Nonlinear Secret Sharing Immune against Cheating

Josef Pieprzyk
Department of Computing
Macquarie University
Sydney , NSW 2109, AUSTRALIA
E-mail: josef@ics.mq.edu.au

Xian-Mo Zhang
School of IT and CS
University of Wollongong
Wollongong NSW 2522, AUSTRALIA
E-mail: xianmo@cs.uow.edu.au

Abstract

The paper investigates the design of secret sharing that is immune against cheating (as defined by the Tompa-Woll attack). We examine secret sharing with binary shares and secrets. Bounds on the probability of successful cheating are given for two cases. The first case relates to secret sharing based on bent functions and results in a non-perfect scheme. The second case considers perfect secret sharing built on highly nonlinear balanced Boolean functions.

1. Introduction

Secret sharing is a cryptographic tool that allows to convert the control over cryptographic algorithms and protocols from a single participant to a group of participants. Secret sharing embedded into encryption/decryption algorithms gave rise to the well-known concept of group-oriented cryptography in which the cryptographic algorithm can be successfully executed only if there is a big enough group of participants who have agreed to collaborate.

The assumption about trust is vital to make the concept of group cryptography work. Numerous examples, however, show that in some circumstances, people can be tempted to behave dishonestly especially when they can get a substantial advantage with no risk involved. The group oriented cryptography applies two basic approaches to combat cheating:

- verification of the final state of the protocol or algorithm – this allows to identify whether or not the final result is correct or in other words, participants are able to detect whether or not the protocol has failed to achieve the expected result (additionally collaborating participants may be able to identify the cheater(s)),
- removal of the main incentive of cheating – a potential cheater is not able to get advantage over other (honest) participants. In other words, an unsuccessful run of the protocol/algorithm provides no useful information for the cheater.

In the verification approach, some information about secret sharing is made public and can be used to verify whether the supplied input data or the results are consistent. Particular implementations of verification varies depending on whether the secret sharing in hand is conditionally or unconditionally secure.

The second approach is, in general, more efficient (no verification information to store and no extra verification steps) and more importantly is a real option when the final result, if wrong, will be instantly identified and rejected while providing no information about the correct result to the cheater. The cheater would be equivalent to a participant who does not agree to collaborate but, for some reasons, does not want to say “no”.

The paper deals with cheating prevention in unconditionally secure secret sharing. We assume that at the pooling stage, the cheating participant fails to provide the correct shares while other participants follow honestly the protocol. The combiner recovers the secret are returns to all currently active participants. We expect that the cheater will not be “substantially” better off in guessing the secret before and after the pooling.

The paper is structured as follows. Section 2 sets up the scene for the paper and introduces the nonlinear secret sharing. Section 3 gives a background of binary sequences that is used further in the paper. Defining functions of secret sharing are defined and their properties are investigated in Section 4. Sections 5 and 6 discuss immunity against cheating when defining functions of secret sharing are bent or highly nonlinear balanced boolean functions. Closing conclusions and future research directions close the paper.

2. Model of Secret Sharing

We are going to use the following notations;

- $\mathcal{P} = \{P_1, \ldots, P_n\}$ is a group of n participants who collectively hold a secret $K \in \mathcal{K}$,
- $\mathcal{K}$ is a set from which the secret K is drawn. When it is chosen at random (with the uniform probability), we write $K \in_R \mathcal{K}$.
- $\mathcal{S}$ is a set from which all shares are selected. The notation $s_i \in \mathcal{S}$ reads that a share s_i assigned to the participant P_i has been chosen from $\mathcal{S}$.
- Γ is the access structure or the collection of all subgroups of $\mathcal{P}$ that are authorised to jointly recover the secret.
- (t,n) threshold secret sharing allows any subgroup with at least t members to recover the secret. In other words, $\Gamma = \{\mathcal{A} | \#\mathcal{A} \geq t\}$.

Secret sharing can be seen as a set of *distribution rules* [12], 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 $\mathcal{T}_K$.

Given secret sharing with $\mathcal{F}$ and the access structure Γ. Secret sharing is *perfect* if

- any authorised subgroup $\mathcal{A} \in \Gamma$ is able to identify the unique secret (i.e. they can jointly identify a single row in the table $\mathcal{T}$),
- any unauthorised subgroup $\mathcal{A} \notin \Gamma$ has to choose secret from the set of possible candidates with the probability of success equal to $\frac{1}{\#\mathcal{K}}$ assuming that K is chosen at random (i.e. the collection of rows corresponding to the shares held by $\mathcal{A}$ consists of secrets which are uniformly distributed).

Tompa and Woll [13] observed that all linear secret sharing schemes are vulnerable to cheating by dishonest participants. Their attack further referred to as the TW attack, proceeds as follows. Given a (t,n) threshold scheme and a linear function $\ell_{\mathcal{A}} : \mathcal{S}^t \to \mathcal{K}$ which for a collection of t shares and the currently active subgroup
$\mathcal{A} = \{P_1, \ldots, P_t\} \in \Gamma$ uniquely determines the secret K. Assume that our cheater is P_1.

- At the pooling stage, instead of the valid share s_1, P_1 submits a fake one $s_1^* = s_1 + \delta$.
- The combiner takes all shares and computes the secret $K^* = \ell_{\mathcal{A}}(s_1^*, s_2, \ldots, s_c)$. The secret K^* is returned to $\mathcal{A}$ via secure channels.
- Knowing the modification δ, the cheater computes $\Delta = \ell_{\mathcal{A}}(\delta, 0, \ldots, 0)$, and recovers the valid secret $K = K^* - \Delta$. Note that P_1 does not know shares of honest participants from $\mathcal{A}$.

The attack works because linearity of the scheme assures the cheater that

$$\begin{aligned} K^* &= \ell_{\mathcal{A}}(s_1^*, s_2, \ldots, s_c) = \ell_{\mathcal{A}}((s_1, \ldots, s_c) \\ &\quad +(\delta, 0, \ldots, 0)) = K + \Delta \end{aligned}$$

As the result, honest participants are left with an invalid secret while the cheater has the valid one.

Publicly verifiable secret sharing (see [3, 5, 11, 9]) provide a solution to this problem in the conditionally secure setting. In the unconditionally secure setting, Rabin and Ben-Or [6] used a system of linear equations to validate shares before they are passed into the combiner. Carpentieri in [1] constructed a similar scheme but with shorter shares. Carpentieri, De Santis and Vaccaro [2] argued that share expansion is unavoidable to detect cheating.

In this work we address cheating prevention in the unconditionally secure setting by removing linearity, which is the main property of secret sharing that makes cheating successful. We study nonlinear secret sharing. An additional attraction of this approach is that it uses a similar model to that already well developed in the theory of S-boxes. One would expect that some results obtained there are applicable in cheating prevention. We concentrate on the binary case when $\mathcal{K} = \mathcal{S} = \{0, 1\}$ and arithmetics is done in $GF(2)$.

3. Binary Sequences

We consider a mapping f from V_n to $GF(2)$ where V_n is the vector space of n tuples of elements from $GF(2)$. f is also called a *function* on V_n. The *truth table* of a function f is a sequence defined by $(f(\alpha_0),\ f(\alpha_1),\dots,f(\alpha_{2^n-1}))$, where $\alpha_0=(0,\dots,0,0)$, $\alpha_1=(0,\dots,0,1)$, …, $\alpha_{2^n-1}=(1,\dots,1,1)$. Each α_j is said to be the *binary representation* of integer j, $j=0,1,\dots,2^n-1$. A function f is said to be *balanced* if its truth table contains an equal number of zeros and ones. An *affine* function f on V_n is a function that takes the form of $f(x)=f(x_1,\dots,x_n)=a_1x_1\oplus\cdots\oplus a_nx_n\oplus c$, where $x=(x_1,\dots,x_n)$ and $\oplus$ denotes the addition in $GF(2)$, $a_j,c\in GF(2)$, $j=1,2,\dots,n$. Furthermore f is called a *linear* function if $c=0$. It is easy to verify that any nonzero affine function is balanced. Let $\langle,\rangle$ denote the scalar product of two vectors. There precisely 2^n linear functions on V_n. We can denote all the 2^n linear functions by $\varphi_0,\varphi_1,\dots,\varphi_{2^n-1}$, where $\varphi_j(x)=\langle\alpha_j,x\rangle$. The *Hamming weight* of a vector $\alpha\in V_n$, denoted by $HW(\alpha)$, is the number of nonzero coordinates of α. The Hamming weight of a function f, denoted by $HW(f)$, is the number of nonzero terms in the truth table of f. The *nonlinearity* of a function f on V_n, denoted by N_f, is the minimal Hamming distance between f and all affine functions on V_n, i.e., $N_f=\min_{i=1,2,\dots,2^{n+1}}HW(f\oplus\psi_i)$ where ψ_1, ψ_2, …, $\psi_{2^{n+1}}$ are all the affine functions on V_n. High nonlinearity can be used to resist a linear attack. From [4], we know that $N_f\le 2^{n-1}-2^{\frac{1}{2}n-1}$. A special class of functions is called bent. There exist equivalent definitions of bent functions [8]. For example, a function f on V_n is said to be *bent* if and only if $f(x)\oplus f(x\oplus\alpha)$, is balanced where α is any nonzero vector in V_n. Bent functions have a series of interesting properties. For example, the number of zeros of any bent function on V_n is $\pm 2^{\frac{1}{2}n-1}+2^{n-1}$ [8], in other words, the number of ones of any bent function on V_n is $\mp 2^{\frac{1}{2}n-1}+2^{n-1}$. The sum of any bent function on V_n and any affine function on V_n is bent. Bent functions are not balanced and bent functions on V_n exist only when n is even. Furthermore, it is well known that any bent function f on V_n achieves the maximum nonlinearity, i.e., $N_f=2^{n-1}-2^{\frac{1}{2}n-1}$. We illustrate bent functions by an example. It is easy to prove that both $g(x_1,\dots,x_6)=x_1x_2\oplus x_3x_4\oplus x_5x_6$ and $h(x_1,\dots,x_6)=1\oplus x_1x_2\oplus x_3x_4\oplus x_5x_6$ are bent functions on V_6. Then $N_g=N_h=2^{6-1}-2^{3-1}=28$. By a straightforward verification, we find that the number of zero of g is $36=2^{3-1}+2^{6-1}$ and the number of ones of g is $28=-2^{3-1}+2^{6-1}$ while the number of zero of h is 28 and the number of ones of h is 36.

4. Defining Functions of Secret Sharing

Given a (n,n) threshold scheme defined by its distribution table $\mathcal{T}$. We define a function $f:V_n\to\{0,1\}$ and fix an integer c; $1\le c\le n$, which points the position (column) of the cheater P_c in $\mathcal{T}$. We introduce the following notations:

- $\alpha=(s_1,\dots,s_n)$ is the sequence of shares held by $\mathcal{P}$ and the secret $K=f(\alpha)$,
- $\alpha^*=(s_1,\dots,s_{c-1},1\oplus s_c,s_{c+1},\dots,s_n)$ is the sequence of shares submitted to the combiner where P_c modified her share. The sequence $\delta_c=(0,\dots,0,1,0,\dots,0)$ contains all zero except the c-th position and represents modification done by the cheater, $K^*=f(\alpha^*)$ is the invalid secret returned by combiner,
- $\Omega^*_\alpha=\{(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_n)|\ f(x_1,\dots,x_{c-1},1\oplus\ s_c,x_{c+1},\dots,x_n)=K^*\}$ is 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 determines the view of the cheater after getting back K^* from the combiner.
- $\Omega_\alpha=\{(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_n)|f(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_n)=K\}$

The function f defines the secret sharing. We are going to call it the *defining function*. The vector $\delta_c=(0,\dots,0,1,0,\dots,0)$ is called the *cheating vector*. $\alpha=(s_1,\dots,s_n)$ is called the *original vector*. The value of $\rho_{c,\alpha}=\#(\Omega^*_\alpha\cap\Omega_\alpha)/\#\Omega^*_\alpha$, where $\#X$ denotes the number of elements in the set X, expresses the probability of successful cheating with respect to $\alpha=(s_1,\dots,s_n)$. As the original vector $\alpha=(s_1,\dots,s_n)$ is always in $\Omega^*_\alpha\cap\Omega_\alpha$, the probability of successful cheating is always nonzero or $\rho_{c,\alpha}>0$.

Theorem 1 *Given secret sharing with its distribution table $\mathcal{T}$ and the defining function $f:V_n\to\{0,1\}$. Let c be any integer with $1\le c\le n$ and $\alpha=(s_1,\dots,s_n)$ be any vector in V_n. Then there exists a vector $\alpha'\in V_n$ such that $\rho_{c,\alpha}+\rho_{c,\alpha'}=1$ otherwise $\rho_{c,\alpha}=1$.*

Proof. Write $\alpha^*=(s_1,\dots,s_{c-1},1\oplus s_c,s_{c+1},\dots,s_n)$. Set $K=f(\alpha)$ and $K^*=f(\alpha^*)$. Let

$$\begin{aligned}\Omega^*_\alpha &= \{(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_n)|f(x_1,\dots,\\ &\qquad x_{c-1},\oplus s_c,x_{c+1},\dots,x_n)=K^*\}\end{aligned}$$

and

$$\begin{aligned}\Omega_\alpha &= \{(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_n)|f(x_1,\dots,\\ &\qquad x_{c-1},s_c,x_{c+1},\dots,x_n)=K\}\end{aligned}$$

Note that Ω^*_α can be expressed as $\Omega^*_\alpha=\Omega^*_0\cup\Omega^*_1$ where

$$\begin{aligned}\Omega^*_0 &= \{(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_n)|f(x_1,\dots,\\ &\qquad x_{c-1},1\oplus s_c,x_{c+1},\dots,x_n)=K^*\ \text{ and}\\ &\qquad f(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_n)=K\}\end{aligned}$$

and

$$\begin{aligned}\Omega_1^* &= \{(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_n)|f(x_1,\dots,\\ &\quad x_{c-1},1\oplus s_c,x_{c+1},\dots,x_n)=K^* \text{ and}\\ &\quad f(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_n)=1\oplus K\}\end{aligned}$$

Obviously $\Omega_\alpha^*\cap\Omega_\alpha=\Omega_0^*$. Thus

$$\rho_{c,\alpha}=\#(\Omega_\alpha^*\cap\Omega_\alpha)/\#\Omega_\alpha^*=\#\Omega_0^*/\#\Omega_\alpha^* \qquad (1)$$

There exist two cases to be considered: $\Omega_1^*\neq\emptyset$, where $\emptyset$ denotes the empty set, and $\Omega_1^*=\emptyset$.

The case 1: $\Omega_1^*\neq\emptyset$. Thus there exists a vector $\alpha'\in\Omega_1^*$ where $\alpha'=(s_1',\dots,s_{c-1}',s_c,s_{c+1}',\dots,s_n')$ satisfying $f(s_1',\dots,s_{c-1}',1\oplus s_c,s_{c+1}',\dots,s_n')=K^*$ and $f(s_1',\dots,s_{c-1}',s_c,s_{c+1}',\dots,s_n')=1\oplus K$.

Using the cheating scheme on α', that is the original vector, we have

$$\begin{aligned}\Omega_{\alpha'}^* &= \{(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_n)|f(x_1,\dots,\\ &\quad x_{c-1},1\oplus s_c,x_{c+1},\dots,x_n)=K^*\}\end{aligned}$$

Thus $\Omega_{\alpha'}^*=\Omega_\alpha^*$. Let

$$\begin{aligned}\Omega_{\alpha'} &= \{(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_n)|f(x_1,\dots,\\ &\quad x_{c-1},s_c,x_{c+1},\dots,x_n)=1\oplus K\}\end{aligned}$$

Obviously $\Omega_{\alpha'}^*\cap\Omega_{\alpha'}=\Omega_1^*$. Thus

$$\rho_{c,\alpha'}=\#(\Omega_{\alpha'}^*\cap\Omega_{\alpha'})/\#\Omega_{\alpha'}^*=\#\Omega_1^*/\#\Omega_\alpha^* \qquad (2)$$

Combing (1) and (2), we can prove that $\rho_{c,\alpha}+\rho_{c,\alpha'}=1$.

The case 2: $\Omega_1^*=\emptyset$. Thus $\Omega_\alpha^*=\Omega_0^*(=\Omega_0)$ and thus $\Omega_\alpha^*\cap\Omega_\alpha=\Omega_0^*=\Omega_\alpha^*$. This proves that $\rho_{c,\alpha}=\#(\Omega_\alpha^*\cap\Omega_\alpha)/\#\Omega_\alpha^*=1$. The proof is completed.

Theorem 1 implies that the probability of successful cheating is always higher than $\frac{1}{2}$.

5. Secret Sharing Based on Bent Defining Functions

As we are dealing with binary case $K\in\{0,1\}$, the cheater can always succeed with probability $\frac{1}{2}$. Ideally, one would hope that the probability of cheater success is as close as possible to $\frac{1}{2}$ or $|\rho_{c,\alpha}-\frac{1}{2}|$ is as small as possible. Our considerations are restricted to the case where $\mathcal{P}$ includes an even number of participants (n is even). This restriction results from the fact that the defining function f is bent (bent functions exist for an even number of variables).

Theorem 2 *Let $f(x)=x_1x_2\oplus\cdots\oplus x_{2k-1}x_{2k}$ where $n=2k\geq 4$ (from [8] f is a bent function $V_{2k}\to\{0,1\}$). Given secret sharing based on the defining function f. Then*

(i) the probability of successful cheating equals

$$\rho_{c,\alpha}=\begin{cases}\frac{1}{2}\pm 2^{-\frac{n}{2}} & \textit{if } s_c=0\\ \frac{1}{2} & \textit{if } s_c=1\end{cases}$$

for any integer c with $1\leq c\leq n$ and any vector $\alpha=(s_1,\dots,s_n)$,

(ii) the nonlinearity of f satisfies $N_f=2^{n-1}-2^{\frac{1}{2}n-1}$.

Proof Without the loss of generality, we assume that the cheater is P_n so $\delta_c=\alpha^*\oplus\alpha=(0,\dots,0,1)$ and $c=n$. The dealer has set up secret sharing for the vector $\alpha=(s_1,\dots,s_{2k})\in V_n$ with the secret $f(\alpha)=K\in GF(2)$. The cheater P_n submits a false share so the vector used by the combiner is α^* and the returned secret is $K^*=f(\alpha^*)$, where $K^*\in GF(2)$.

First we consider the case when $s_{2k}=0$. The set

$$\Omega_\alpha^*=\{(x_1,\dots,x_{2k-1},0)|f(x_1,\dots,x_{2k-1},1)=K^*\}$$

or

$$\begin{aligned}\Omega_\alpha^* &= \{(x_1,\dots,x_{2k-1},0)|x_1x_2\oplus\cdots\oplus x_{2k-3}x_{2k-2}\\ &\quad \oplus x_{2k-1}=K^*\}\end{aligned}$$

can be represented as $\Omega_\alpha^*=\Omega_0^*\cup\Omega_1^*$. where

$$\begin{aligned}\Omega_0^* &= \{(x_1,\dots,x_{2k-2},0,0)|x_1x_2\oplus\cdots\oplus x_{2k-3}x_{2k-2}\\ &\quad =K^*\}\end{aligned}$$

and

$$\begin{aligned}\Omega_1^* &= \{(x_1,\dots,x_{2k-2},1,0)|x_1x_2\oplus\cdots\oplus x_{2k-3}x_{2k-2}\\ &\quad =1\oplus K^*\}\end{aligned}$$

Similarly, the set

$$\Omega_\alpha=\{(x_1,\dots,x_{2k-1},0)|f(x_1,\dots,x_{2k-1},0)=K\}$$

or

$$\begin{aligned}\Omega_\alpha &= \{(x_1,\dots,x_{2k-1},0)|x_1x_2\oplus\cdots\oplus x_{2k-3}x_{2k-2}\\ &\quad =K\}\end{aligned}$$

can be divided into two disjoint subsets $\Omega_\alpha=\Omega_0\cup\Omega_1$ where

$$\begin{aligned}\Omega_0 &= \{(x_1,\dots,x_{2k-2},0,0)|x_1x_2\oplus\cdots\oplus x_{2k-3}x_{2k-2}\\ &\quad =K\}\end{aligned}$$

and

$$\begin{aligned}\Omega_1 &= \{(x_1,\dots,x_{2k-2},1,0)|x_1x_2\oplus\cdots\oplus x_{2k-3}x_{2k-2}\\ &\quad =K\}\end{aligned}$$

The invalid secret K^* can be either equal to K or $K \oplus 1$. Without the loss of generality, we assume that $K = 1 \oplus K^*$ and then $\Omega^*_\alpha \cap \Omega_\alpha = \Omega^*_1 = \Omega_1$.

Note that $x_1x_2 \oplus \cdots \oplus x_{2k-3}x_{2k-2}$ is a bent function on V_{2k-2} [8]. From a property of bent functions mentioned in Section 3, we know that $\#\Omega_1 = 2^{2k-3} \pm 2^{k-2}$. On the other hand, it is easy to see that $f(x_1, \ldots, x_{2k-1}, 1)$ is balanced. Thus $\#\Omega^*_\alpha = 2^{2k-2}$ and thus

$$\begin{aligned} \rho_{n,\alpha} &= \#(\Omega^*_\alpha \cap \Omega_\alpha)/\#\Omega^*_\alpha = \#\Omega_1/\#\Omega^*_\alpha = \frac{1}{2} \pm 2^{-k} \\ &= \frac{1}{2} \pm 2^{-\frac{n}{2}} \end{aligned}$$

Next we turn to the case $s_{2k} = 1$. Again we take into account the set

$$\Omega^*_\alpha = \{(x_1, \ldots, x_{2k-1}, 1) | f(x_1, \ldots, x_{2k-1}, 0) = K^*\}$$

or

$$\begin{aligned} \Omega^*_\alpha &= \{(x_1, \ldots, x_{2k-1}, 1) | x_1x_2 \oplus \cdots \oplus x_{2k-3}x_{2k-2} \\ &\quad = K^*\} \end{aligned}$$

and its partition into $\Omega^*_\alpha = \Omega^*_0 \cup \Omega^*_1$ where

$$\begin{aligned} \Omega^*_0 &= \{(x_1, \ldots, x_{2k-2}, 0, 1) | x_1x_2 \oplus \cdots \oplus x_{2k-3}x_{2k-2} \\ &\quad = K^*\} \end{aligned}$$

and

$$\begin{aligned} \Omega^*_1 &= \{(x_1, \ldots, x_{2k-2}, 1, 1) | x_1x_2 \oplus \cdots \oplus x_{2k-3}x_{2k-2} \\ &\quad = K^*\} \end{aligned}$$

Obviously $\#\Omega^*_0 = \#\Omega^*_1$.

Similarly, we treat the set

$$\Omega_\alpha = \{(x_1, \ldots, x_{2k-1}, 1) | f(x_1, \ldots, x_{2k-1}, 1) = K\}$$

or

$$\begin{aligned} \Omega_\alpha &= \{(x_1, \ldots, x_{2k-1}, 1) | x_1x_2 \oplus \cdots \oplus x_{2k-3}x_{2k-2} \\ &\quad \oplus x_{2k-1} = K\} \end{aligned}$$

and its two subsets $\Omega_\alpha = \Omega_0 \cup \Omega_1$ where

$$\begin{aligned} \Omega_0 &= \{(x_1, \ldots, x_{2k-2}, 0, 1) | x_1x_2 \oplus \cdots \oplus x_{2k-3}x_{2k-2} \\ &\quad = K\} \end{aligned}$$

and

$$\begin{aligned} \Omega_1 &= \{(x_1, \ldots, x_{2k-2}, 1, 1) | x_1x_2 \oplus \cdots \oplus x_{2k-3}x_{2k-2} \\ &\quad = 1 \oplus K\} \end{aligned}$$

Note that the invalid secret K^* can be either equal to K or $K \oplus 1$. Without the loss of generality, we assume that $K^* = 1 \oplus K$ and then $\Omega^*_\alpha \cap \Omega_\alpha = \Omega^*_1 = \Omega_1$.

Therefore

$$\rho_{n,\alpha} = \#(\Omega^*_\alpha \cap \Omega_\alpha)/\#\Omega^*_\alpha = \#\Omega^*_1/\#\Omega^*_\alpha = \frac{1}{2}.$$

Therefore we have proved the statement *(i)* of the theorem for $\delta_n = \alpha \oplus \alpha^* = (0, \ldots, 0, 1)$.

Using the same arguments, we can prove the part (i) of the theorem for δ_c, $c = 1, \ldots, n$.

Since bent functions achieve the maximum nonlinearity we have proved the statement *(ii)*. The proof is completed.

We now illustrate nonlinear secret sharing with the bent defining function.

Example 1 Let the group $\mathcal{P}$ include four participants and the defining function $f(x) = x_1x_2 \oplus x_3x_4$. It is easy to find the truth table of f which is fully characterised by the sequence $0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0$. The secret sharing can be described as the following table:

f	S_1	S_2	S_3	S_4
0	0	0	0	0
0	0	0	0	1
0	0	0	1	0
1	0	0	1	1
0	0	1	0	0
0	0	1	0	1
0	0	1	1	0
1	0	1	1	1
0	1	0	0	0
0	1	0	0	1
0	1	0	1	0
1	1	0	1	1
1	1	1	0	0
1	1	1	0	1
1	1	1	1	0
0	1	1	1	1

Assume that the dealer fixed the shares $\alpha = (1, 1, 0, 0) \in V_4$ and the secret $K = f(1, 1, 0, 0) = 1$. Our cheater is P_4. Thus $\delta_4 = (0, 0, 0, 1)$ and $c = 4$. The combiner obtains the sequence $\alpha^* = (1, 1, 0, 1)$ with the last share changed by the cheater and returns the invalid secret $K^* = f(1, 1, 0, 1) = 1$. On receiving K^*, the cheater can identify the set $\Omega^*_\alpha = \{(x_1, x_2, x_3, 0) | f(x_1, x_2, x_3, 1) = 1\}$ which is $\Omega^*_\alpha = \{(0, 0, 1, 0), (0, 1, 1, 0), (1, 0, 1, 0), (1, 1, 0, 0), \}$. The set $\Omega_\alpha = \{(x_1, x_2, x_3, 0) | f(x_1, x_2, x_3, 0) = 1\}$ becomes $\Omega_\alpha = \{(1, 1, 0, 0), (1, 1, 1, 0)\}$.

The intersection $\Omega^*_\alpha \cap \Omega_\alpha = \{(1, 1, 0, 0)\}$ and the probability of successful cheating is $\rho_{4,\alpha} = \#(\Omega^*_\alpha \cap \Omega_\alpha)/\#\Omega^*_\alpha = \frac{1}{4} = \frac{1}{2} - 2^{-\frac{n}{2}}$ where $n = 4$ and $\alpha = (1, 1, 0, 0)$. Using Theorem 2 or by a straightforward verification, we get that $N_f = 6 = 2^{n-1} - 2^{\frac{1}{2}n-1}$ where $n = 4$.

Nonlinear secret sharing based on bent functions over $GF(2)$ possesses the following properties:

- The resulting secret sharing is non-perfect. To make it perfect, the defining function must be balanced.

- The threshold parameter t and the number n of participants in $\mathcal{P}$ are restricted. The threshold parameter indicates the number of shares uniquely identifying a single row of the table $\mathcal{T}$ or equivalently, the number of variables for the defining function f. We could add as many participants as we can define vectors in V_t whose any collection of t are independent. It is easy to verify that if $x_1, \ldots, x_t \in V_t$ are independent then we can create only one extra vector $x_1 \oplus \ldots \oplus x_t$ so that any collection of t vectors are independent. In other words, in $GF(2)$, we can define two classes of nonlinear secret sharing: (n, n) or $(n, n+1)$ where n is even.

6. Secret Sharing with Balanced Defining Functions

As noted already, perfectness of secret sharing requires defining functions to be balanced. Let $W = \{\gamma | \gamma \in V_m$ and $HW(\gamma)$ is even$\}$. Clearly, W is an $(m-1)$-dimensional subspace of V_m and thus W contains 2^{m-1} vectors. The set

$$W^* = (W - \{(0, \ldots, 0)\}) \cup \{(1, \ldots, 1)\} \qquad (3)$$

where W^* is regarded as a multiple set when m is even as it contains the vector $(1, \ldots, 1)$ twice. Let A be an $2^{m-1} \times m$ matrix whose 2^{m-1} rows include all the 2^{m-1} vectors of W and A^* be an $2^{m-1} \times m$ matrix whose 2^{m-1} rows include all the 2^{m-1} vectors of W^*. It is easy to see that each row of A has an even Hamming weight and each column of A is balanced. Therefore A^* satisfies (a) the Hamming weight of each row is at least two, (b) each column precisely contains $2^{m-2} - 1$ zeros and $2^{m-2} + 1$ ones. Note that if m is odd then A^* contains distinct 2^{m-1} rows, and if m is even then A^* contains $2^{m-1} - 2$ distinct rows and two all-one rows.

Theorem 3 *Let $n \equiv 1 \pmod 4$, m be odd and $n = 2m - 1$. Let π be a mapping from V_{m-1} to W^* defined in (3) such that $\pi(\beta) \neq \pi(\beta')$ whenever $\beta \neq \beta'$, Let $f(x) = \pi(y)z^T$ be the defining function of secret sharing, where $x = (x_1, \ldots, x_{2m-1})$, $y = (x_1, \ldots, x_{m-1})$ and $z = (x_m, \ldots, x_{2m-1})$, Further let $\delta_c = (0, \ldots, 0, 1, 0, \ldots, 0) \in V_{2m-1}$ be the cheating vector, where the c-th coordinate is nonzero. Then for any vector $\alpha = (s_1, \ldots, s_{2m-1}) \in V_{2m-1}$, we have the following:*

(i) the probability of success of the cheater $P_c \in \mathcal{P}$ is

$$\rho_{c,\alpha} = \begin{cases} \frac{1}{2} \pm 2^{-m+1} & \textit{if } m \leq c \leq 2m-1 \\ \frac{1}{2} & \textit{if } 1 \leq c \leq m-1 \end{cases}$$

(ii) the resulting secret sharing is perfect or in other words, the defining function f is balanced,

(iii) the nonlinearity of f satisfies $N_f = 2^{2m-2} - 2^{m-1}$.

Proof Note that π can be expressed as $\pi(y) = (h_1(y), \ldots, h_m(y))$ where each h_j is a function on V_{m-1}. Thus $f(x) = \pi(y)z^T = h_1(y)x_m \oplus \cdots \oplus h_m(y)x_{2m-1}$. Given an arbitrary vector $\alpha = (s_1, \ldots, s_{2m-1}) \in V_{2m-1}$ and the corresponding secret $f(\alpha) = K$ where $K \in GF(2)$. The invalid secret is $f(\alpha \oplus \delta_c) = K^*$ where $K^* \in GF(2)$.

There exist two cases to be considered: $m \leq c \leq 2m-1$ and $1 \leq c \leq m-1$.
<u>The case 1:</u> $m \leq c \leq 2m-1$. The set

$$\begin{aligned} \Omega^*_\alpha = \; & \{(x_1, \ldots, x_{c-1}, s_c, x_{c+1}, \ldots, x_{2m-1}) | \\ & f(x_1, \ldots, x_{c-1}, 1 \oplus s_c, x_{c+1}, \ldots, x_{2m-1}) \\ & = K^*\} \end{aligned}$$

Then it can be represented as

$$\begin{aligned} \Omega^*_\alpha = \; & \{(x_1, \ldots, x_{c-1}, s_c, x_{c+1}, \ldots, x_{2m-1}) | \\ & h_1(y)x_m \oplus \cdots \oplus h_{c-m}(y)x_{t-1} \\ & \oplus h_{c-m+1}(y)(1 \oplus s_c) \oplus h_{c-m+2}(y)x_{c+1} \\ & \oplus \cdots \oplus h_m(y)x_{2m-1} = K^*\} \end{aligned}$$

and $\Omega^*_\alpha = \Omega^*_0 \cup \Omega^*_1$, where

$$\begin{aligned} \Omega^*_0 = \; & \{(x_1, \ldots, x_{c-1}, s_c, x_{c+1}, \ldots, x_{2m-1}) | \\ & h_1(y)x_m \oplus \cdots \oplus h_{c-m}(y)x_{c-1} \\ & \oplus h_{c-m+2}(y)x_{c+1} \oplus \cdots \oplus h_m(y)x_{2m-1} = K^* \\ & \text{when } h_{c-m+1}(y) = 0\} \end{aligned}$$

and

$$\begin{aligned} \Omega^*_1 = \; & \{(x_1, \ldots, x_{c-1}, s_c, x_{c+1}, \ldots, x_{2m-1}) | \\ & h_1(y)x_m \oplus \cdots \oplus h_{c-m}(y)x_{c-1} \oplus 1 \oplus s_c \\ & \oplus h_{c-m+2}(y)x_{c+1} \oplus \cdots \oplus h_m(y)x_{2m-1} = K^* \\ & \text{when } h_{c-m+1}(y) = 1\} \end{aligned}$$

Due to the property (a) of the matrix A^*,

$$(h_1(y), \ldots, h_{c-m}(y), h_{c-m+2}(y), \ldots h_m(y)) \neq (0, \ldots, 0)$$

for any $y \in V_{m-1}$. Thus for any fixed $y \in V_{m-1}$, the linear equation on $x_m, \ldots, x_{2m-1}$,

$$\begin{aligned} & h_1(y)x_m \oplus \cdots \oplus h_{c-m}(y)x_{c-1} \oplus h_{c-m+2}(y)x_{c+1} \\ & \oplus \cdots \oplus h_m(y)x_{2m-1} = K^* \end{aligned}$$

has precisely 2^{m-1} solutions. Due to the property (b) of the matrix A^*, h_{c-m+1} takes on the value of zero precisely

$2^{m-2}-1$ times. Therefore $\#\Omega_0^* = 2^{m-1}(2^{m-2}-1)$. Using the same arguments, we argue that $\#\Omega_1^* = 2^{m-1}(2^{m-2}+1)$. Therefore $\#\Omega_\alpha^* = 2^{2m-2}$. Consider the set

$$\begin{aligned}\Omega_\alpha &= \{(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_{2m-1})| \\ &\quad f(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_{2m-1}) = K\}\end{aligned}$$

It can be specialized as

$$\begin{aligned}\Omega_\alpha &= \{(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_{2m-1})|h_1(y)x_m \\ &\quad \oplus \cdots \oplus h_{c-m}(y)x_{c-1} \oplus h_{c-m+1}(y)s_c \\ &\quad \oplus h_{c-m+2}(y)x_{c+1} \oplus \cdots \oplus h_m(y)x_{2m-1} = K\}\end{aligned}$$

The set can be represented as $\Omega_\alpha = \Omega_0 \cup \Omega_1$, where

$$\begin{aligned}\Omega_0 &= \{(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_{2m-1})| \\ &\quad h_1(y)x_m \oplus \cdots \oplus h_{c-m}(y)x_{c-1} \\ &\quad \oplus h_{c-m+2}(y)x_{c+1} \oplus \cdots \oplus h_m(y)x_{2m-1} = K \\ &\quad \text{when } h_{c-m+1}(y) = 0\}\end{aligned}$$

and

$$\begin{aligned}\Omega_1 &= \{(x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_{2m-1})| \\ &\quad h_1(y)x_m \oplus \cdots \oplus h_{c-m}(y)x_{c-1} \oplus s_c \\ &\quad \oplus h_{c-m+2}(y)x_{c+1} \oplus \cdots \oplus h_m(y)x_{2m-1} = K \\ &\quad \text{when } h_{c-m+1}(y) = 1\}\end{aligned}$$

Note that K^* is identified with either K or $1 \oplus K$. When $K^* = K$, it is easy to see that $\Omega_0^* = \Omega_0$. Thus we have $\Omega_\alpha^* \cap \Omega_\alpha = \Omega_0^*$ and thus $\rho_{c,\alpha} = \#(\Omega_\alpha^* \cap \Omega_\alpha)/\#\Omega_\alpha^* = \#\Omega_0^*/\#\Omega_\alpha^* = \frac{1}{2} - 2^{-m+1}$. Similarly, when $K^* = 1 \oplus K$, $\Omega_1^* = \Omega_1$ thus $\Omega_\alpha^* \cap \Omega_\alpha = \Omega_1^*$ and thus $\rho_{c,\alpha} = \#(\Omega_\alpha^* \cap \Omega_\alpha)/\#\Omega_\alpha^* = \#\Omega_1^*/\#\Omega_\alpha^* = \frac{1}{2} + 2^{-m+1}$.

The case 2: $1 \le c \le m-1$. Write $y_{s_c} = (x_1,\dots,x_{c-1},s_c,x_{c+1},\dots,x_{m-1}) \in V_{m-1}$ and $y_{1\oplus s_c} = (x_1,\dots,x_{c-1},1 \oplus s_c,x_{c+1},\dots,x_{m-1}) \in V_{m-1}$. Then we can write $\Omega_\alpha^* = \{(y_{s_c},z)|\pi(y_{1\oplus s_c})z^T = K^*\}$ and $\Omega_\alpha = \{(y_{s_c},z)|\pi(y_{s_c})z^T = K\}$. Note that $\pi(\beta) \neq 0$ for any $\beta \in V_{m-1}$. Thus for any fixed $y_{1\oplus s_c}$, the linear equation $\pi(y_{1\oplus s_c})z^T = K^*$ on $z = (x_m,\dots,x_{2m-1})$ has precisely 2^{m-1} solutions. Therefore $\#\Omega_\alpha^* = 2^{m-2} \cdot 2^{m-1} = 2^{2m-3}$. Note further that $\pi(y_{s_c}) \neq \pi(y_{1\oplus s_c})$. Thus the group of linear equations $\pi(y_{1\oplus s_c})z^T = K^*$ and $\pi(y_{s_c})z^T = K$ are linearly independent and thus $\#(\Omega_\alpha^* \cap \Omega_\alpha) = 2^{m-2} \cdot 2^{m-2} = 2^{2m-4}$. Finally we have $\rho_{c,\alpha} = \#(\Omega_\alpha^* \cap \Omega_\alpha)/\#\Omega_\alpha^* = \frac{1}{2}$. The first part of the theorem has been proved.

Now we consider the perfectness of the scheme. Since $\pi(\beta) \neq 0$ for any $\beta \in V_{m-1}$, $f(\beta,z) = \pi(\beta)z^T$ is a nonzero linear function on V_m for each fixed $\beta \in V_{m-1}$, and thus it is balanced. This proves that the function $f(x) = \pi(y)z^T$ is balanced on V_{2m-1}.

We are coming to the last part of our proof related to the nonlinearity of the defining function f. From [10], the function defined in Theorem 3 can be expressed in an equivalent form. From the same literature, the nonlinearity of this kind of function can be computed easily and thus we have proved the statement *(iii)*. However we now would like give a direct proof. Note that any affine function ψ on V_{2m-1} can be written as $\psi(x) = C \oplus \beta y^T \oplus \gamma z^T$, where $y, \beta \in V_{m-1}$ and $\gamma \in V_m$ $x = (y,z)$ and C is any constant in $GF(2)$.

$$\begin{aligned}HW(f \oplus \psi) &= HW(C \oplus \beta y^T \oplus \gamma z^T \oplus \pi(y)z^T) \\ &= \sum_{\sigma \in V_k} HW(C \oplus \beta\sigma^T \oplus \gamma z^T \oplus \pi(\sigma)z^T)\end{aligned}$$

Clearly for any fixed $\sigma \in V_{m-1}$ with $\pi(\sigma) \neq \gamma$, $C \oplus \beta\sigma^T \oplus \gamma z^T \oplus \pi(\sigma)z^T$ is a non-constant affine function on V_m and thus balanced. In this case we have $HW(C \oplus \beta\sigma^T \oplus \gamma z^T \oplus \pi(\sigma)z^T) = 2^{m-1}$. Thus we obtain

$$\begin{aligned}&HW(f \oplus \psi) && (4)\\ &= \sum_{\sigma \in V_k} HW(C \oplus \beta\sigma^T \oplus \gamma z^T \oplus \pi(\sigma)z^T) \\ &= \sum_{\pi(y) \neq \gamma} 2^{m-1} = 2^{m-1}(2^{m-1}-1) && (5)\end{aligned}$$

On the other hand, there uniquely exists a vector $\sigma' \in V_{m-1}$ with $\pi(\sigma') = \gamma$. For σ', we have

$$\begin{aligned}&HW(C \oplus \beta{\sigma'}^T \oplus \gamma z^T \oplus \pi(\sigma')z^T) = \\ &HW(C \oplus \beta{\sigma'}^T) = \begin{cases} 0 & \text{if } C \oplus \beta{\sigma'}^T = 0 \\ 2^{m-1} & \text{if } C \oplus \beta{\sigma'}^T = 1 \end{cases}\end{aligned}$$

Since C, as the constant term of an affine function, can arbitrarily take on values in $\{0,1\}$. Thus we can alway modify C so that $C \oplus \beta{\sigma'}^T = 0$, and then $HW(C \oplus \beta{\sigma'}^T \oplus \gamma z^T \oplus \pi(\sigma')z^T) = 0$. We have proved that $N_f = 2^{2m-2} - 2^{m-1}$. Therefore the proof is completed.

The matrix A^* has different properties depending whether m is odd or even. We now consider the case of even m.

Theorem 4 *Let $n \equiv 3 \pmod 4$, m be even and $n = 2m-1$. Let π be a mapping from V_{m-1} to W^* defined in (3) such that (a) $\pi(0,\dots,0) = \pi(1,\dots,1) = (1,\dots,1)$, (b) $\pi(\beta) \neq \pi(\beta')$ if $\beta \neq \beta'$ except for the case that $\beta = (0,\dots,0)$ and $\beta' = (1,\dots,1)$. Let $f(x) = \pi(y)x^T$, where $x = (x_1,\dots,x_{2m-1})$, $y = (x_1,\dots,x_{m-1})$ and $z = (x_m,\dots,x_{2m-1})$, be the defining function of the secret sharing. Let $\delta_c = (0,\dots,0,1,0,\dots,0) \in V_{2m-1}$ be the cheating vector, where only c-th coordinate is nonzero. Then for any vector $\alpha = (s_1,\dots,s_{2m-1}) \in V_{2m-1}$, we have the following:*

(i) the probability of success of the cheater $P_c \in \mathcal{P}$ is

$$\rho_{c,\alpha} = \begin{cases} \frac{1}{2} \pm 2^{-m+1} & \text{if } m \le c \le 2m-1 \\ \frac{1}{2} & \text{if } 1 \le c \le m-1 \end{cases}$$

(ii) the resulting secret sharing is perfect or in other words, the defining function f is balanced,

(iii) the nonlinearity of f satisfies $N_f = 2^{2m-2} - 2^m$.

Proof. The proof of the statement *(i)* is similar to that of Theorem 3 because of the properties (a) and (b) of the mapping π mentioned in Theorem 4. The statements *(ii)* can be derived in the same way as in the proof of the previous theorem. As mentioned in the proof of the previous theorem, we do not need prove the statement *(iii)* directly. From [10], the nonlinearity of the function f can be determined easily. The proof is completed.

7. Conclusions and Further Extensions

We defined nonlinear secret sharing and investigated its properties for the binary case. The main motivation was to make secret sharing immune against the TW attack. We considered two classes of secret sharing. The first class is based on bent functions and clearly leads to non-perfect secret sharing. The second class with balanced defining functions includes perfect secret sharing schemes. For both classes, we have proved the bounds for the probability of successful cheating. The work can be extended by conducting investigations into nonlinear secret sharing with shares from an arbitrary $GF(q)$, where $q \neq 2$. An interesting extension is to examine case with many cheaters who conspire against honest participants.

Acknowledgement

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

References

[1] M. Carpentieri. A perfect threshold secret sharing scheme to identify cheaters. *Designs, Codes and Cryptography*, 5(3):183–187, 1995.

[2] M. Carpentieri, A. De Santis, and U. Vaccaro. Size of shares and probability of cheating in threshold schemes. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT'93*, LNCS No. 765, pages 118–125. Springer-Verlag, 1993.

[3] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In *Proceedings of the* 28*th IEEE Symposium on Foundations of Computer Science*, pages 427–437. IEEE, 1987.

[4] F.J. MacWilliams and N.J.A. Sloane. *The theory of error-correcting codes*. North-Holland, Amsterdam, 1977.

[5] T.P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In J. Feigenbaum, editor, *Advances in Cryptology - CRYPTO'91*, LNCS No. 576, pages 129–140. Springer-Verlag, 1992.

[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] A. Renvall, and C, Ding. A nonlinear secret sharing scheme. *ACISP'96*, LNCS No. 1172, pages 56–66. Springer-Verlag, 1996.

[8] O.S. Rothaus. On bent functions. *Journal of Combinatorial Theory*, Series A, 20:300–305, 1976.

[9] B. Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic voting. In M. Wiener, editor, *Advances in Cryptology - CRYPTO'99*, LNCS No. 1666, pages 148–164. Springer-Verlag, 1999.

[10] J. Seberry, X. M. Zhang, and Y. Zheng. On constructions and nonlinearity of correlation immune functions. In *Advances in Cryptology - EUROCRYPT'93*, LNCS No. 756, pages 181–199. Springer-Verlag, 1994.

[11] M. Stadler. Publicly verifiable secret sharing. In U. Maurer, editor, *Advances in Cryptology - EUROCRYPT'96*, LNCS No. 1070, pages 190–199. Springer-Verlag, 1996.

[12] D.R. Stinson. *Cryptography: Theory and Practice*. CRC Press, 1995.

[13] Martin Tompa and Heather Woll. How to share a secret with cheaters. In A.M. Odlyzko, editor, *Advances in Cryptology - CRYPTO'86*, LNCS No. 263, pages 261–265. Springer-Verlag, 1987.