ON CODES, MATROIDS AND SECURE MULTI-PARTY COMPUTATION FROM LINEAR SECRET SHARING SCHEMES

R. Cramer, V. Daza, I. Gracia, J. Jiménez Urroz,

G. Leander, J. Martí-Farré, C. Padró

CWI Amsterdam, UPC Barcelona, Ruhr-University Bochum

SHAMIR'S SECRET SHARING SCHEME

In **Shamir's (d, n)-threshold scheme**,
we have n **players** and $x_0, x_1, \dots, x_n \in \mathbb{K}$

$f(x) = a_0 + a_1 x + \cdots + a_{d-1} x^{d-1} \in \mathbb{K}[x]$ a random polynomial
$(f(x_1), \dots, f(x_n))$ are **shares** for the **secret value** $f(x_0) \in \mathbb{K}$

Shamir 1979

It has a (d, n)-**threshold access structure**

It is **linear** and **ideal**

If $n \geq 2d - 1$, it is **multiplicative**,
if $n \geq 3d - 2$, it is **strongly multiplicative**

SHAMIR'S SECRET SHARING SCHEME IS MULTIPLICATIVE

$(f(x_1), \ldots, f(x_n))$ shares for the secret $k = f(x_0)$
$(g(x_1), \ldots, g(x_n))$ shares for the secret $k' = g(x_0)$

Then, for every subset $A \subset P$ with $2d-1$ players

$$kk' = f(x_0)g(x_0) = \sum_{i \in A} \lambda_{i,A} f(x_i)g(x_i)$$

The values $(\lambda_{i,A})_{i \in A}$ do not depend on the random choice of f, g

If $n \geq 2d-1$, Shamir's scheme is **multiplicative**

If $n \geq 3d-2$, it is **strongly multiplicative**:
for every **unqualified subset** $B \notin \Gamma$, the shares of
the players in $A = P - B$ are enough to compute the multiplication

SHAMIR'S SECRET SHARING SCHEME AND MULTI-PARTY COMPUTATION

Since Shamir's scheme is **linear**, shares for $\mu k + \mu' k' \in \mathbb{K}$
can be found by computing the same
linear combination on shares of k and k'

Since Shamir's scheme is **multiplicative**, shares for
the **product** $kk' \in \mathbb{K}$ can be obtained from shares of k and k'

By using those properties, a **multi-party computation** protocol
secure against an **adversary** controlling
up to $d-1$ players is obtained
Passive adversary if $n \geq 2d-1$, **active** adversary if $n \geq 3d-2$

Ben-Or & Goldwasser & Wigderson 1988
Chaum & Crépeau & Damgård 1988

GENERAL SECURE MULTI-PARTY COMPUTATION (1)

How to find an efficient **multi-party computation protocol** for a **general** (non-threshold) adversary?

Theorem There exists a **MPC protocol** for an **adversary structure** $\mathcal{A} \subset P$ if and only if
$\mathcal{A}$ is $\mathcal{Q}_2$ for a **passive** adversary ($n \geq 2d - 1$ if threshold)
$\mathcal{A}$ is $\mathcal{Q}_3$ for an **active** adversary ($n \geq 3d - 2$ if threshold)

Hirt & Maurer 1997

GENERAL SECURE MULTI-PARTY COMPUTATION (2)

Theorem For an **(active)** adversary $\mathcal{A} \subset P$,
one can efficiently obtain a **MPC protocol** from any
(strongly) multiplicative linear secret sharing scheme
with access structure Γ with $\Gamma \cap \mathcal{A} = \emptyset$

In the **active** case, **strong multiplication** is not needed
if a negligible error probability is admitted

Cramer & Damgård & Maurer 2000

Corollary For a **threshold** adversary,
Shamir's scheme provides efficient MPC protocols

MULTIPLICATIVE LINEAR SECRET SHARING SCHEMES

For an access structure Γ, the values $\lambda_{\mathbb{K}}(\Gamma)$, $\mu_{\mathbb{K}}(\Gamma)$, $\mu'_{\mathbb{K}}(\Gamma)$ are, respectively, the **complexities** of the best $\mathbb{K}$-**LSSS**, $\mathbb{K}$-**MLSSS**, $\mathbb{K}$-**SMLSSS** for Γ

$\lambda_{\mathbb{K}}(\Gamma) = \mu_{\mathbb{K}}(\Gamma) = \mu'_{\mathbb{K}}(\Gamma) = n$ if Γ is a **threshold** structure

Theorem If Γ is $\mathcal{Q}_2$, then $\mu_{\mathbb{K}}(\Gamma) \leq 2\lambda_{\mathbb{K}}(\Gamma)$

Cramer & Damgård & Maurer 2000

Corollary In the **passive** case, **a MPC protocol** for a $\mathcal{Q}_2$ adversary structure $\mathcal{A}$ is efficiently obtained from **any LSSS** with $\mathcal{Q}_2$ access structure Γ with $\Gamma \cap \mathcal{A} = \emptyset$

OPEN PROBLEMS ON MULTIPLICATIVE LINEAR SECRET SHARING SCHEMES

Open Problem Is it possible to efficiently construct a **strongly multiplicative LSSS** from any LSSS?
Or, is $\mu'_{\mathbb{K}}(\Gamma)$ polynomial on $\lambda_{\mathbb{K}}(\Gamma)$?

Open Problem In which situations can we remove the factor 2 in $\mu_{\mathbb{K}}(\Gamma) \leq 2\lambda_{\mathbb{K}}(\Gamma)$?

Or, with some restrictions:

Suppose Γ is **self-dual ($\equiv$ minimally $\mathcal{Q}_2$)** with $\lambda_{\mathbb{K}}(\Gamma) = n$
Is there a finite field $\mathbb{L} \supset \mathbb{K}$ such that $\mu_{\mathbb{L}}(\Gamma) = \lambda_{\mathbb{L}}(\Gamma) = n$?

OUR RESULTS

We find a connection between the **first open problem** and **efficient error-correction in linear codes**

The **second open problem** is proved to be equivalent to an open problem on **Matroid Theory** and we take the first steps to solve it

LINEAR CODES AND LINEAR SECRET SHARING SCHEMES

A **LSSS** can be represented by a $d \times (\lambda + 1)$ matrix M

$$(x_1, \ldots, x_d) \begin{pmatrix} \uparrow & \uparrow & & \uparrow \\ \pi_0 & \pi_1 & \cdots & \pi_n \\ \downarrow & \downarrow & & \downarrow \end{pmatrix} = (k, s_1, \ldots, s_n)$$

where the linear mappings $\pi_i \colon E \to E_i$ define the LSSS

M can be seen as a **generator matrix** of a **linear code** with **dimension** $d = \dim E$ and **length** $\lambda + 1$.

RECONSTRUCTING THE SECRET IN THE PRESENCE OF ERRORS

Let $(k, s_1, \ldots, s_n)$ be a distribution of shares by a **LSSS**.
Suppose that some **shares** have been **corrupted**:
$(c_1, \ldots, c_n) = (s_1 + e_1, \ldots, s_n + e_n)$,
where $A = \{i \in P : e_i \neq 0\} \notin \Gamma$

Can the secret k be reconstructed from $(c_1, \ldots, c_n)$?

Yes, if Γ is $\mathcal{Q}_3$. But, **efficiently**?

Theorem Yes, if the scheme is **strongly multiplicative**

Proof Similar to Pellikaan's generalization of
Berlekamp-Welch decoding algorithm for Reed-Solomon codes

MATROIDS, CODES AND IDEAL SECRET SHARING SCHEMES

An **ideal** $\mathbb{K}$-**LSSS** is represented by a $d \times (n+1)$ matrix M

$$(x_1, \ldots, x_d) \begin{pmatrix} \uparrow & \uparrow & & \uparrow \\ \pi_0 & \pi_1 & \cdots & \pi_n \\ \downarrow & \downarrow & & \downarrow \end{pmatrix} = (k, s_1, \ldots, s_n)$$

M can be seen as a **generator matrix** of a **linear code** with **dimension** $d = \dim E$ and **length** $n+1$.

Besides, M defines a $\mathbb{K}$-**representable matroid** $\mathcal{M}$

All generator matrices of a **code** define the same **matroid**

A **matroid** defines an **access structure**:

$A \in \Gamma \iff \pi_0 \in \langle \pi_i | i \in A \rangle \iff \text{rank}(A \cup \{0\}) = \text{rank}(A)$

DUALITY

The dual code: Let $\mathcal{C}$ be a $[n+1,d]$-linear code
with generator matrix M and **parity check matrix** N ($MN^\top = 0$)
The **dual code** $\mathcal{C}^\perp$ is the $[n+1,n-d+1]$-linear code
with generator matrix N.

The dual matroid: $B \subset Q$ basis of $\mathcal{M}^* \iff Q - B$ basis of $\mathcal{M}$

The dual access structure: $A \in \Gamma^* \iff P - A \notin \Gamma$

TWO EQUIVALENT OPEN PROBLEMS

Self-dual code $\longrightarrow$ SD matroid $\longleftrightarrow$ SD access structure

Open Problem
Let Γ be a **self-dual access structure** with $\lambda_{\mathbb{K}}(\Gamma) = n$
Does there exist a finite field $\mathbb{L} \supset \mathbb{K}$
such that $\mu_{\mathbb{L}}(\Gamma) = \lambda_{\mathbb{L}}(\Gamma) = n$?

Open Problem
Let $\mathcal{M}$ be a $\mathbb{K}$-**representable self-dual matroid**
Do there exist a finite field $\mathbb{L} \supset \mathbb{K}$ and a
self-dual code $\mathcal{C}$ representing $\mathcal{M}$ over $\mathbb{L}$?

The answer is affirmative for: **uniform** matroids $U_{d,2d}$,
self-dual **binary** ($\mathbb{K} = \mathbb{Z}_2$) matroids, $\mathcal{M}_1 \oplus \mathcal{M}_2$

A NEW FAMILY OF SELF-DUALLY REPRESENTABLE MATROIDS

Definition A matroid $\mathcal{M}$ is **bipartite** if there is a partition $Q = X_1 \cup X_2$ such that every permutation $\sigma : Q \to Q$ with $\sigma(X_1) = X_1$ is an automorphism of $\mathcal{M}$.

Theorem All bipartite matroids are representable

Padró & Sáez 1998, Ng & Walker 2001

Theorem Every **self-dual bipartite matroid** is represented by a self-dual code

The **proof** deals with polynomial equations
So, some **Algebraic Geometry** has been used

A NEW FAMILY OF SELF-DUALLY REPRESENTABLE MATROIDS

Therefore, we have found a wide new family of
self-dually representable matroids

Most of them are **indecomposable**

This family is a natural step from **self-dual uniform matroids**

The techniques in the proof may be useful
for future research on that open problem

CONCLUSION

We have studied two open problems about the **multiplicative property** of **linear secret sharing schemes**

We have done that by using some connections to **Code Theory** and **Matroid Theory**

Strong multiplication in LSSS implies **efficient error correction**

The other open problem is proved to be equivalent to a challenging open problem on **Matroid Theory**

Some steps have been taken on its solution