Asymptotically Good Ideal LSSS with Strong Multiplication over *Any* Fixed Finite Field

Ignacio Cascudo (Oviedo), Hao Chen (Shanghai),
Ronald Cramer (CWI/Leiden), Chaoping Xing (Singapore)

Shamir's t-out-of-n Threshold SSS (1979)

Description

$\mathbb{F}_q$: *finite field*

$t, n \in \mathbb{Z} \ : n < |\mathbb{F}_q| = q, \quad 1 \leq t < n$

$x_1, \ldots, x_n \in \mathbb{F}_q \setminus \{0\} \ : x_i \neq x_j \ (i \neq j)$

Shamir's scheme $\Sigma(n, t, q, x_1, \ldots, x_n)$ *is a vector of* $n + 1$ *random variables*

$$(S_0, S_1, \ldots, S_n),$$

where

$$S_0 = f(0) \in \mathbb{F}_q, S_1 = f(x_1) \in \mathbb{F}_q, \ldots, S_n = f(x_n) \in \mathbb{F}_q,$$

with $f(X) \in \mathbb{F}_q[X]$ *uniformly random such that* $\deg f \leq t$,

n *is "the* number of players*" and* t *is the* threshold.

S_0 *is the secret and* $S_1, \ldots, S_n$ *are the shares.*

The Standard Properties

Notation (Random Variables)

$S = (S_0, S_1, \ldots, S_n)$: *the full vector of secret and shares.*
$S_A = (S_i)_{i \in A}$: *S restricted to the S_i with $i \in A$.*

The *standard* properties of Shamir's scheme:

- **Linearity**: The support of S is an $\mathbb{F}_q$-vector space, with the uniform distribution imposed on it.
- **Ideal**: The size of a share is the size of the secret, i.e., $H(S_i) = H(S_0)$ for $i = 1 \ldots n$.
- For all $A \subseteq \{1, \ldots, n\}$ the following holds:
  - If $|A| = t + 1$, then $H(S_0|S_A) = 0$ ($t+1$**-reconstruction**)
  - If $|A| = t$, then $H(S_0|S_A) = H(S_0)$ (t**-privacy**)

Remark (Weaker condition $n \leq q$, instead of $n < q$)

$n \leq |\mathbb{F}_q|$: *also use "the point x_∞ at infinity" on projective line.*
Comes down to placing secret in highest coefficient of $f(X)$.

Special Property: Strong Multiplication

Definition (The Random Variable $\widehat{S}$)

- Sample from S twice independently: vectors

$$\mathbf{s} = (s_0, s_1, \ldots, s_n), \mathbf{s}' = (s'_0, s'_1, \ldots, s'_n) \in \mathbb{F}_q^{n+1}.$$

- $\widehat{S} := (\widehat{S}_0, \widehat{S}_1, \ldots, \widehat{S}_n)$: from their **pairwise product $\mathbf{s} * \mathbf{s}'$**:

$$\widehat{S}_0 = s_0 \cdot s'_0 \in \mathbb{F}_q, \ldots, \widehat{S}_n = s_n \cdot s'_n \in \mathbb{F}_q.$$

Definition (The Conditions for t-Strong Multiplication)

- $1 \leq t < n$ and there is t**-privacy.**
- $(n-t)$**-product reconstruction**: for any A with $|A| = n - t$,

$$H(\widehat{S}_0 | \widehat{S}_A) = 0 :$$

"The product of two secrets is determined by the pairwise product of the share-vectors, in fact, by any $(n-t)$-subvector of that pairwise product."

Strong Multiplication: Continued

Theorem (Strong Multiplication in Shamir's SSS)

There is t-strong multiplication if and only if $t < n/3$.

The proof uses of course Lagrange's Interpolation Theorem.

Remark (Applications (I))

- *Crucial in the "Fundamental Theorem" on multiparty computation i.t.-secure against an active adversary.*

  *(*Ben-Or/Goldwasser/Wigderson, Chaum/Crépeau/Damgaard, STOC 1988*).*
- *Technical handle for the (intricate) reduction of secure multiplication to secure evaluation of linear forms.*
- *Strong multiplication as an abstract property in general linear secret sharing:* Cramer/Damgaard/Maurer, EUROCRYPT 2000*.*

Extension of the Definition to Linear SSS

Definition

- $\Sigma = (S_0, S_1, \ldots, S_n)$: **arbitrary** "ideal" LSSS over $\mathbb{F}_q$. Note: not even necessarily t-threshold! Write $n(\Sigma) = n$.
- Define ***t*-strong multiplication** analogously: $1 \leq t < n$, *t-privacy*, $(n-t)$*-product reconstruction*.
- $\widehat{\tau}(\Sigma) = \frac{3t}{n-1}$ is the **corruption tolerance** (where t is taken maximal for Σ).

(Ideal) LSSS don't typically satisfy strong multiplication.

Lemma (Basic Implications)

Suppose Σ as above has t-strong multiplication.

- *t-strong multiplication implies $n - 2t$ reconstruction. Hence corruption tolerance $\widehat{\tau}(\Sigma) \leq 1$ (since $t < \frac{n}{3}$).*
- *Particularly, $\widehat{\tau}(\Sigma) = 1$, i.e. $n - 1 - 3t = 0$, iff Σ is t-threshold (t-privacy and $(t+1)$-reconstruction).*

Limitations on Corruption Tolerance (I)

Notation (Infinite Families over Fixed Finite Field $\mathbb{F}_q$)

$\mathcal{F}$: family $\{\Sigma_n\}_{n \in \mathcal{N}}$ of "ideal" LSSS Σ_n over $\mathbb{F}_q$ such that

- *Index-set: $\mathcal{N} \subset \mathbb{Z}_{>0}$, $|\mathcal{N}| = \infty$, $n(\Sigma_n) = n$ for all $n \in \mathcal{N}$.*
- *Σ_n has $t(n)$-strong multiplication for all $n \in \mathcal{N}$.*

Remark

Definition is Non-Vacuous: *for every $\mathbb{F}_q$, such infinite families exist. E.g., from certain classical codes + replication.*

Note: *$\mathbb{F}_q$ is fixed $\Rightarrow < \infty$ Shamir-Schemes with strong multiplication (since $n < q$).*

The latter **not** just a limitation of Shamir's SSS:

Theorem (Max Possible Corruption Tolerance is Scarce)

For each infinite family $\mathcal{F} = \{\Sigma_n\}_{n \in \mathcal{N}}$ there are at most $< \infty$ many $n \in \mathcal{N}$ such that $\widehat{\tau}(\Sigma_n) = 1$, i.e., $n - 1 - 3t(n) = 0$.

Limitations on Corruption Tolerance (II)

Proof (From Connection with Max. Dist. Sep. Codes (MDS))

- *By basic implication:* $n - 1 - 3t(n) = 0 \Rightarrow \Sigma_n$ *is* t*-threshold.*
- *This Implies a (non-trivial) MDS* $\mathbb{F}_q$*-code of length* $n + 1$*.*
- **Fact***: for fixed q, at most* $< \infty$ *possible lengths.*

Remark

The gap $n - 1 - 3t$ cannot even be constant*: it must grow as a function of n (and q). More later on.*

Remark

Moreover: elementary approaches seem to give **vanishing corruption tolerance***. Example: replication of self-dual codes,* $t = \sqrt{n}$*.*

These observations motivate the following question:

Limitations on Corruption Tolerance (III)

Question

Asymptotically speaking ($n \to \infty$), is **constant-rate** *corruption tolerance possible over a* **fixed** *finite field?*

Definition (Corruption Tolerance of an Infinite Family over $\mathbb{F}_q$)

$$\widehat{\tau}(\mathcal{F}) = \limsup_{n \in \mathcal{N}} \widehat{\tau}(\Sigma_n), \quad \text{where} \quad \widehat{\tau}(\Sigma_n) = \frac{3 \cdot t(n)}{n-1}.$$

Definition (Asymptotic Optimal Corruption Tolerance over $\mathbb{F}_q$)

$$\widehat{\tau}(q) = \limsup_{\mathcal{F}} \widehat{\tau}(\mathcal{F}),$$

where $\mathcal{F}$ ranges over all possible families.

Question (Rephrased)

Is there a finite field $\mathbb{F}_q$ with $\widehat{\tau}(q) > 0$?

Known Results (Cast in Present Definitions)

Theorem (Chen and Cramer, CRYPTO 2006)

Let $\mathbb{F}_q$ be a finite field. If Ihara's constant $A(q) > 4$, then

$$\widehat{\tau}(q) \geq \left(1 - \frac{4}{A(q)}\right) > 0.$$

For instance, if $q \geq 49$, q square, then $A(q) = \sqrt{q} - 1 > 0$. This is by Ihara (81), Garcia/Stichtenoth (96). Hence,

$$\widehat{\tau}(q) \geq \left(1 - \frac{4}{\sqrt{q} - 1}\right) > 0.$$

Remark (Cases As Yet Unresolved)

The Drinfeld-Vladuts Bound: $A(q) \leq \sqrt{q} - 1$ **always**.

So: condition **false** *if $|\mathbb{F}_q| < 49$. Plus:*

possibly some "?" for $|\mathbb{F}_q| > 49$. Note $\# < \infty$: Serre's Thm (85).

Known Results (Continued)

Proof (from Towers $\mathcal{T}$ of Algebraic Function Fields $\mathbb{F}$ over $\mathbb{F}_q$)

- *Take $\mathcal{T}$ with $\frac{\mathbb{P}_1(\mathbb{F}_q)}{g(\mathbb{F})} \to A(q)$.*
- *$q \geq 49$, q square: on Drinfeld-Vladuts bound (Ihara (1981) Garcia/Stichtenoth (1996)).*
- *Large enough q ($> 2^{91}$): Serre's Theorem (1985).*
- Evaluation (Goppa) codes*:*
  from function spaces $\mathcal{L}(G) \subset \mathbb{F}$ and n points in $\mathbb{F}$ degree 1.
- *If*

  $$n > 4(g(\mathbb{F}) + 1), 3t < n - 4 \cdot g(\mathbb{F}),$$

  take

  $$G \in Div(\mathbb{F}), deg(G) = 2 \cdot g(\mathbb{F}) + t.$$

-

  $$C = \{(f(P_0), f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^{n+1} \ : \ f \in \mathcal{L}(G)\}.$$

Applications (II)

Original Motivation (CC06): extended Fundamental MPC Theorem with *constant-rate corruption tolerance,* $\mathbb{F}_q$ *fixed*.

But: $\exists$ **novel, fundamental use for the CC06 "special SSS"**;

Paradigm Shift (Modes of Use (2007–))

"Asymptotic SSS & MPC": now powerful even in 2-party crypto*.*
"Players": virtual processes, myriad; Asymptotics: performance.

1. *Ishai, Kushilevitz, Ostrovsky, Sahai* (*STOC 07*): Two-party zero knowledge for circuit-SAT with $O(1)$ communication per gate from "MPC in the Head."
2. *Ishai, Prabkharan, Sahai* (*CRYPTO 08*): Generalizations to two-party secure computation.
3. *Damgaard, Nielsen, Wichs* (*EUROCRYPT 08*): Isolated Zero Knowledge
4. *Ishai, Kushilevitz, Ostrovsky, Sahai* (*FOCS 09*): Two-Party Correlation Extractors

Results of the Present Work (I)

Result (1: Main Theorem)

$\widehat{\tau}(q) > 0$ *for* **all** *finite fields* $\mathbb{F}_q$*. So this* **includes** $\mathbb{F}_2$ *in particular.*

Explicit *lower bounds on* $\widehat{\tau}(q)$ *also given (see later).*

Result (2)

- **Capturing** *"ideal" LSSS with strong multiplication in terms of* **coding theory***:* **the class** $\mathcal{C}^{\dagger}(\mathbb{F}_q)$*.*

  Asymptotic optimal corruption tolerance $\widehat{\tau}(q)$ *is an* intrinsic property *of the class of codes* $\mathcal{C}^{\dagger}(\mathbb{F}_q)$*.*

  The definitions are oblivious *of secret sharing and multi-party computation.*

  From now on, we identify the class of "ideal" LSSS with strong multiplication with the class $\mathcal{C}^{\dagger}(\mathbb{F}_q)$*.*

Results of the Present Work (II)

Result (3)

Over each finite field $\mathbb{F}_q$, there is an infinite family $\mathcal{F}$ of t-strongly multiplicative such that

- $\mathcal{F}$ *is* **bad**, *i.e.,* $\widehat{\tau}(\mathcal{F}) = 0$.
- $\mathcal{F}$ *is "***elementary***", "no algebraic geometry."*
- **yet** $t = \Omega(n/((\log\log n)\log n)$.

Result (4)

First (nontrivial) **upper bound** *for t-strong multiplication as a function of q, n:*
Asymptotically, the **gap** *satisfies* $n - 1 - 3t = \Omega(\log n)$.

Lower bounds for $\widehat{\tau}(q)$ (I)

Definition

We define $\nu(q)$ as follows:

$$\nu(q) = \begin{cases} 1/35 \approx 2.86\% & q = 2 \\ 1/18 \approx 5.56\% & q = 3 \\ 3/35 \approx 8.57\% & q = 4 \\ 5/54 \approx 9.26\% & q = 5 \\ 1 - \frac{4}{\sqrt{q}-1} & q \text{ square }, q \geq 49 \\ \frac{1}{3}(1 - \frac{4}{q-1}) & \text{remaining } q \end{cases}$$

Theorem

Let $\mathbb{F}_q$ be a finite field. Then $\widehat{\tau}(q) \geq \nu(q)$.

Remark

$$\limsup_k \widehat{\tau}(q^k) = 1.$$

Lower bounds for $\widehat{\tau}(q)$ (II)

The proof combines CC06 with a **dedicated field descent method** based on **multiplication friendly embeddings.**

Definition (Multiplication-Friendly Embeddings (MFE))

An MFE is a tuple (q, m, e, σ, ψ) as follows.

- e is a positive integer (the *expansion*)
- $\sigma : \mathbb{F}_{q^m} \to \mathbb{F}_q^e$ is an $\mathbb{F}_q$-linear map
- $\psi : \mathbb{F}_q^e \to \mathbb{F}_{q^m}$ is an $\mathbb{F}_q$-linear map such that

$$xy = \psi(\sigma(x) * \sigma(y)) \; \forall x, y \in \mathbb{F}_{q^m}.$$

Remark

Extension field $\mathbb{F}_{q^m}$ is represented into "expansion" $\mathbb{F}_{q^e}$ such that representations of $\mathbb{F}_{q^m}$-products are obtained by taking the pairwise-product of their respective representations and applying an $\mathbb{F}_q$-linear map. "**Small" expansion is possible"**.

Lower bounds for $\widehat{\tau}(q)$ (III)

- m: smallest extension degree m with known $\widehat{\tau}(q^m) > 0$.
- Possible by CC06: suffices that $q^m \geq 49$ and q^m even.
- MFE (q, m, e, σ, ψ) with "small expansion" e (see later).
- Infinite family of codes $C \in \mathcal{C}^\dagger(\mathbb{F}_{q^m})$ on the known bound. Wlog, "secret in 0-th coordinate." Write $n = n(C)$.
- $G \subset \mathbb{F}_{q^m}^{n+1}$: $\mathbb{F}_q$-linear subspace that is $\mathbb{F}_q$-rational in the 0-th coordinate:

$$G = C \cap (\mathbb{F}_q \bigoplus (\mathbb{F}_{q^m})^n).$$

- $C_1 \in C^\dagger(\mathbb{F}_q)$: replace each $(c_0, c_1, \ldots, c_n) \in G$ by

$$(c_0, \sigma(c_1), \ldots, \sigma(c_n)) \in \mathbb{F}_q^{1+en}.$$

  Note: $n(C_1) = en$.
- In reality: slightly more refined descent strategy.

Lower bounds for $\widehat{\tau}(q)$ (IV)

Theorem

- $C_1 \in C^\dagger(\mathbb{F}_q)$.
- $t(C_1) \geq t(C)$ and $r(\widehat{C_1}) \leq e \cdot n(\widehat{C_1}) - t(C)$.
- *Hence:* $\widehat{t}(C_1) \geq \widehat{t}(C)$.

Corollary (of a more general theorem)

- *There exists an MFE of* $\mathbb{F}_{q^2}$ *over* $\mathbb{F}_q$ *with expansion 3.*
- *There exists an MFE of* $\mathbb{F}_{64}$ *over* $\mathbb{F}_4$ *with expansion 5.*

Example (The Sweetest Case: $\mathbb{F}_2$)

- $\widehat{\tau}(64) \geq (1 - \frac{4}{\sqrt{64}-1}) = \frac{3}{7}$ *by CC06.*
- *Descend from* $\mathbb{F}_{64}$ *to* $\mathbb{F}_4$*: lose a factor 5.*
- *Descend from* $\mathbb{F}_4$ *to* $\mathbb{F}_2$*: lose another factor 3.*
- $\widehat{\tau}(2) \geq \frac{1}{3} \cdot \frac{1}{5} \cdot \frac{3}{7} = \frac{3}{105} = \frac{1}{35}$.

Asymptotically Bad Yet "Elementary" Schemes

Remark

Let $\mathbb{F}_q$ be arbitrary. There is an infinite family of codes $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ whose construction uses only elementary linear algebra and yet $\widehat{t}(C) = \Omega(n(C)/((\log\log n(C))\log n(C))$.

Proof Sketch

- Idea*: Shamir's t-strong multiplication over extensions of $\mathbb{F}_q$ + iterative dedicated descent." More concretely:*
- *Take* **a family of Reed-Solomon codes** $C_m \in \mathcal{C}^{\dagger}(\mathbb{F}_{q^{2^m}})$ *for an infinite number of m.*
- **Apply iteratively** *an MFE for quadratic extensions.*
- *The codes $C'_m \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$ thus obtained satisfy the properties.*

Growth of the Gap $n(C) - 1 - 3 \cdot \widehat{t}(C)$

Theorem

Let $C \in \mathcal{C}^{\dagger}(\mathbb{F}_q)$. We have $\widehat{t}(C) \leq \frac{1}{3} \cdot (n(C) - \frac{1}{2} \cdot \log_q(n(C) + 2))$

Proof: by a generalization of a theorem by Karchmer and Wigderson (1993) combined with ideas by Cramer and Fehr (CRYPTO 2002).

Remark

This significantly strengthens the limitations implied by the non-existence of certain MDS-codes;
the codes must travel away from "highest corruption tolerance" at least at **logarithmic speed**.

Remark

This does **not** *imply that* $\widehat{\tau}(q) < 1$

Open questions

- Is there an *elementary proof* that $\widehat{\tau}(q) > 0$ which avoids the use of good towers of algebraic function fields altogether?

  (Seem *required* though in our context...as opposed to asymptotic coding theory case)

- Can we find better lower bounds for $\widehat{\tau}(q)$?

  (*For small fields, yes: Cascudo/Cramer/Xing 2009*, using more advanced algebraic geometry and novel measure on towers)

- Can we prove $\widehat{\tau}(q) < 1$ for some (or all) q?