Ramp secret sharing schemes from one-point AG codes

Olav Geil (AAU), Stefano Martin (AAU), Ryutaroh Matsumoto (TITECH), Diego Ruano (AAU), Yuan Luo (SJTU)

Workshop on Applications of Algebraic Geometry in Secret Sharing and Coding Theory
Aalborg University, June 30th 2014

Ramp secret sharing scheme

Secret: $\vec{s} \in \mathbb{F}_q^\ell$, $\ell \geq 1$. Shares $x_i \in \mathbb{F}_q$, $i = 1, \ldots, n$.

Linear schemes:

$C_2 \subsetneq C_1 \subseteq \mathbb{F}_q^n$ linear codes.

$\{\vec{b}_1, \ldots, \vec{b}_{k_2}\}$ basis for C_2.
$\{\vec{b}_1, \ldots, \vec{b}_{k_2}, \vec{b}_{k_2+1}, \ldots, \vec{b}_{k_1}\}$ basis for C_1.
$\mathrm{codim}(C_1, C_2) = k_1 - k_2 = \ell$.

Secret: $\vec{s} = (s_1, \ldots, s_\ell) \in \mathbb{F}_q^\ell$.
Shares: $(x_1, \ldots, x_n) = d_1 \vec{b}_1 + \cdots + d_{k_2} \vec{b}_{k_2} + s_1 \vec{b}_{k_2+1} + \cdots + s_\ell \vec{b}_{k_1}$
where $d_1, \ldots, d_{k_2} \in \mathbb{F}_q$ are chosen by random.

Ramp secret sharing scheme

Secret: $\vec{s} \in \mathbb{F}_q^\ell$, $\ell \geq 1$. Shares $x_i \in \mathbb{F}_q$, $i = 1, \ldots, n$.

<u>Linear schemes:</u>
$C_2 \subsetneq C_1 \subseteq \mathbb{F}_q^n$ linear codes.

$\{\vec{b}_1, \ldots, \vec{b}_{k_2}\}$ basis for C_2.
$\{\vec{b}_1, \ldots, \vec{b}_{k_2}, \vec{b}_{k_2+1}, \ldots, \vec{b}_{k_1}\}$ basis for C_1.
$\mathrm{codim}(C_1, C_2) = k_1 - k_2 = \ell$.

Secret: $\vec{s} = (s_1, \ldots, s_\ell) \in \mathbb{F}_q^\ell$.
Shares: $(x_1, \ldots, x_n) = d_1 \vec{b}_1 + \cdots + d_{k_2} \vec{b}_{k_2} + s_1 \vec{b}_{k_2+1} + \cdots + s_\ell \vec{b}_{k_1}$
where $d_1, \ldots, d_{k_2} \in \mathbb{F}_q$ are chosen by random.

Ramp secret sharing scheme

Secret: $\vec{s} \in \mathbb{F}_q^\ell$, $\ell \geq 1$. Shares $x_i \in \mathbb{F}_q$, $i = 1, \ldots, n$.

<u>Linear schemes:</u>
$C_2 \subsetneq C_1 \subseteq \mathbb{F}_q^n$ linear codes.

$\{\vec{b}_1, \ldots, \vec{b}_{k_2}\}$ basis for C_2.
$\{\vec{b}_1, \ldots, \vec{b}_{k_2}, \vec{b}_{k_2+1}, \ldots, \vec{b}_{k_1}\}$ basis for C_1.
$\mathrm{codim}(C_1, C_2) = k_1 - k_2 = \ell$.

Secret: $\vec{s} = (s_1, \ldots, s_\ell) \in \mathbb{F}_q^\ell$.
Shares: $(x_1, \ldots, x_n) = d_1 \vec{b}_1 + \cdots + d_{k_2} \vec{b}_{k_2} + s_1 \vec{b}_{k_2+1} + \cdots + s_\ell \vec{b}_{k_1}$
where $d_1, \ldots, d_{k_2} \in \mathbb{F}_q$ are chosen by random.

Thresholds

Recall, $\vec{s} = (s_1, \dots, s_\ell)$.

Definition

For $m = 1, \dots, \ell$, t_m and r_m are the unique numbers such that:

- No group of t_m participants can recover m q-bits of information about $\vec{s}$, but some groups of size $t_m + 1$ can.
- All groups of size r_m can recover m q-bits of information about $\vec{s}$, but some groups of size $r_m - 1$ cannot.

How to find r_m and t_m

From [Bains, 2008], [Kurihara et al. 2012], [G. et al. 2014] we have:

Theorem

$$\begin{aligned} t_m &= M_m((C_2)^{\perp}, (C_1)^{\perp}) - 1 \\ r_m &= n - M_{\ell-m+1}(C_1, C_2) + 1, \end{aligned}$$

where $M_m(C_1, C_2)$ is the m-th relative generalized Hamming weight for C_1 with respect to C_2.

$|\operatorname{supp}\{(0,0,1,1,0),(0,1,0,1,1)\}| = 4$

Definition

Let $C_2 \subsetneq C_1$ be linear codes and $\ell = \dim(C_1) - \dim(C_2)$. For $m = 1, \ldots, \ell$ we have:

$$M_m(C_1, C_2) = \min\{|\operatorname{supp}(D)| \mid D \text{ is a linear subcode of } C_1, \; D \cap C_2 = \{\vec{0}\} \text{ and } \dim(D) = m\}.$$

One-point AG codes

$P_1, \ldots, P_n, Q$ rational places in function field of trdg=1.

We consider $\mu_2 < \mu_1$

$$C_2 = C_{\mathcal{L}}(D = P_1 + \cdots + P_n, \mu_2 Q) \subseteq C_1 = C_{\mathcal{L}}(D, \mu_1 Q) \subseteq \mathbb{F}_q^n.$$

We have a general method to estimate (find) RGHWs of these codes.

For Hermitian codes often sharp.

One-point AG codes

$P_1, \ldots, P_n, Q$ rational places in function field of trdg=1.

We consider $\mu_2 < \mu_1$

$$C_2 = C_{\mathcal{L}}(D = P_1 + \cdots + P_n, \mu_2 Q) \subseteq C_1 = C_{\mathcal{L}}(D, \mu_1 Q) \subseteq \mathbb{F}_q^n.$$

We have a general method to estimate (find) RGHWs of these codes.

For Hermitian codes often sharp.

Estimating RGHW of AG codes

$H(Q)$ Weierstrass semigroup of Q.

$$H^*(Q) = \{m \in H(Q) \mid C_{\mathcal{L}}(D, mQ) \neq C_{\mathcal{L}}(D, (m-1)Q)\}.$$

Example:
$H(Q) = \langle 3, 4 \rangle = \{0, 3, 4, 6, 7, 8, \ldots\}$

$H^*(Q) = \{0, 3, 4, 6, 7, 8, \ldots, 26, 28, 29, 32\}$.

If $D \subseteq C_{\mathcal{L}}(D, 20Q)$, $D \cap C_{\mathcal{L}}(D, 16Q) = \{\vec{0}\}$, $\dim D = 2$

then $D = \mathrm{span}_{\mathbb{F}_q}\big\{\big(f_1(P_1), \ldots, f_1(P_n)\big), \big(f_2(P_1), \ldots, f_2(P_n)\big)\big\}$

where $-\nu_Q(f_1), -\nu_Q(f_2) \in \{17, 18, 19, 20\}$, $-\nu_Q(f_1) \neq -\nu_Q(f_2)$.

Estimating RGHW of AG codes

$H(Q)$ Weierstrass semigroup of Q.

$$H^*(Q) = \{m \in H(Q) \mid C_{\mathcal{L}}(D, mQ) \neq C_{\mathcal{L}}(D, (m-1)Q)\}.$$

Example:
$H(Q) = \langle 3, 4 \rangle = \{0, 3, 4, 6, 7, 8, \ldots\}$

$$H^*(Q) = \{0, 3, 4, 6, 7, 8, \ldots, 26, 28, 29, 32\}.$$

If $D \subseteq C_{\mathcal{L}}(D, 20Q)$, $D \cap C_{\mathcal{L}}(D, 16Q) = \{\vec{0}\}$, $\dim D = 2$

then $D = \text{span}_{\mathbb{F}_q}\Big\{\big(f_1(P_1), \ldots, f_1(P_n)\big), \big(f_2(P_1), \ldots, f_2(P_n)\big)\Big\}$

where $-\nu_Q(f_1), -\nu_Q(f_2) \in \{17, 18, 19, 20\}$, $-\nu_Q(f_1) \neq -\nu_Q(f_2)$.

Estimating RGHW of AG codes

$H(Q)$ Weierstrass semigroup of Q.

$H^*(Q) = \{m \in H(Q) \mid C_{\mathcal{L}}(D, mQ) \neq C_{\mathcal{L}}(D, (m-1)Q)\}$.

Example:
$H(Q) = \langle 3, 4 \rangle = \{0, 3, 4, 6, 7, 8, \ldots\}$

$H^*(Q) = \{0, 3, 4, 6, 7, 8, \ldots, 26, 28, 29, 32\}$.

If $D \subseteq C_{\mathcal{L}}(D, 20Q)$, $D \cap C_{\mathcal{L}}(D, 16Q) = \{\vec{0}\}$, $\dim D = 2$

then $D = \text{span}_{\mathbb{F}_q}\{(f_1(P_1), \ldots, f_1(P_n)), (f_2(P_1), \ldots, f_2(P_n))\}$

where $-\nu_Q(f_1), -\nu_Q(f_2) \in \{17, 18, 19, 20\}$, $-\nu_Q(f_1) \neq -\nu_Q(f_2)$.

Estimating RGHW of AG codes - cont

$H^*(Q) = \{0, 3, 4, 6, 7, 8, \ldots, 26, 28, 29, 32\}$.

...say $-\nu_Q(f_1) = 19$, $-\nu_Q(f_2) = 20$.

$19 + H^*(Q) = \{19, 22, 23, 25, \ldots, 45, 47, 48, 51\}$
$20 + H^*(Q) = \{20, 23, 24, 26, \ldots, 46, 48, 49, 52\}$

$|\,\mathrm{supp}(D)\,| \geq |\, H^*(Q) \cap ((19 + H^*(Q)) \cup (20 + H^*(Q)))\,|$.

In other words: we count how much we hit inside $H^*(Q)$

Estimating RGHW of AG codes - cont

$H^*(Q) = \{0, 3, 4, 6, 7, 8, \ldots, 26, 28, 29, 32\}$.

...say $-\nu_Q(f_1) = 19$, $-\nu_Q(f_2) = 20$.

$19 + H^*(Q) = \{19, 22, 23, 25, \ldots, 45, 47, 48, 51\}$
$20 + H^*(Q) = \{20, 23, 24, 26, \ldots, 46, 48, 49, 52\}$

$|\,\mathrm{supp}(D)\,| \geq |\, H^*(Q) \cap \big((19 + H^*(Q)) \cup (20 + H^*(Q))\big)\,|$.

In other words: we count how much we hit inside $H^*(Q)$

PURE MAGIC: $\mid H^*(Q) \cap (20 + H^*(Q)) \mid = n - 20 = 27 - 20 = 7.$

We need to add, what 19 hits, but 20 does NOT hit.

Recall, $H^*(Q) = \{0, 3, 4, 6, 7, \text{something}\}.$

$$\begin{array}{ccccccccccc}
 & * & \cdot & \cdot & * & * & \cdot & * & * & * & \cdots \\
* & \cdot & \cdot & * & * & \cdot & * & * & * & * & \cdots \\
\uparrow & & & \uparrow & & & \uparrow & & & &
\end{array}$$

That is, we hit 3 more. In total we hit $n - 20 + 3 = 10.$

Universal method.

Estimating RGHW of AG codes - cont

PURE MAGIC: $|\ H^*(Q) \cap (20 + H^*(Q))\ | = n - 20 = 27 - 20 = 7.$

We need to add, what 19 hits, but 20 does NOT hit.

Recall, $H^*(Q) = \{0, 3, 4, 6, 7, \text{something}\}$.

$$
\begin{array}{ccccccccccc}
 & * & \cdot & \cdot & * & * & \cdot & * & * & * & \cdots \\
* & \cdot & \cdot & * & * & \cdot & * & * & * & * & \cdots \\
\uparrow & & & \uparrow & & & \uparrow & & & &
\end{array}
$$

That is, we hit 3 more. In total we hit $n - 20 + 3 = 10$.

Universal method.

Estimating RGHW of AG codes - cont

PURE MAGIC: $| H^*(Q) \cap (20 + H^*(Q)) | = n - 20 = 27 - 20 = 7$.

We need to add, what 19 hits, but 20 does NOT hit.

Recall, $H^*(Q) = \{0, 3, 4, 6, 7, \text{something}\}$.

$$
\begin{array}{ccccccccccc}
 & * & \cdot & \cdot & * & * & \cdot & * & * & * & \cdots \\
* & \cdot & \cdot & * & * & \cdot & * & * & * & * & \cdots \\
\uparrow & & & \uparrow & & & \uparrow & & & &
\end{array}
$$

That is, we hit 3 more. In total we hit $n - 20 + 3 = 10$.

Universal method.

Now $-\nu_Q(f_1) = 18$, $-\nu_Q(f_2) = 20$.

$$
\begin{array}{cccccccccccc}
 & & * & \cdot & \cdot & * & * & \cdot & * & * & * & \cdots \\
* & \cdot & \cdot & * & * & \cdot & * & * & * & * & * & \cdots \\
\uparrow & & & \uparrow & \uparrow & & & \uparrow & & & &
\end{array}
$$

In total we hit $n - 20 + 4 = 11$.

Estimating RGHW of one-point AG codes

A general method to estimate RGHW of ANY one-point AG codes.

Theorem

Consider the Hermitian curve $x^{q+1} - y^q - y$ over $\mathbb{F}_{q^2}$. Let μ_1, μ_2 be non-negative integers with $1 \leq \mu_1 - \mu_2 \leq q+1$. For $1 \leq m \leq \dim(C_{\mathcal{L}}(D, \mu_1 Q)) - \dim(C_{\mathcal{L}}(D, \mu_2 Q))$ we have

$$M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) \geq n - \mu_1 + q(m-1) - (m-2)(m-1)/2.$$

The bound is sharp in most cases.