Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography

2014 EUROPEAN SCHOOL OF INFORMATION THEORY

Relative generalized Hamming weights

Olav Geil[1], Stefano Martin[1], Ryutaroh Matsumoto[2] and Diego Ruano[1]
[1]Department of Mathematical Sciences, Aalborg University, Denmark
[2]Department of Communications and Integrated Systems, Tokyo Institute of Technology, Japan

Ramp secret sharing schemes

A ramp secret sharing scheme with t-privacy and r-reconstruction is an algorithm that given an input $\vec{s} \in \mathbb{F}_q^\ell$, outputs a vector $\vec{x} \in \mathbb{F}_q^n$, the vector of shares that we want to share among n players, such that given a collection of shares $\{x_i \mid i \in \mathcal{I}\}$, one has no information about $\vec{s}$ if $\#\mathcal{I} \leq t$ and one can recover $\vec{s}$ if $\#\mathcal{I} \geq r$ [2].

Ramp secret sharing schemes from linear codes

Let $C_2 \subsetneq C_1 \subset \mathbb{F}_q^n$. Set $k_2 = \dim(C_2)$ and $k_1 = \dim(C_1)$ and let $L \subset \mathbb{F}_q^n$ be such that $C_1 = L \oplus C_2$. We denote by $\ell = \dim(L) = k_1 - k_2$. We consider $\vec{x} = \psi(\vec{s}) + \vec{c}_2 \in C_1$ where $\vec{s} \in \mathbb{F}_q^\ell$ is the secret, $\psi : \mathbb{F}_q^\ell \to L$ is a vector space isomorphism and $\vec{c}_2 \in C_2$ is chosen randomly (uniformly distributed). The n shares consist of the n coordinates of $\vec{x}$.

The mutual information

Let $\mathcal{I} \subset \mathcal{J} = \{1, \ldots, n\}$, we consider that an adversary obtains the shares $\{x_i \mid i \in \mathcal{I}\}$. The amount of information in q-bits that the adversary obtains is measured by $I(\vec{S}; f_{\mathcal{I}}(\vec{X}))$, the mutual information. Here $\vec{S}$ is the random variable that represents the secrets, the shares obtained by the adversary are denoted by $f_{\mathcal{I}}(\vec{x}) = (x_i \mid i \in \mathcal{I})$, where $f_{\mathcal{I}} : \mathbb{F}_q^n \to \mathbb{F}_q^{\#\mathcal{I}}$, and the random variable $\vec{X}$ represents the shares.

Definition: The function $\bar{\rho}$

$\bar{\rho} : \mathbb{F}_q^n \to \mathcal{J} \cup \{0\}$ is given as follows. For non-zero $\vec{c}$ we have $\bar{\rho}(\vec{c}) = i$ where i is the unique integer such that

$$\vec{c} \in \mathrm{Span}\{\vec{b}_1, \ldots, \vec{b}_i\} \backslash \mathrm{Span}\{\vec{b}_1, \ldots, \vec{b}_{i-1}\}, \quad \bar{\rho}(\vec{0}) = 0.$$

Definition: The component wise product

$$(\alpha_1, \ldots, \alpha_n) * (\beta_1, \ldots, \beta_n) = (\alpha_1\beta_1, \ldots, \alpha_n\beta_n).$$

Definition: The one-way well-behaving property

An ordered pair $(i, j) \in \mathcal{J} \times \mathcal{J}$ is said to be one-way well-behaving (OWB) if $\bar{\rho}(\vec{b}_{i'} * \vec{b}_j) < \bar{\rho}(\vec{b}_i * \vec{b}_j)$ holds true for all $i' \in \mathcal{J}$ with $i' < i$.

The set Λ_i

For $i \in \mathcal{J}$ we define

$\Lambda_i = \{l \in \mathcal{J} \mid \exists j \in \mathcal{J}$ such that (i, j) is OWB and $\bar{\rho}(\vec{b}_i * \vec{b}_j) = l\}$.

A linear ramp secret sharing scheme can be described as a coset 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 is

$$\min_{\mathcal{I} \subset \mathcal{J}} \{\#\mathcal{I} \mid I(\vec{S}; f_{\mathcal{I}}(\vec{X})) = m\} =$$

$$\min_{\mathcal{I} \subset \mathcal{J}} \{\#\mathcal{I} \mid \dim((C_2^\perp \cap V_{\mathcal{I}})/(C_1^\perp \cap V_{\mathcal{I}})) = m\} = M_m(C_2^\perp, C_1^\perp).$$

In particular $t = M_1(C_2^\perp, C_1^\perp) - 1$ [1,4]. (See also for the special case of $\ell = 1$ [3]).

Definition: Relative Generalized Hamming Weights

The mth relative generalized Hamming weight (RGHW), with $m \in \{1, \ldots, \ell\}$ [5]:

$$M_m(C_1, C_2) = \min_{\mathcal{I} \subset \mathcal{J}} \{\#\mathcal{I} \mid \dim((C_1 \cap V_{\mathcal{I}})/(C_2 \cap V_{\mathcal{I}})) = m\}$$

where $V_{\mathcal{I}} = \{\vec{x} \in \mathbb{F}_q^n : x_i = 0 \ \forall i \notin \mathcal{I}\}$.

Theorem: Feng-Rao bound with OWB property for primary code

Consider $C_2 \subseteq C_1$. Let u be the smallest element in $\bar{\rho}(C_1)$ that is not in $\bar{\rho}(C_2)$. For $m = 1, \ldots, \dim C_1 - \dim C_2$ we have

$$M_m(C_1, C_2) \geq \min\{\#\cup_{s=1}^m \Lambda_{i_s} \mid u \leq i_1 < \cdots < i_m \ i_1, \ldots, i_m \in \bar{\rho}(C_1 \backslash \{\vec{0}\})\}.$$

Definition: The value $Z(\Lambda, \mu, m)$

Consider a numerical semigroup Λ and a positive integer μ. Define $Z(\Lambda, \mu, 1) = 0$ and for $1 < m \leq \mu$

$$Z(\Lambda, \mu, m) = \min\{\#\{\alpha \in \cup_{s=1}^{m-1}(i_s + \Lambda) \mid \alpha \notin \Lambda\} \mid -\mu + 1 \leq i_1 < \cdots < i_{m-1} \leq -1\}.$$

Lemma: The value $Z(\langle a, a+1\rangle, \mu, m)$

Let $a \geq 2$ be an integer. Define $\Lambda = \langle a, a+1\rangle$. For integers m, μ with $1 \leq m \leq \mu \leq a+1$ it holds that

$$Z(\Lambda, \mu, m) = \sum_{s=0}^{m-2}(a - s) = a(m-1) - (m-2)(m-1)/2.$$

Hermitian codes

The Hermitian function field over $\mathbb{F}_{q^2}$ (q a prime power) is given by the equation $x^{q+1} - y^q - y$ and it possesses exactly $q^3 + 1$ rational places $P_1, \ldots, P_{q^3}, Q$. The Weierstrass semigroup of Q, $H(Q) = \langle \rho(x) = q, \rho(y) = q+1\rangle$, has $g = q(q-1)/2$ gaps and conductor $c = q(q-1)$. Let $D = P_1 + \cdots + P_{q^3}$. In the following by a Hermitian code we shall mean a code of the form $C_{\mathcal{L}}(D, \mu Q)$.

Definition: $(t_1, \ldots, t_\ell)$-privacy and $(r_1, \ldots, r_\ell)$-reconstruction

We say that a ramp secret sharing scheme has $(t_1, \ldots, t_\ell)$-privacy and $(r_1, \ldots, r_\ell)$-reconstruction if $t_1, \ldots, t_\ell$ are chosen largest possible and $r_1, \ldots, r_\ell$ are chosen smallest possible such that:

- an adversary cannot obtain m q-bits of information about $\vec{s}$ with any t_m shares,
- it is possible to recover m q-bits of information about $\vec{s}$ with any collection of r_m shares.

In particular, one has $t = t_1$ and that $r = r_\ell$.

Theorem: Computation of r_m and t_m

Let C_1/C_2 where $\dim C_1 - \dim C_2 = \ell$ be a linear ramp secret sharing scheme with $(t_1, \ldots, t_\ell)$-privacy and $(r_1, \ldots, r_\ell)$-construction. Then for $m = 1, \ldots, \ell$ we have $t_m = M_m(C_2^\perp, C_1^\perp) - 1$ and $r_m = n - M_{\ell-m+1}(C_1, C_2) + 1$. In particular, $t = M_1(C_2^\perp, C_1^\perp) - 1$ and $r = n - M_1(C_1, C_2) + 1$.

Notation for AG-codes

Given an algebraic function field F of transcendence degree one, let $P_1, \ldots, P_n, Q$ be distinct rational places. For $f \in F$ write $\rho(f) = -\nu_Q(f)$ and denote by $H(Q)$ the Weierstrass semigroup of Q. That is, $H(Q) = \rho(\cup_{\mu=0}^\infty \mathcal{L}(\mu Q))$. In the following let $\{f_\lambda \mid \lambda \in H(Q)\}$ be any fixed basis for $R = \cup_{\mu=0}^\infty \mathcal{L}(\mu Q)$ with $\rho(f_\lambda) = \lambda$ for all $\lambda \in H(Q)$. Let $D = P_1 + \cdots + P_n$.

Theorem: Bound for the RGHW's of AG codes

Let μ_1, μ_2 be positive integers with $\mu_2 < \mu_1$.
For $m = 1, \ldots, \dim C_{\mathcal{L}}(D, \mu_1 Q) - \dim C_{\mathcal{L}}(D, \mu_2 Q)$ we have

$$M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) \geq n - \mu_1 + Z(H(Q), \mu, m),$$

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

Theorem: Bound for the RGHW's of Hermitian codes

Let $\mu, \widetilde{\mu}$ be positive integers satisfying

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

Then for $C_1 = C_{\mathcal{L}}(D, \mu Q)$ and $C_2 = C_{\mathcal{L}}(D, (\mu - u)Q)$ we have $\dim C_1 - \dim C_2 = \dim C_2^\perp - \dim C_1^\perp = \widetilde{\mu}$. For $m = 1, \ldots, \widetilde{\mu}$

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

$$n - M_{\widetilde{\mu}+1-m}(C_2^\perp, C_1^\perp) + 1 \leq n - \mu + q(q-1) + \widetilde{\mu} - 1 - \sum_{s=0}^{\widetilde{\mu}-m-1}(q - s). \quad (4)$$

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

$$2q(q-1) - 2 + \widetilde{\mu} < \mu < n - q(q-1).$$

References

[1] T. Bains. Generalized Hamming weights and their applications to secret sharing schemes. Master's thesis, Univ. Amsterdam, 2008.

[2] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan. Secure computation from random error correcting codes. In *Advances in cryptology—EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Comput. Sci.*, pages 291–310. Springer, Berlin, 2007.

[3] I. M. Duursma and S. Park. Coset bounds for algebraic geometric codes. *Finite Fields Appl.*, 16(1):36–55, 2010.

[4] J. Kurihara, T. Uyematsu, and R. Matsumoto. Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight. *IEICE Trans. Fundamentals*, E95-A(11):2067–2075, Nov. 2012.

[5] Y. Luo, C. Mitrpant, A. J. Han Vinck, and K. Chen. Some new characters on the wire-tap channel of type II. *IEEE Trans. Inform. Theory*, 51(3):1222–1229, 2005.

[6] O. Geil, S. Martin, R. Matsumoto, and D. Ruano. Relative generalized Hamming weights of one-point algebraic geometric codes. *Manuscript*, page 27.