

Codes on planes and curves

Iwan Duursma

AAECC-18, Tarragona

June 10, 2009

- Secret sharing
- Secure computation
- Coset bounds
- Secret reconstruction
- Examples

## General LSSS

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

- $\mathbb{F}$  a field,  $E$  of finite dimension over  $\mathbb{F}$ .
- $E_0 = \mathbb{F}$ .  $E_1, \dots, E_n$  of finite dimension over  $\mathbb{F}$ .
- 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  $A \subseteq \mathcal{P}$  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 LSSS

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

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

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

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

## Linear codes for coding theory vs secret sharing

Linear codes are used to guarantee efficient and reliable communication in the presence of noise.

- efficient

$(k \geq t)$  There exist  $t$  independent coordinates

$(d^\perp > t)$  Any subset of size  $t$  is independent (stronger)

- reliable

$(d > t)$  Any  $t$  erasures can be corrected

$(d > 2t)$  Any  $t$  errors can be corrected (stronger)

## Secret sharing version 1

Secret sharing asks for privacy and security in the presence of an adversary.

- privacy

$(k > t)$  An adversary of size  $t$  can not recover the codeword

$(d^\perp > t + 1)$  An adversary of size  $t$  can not recover another symbol (stronger)

- security

$(d > t)$  Codeword is uniquely determined with  $t$  shares missing

$(d > 2t)$  Codeword is uniquely determined with  $t$  shares corrupted (stronger)

## Cosets

Let  $\widehat{C}$  be a code of length  $n + 1$  with coordinates  $\{0, 1, \dots, n\}$  and let  $C_0 \subseteq C$  be the shortened code and the punctured code, respectively.

The coset distance  $d_0 = d(C/C_0)$  equals the largest distance between any two cosets, that is the minimal weight of a vector  $c \in C \setminus C_0$ .

For dual codes  $D = C_0^\perp$  and  $D_0 = C^\perp$ ,  $d_0^\perp = d(D/D_0)$ .

## Coset distance

The code

$$\hat{C} = \left( \begin{array}{cccccc|c} 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{array} \right)$$

has dual distance  $d^\perp = 2$ .

$$\hat{C}^\perp = \left( \begin{array}{cccccc|c} 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{array} \right)$$

The weight of a vector that is nonzero in the last position is at least  $4 > 2$ . And  $d(C^\perp/C_0^\perp) = 3$ .

## Secret sharing version 2

- privacy

$(d_0^\perp > t)$  An adversary of size  $t$  can not recover the secret.

- security

$(d_0 > t)$  The secret is uniquely determined with  $t$  shares missing

$(d_0 > 2t)$  The secret is uniquely determined with  $t$  shares corrupted

## Two-variable example

Who can recover  $f(0, 0)$ ?

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

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

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

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

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

## Shift bound (Coset bound, Rejection bound)

Let  $C/C_0$  be an extension of  $\mathbb{F}$ -linear codes with corresponding extension of dual codes  $D/D_0$  such that  $\dim C/C_0 = \dim D/D_0 = 1$ .

If there exist vectors  $a_1, \dots, a_w$  and  $b_1, \dots, b_w$  such that

$$\begin{cases} a_i * b_j \in D_0 & \text{for } i + j \leq w, \\ a_i * b_j \in D \setminus D_0 & \text{for } i + j = w + 1, \end{cases}$$

then  $d(C/C_0) \geq w$ .

Proof: For a vector  $c \in C \setminus C_0$ , the vectors  $a_1 * c, \dots, a_w * c$  are linearly independent (with the functionals  $b_1, \dots, b_w$  as witnesses). But then  $c$  has weight  $\geq w$ .

## Secure computation

A LSSS  $\Sigma$  is *nondegenerate* if the secret can be reconstructed as a linear combination of all the shares.

That is, there exist  $r_1, \dots, r_n \in \mathbb{F}$  such that

$$\pi_0(x) = \sum_i r_i \pi_i(x), \quad \text{for all } x \in E.$$

The same values reconstruct the sum  $\pi_0(x) + \pi_0(y)$  of two secrets from the pairwise sums  $\pi_i(x) + \pi_i(y)$  of their shares.

Call  $\Sigma$  *additive in  $n-t$  positions* if for any subset  $A \subset \mathcal{P}$  of size  $t$  there exists a choice for  $r_1, \dots, r_n \in \mathbb{F}$  with  $r_i = 0$  for  $i \in A$ .

## Multiplicative LSSSs

To implement secure protocols for multiparty computations that involve addition and multiplication, a stronger property is needed.

A LSSS  $\Sigma$  is *multiplicative* if the product  $\pi_0(x) \cdot \pi_0(y)$  of two secrets can be reconstructed as a linear combination of the pairwise products  $\pi_i(x) \cdot \pi_i(y)$  of the shares, i.e. if there exist  $r_1, \dots, r_n \in \mathbb{F}$  such that

$$\pi_0(x)\pi_0(y) = \sum_i r_i \pi_i(x)\pi_i(y), \quad \text{for all } x, y \in E.$$

Call  $\Sigma$  *multiplicative in  $n - t$  positions* if for any subset  $A \subset \mathcal{P}$  of size  $t$  there exists a choice for  $r_1, \dots, r_n \in \mathbb{F}$  with  $r_i = 0$  for  $i \in A$ .

The conditions for efficient and reliable communication using a code  $C$  are

$$(d^\perp > t) \text{ and } (d > 2t)$$

The LSSS defined by  $C$  and a maximal subcode  $C_0$  guarantees privacy and security for an adversary of bounded size  $t$  if

$$(d_0^\perp > t) \text{ and } (d_0 > 2t)$$

The LSSS can be used for secure computation including addition and multiplication if moreover

$$(d_0(C * C) > t)$$

## AG LSSSs

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

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

## Secret sharing

(Chen and Cramer 2006)

For  $f \in L(G)$ , and for distinct points  $\mathcal{P} = \{P_1, \dots, P_n\}$  and  $P$ , what is the minimal size of a set  $A \subset \mathcal{P}$  such that the values of  $f$  in  $A$  uniquely determine  $f(P)$ ?

$f(P)$  is uniquely determined by  $\{f(P_i) : P_i \in A\}$  if and only if

$$L(G - A) = L(G - A - P).$$

Riemann(-Roch):

$$\deg G = 2g + t \Rightarrow |A| > t.$$

## Improvement using coset bound argument

For  $G$  of degree  $2g + t$ , and for  $A$  of degree at most  $t$ ,

$$L(G - A) \neq L(G - A - P).$$

For an improvement, let

$$0 \leq \alpha_1 \leq \cdots \leq \alpha_{g+t+1} \leq 2g + t$$

be the vanishing orders at  $P$ , and let

$$\Delta = \{\alpha_i : \alpha_i \text{ is a nongap for } P\}.$$

Then  $|\Delta| \geq t + 1$  and  $L(G - A) \neq L(G - A - P)$  for all  $A$  of degree less than  $|\Delta|$ .

## Proof

For  $\alpha_i \in \Delta$ , choose

$$f_i \in L(G - \alpha_i P) \setminus L(G - \alpha_i - P)$$

$$g_i \in L(\alpha_i P) \setminus L(\alpha_i P - P)$$

Then  $f_i g_i \in L(G) \setminus L(G - P)$ .

Assume  $|A| < |\Delta|$ . There exists  $g \in \langle g_i | \alpha_i \in \Delta \rangle$  such that  $g$  vanishes at  $A$ . If  $g$  has pole order  $\alpha_i$  at  $P$  then  $f_i g \in L(G - A) \setminus L(G - A - P)$  and  $L(G - A) \neq L(G - A - P)$ .

## Example

Hermitian curve of degree  $m = 5$  and genus  $g = 6$

For  $G = 14P$  (designed rejection bound is  $t = 2$ ),

$$\Delta = \{0, 4, 5, 9, 10, 14\} \subseteq \{0, 1, 2, 4, 5, 6, 9, 10, 14\}$$

and  $|A| < 6$  is rejected.

For  $G = 15P$  (designed rejection bound  $t = 3$ ),

$$\Delta = \{0, 5, 10, 15\} \subseteq \{0, 1, 2, 3, 5, 6, 7, 10, 11, 15\}$$

and  $|A| < 4$  is rejected.

## Pigeonhole proof of coset bound

For  $G$  of degree  $\deg G = 2g + t$ , the AG-LSSS  $\Sigma_0(G, \mathcal{P})$  rejects any subset of size at most  $t$ .

Proof: Let  $f_0, \dots, f_g \in L(G - Q_1 \cdots - Q_t)$  be functions with increasing orders of vanishing at  $P_0$  in the range  $\{0, \dots, 2g\}$ . And let  $h_0, \dots, h_g \in L(2gP_0)$  be functions with increasing pole order at  $P_0$  in the range  $\{0, \dots, 2g\}$ . By the pigeonhole principle there exist  $f_i$  and  $g_j$  such that  $f_i g_j$  is a unit at  $P_0$ .

**Theorem** (Chen and Cramer 2006)

For a divisor  $G$  of degree  $\deg G = 2g + t$ , and for a set of rational points  $\mathcal{P}$  of size  $n$ , the AG-LSSS  $\Sigma_0(G, \mathcal{P})$  is multiplicative in  $n - t$  positions if  $3t < n - 4g$ .

Proof: A subset of  $n - t$  players can interpolate the product  $fg$  of two functions  $f, g \in L(G)$  if  $2 \deg G < n - t$ , that is if  $3t < n - 4g$ . Unqualified subsets for  $\Sigma$  are of size at most  $t + 2g$ .

The theorem shows that for a curve  $\mathcal{X}/\mathbb{F}$  of genus  $g$  with  $N$  rational points, and for  $3t + 4g < n \leq N - 1$ , there exist linear secret sharing schemes  $\Sigma = \Sigma_0(G, \mathcal{P})$  on  $n$  participants such that

- $\Sigma$  reject all subsets of size  $t$ , and
- $\Sigma$  reconstructs products of secrets from any  $n - t$  products of shares.

As a consequence efficient linear secret sharing schemes for an increasing number of participants can be constructed over a small base field using asymptotically good families of curves.

## Secret reconstruction

Let  $(s_1, \dots, s_n)$  be a vector of possibly corrupted shares for the secret  $s = f(P_0)$ , where the true shares are given by  $(f(P_1), \dots, f(P_n))$ , for some  $f \in L(G)$ .

If  $t$  shares are corrupted, such that  $2t + 1 \leq n - \deg G$ , then the secret can be reconstructed as follows.

Let  $C_L(F + F^*, \mathcal{P} + P_0) = C_L(G, \mathcal{P} + P_0)^\perp$ , and let  $(g, h) \in L(F) \times L(F^*)$  be such that  $g(P_0) = h(P_0) = 1$ , and

$$\sum_{i=1}^n s_i g(P_i) h_0(P_i) = 0, \text{ for all } h_0 \in L(F^* - P_0).$$

$$\sum_{i=1}^n s_i g_0(P_i) h(P_i) = 0, \text{ for all } g_0 \in L(F - P_0).$$

Such a pair exists if

$$L(F-Q) \neq L(F-Q-P_0) \text{ and } L(F^*-Q) \neq L(F^*-Q-P_0).$$

In that case,  $s = -\sum_{i=1}^n g(P_i)h(P_i)$ .

If either  $L(F-Q) \neq L(F-Q-P_0)$  or  $L(F^*-Q) \neq L(F^*-Q-P_0)$  but not both then a pair  $(g, h)$  may not exist. If it exists then the formula produces the correct value for  $s$ . A pair exists but produces an incorrect value for  $s$  only if  $L(F-Q) = L(F-Q-P_0)$  and  $L(F^*-Q) = L(F^*-Q-P_0)$ .

For  $\deg(F + F^*) = (2g - 2) + (n + 1) - \deg G = 2g + 2t$ ,  
choose

$$(\deg F, \deg F^*) = (t, t + 2g), \dots, (t + 2g, t)$$

In this range,

$$L(F - Q) \neq L(F - Q - P_0) \text{ and } L(F^* - Q) \neq L(F^* - Q - P_0)$$

occurs more often than

$$L(F - Q) = L(F - Q - P_0) \text{ and } L(F^* - Q) = L(F^* - Q - P_0)$$