A linear ramp secret sharing scheme can be described as a cost construction $C_1/C_2$ where $C_2 \subseteq C_1$ are linear codes. It was shown in [1, 4] that the corresponding relative generalized Hamming weights (RGHW) express the worst case information leakage to unauthorized sets in such a system. Furthermore RGHWs can also be used to express the best case information leakage. To estimate RGHW of one-point algebraic geometric codes is possible by applying carefully the Feng–Rao bounds for primary as well as dual codes.

**The t-privacy**

The smallest possible number of shares for which the adversary can determine $m$-q-bits of information

$$I_{\mathcal{C}_1} = \min\{ I(S; f(x)) \mid |f(x)| = m \} = M_m(C_2^t, C_1^t)$$

in particular $t = M_m(C_2^t, C_1^t) - 1$ [1,4]. (See also for the special case of $\ell = 1$ [3]).

**Theorem: Computation of $r_m$ and $\ell_m$**

Let $C_1/C_2$ where dim $C_1 \cap C_2 = 0$ be a linear ramp secret sharing scheme with $(t_1, t_2)$-privacy and $(r_1, r_2)$-reconstruction. Then for $m = 1, \ldots, \ell_m$ we have

$$r_m = M_m(C_2^t, C_1^t) - 1$$

and

$$r_m = M_m(C_2^t, C_1^t) - 1$$

in particular, $t = M_m(C_2^t, C_1^t) - 1$ and $m = r - M_m(C_2^t, C_1^t) + 1$.

**Notation for AG-codes**

Given an algebraic function field $F$ of transcendence degree one, let $P_1, \ldots, P_n$ be distinct rational places. For $f \in F$ write $\rho(f) = -\log_2(f)$ and denote by $H(Q)$ the Weisstrass semigroup of $Q$. That is, $H(Q) = \{ \log\mathcal{L}(\mathcal{O}(Q)) \}$. In the following let $\{ f_i \}^\alpha \in H(Q)$ be any fixed basis for $R = \mathcal{O}(Q)(\mathcal{O}(Q))$ with $\rho(f_i) = \alpha$ for all $\lambda \in H(Q)$. Let $D = P_1 + \cdots + P_n$.

**Theorem: Bound for the RGHW’s of AG-codes**

Let $\mu_1, \mu_2$ be positive integers with $\mu_2 > \mu_1$. For $m = 1, \ldots, \dim C_2(D, D\mu_1) - \dim C_2(D, D\mu_2)$ we have

$$M_m(C_2(D, D\mu_1), C_2(D, D\mu_2)) \geq n - \mu_2 + Z(H(Q), \mu, m),$$

where $\mu = \mu_2 - \mu_1$.

**Theorem: Bound for the RGHW’s of Hermitian codes**

Let $\mu, \mu_1$ be positive integers satisfying

$$\mu \leq q < 1, \quad q^{-1} - 1 + \mu \leq q - 1.$$ (2)

Then for $C_1 = C_2(\mu, Q)$ and $C_2 = C_2(D, (\mu - 1)Q)$, we have

$$M_m(C_1, C_2) \geq n - \mu + \sum_{s=0}^{n-2} (q-s)$$ (3)

Equality holds simultaneously in (3) and (4) when the last part of (2) is replaced with

$$2g(q-1) - 2 < \mu < q-1.$$ (5)

**References**


