(sk)} \\ &= q^{-n}\sum_{s\in\mathbb{F}_q^n} W_f(s)\overline{W_f(s)}\sum_{k\in V}\theta^{tr(sk)} = \frac{1}{|V^\perp|}\sum_{s\in V^\perp} W_f(s)\overline{W_f(s)}. \end{aligned}$$

$\square$

Theorem 17 *If f is t-resilient and satisfies the propagation criterion of degree l, then $t + l \leq n - 1$.*

Proof. Consider equation (4) with $V_a = \{u \in \mathbb{F}_q^n : u_i = 0 \text{ if } a_i \neq 0\}$ for any a such that $wt(a) = l$. The dual vector space is defined by $V^\perp = \{u \in \mathbb{F}_q^n : u_i = 0 \text{ if } a_i = 0\}$. As a consequence, equation (4) leads to

$$q^{2n-p} = \sum_{s\in V^\perp} W_f(s)\overline{W_f(s)}. \tag{5}$$

Because $wt(u) \leq n-l$ for any $u \in V^{\perp}$ and f is t-reslient, t should be strictly less than $n-l$, because otherwise we arrive at contradiction with equation (5). $\square$

This theorem leads to the same bound on the number of cheaters as proven by D'Arco *et*. al. The proof is totally different, much shorter and exploits a relation between the properties of the defining function of the SSS. Moreover, from Theorem 17, we derive that any (n, n) perfect SSS can never be cheating immune because an (n, n) perfect SSS is defined by a $(n-1)$-resilient function.

REFERENCES

[1] P. D'Arco, W. Kishimoto, D. Stinson, On Cheating-Immune Secret Sharing, *International Workshop on Coding and Cryptography (WCC 2003)*, 2003.

[2] P. D'Arco, W. Kishimoto, D. Stinson, Properties and Constraints of Cheating-Immune Secret Sharing Scheme, *Applied Discrete Mathematics* (to appear).

[3] K. Gopalakrishan, D.R. Stinson, Three Characterizations of Non-Binary Correlation-Immune and Resilient Functions, Designs, Codes and Cryptography, Vol. 5, pp. 241-251, 1995.

[4] J. Pieprzyk, X.-M. Zhang, Cheating Immune Secret Sharing, *ICICS 2001*, LNCS 2229, pp. 144-149, 2001.

[5] J. Pierpzyk, X.M. Zhang, Constructions of Cheating Immune Secret Sharing, *ICICS 2001*, LNCS 2288, pp. 226-243, 2002.

[6] J. Pieprzyk, X.-M. Zhang, Cheating Prevention in Secret Sharing over $GF(p^t)$, *Indocrypt 2001*, LNCS 2247, pp. 79-90, 2001.

[7] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts and J. Vandewalle, Propagation Characteristics of Boolean Functions, *EUROCRYPT'90*, LNCS 473, pp. 161-173, 1991.

[8] T. Siegenthaler, Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications, *IEEE Trans. on Inf. Theory*, Vol. 30, Nr. 5, pp. 776-780, 1984.

[9] M. Tompa, H. Woll, How to Share a Secret with Cheaters, Journal of Cryptography, Vol, 1, Nr. 2, 1988, pp. 133-138.

[10] Y. Zheng, X.M. Zhang. On Relationships among Avalanche, Nonlinearity, and Correlation Immunity, *Asiacrypt 2000*, LNCS 1976, 470-482, 2000.