Strongly self-orthogonal codes for secure computation

Iwan Duursma

April 18, 2007

Linear secret sharing schemes **3**
General LSSSs 4
Access structure 5
Adversary model 6
Ideal LSSSs 7
AG Codes 8
AG LSSSs 9

Ideal LSSSs **10**
Sharing on $*$ 11
Interpolation 12
Pairing 13

Secure multi-party computation **14**
Sums and products 15
Multiplicative LSSSs 16
Strongly multiplicative LSSSs 17
Error-free protocols 18
Strongly self-orthogonal codes 19

Composition of schemes **20**
Ramp schemes 21
Minimum distance 22
Composition Σ 23
Composition C 24
Sharing on $*\times*$ 25
Example 26
Sharing on $\times$ 27
Pairing on $\times$ 28
Cont. 29
Shift bound 30
Example 31

AG LSSSs **32**
Hermitian codes 33

Bounds . . . 34
Secret reconstruction . . . 35

Overview

Linear secret sharing schemes

Ideal LSSSs

Secure multi-party computation

Composition of schemes

AG LSSSs

Linear secret sharing schemes 3 / 35

LSSSs

Linear secret sharing schemes

- General LSSSs
- Access structure
- Adversary model
- Ideal LSSSs
- AG Codes
- AG LSSSs

General LSSSs

A $\mathbb{K}-$*linear secret sharing scheme* ($\mathbb{K}-$ LSSS) $\Sigma = \Sigma(\Pi)$ is a sequence $\Pi = (\pi_0, \pi_1, \dots, \pi_n)$ of $\mathbb{K}$-linear maps $\pi_i : E \longrightarrow E_i$.

- $\mathbb{K}$ a field, E of finite dimension over $\mathbb{K}$.
- $E_0 = \mathbb{K}$. $E_1, \dots, E_n$ of finite dimension over $\mathbb{K}$.
- For $\mathbf{x} \in E$, $s = \pi_0(\mathbf{x})$ is the *secret* and $(\pi_1(\mathbf{x}), \dots, \pi_n(\mathbf{x}))$ is the *vector of shares*.
- $\mathcal{P} = \{1, 2 \dots, n\}$ is the set of players or participants.

Access structure

A subset of players $A \subseteq \mathcal{P}$ is *qualified* for the LSSS $\Sigma(\Pi)$ if the players in A can recover the secret value from their shares.

A subset $A \subseteq P$ is qualified if and only if

$$\bigcap_{i \in A} \ker \pi_i \subseteq \ker \pi_0.$$

The *access structure* $\Gamma(\Pi)$ is the set of all qualified subsets.

Adversary model

The *adversary structure* $\Delta(\Pi)$ is the set of all unqualified subsets.
An adversary can corrupt the shares of players in an unqualified subset A.

- Passive model: the adversary has insight in the shares of players in A.
- Active model: the adversary is able to modify the shares of players in A.

Ideal LSSSs

A $\mathbb{K}-$ LSSS $\Sigma = \Sigma(\Pi)$ is called *ideal* if $E_i = \mathbb{K}$ for every $i \in P$.

In the ideal case, $\Pi = (\pi_1, \ldots, \pi_n, \pi_0)$ defines a linear map $\Pi : E \longrightarrow \mathbb{K}^{n+1}$.

The image $C = C(\Pi) \subseteq \mathbb{K}^{n+1}$ is a linear code of length $n+1$ over $\mathbb{K}$. If the π_i generate E^* then $\dim C = \dim E$.

Conversely, every linear code together with a choice of a special coordinate determines an ideal LSSS.

AG Codes

Let $X/\mathbb{K}$ be an algebraic curve (absolutely irreducible, projective, nonsingular), and let

- $\mathcal{P} = \{P_1, \ldots, P_n\} \subset X(\mathbb{K})$, a collection of n rational points.
- G, a divisor with support disjoint from $\mathcal{P}$.

The geometric Goppa Code $C_L(\mathcal{P}, G) \subset \mathbb{K}^n$ is the set of vectors

$$\{(f(P_1), \ldots, f(P_n)) : f \in L(G)\},$$

where $L(G) = \{f : (f) + G \geq 0\} \cup \{0\}$.

AG LSSSs

The data $(X/\mathbb{K}, \mathcal{P}, G)$ for an AG code defines an ideal LSSS $\Sigma = \Sigma(\Pi)$ after assigning a special point P_0. In $\Pi : E \longrightarrow \mathbb{K}^{n+1}$, let $E = L(G)$ and $\Pi = Ev_{\mathcal{P}}$.

$$\begin{aligned}\Pi(f) &= (\pi_1(f), \ldots, \pi_n(f), \pi_0(f)),\\ &= (f(P_1), \ldots, f(P_n), f(P_0)).\end{aligned}$$

More generally, let $\mathcal{P}$ be a set of n effective divisors $\{D_1, \ldots, D_n\}$, and, for $D_i \in \mathcal{P}$, let π_i be the natural surjection $L(G) \longrightarrow L(G)/L(G - D_i)$. The resulting LSSS is in general not ideal.

Ideal LSSSs 10 / 35

Ideal LSSSs

Ideal LSSSs
Sharing on $\mathbb{K}^*$
Interpolation
Pairing

Sharing on $\mathbb{K}^*$

Let $x_1, \ldots, x_n \in \mathbb{K}^*$ be n distinct elements, and let $x_0 = 0$. The Shamir secret sharing scheme $\Sigma(\Pi)$ is defined by

$$\Pi \; : \; \mathbb{K}[x]_{\leq t} \longrightarrow \mathbb{K}[x]/(x - x_1) \times \cdots \times \mathbb{K}[x]/(x - x_n) \times \mathbb{K}[x]/(x - x_0).$$

For $h = (x - a_1) \cdots (x - a_{t+1})$,

$$\mathbb{K}[x]/(x - a_1) \times \cdots \times \mathbb{K}[x]/(x - a_{t+1}) \simeq \mathbb{K}[x]/(h) \simeq \mathbb{K}[x]_{\leq t} \longrightarrow \mathbb{K}[x]/(x - x_0).$$

Interpolation

For $h = (x - a_1) \cdots (x - a_{t+1})$,

$$\mathbb{K}[x]/(x - a_1) \times \cdots \times \mathbb{K}[x]/(x - a_{t+1}) \simeq \mathbb{K}[x]/(h) \simeq \mathbb{K}[x]_{\leq t} \longrightarrow \mathbb{K}[x]/(x - x_0).$$

With Lagrange interpolation,

$$(s_1, \ldots, s_{t+1}) \mapsto s_0 = -h(0)\left(\frac{s_1}{a_1 h'(a_1)} + \cdots + \frac{s_{t+1}}{a_{t+1} h'(a_{t+1})}\right)$$

(or with: CRT, Cramer's rule, residues of differentials)

Pairing

For distinct elements $x_0, x_1, \ldots, x_n \in \mathbb{K}$ and for $h = (x - x_0)(x - x_1) \ldots (x - x_n)$, let $L = \mathbb{K}[x]/(h)$. Define $\langle \, , \, \rangle : L \times L \longrightarrow \mathbb{K}$,

$$\langle f, g \rangle = \sum_{i=0}^{n} r_i f(x_i) g(x_i), \qquad r_i = h'(x_i)^{-1}.$$

Then

$$f \in L_{\leq t} \Leftrightarrow \langle f, g \rangle = 0, \quad \text{for all } g \in L_{<n-t},$$
$$g \in L_{\leq n-t} \Leftrightarrow \langle f, g \rangle = 0, \quad \text{for all } f \in L_{<t},$$

and $\langle x^t, x^{n-t} \rangle = 1$.

Secure MPC

Secure multi-party computation

- Sums and products
- Multiplicative LSSSs
- Strongly multiplicative LSSSs
- Error-free protocols
- Strongly self-orthogonal codes

Sums and products

The Shamir $(t+1,n)$ threshold scheme computes n shares as values of a polynomial of degree t.

Let $(a_1,\ldots,a_n)$ be shares of a obtained with a polynomial f, and let $(b_1,\ldots,b_n)$ be shares of b obtained with a polynomial g.

Addition: $(a_1+b_1,\ldots,a_n+b_n)$ are shares of $a+b$ for the polynomial $f+g \in \mathbb{K}[x]_{\leq t}$.

Multiplication: $(a_1 \cdot b_1,\ldots,a_n \cdot b_n)$ are shares of $a \cdot b$ for $fg \in \mathbb{K}[x]_{\leq 2t}$.

Multiplicative LSSSs

A scheme is *multiplicative* if each player can compute from his shares a_i, b_i, for secrets a, b, respectively, a value c_i such that the product ab is a linear combination of the c_i.

The Shamir $(t+1,n)$ threshold scheme is multiplicative for $n > 2t$.

A multiplicative scheme is necessarily $\mathcal{Q}_2$ (the set of players is not the union of two unqualified subsets).

Every $\mathcal{Q}_2$ LSSS can be modified into a multiplicative LSSS with the same access structure. [Cramer, Damgard, Maurer '00]

Strongly multiplicative LSSSs

A scheme is *s*trongly multiplicative if for every unqualified subset of players $A \subseteq \mathcal{P}$, the product ab is a linear combination of the c_i, $i \notin A$.

The Shamir $(t+1, n)$ threshold scheme is strongly multiplicative for $n > 3t$.

A strongly multiplicative scheme is necessarily $\mathcal{Q}_3$ (the set of players is not the union of three unqualified subsets).

Open problem: It is not known whether it is possible to obtain from a given LSSS with $\mathcal{Q}_3$ access structure a strongly multiplicative LSSS with the same access structure and of complexity polynomial in the complexity of the given LSSS.

Error-free protocols

[Cramer, Damgard, Maurer '00]

Given a field $\mathbb{K}$, an arithmetic circuit C over $\mathbb{K}$, and a strongly multiplicative LSSS Σ,
there is an error-free protocol for multi-party computation of C,
secure against an active adversary (able to modify shares belonging to an unqualified subset)
of complexity polynomial in the size of $\mathbb{K}, C$, and Σ,
in the information-theoretic scenario (players can communicate over pairwise secure channels).

Strongly self-orthogonal codes

A code C is *strongly self-orthogonal* if for any three codewords $a, b, c \in C$, $\sum a_i b_i c_i = 0$.

Let $\Sigma(\Pi)$ be a LSSS such that $C(\Pi)$ is strongly self-orthogonal. Then $\Sigma(\Pi)$ is strongly multiplicative (with respect to the full adversary structure $\Delta(\Pi)$).

Proof: Use

$$A \subset \Delta(\Pi) \Leftrightarrow \exists c \in C : c_i = 0, i \in A, c_0 = 1.$$

Composition

Composition of schemes

Ramp schemes
Minimum distance
Composition Σ
Composition C
Sharing on $\mathbb{K}^* \times \mathbb{K}^*$
Example
Sharing on $\mathbb{K} \times \mathbb{K}$
Pairing on $\mathbb{K} \times \mathbb{K}$
Cont.
Shift bound
Example

Blakely-Meadows 1984

A LSSS with n players is called a $(k, L, n)-$threshold ramp scheme if

- k is minimal such that any subset of k players is qualified.
- $k - L$ is maximal such that any subset of $k - L$ is unqualified.

$$\underbrace{0 \cdots k-L}_{\text{Rejected}} \quad \underbrace{\cdots}_{?} \quad \underbrace{k \cdots n}_{\text{Accepted}} \quad (\Sigma)$$

$$\underbrace{0 \cdots n-k}_{\text{Rejected}} \quad \underbrace{\cdots}_{?} \quad \underbrace{n-k+L \cdots n}_{\text{Accepted}} \quad (\Sigma^*)$$

Minimum distance

For $x, y \in \mathbb{K}^{n+1}$, the Hamming distance $d(x, y) = |\{i : x_i \neq y_i\}|$.

The minimum distance d of a code is the minimum Hamming distance between any two codewords.

An error-correcting code can correct any t errors uniquely if and only if $d > 2t$.

For a LSSS $\Sigma(\Pi)$,

$$d^* - 2 \leq k - L \quad \text{and} \quad k \leq n - d + 2.$$

where d and d^* are the minimum distance of the code $C(\Pi)$ and its dual, respectively. In general, equality does not hold.

Composition Σ

Let $\Sigma = \Sigma_1 \circ \Sigma_2$ be the composition of two threshold schemes (k_1, n_1) and (k_2, n_2). Σ accepts those subsets of $P = \{1, \ldots, n_1\} \times \{1, \ldots, n_2\}$ that intersect at least k_1 of the n_1 subsets $\{i\} \times \{1, \ldots, n_2\}$ in at least k_2 elements.

$$\begin{array}{cc} & (k_2, n_2) \\ & \begin{array}{ccccc} \cdot & \cdot & \cdot & \cdot & \cdot \end{array} \\ (k_1, n_1) & \begin{array}{ccccc} \cdot & * & * & * & \cdot \end{array} \\ & \begin{array}{ccccc} \cdot & \cdot & * & * & * \end{array} \end{array}$$

$$n = n_1 n_2$$
$$(n - k + 1) = (n_1 - k_1 + 1)(n_2 - k_2 + 1)$$
$$(k - L + 1) = (k_1 - L_1 + 1)(k_2 - L_2 + 1)$$

Composition C

Let

$$C(\Pi_1) = \left(\begin{array}{c|c} 1 & 1 \\ \hline X_1 & 0 \end{array} \right) \quad C(\Pi_2) = \left(\begin{array}{c|c} 1 & 1 \\ \hline X_2 & 0 \end{array} \right)$$

represent $\Sigma(\Pi_1)$ and $\Sigma(\Pi_2)$. Then,

$$C(\Pi) = \left(\begin{array}{c|c} 1 & 1 \\ \hline X_1 \otimes 1 & 0 \\ I \otimes X_2 & 0 \end{array} \right)$$

represents $\Sigma(\Pi) = \Sigma(\Pi_1) \circ \Sigma(\Pi_2)$.

Sharing on $\mathbb{K}^* \times \mathbb{K}^*$

Let $\mathcal{P} = A \times B$, $|A| = n_1, |B| = n_2, n = n_1 n_2$.
Let $1 \leq k_1 \leq n_1$, $1 \leq k_2 \leq n_2$.
Let E be the space of polynomials $f(x, y)$ of the form

$$p_0(x) + p_1(x)y + \cdots + p_{k_2-1}(x)y^{k_2-1},$$

such that $\deg(p_0) = k_1 - 1$, and $\deg(p_i) = n_1$, $1 \leq i \leq k_2 - 1$.

The secret is $f(0, 0)$, the shares are $f(a, b)$, $a \in A, b \in B$. A set of players has access to the secret if and only if it has at least k_2 members in at least k_1 of the susbsets $a \times B$.

Example

For a $(2, 3) \circ (3, 5)$ threshold scheme, use

$$f(x, y) \in \langle (1, x), \quad (1, x, x^2)y, \quad (1, x, x^2)y^2 \rangle.$$

For a $(3, 5) \circ (2, 3)$ threshold scheme, use

$$f(x, y) \in \langle (1, y, y^2), \quad (1, y, y^2, y^3, y^4)x \rangle.$$

	b_1	b_2	b_3	b_4	b_5
a_1	·	·	·	·	·
a_2	·	*	*	*	·
a_3	·	·	*	*	*

	b_1	b_2	b_3	b_4	b_5
a_1	·	·	*	·	*
a_2	·	*	*	·	*
a_3	·	*	·	·	·

Sharing on $\mathbb{K} \times \mathbb{K}$

Let $\mathcal{P} = A \times B$, $|A| = n_1, |B| = n_2, n = n_1 n_2$.
Let $1 \leq k_1 \leq n_1$, $1 \leq k_2 \leq n_2$.
Let E be the space of polynomials $f(x, y)$ of the form

$$p_0(x) + p_1(x)y + \cdots + p_{k_2-1}(x)y^{k_2-1},$$

such that $\deg(p_i) = n_1$, $0 \leq i \leq k_2 - 2$ and $\deg(p_{k_2-1}) = k_1 - 1$,

The secret is $[x^{k_1-1}y^{k_2-1}]f$, the shares are $f(a, b)$, $a \in A, b \in B$. A set of players has access to the secret if and only if it has at least k_2 members in at least k_1 of the susbsets $a \times B$.

Pairing on $\mathbb{K} \times \mathbb{K}$

For $A, B \subseteq \mathbb{K}$, let $h_A(x) = \prod_{a \in A}(x - a)$, $h_B(x) = \prod_{b \in B}(y - b)$, and let

$$L = \mathbb{K}[x, y]/(h_A, h_B) = \langle x^i y^j : 0 \le i < n1, 0 \le j < n2 \rangle.$$

For given k_1 and k_2, let $\phi = x^{k_1 - 1} y^{k_2 - 1}$ and $\phi^* = x^{n_1 - k_1} y^{n_2 - k_2}$. Define

$$L_{\le \phi} = \langle x^i y^j : x^i y^j \le \phi \rangle = L_{< \phi} \oplus \langle \phi \rangle.$$
$$L_{\le \phi^*} = \langle x^i y^j : x^i y^j \le \phi^* \rangle = L_{< \phi^*} \oplus \langle \phi^* \rangle.$$

Where $x^{i_1} y^{j_1} \le x^{i_2} y^{j_2}$ if $(j_1 < j_2)$ or $(j_1 = j_2$ and $i_1 \le i_2)$.

Cont.

Define $\langle \, , \, \rangle : L \times L \longrightarrow \mathbb{K}$,

$$\langle f, g \rangle = \sum_{a \in A, b \in B} r_{a,b} f(a, b) g(a, b), \quad r_{a,b} = h'_A(a)^{-1} h'_B(b)^{-1}.$$

Then

$$f \in L_{\le \phi} \Leftrightarrow \langle f, g \rangle = 0, \quad \text{for all } g \in L_{< \phi^*},$$
$$g \in L_{\le \phi^*} \Leftrightarrow \langle f, g \rangle = 0, \quad \text{for all } f \in L_{< \phi},$$

and $\langle \phi, \phi^* \rangle = 1$.

Shift bound

(Shift bound) To show that $f \in \phi + L_{< \phi}$ is nonzero in at least d points of $\mathcal{P}$, it suffice to give elements $g_1, \ldots, g_d \in L$ such that the linear forms $\langle f g_1, - \rangle, \ldots, \langle f g_d, - \rangle$ are linearly independent. To show that the linear forms are linearly independent it suffices to give elements $h_1, \ldots, h_d \in L$ such that the $d \times d$ matrix $\langle f g_i, h_j \rangle$ $(= \langle f, g_i h_j \rangle)$ is regular.

For the LSSS $\Sigma(\Pi)$ with $E = L_{\le \phi}$ we use $\{g_1, \ldots, g_d\} = \{h_1, \ldots, h_d\} = \{x^i y^j : 0 \le i \le n1 - k1, 0 \le j \le n2 - k2\}$.

With the partial ordering $g_1 \le \ldots \le g_d$ and $h_1 \le \ldots \le h_d$ inherited from L, the matrix $\langle f, g_i h_j \rangle$ is triangular with nonzero elements on the diagonal.

Example

For $(k_1, n_1) = (2, 3)$, $(k_2, n_2) = (3, 5)$: $\phi = xy^2$, $\phi^* = xy^2$. Let $g, h = 1 \leq x \leq y \leq xy \leq y^2 \leq xy^2$.

For $(k_1, n_1) = (3, 5)$, $(k_2, n_2) = (2, 3)$: $\phi = x^2y$, $\phi^* = x^2y$. Let $g, h = 1 \leq x \leq x^2 \leq y \leq xy \leq x^2y$.

1	x	y	xy	y^2	xy^2
x	x^2	xy	x^2y	xy^2	
y	xy	y^2	xy^2		
xy	x^2y	xy^2			
y^2	xy^2				
xy^2					

$(\phi = \phi^* = xy^2)$

1	x	x^2	y	xy	x^2y
x	x^2	1	xy	x^2y	
x^2	xy	x	x^2y		
y	xy	x^2y			
xy	x^2y				
x^2y					

$(\phi = \phi^* = x^2y)$

AG LSSSs 32 / 35

AG LSSSs

AG LSSSs
- Hermitian codes
- Bounds
- Secret reconstruction

Hermitian codes

Let $X/\mathbb{K} : y^r + y = x^{r+1}$, with $|\mathbb{K}| = q = r^2$. Then $|X(\mathbb{K})| = r^3 + 1$.

For the r^3 finite points,

$$L = \mathbb{K}[x, y]/(x^q - x, y^r + y - x^{r+1}).$$

For a set of players that includes the point at infinity

$$L = \mathbb{K}[x, y]/(x(y^q - y)/(y^r + y), y^r + y - x^{r+1}).$$

Bounds

[Chen, Cramer '06]
The generalization of the Shamir secret sharing scheme uses a divisor $G = (t + 2g)P_\infty$ in $E = L(G)$.

$\Sigma(G)$ is strongly multiplicative wrt Δ if $n > 3t + 6g$.
$\Sigma(G)$ is strongly multiplicative wrt $\Delta_{\leq t}$ if $n > 3t + 4g$.

[]
For a carefully chosen divisor G, $\Sigma(G)$ is strongly multiplicative wrt Δ for $n > 3t + 4g$.

Secret reconstruction

For a LSSS with a strongly self-orthogonal code, we have

$$f \in L_{\leq \phi} \Leftrightarrow \langle f, g \rangle = 0, \quad \text{for all } g \in L_{<\phi^*},$$

with $\phi^* = \phi^2$.

If the shares for f are corrupted on $A \subset \Delta$, then the secret can be reconstructed as follows. If $g_2 \in L_{\leq \phi} \backslash L_{<\phi}$ is such that

$$\langle f, g_1 g_2 \rangle = 0, \quad \text{for all } g_1 \in L_{<\phi},$$

then the secret can be recovered as $\langle f, \phi g_2 \rangle$.