The Torsion-Limit for Algebraic Function Fields and Its Application to Arithmetic Secret Sharing

Ignacio Cascudo (CWI Amsterdam)
Ronald Cramer (CWI & Leiden Univ.)
Chaoping Xing (NTU Singapore)

CRYPTO 2011

Thursday, August 18, 2011

n-Codes

Let $\mathbb{F}_q$ be a finite field, $k, n \in \mathbb{Z}_{\geq 1}$ (k "size of the secret", n "number of shares").

Definition (n-Code)

An n-code for $\mathbb{F}_q^k$ is a $\mathbb{F}_q$-vector subspace

$$C \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$$

such that

n-Codes

Let $\mathbb{F}_q$ be a finite field, $k, n \in \mathbb{Z}_{\geq 1}$ (k "size of the secret", n "number of shares").

Definition (n-Code)

An n-code for $\mathbb{F}_q^k$ is a $\mathbb{F}_q$-vector subspace

$$C \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$$

such that

1. The "secret" coordinate* of C can take any value in $\mathbb{F}_q^k$.

*Think of $\mathbf{x} \in C$ as $\mathbf{x} = (\mathbf{x}_0, x_1, \ldots, x_n)$ where:
$\mathbf{x}_0 \in \mathbb{F}_q^k$ secret "coordinate"
$x_1, \ldots, x_n \in \mathbb{F}_q$ share coordinates.

n-Codes

Let $\mathbb{F}_q$ be a finite field, $k, n \in \mathbb{Z}_{\geq 1}$ (k "size of the secret", n "number of shares").

Definition (n-Code)

An n-code for $\mathbb{F}_q^k$ is a $\mathbb{F}_q$-vector subspace

$$C \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$$

such that

1. The "secret" coordinate* of C can take any value in $\mathbb{F}_q^k$.
2. The n "share" coordinates of C jointly determine the secret coordinate.

*Think of $\mathbf{x} \in C$ as $\mathbf{x} = (\mathbf{x}_0, x_1, \ldots, x_n)$ where:
$\mathbf{x}_0 \in \mathbb{F}_q^k$ secret "coordinate"
$x_1, \ldots, x_n \in \mathbb{F}_q$ share coordinates.

Definition (r-reconstructing)

An n-code C for $\mathbb{F}_q^k$ is *r-reconstructing* $(1 \leq r \leq n)$ if it holds that any r shares determine the secret.

Note that an n-code is n-reconstructing by definition.

Definition (r-reconstructing)

An n-code C for $\mathbb{F}_q^k$ is *r-reconstructing* $(1 \leq r \leq n)$ if it holds that any r shares determine the secret.

Note that an n-code is n-reconstructing by definition.

Definition (t-Disconnected and t-Uniform n-Code)

An n-code C for $\mathbb{F}_q^k$ is *t-disconnected* if $t = 0$, or else if $1 \leq t < n$, the secret is "*independent*" of any t shares.

Definition (r-reconstructing)

An n-code C for $\mathbb{F}_q^k$ is *r-reconstructing* ($1 \leq r \leq n$) if it holds that any r shares determine the secret.

Note that an n-code is n-reconstructing by definition.

Definition (t-Disconnected and t-Uniform n-Code)

An n-code C for $\mathbb{F}_q^k$ is *t-disconnected* if $t = 0$, or else if $1 \leq t < n$, the secret is "*independent*" of any t shares.

If, additionally, any set of t shares is uniformly distributed in $\mathbb{F}_q^t$ C has *t-uniformity*.

Definition (Powers of an n-Code)

Let $d \in \mathbb{Z}_{>0}$.For C an n-code for $\mathbb{F}_q^k$, let

$$C^{*d} := \mathbb{F}_q < \{\mathbf{c}^{(1)} * \ldots * \mathbf{c}^{(d)} : \mathbf{c}^{(1)}, \ldots, \mathbf{c}^{(d)} \in C\} > .$$

(where $*$ denotes coordinatewise product)

Definition (Powers of an n-Code)

Let $d \in \mathbb{Z}_{>0}$.For C an n-code for $\mathbb{F}_q^k$, let

$$C^{*d} := \mathbb{F}_q < \{\mathbf{c}^{(1)} * \ldots * \mathbf{c}^{(d)} : \mathbf{c}^{(1)}, \ldots, \mathbf{c}^{(d)} \in C\} > .$$

(where $*$ denotes coordinatewise product)

Remark (Powering Need Not Preserve n-Code)

Let $C \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$ be an n-code for S. Consider C^{*d} $(d \geq 2)$.

- *Trivially, the secret coordinate of C^{*d} can take any value.*

Definition (Powers of an n-Code)

Let $d \in \mathbb{Z}_{>0}$.For C an n-code for $\mathbb{F}_q^k$, let

$$C^{*d} := \mathbb{F}_q < \{\mathbf{c}^{(1)} * \ldots * \mathbf{c}^{(d)} : \mathbf{c}^{(1)}, \ldots, \mathbf{c}^{(d)} \in C\} > .$$

(where $*$ denotes coordinatewise product)

Remark (Powering Need Not Preserve n-Code)

Let $C \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$ be an n-code for S. Consider C^{*d} $(d \geq 2)$.

- *Trivially, the secret coordinate of C^{*d} can take any value.*
- **But***: the share coordinates of C^{*d}* need not *determine the secret coordinate.*

Definition (Powers of an n-Code)

Let $d \in \mathbb{Z}_{>0}$.For C an n-code for $\mathbb{F}_q^k$, let

$$C^{*d} := \mathbb{F}_q < \{\mathbf{c}^{(1)} * \ldots * \mathbf{c}^{(d)} : \mathbf{c}^{(1)}, \ldots, \mathbf{c}^{(d)} \in C\} > .$$

(where $*$ denotes coordinatewise product)

Remark (Powering Need Not Preserve n-Code)

Let $C \subset \mathbb{F}_q^k \times \mathbb{F}_q^n$ be an n-code for S. Consider C^{*d} $(d \geq 2)$.

- *Trivially, the secret coordinate of C^{*d} can take any value.*
- **But***: the share coordinates of C^{*d}* need not *determine the secret coordinate.*
- *Thus:* C^{*d} **need not be an n-code for $\mathbb{F}_q^k$.**

Arithmetic Secret Sharing Schemes

Definition

An (n, t, d, r)*-arithmetic secret sharing scheme for* $\mathbb{F}_q^k$ *(over* $\mathbb{F}_q$*)* is an n-code C for $\mathbb{F}_q^k$ such that:

1. $t \geq 1$, $d \geq 2$.
2. The n-code C is t-disconnected.
3. C^{*d} is in fact an n-code for $\mathbb{F}_q^k$.
4. The n-code C^{*d} is r-reconstructing.

Arithmetic Secret Sharing Schemes

Definition

An (n, t, d, r)*-arithmetic secret sharing scheme for* $\mathbb{F}_q^k$ *(over* $\mathbb{F}_q$*)* is an n-code C for $\mathbb{F}_q^k$ such that:

1. $t \geq 1$, $d \geq 2$.
2. The n-code C is t-disconnected.
3. C^{*d} is in fact an n-code for $\mathbb{F}_q^k$.
4. The n-code C^{*d} is r-reconstructing.

The arithmetic SSS has *uniformity* if, in addition, the n-code C has t-uniformity.

Arithmetic Secret Sharing Schemes

Definition

An (n, t, d, r)*-arithmetic secret sharing scheme for* $\mathbb{F}_q^k$ *(over* $\mathbb{F}_q$*)* is an n-code C for $\mathbb{F}_q^k$ such that:

1. $t \geq 1$, $d \geq 2$.
2. The n-code C is t-disconnected.
3. C^{*d} is in fact an n-code for $\mathbb{F}_q^k$.
4. The n-code C^{*d} is r-reconstructing.

The arithmetic SSS has *uniformity* if, in addition, the n-code C has t-uniformity.

An $(n, t, 2, n - t)$-arithmetic SSS is a t*-strong multiplicative linear SSS* (Cramer/Damgaard/Maurer EUROCRYPT 2000).

This notion is in turn generalized by *arithmetic codices.*

Remark (Arithmetic SSS exist)

If $n + k \leq q$ and $d(t + k - 1) < n - t$, then:

Shamir (or Franklin/Yung for $k > 1$) schemes are $(n, t, d, n - t)$-arithmetic SSS with uniformity for $\mathbb{F}_q^k$.

Remark (Arithmetic SSS exist)

If $n + k \leq q$ and $d(t + k - 1) < n - t$, then:

Shamir (or Franklin/Yung for $k > 1$) schemes are $(n, t, d, n - t)$-arithmetic SSS with uniformity for $\mathbb{F}_q^k$.

Question (2006):
What happens if q is fixed and n is unbounded?
Can positive rates ($t = \Omega(n)$) be achieved?

(Note: We consider d constant, as otherwise $t = \Omega(n)$ is provably imposible).

Previous results

Can positive rates ($t = \Omega(n)$) be achieved?

Previous results

Can positive rates ($t = \Omega(n)$) be achieved?

- Chen/Cramer (2006): Yes, if $A(q) > 2d$.* Includes q square with $q > (2d+1)^2$ and all q very large.

*$A(q)$ Ihara's constant of $\mathbb{F}_q$

Previous results

Can positive rates ($t = \Omega(n)$) be achieved?

- Chen/Cramer (2006): Yes, if $A(q) > 2d$.* Includes q square with $q > (2d+1)^2$ and all q very large.
- Cascudo/Chen/Cramer/Xing(2009): For $d = 2$ and **without uniformity**, *any* finite field $\mathbb{F}_q$.

*$A(q)$ Ihara's constant of $\mathbb{F}_q$

Applications

Original application: IT-secure multi-party computation, **malicious adversary case** (Cramer/Damgaard/Maurer 2000).

Asymptotical version of BenOr/Goldwasser/Wigderson88, Chaum/Crépeau/Damgaard88

Applications

Original application: IT-secure multi-party computation, **malicious adversary case** (Cramer/Damgaard/Maurer 2000).

Asymptotical version of BenOr/Goldwasser/Wigderson88, Chaum/Crépeau/Damgaard88

But lately: Unexpected applications in *two-party cryptography*, usually via MPC-in-the-head paradigm:

“secure two-party computation” with small error and low communication.
“Players” are virtual processes!.

- (STOC 2007) Ishai/Kushilevitz/Ostrovsky/Sahai:
  Zero knowledge from multi-party computation.
- (TCC 2008) Harnik/Ishai/Kushilevitz/BuusNielsen:
  OT-Combiners via Secure Computation.
- (CRYPTO 2008) Ishai/Prabhakaran/Sahai:
  Founding Cryptography on Oblivious Transfer - Efficiently.
- (FOCS 2009) Ishai/Kushilevitz/Ostrovsky/Sahai:
  Extracting Correlations. Requires uniformity.
- (CRYPTO 2011, Previous talk!)
  Ishai/Kushilevitz/Ostrovsky/Prabhakaran/Sahai/Wullschleger:
  Constant-Rate Oblivious Transfer from Noisy Channels.
- (2011) Cramer/Damgaard/Pastro:
  Amortized Complexity of Zero Knowledge Proof of Multiplicative Relations. Note: $d > 2$ here.

Efficient error correction

Theorem (Cramer/Daza/Gracia/Jimenez/Leander/Marti/Padro, CRYPTO 05)

Let C be a $(n, t, 2, n-t)$-arithmetic SSS for $\mathbb{F}_q^k$ over $\mathbb{F}_q$. Then C has efficient error correction of the secret in the presence of t faulty shares.

Efficient error correction

Theorem (Cramer/Daza/Gracia/Jimenez/Leander/Marti/Padro, CRYPTO 05)

Let C be a $(n, t, 2, n-t)$-arithmetic SSS for $\mathbb{F}_q^k$ over $\mathbb{F}_q$. Then C has efficient error correction of the secret in the presence of t faulty shares.

We generalize this:

Theorem

Let C be a $(n, t, d, n-t)$-arithmetic SSS for $\mathbb{F}_q^k$ over $\mathbb{F}_q$. Then $C^{*(d-1)}$ has efficient error correction of the secret in the presence of t faulty shares.

Main results

In this paper:

- We introduce a new technique to construct algebraic geometric SSS.
- We define a new AG notion (torsion limit) and prove bounds for it.
- As a result we get (case $d = 2$):

Theorem

For $q = 8, 9$ and all $q \geq 16$ there is an infinite family of $(n, t, 2, n-t)$-arithmetic SSS for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with t-uniformity where n is unbounded, $k = \Omega(n)$ and $t = \Omega(n)$.

Main results

In this paper:

- We introduce a new technique to construct algebraic geometric SSS.
- We define a new AG notion (torsion limit) and prove bounds for it.
- As a result we get (case $d = 2$):

Theorem

For $q = 8, 9$ and all $q \geq 16$ there is an infinite family of $(n, t, 2, n-t)$-arithmetic SSS for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with t-uniformity where n is unbounded, $k = \Omega(n)$ and $t = \Omega(n)$.

CC06 could only achieve this for q square, $q > 49$.
Furthermore, in many cases, we achieve a larger rate t/n.

Algebraic Geometric codes

Let F an algebraic function field over $\mathbb{F}_q$.

Definition

For G a divisor of F, $P_1, \ldots, P_n, Q_1, \ldots, Q_k$ rational places of F, $P_i, Q_j \notin \mathrm{supp} G$, denote $D := \sum P_i + \sum Q_j$ and consider the AG-code:

$$C(G; D) = \{(f(Q_1), \ldots, f(Q_k), f(P_1), \ldots, f(P_n)) \,|f \in \mathcal{L}(G)\}$$

Algebraic Geometric codes

Let F an algebraic function field over $\mathbb{F}_q$.

Definition

For G a divisor of F, $P_1, \ldots, P_n, Q_1, \ldots, Q_k$ rational places of F, $P_i, Q_j \notin \mathrm{supp} G$, denote $D := \sum P_i + \sum Q_j$ and consider the AG-code:

$$C(G; D) = \{(f(Q_1), \ldots, f(Q_k), f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(G)\}$$

Remark

If $C = C(G; D)$, then $C^{*d} \subseteq C(dG; D)$.

Arithmetic SSS from Algebraic Geometric Codes

For $A \subset \{1, \ldots, n\}$ with $A \neq \emptyset$, define $P_A = \sum_{j \in A} P_j \in \mathrm{Div}(F)$.
Let $K \in \mathrm{Div}(F)$ be a canonical divisor.

Theorem

If the "Riemann-Roch system of equations"

$$\{\ell(dX - D + P_A + Q) = 0,\ \ell(K - X + P_A + Q) = 0\}_{A \subset \mathcal{I}^*, |A| = t}$$

has solution $X := G$, then $C(G; D)$ is an $(n, t, d, n-t)$-arithmetic secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ (with uniformity).

Arithmetic SSS from Algebraic Geometric Codes

For $A \subset \{1, \ldots, n\}$ with $A \neq \emptyset$, define $P_A = \sum_{j \in A} P_j \in \mathrm{Div}(F)$.
Let $K \in \mathrm{Div}(F)$ be a canonical divisor.

Theorem

If the "Riemann-Roch system of equations"

$$\{\ell(dX - D + P_A + Q) = 0,\ \ell(K - X + P_A + Q) = 0\}_{A \subset \mathcal{I}^*, |A| = t}$$

has solution $X := G$, then $C(G; D)$ is an $(n, t, d, n-t)$-arithmetic secret sharing scheme for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ (with uniformity).

In CC06: Strong conditions on F (large number rational places)
$\Rightarrow$ **any** divisor of a certain degree is a solution.

Solvability of RR systems

Let h be the class number of F, A_r number of effective divisors of degree r.

Theorem

Consider the system:

$$\{\ell(d_i X + Y_i) = 0\}_{i=1}^{L}.$$

If for some $s \in \mathbb{Z}$,

$$h > \sum_{i=1}^{L} A_{r_i(s)} \cdot |\mathcal{J}_F[d_i]|,$$

where $r_i(s) = d_i s + deg Y_i$, $i = 1, \ldots, L$,
then the system has a solution G of degree s.

- Bounds on A_r/h were obtained in several works in coding theory.
- $|\mathcal{J}_F[d]|$ not previously studied in that context (as far as we know).
- This is because the role of $|\mathcal{J}_F[d]|$ is linked to the requirements on C^{*d}.

The Torsion Limit

For $F/\mathbb{F}_q$ a function field, and $r \in \mathbb{Z}_{>1}$ we consider the r-torsion point group in $\mathcal{J}_F$, i.e., $\mathcal{J}_F[r] := \{[D] \in \mathcal{J}_F : \ r[D] = 0\}$.

Definition

For a family $\mathcal{F} = \{F/\mathbb{F}_q\}$ of function fields with $g(F) \to \infty$, we define its r-torsion limit:

$$J_r(\mathcal{F}) := \liminf_{F \in \mathcal{F}} \frac{\log_q |\mathcal{J}_F[r]|}{g(F)}.$$

The Torsion Limit

For $F/\mathbb{F}_q$ a function field, and $r \in \mathbb{Z}_{>1}$ we consider the r-torsion point group in $\mathcal{J}_F$, i.e., $\mathcal{J}_F[r] := \{[D] \in \mathcal{J}_F : \; r[D] = 0\}$.

Definition

For a family $\mathcal{F} = \{F/\mathbb{F}_q\}$ of function fields with $g(F) \to \infty$, we define its r-torsion limit:

$$J_r(\mathcal{F}) := \liminf_{F \in \mathcal{F}} \frac{\log_q |\mathcal{J}_F[r]|}{g(F)}.$$

Definition

For a prime power q and a real $a \in (0, A(q)]$, let $\mathfrak{F}$ the (non-empty) set of families $\mathcal{F} = \{F/\mathbb{F}_q\}$ with $g(F) \to \infty$ and $\lim \frac{|\mathbb{P}^{(1)}|(F)}{g(F)} \geq a$. Then define, for $r \in \mathbb{Z}_{>1}$,

$$J_r(q, a) := \liminf_{\mathcal{F} \in \mathfrak{F}} J_r(\mathcal{F}).$$

General result

Theorem

Fix $\mathbb{F}_q$ and $d \geq 2$. Suppose $A(q) > 1 + J_d(q, A(q))$.

Then there is an infinite family of $(n, t, d, n-t)$-arithmetic SSS for $\mathbb{F}_q^k$ over $\mathbb{F}_q$ with t-uniformity such that

- $n \to \infty,\ k = \Omega(n)$ *and* $t = \Omega(n)$.
- $C, \ldots, C^{*(d-1)}$ *have efficient t-error correction for the secret.*

Upper bounds for r-torsion limit, r prime

Theorem

Let $\mathbb{F}_q$ be a finite field and let $r > 1$ be a prime.

(i) *If $r \mid (q-1)$, then $J_r(q, A(q)) \leq \frac{2}{\log_r q}$.*

(ii) *If $r \nmid (q-1)$, then $J_r(q, A(q)) \leq \frac{1}{\log_r q}$*

(iii) *If q is square and $r \mid q$, then $J_r(q, \sqrt{q}-1) \leq \frac{1}{(\sqrt{q}+1)\log_r q}$.*

Conclusions

- Arithmetic SSS are an important abstract primitive in IT secure cryptography.
- Asymptotics have become important: recent applications in two party cryptography.

Conclusions

- Arithmetic SSS are an important abstract primitive in IT secure cryptography.
- Asymptotics have become important: recent applications in two party cryptography.
- Algebraic geometry seem only handle to obtain good asymptotic constructions.
- Probabilistic methods do not seem to work! (as opposed to code theory).

Conclusions

- Arithmetic SSS are an important abstract primitive in IT secure cryptography.
- Asymptotics have become important: recent applications in two party cryptography.
- Algebraic geometry seem only handle to obtain good asymptotic constructions.
- Probabilistic methods do not seem to work! (as opposed to code theory).
- Results: More general definitions and framework, new methodology to construct AG-SSS, existential results not known to be possible before, new notion of torsion limit and upper bounds for it.