Combinatorial Codes for
Detection of Algebraic Manipulation

Serge Fehr
CWI Amsterdam
The Netherlands
fehr@cwi.nl

Joint work with
Ronald Cramer (CWI/Leiden University)
Carles Padró (UPC Barcelona)
\[ G \ni x \]
$G \ni x$
$\mathcal{G} \ni x \sim \delta \in \mathcal{G}$
\( G \ni x \mapsto x + \delta \ni \delta \in G \)
Let $G$ contain $x$, then $x + \delta \rightarrow x + \delta$. Furthermore, $\delta \in G$. 
Examples

One-time-pad encryption:

- \( c = x \oplus k \) perfectly hides \( x \)
- \( \tilde{c} = c \oplus \delta \) decrypts to \( x \oplus \delta \).

Linear secret-sharing scheme:

- shares of non-qualified players perfectly hide secret \( x \)
- incorrect shares enforce reconstruction of \( \tilde{x} \neq x \), where (due to linearity) adversary knows/controls \( \delta = \tilde{x} - x \): apply reconstruction to the differences of all the shares
Algebraic-Manipulation Detection

Algebraic-manipulation detection (AMD) code:

\[ s \rightarrow [E] \rightarrow x \sim \]
Algebraic-Manipulation Detection

Algebraic-manipulation detection (AMD) code:

\[ s \rightarrow [E] \rightarrow [x] \sim \rightarrow [\tilde{x}] \rightarrow [D] \rightarrow \begin{cases} x \\ \nabla \end{cases} \]
Algebraic-Manipulation Detection

Algebraic-manipulation detection (AMD) code:

\[ s \rightarrow [E] \rightarrow [x] \sim \tilde{x} \rightarrow [D] \rightarrow \begin{cases} x \end{cases} \]

Important: We want this to work **without secret key**!

Note: Only care about **detection** (correction is impossible).
Application

Recall: In a secret sharing scheme

- too few shares $\sim$ no info on the shared secret
- sufficiently many shares $\sim$ secret can be reconstructed,

Whereas in a robust secret sharing scheme fraud in the reconstruction phase is detected.

An AMD code allows to make any linear secret sharing scheme robust:

- Share, and decode the reconstructed value.

Note: Also works for dishonest majority (where VS techniques fail).

Robust secret sharing has applications e.g. secure and private storage and secure message transmission.
Recall: In a secret sharing scheme

- too few shares $\rightarrow$ no info on the shared secret
- sufficiently many shares $\rightarrow$ secret can be reconstructed,
  but: incorrect shares $\rightarrow$ incorrect secret is reconstructed
Recall: In a secret sharing scheme

- too few shares $\rightarrow$ no info on the shared secret
- sufficiently many shares $\rightarrow$ secret can be reconstructed,
  but: incorrect shares $\rightarrow$ incorrect secret is reconstructed

Whereas in a robust secret sharing scheme

- fraud in the reconstruction phase is detected
Recall: In a secret sharing scheme

- too few shares $\leadsto$ no info on the shared secret
- sufficiently many shares $\leadsto$ secret can be reconstructed,
  but: incorrect shares $\leadsto$ incorrect secret is reconstructed

Whereas in a robust secret sharing scheme

- fraud in the reconstruction phase is detected

An AMD code allows to make any linear secret sharing scheme robust:
share $x = E(s)$, and decode the reconstructed value $\tilde{x}$.

Note: Also works for dishonest majority (where VSS techniques fail).

Robust secret sharing has applications to e.g. secure and private storage and secure message transmission.
**Definition** An \((m, n)\)-AMD code is given by

- probabilistic encoding map \(E : S \rightarrow G\)
  (where \(S\) = set of cardinality \(m\) and \(G\) = group of order \(n\))
- deterministic decoding function \(D : G \rightarrow S \cup \{\perp\}\)

such that \(D(E(s)) = s\) with probability 1 for any \(s \in S\).
**Definition** An \((m, n)\)-AMD code is given by

- probabilistic encoding map \(E : S \rightarrow G\) (where \(S\) = set of cardinality \(m\) and \(G\) = group of order \(n\))
- deterministic decoding function \(D : G \rightarrow S \cup \{\perp\}\)

such that \(D(E(s)) = s\) with probability 1 for any \(s \in S\).

**Definition** An AMD code is weakly \(\varepsilon\)-secure if for any \(\delta \in G\) and for random \(s \in S\): \(\text{Prob}[D(E(s) + \delta) \notin \{s, \perp\}] \leq \varepsilon\).

**Definition** An AMD code is strongly \(\varepsilon\)-secure if for any \(\delta \in G\) and for any \(s \in S\): \(\text{Prob}[D(E(s) + \delta) \notin \{s, \perp\}] \leq \varepsilon\).
Example I: Algebraic Construction

Cabello, Padró and Sáez, 2002:

Let $F$ be a finite field of odd order $q$. Then

$$E: F \rightarrow F \times F \quad D: F \times F \rightarrow F \cup \{\perp\}$$

$$s \leftrightarrow (s, s^2) \quad (\bar{s}, \bar{p}) \leftrightarrow \bar{s} \text{ if } \bar{s}^2 = \bar{p}, \text{ else } \perp$$

is a weakly $1/q$-secure $(q, q^2)$-AMD code.
Example 1: Algebraic Construction

Cabello, Padró and Sáez, 2002:

Let $\mathbb{F}$ be a finite field of odd order $q$. Then

$$E : \mathbb{F} \rightarrow \mathbb{F} \times \mathbb{F} \quad D : \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F} \cup \{\bot\}$$

$$s \mapsto (s, s^2) \quad (\tilde{s}, \tilde{p}) \mapsto \tilde{s} \text{ if } \tilde{s}^2 = \tilde{p}, \text{ else } \bot$$

is a weakly $1/q$-secure $(q, q^2)$-AMD code.

Proof. To be accepted, $0 = \tilde{s}^2 - \tilde{p} = (s + \partial s)^2 - (s^2 + \partial p) = 2s\partial s + \partial s^2 - \partial p$

and thus $s = (\partial p - \partial s^2)/2\partial s$, which happens with probability $1/|\mathbb{F}|$. □
Example 1: Algebraic Construction

Cabello, Padró and Sáez, 2002:

Let $\mathbb{F}$ be a finite field of odd order $q$. Then

\[
E : \mathbb{F} \rightarrow \mathbb{F} \times \mathbb{F} \quad D : \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F} \cup \{\bot\}
\]

\[
s \mapsto (s, s^2) \quad (\tilde{s}, \tilde{p}) \mapsto \tilde{s} \text{ if } \tilde{s}^2 = \tilde{p}, \text{ else } \bot
\]

is a weakly $1/q$-secure $(q, q^2)$-AMD code.

**Proof.** To be accepted, $0 = \tilde{s}^2 - \tilde{p} = (s + \partial s)^2 - (s^2 + \partial p) = 2s\partial s + \partial s^2 - \partial p$

and thus $s = (\partial p - \partial s^2)/2\partial s$, which happens with probability $1/|\mathbb{F}|$. \qed

Similarly

\[
E : \mathbb{F} \rightarrow \mathbb{F} \times \mathbb{F} \times \mathbb{F} \quad D : \mathbb{F} \times \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F} \cup \{\bot\}
\]

\[
s \mapsto (s, r, s \cdot r) \quad (\tilde{s}, \tilde{r}, \tilde{p}) \mapsto \tilde{s} \text{ if } \tilde{s} \cdot \tilde{r} = \tilde{p}, \text{ else } \bot
\]

is a strongly $1/q$-secure $(q, q^3)$-AMD code.
Example II: Combinatorial Construction

**Definition** \( V \subseteq G \) is a \( t \)-difference-set, if for every \( 0 \neq \delta \in G \):
\[
\delta = v - w \text{ for exactly } t \text{ pairs } v, w \in V.
\]
Example II: Combinatorial Construction

**Definition** \( V \subset G \) is a \( t \)-difference-set, if for every \( 0 \neq \delta \in G \):
\[
\delta = v - w \text{ for exactly } t \text{ pairs } v, w \in V.
\]

**Theorem** Let \( q \) and \( p = q^2 + q + 1 \) both be primes.
Then, there exists a \( 1 \)-difference-set \( V \subset \mathbb{Z}_p \) of size \( q + 1 \).
Definition \( V \subset G \) is a \( t \)-difference-set, if for every \( 0 \neq \delta \in G \):
\[
\delta = v - w \text{ for exactly } t \text{ pairs } v, w \in V.
\]

Theorem Let \( q \) and \( p = q^2 + q + 1 \) both be primes. Then, there exists a \( 1 \)-difference-set \( V \subset \mathbb{Z}_p \) of size \( q + 1 \).

Ogata and Kurosawa, 1996:
Gives rise to a weakly \( 1/(q + 1) \)-secure \( (q + 1, p) \)-AMD code:

\[
E : V \to G \quad D : G \to V \cup \{\bot\}
\]
\[
s \mapsto s \quad \tilde{s} \mapsto \tilde{s} \text{ if } \tilde{s} \in V, \text{ else } \bot
\]
Example II: Combinatorial Construction

**Definition** \( V \subset G \) is a \( t \)-difference-set, if for every \( 0 \neq \delta \in G \):
\[
\delta = v - w \text{ for exactly } t \text{ pairs } v, w \in V.
\]

**Theorem** Let \( q \) and \( p = q^2 + q + 1 \) both be primes. Then, there exists a \( 1 \)-difference-set \( V \subset \mathbb{Z}_p \) of size \( q + 1 \).

Ogata and Kurosawa, 1996:
Gives rise to a weakly \( 1/(q + 1) \)-secure \((q + 1, p)\)-AMD code:

\[
E : V \rightarrow G \quad D : G \rightarrow V \cup \{\bot\}
\]
\[
s \mapsto s \quad \tilde{s} \mapsto \tilde{s} \text{ if } \tilde{s} \in V, \text{ else } \bot
\]

**Proof.** For any \( \delta \in G \), there is only one \( s \in V \) with \( s + \delta \in V \). \( \square \)
Road Map

- Introduction, definition, examples etc.
- The combinatorics of AMD codes
- Measuring the quality of AMD codes, and lower bounds
- A simple construction based on authentication codes
- A construction based on error correcting codes
- A near-optimal polynomial-based construction
Recall: $V \subset G$ is a *t*-difference-set, if $\forall 0 \neq \delta \in G$:
\[
\delta = v - w \text{ for exactly } t \text{ pairs } v, w \in V.
\]

**Definition** $V \subset G$ is a *t*-bounded-difference-set, if $\forall 0 \neq \delta \in G$:
\[
\delta = v - w \text{ for at most } t \text{ pairs } v, w \in V.
\]
Recall: $V \subseteq G$ is a $t$-difference-set, if $\forall 0 \neq \delta \in G$:
\[ \delta = v - w \text{ for exactly } t \text{ pairs } v, w \in V. \]

**Definition** $V \subseteq G$ is a $t$-bounded-difference-set, if $\forall 0 \neq \delta \in G$:
\[ \delta = v - w \text{ for at most } t \text{ pairs } v, w \in V. \]

**Theorem** If $V \subseteq G$ is a $t$-bounded-difference-set, then
\[ E : V \ni s \mapsto s \in G \]
is a (deterministic) weakly $t/|V|$-secure AMD code.
Recall: $V \subset G$ is a $t$-difference-set, if $\forall 0 \neq \delta \in G$:
$\delta = v - w$ for exactly $t$ pairs $v, w \in V$.

**Definition** $V \subset G$ is a $t$-bounded-difference-set, if $\forall 0 \neq \delta \in G$:
$\delta = v - w$ for at most $t$ pairs $v, w \in V$.

**Theorem** If $V \subset G$ is a $t$-bounded-difference-set, then

$$E : V \ni s \mapsto s \in G$$

is a (deterministic) weakly $t/|V|$-secure AMD code.

And, if $E : S \rightarrow G$ is a deterministic weakly $\varepsilon$-secure AMD code, then $V = E(S) \subset G$ is a $\varepsilon|V|$-bounded-difference-set.
**Definition** \( V_1, \ldots, V_m \subset G \) is a \((t_1 \ldots t_m)\)-differential-structure, if

- \( V_i \)'s are non-empty and disjoint, and
- \( \forall i \in \{1, \ldots, m\}, 0 \neq \delta \in G: |(V_i + \delta) \cap \bigcup_{j \neq i} V_j| \leq t_i. \)
**Combinatorics of Strongly Secure Codes**

**Definition** \( V_1, \ldots, V_m \subset G \) is a \((t_1 \ldots t_m)\)-differential-structure, if

- \( V_i \)'s are non-empty and disjoint, and
- \( \forall i \in \{1, \ldots, m\}, 0 \neq \delta \in G: \left| (V_i + \delta) \cap \bigcup_{j \neq i} V_j \right| \leq t_i \).

**Theorem** If \( V_1, \ldots, V_m \subset G \) is a \((t_1 \ldots t_m)\)-differential-structure, then

\[
E : \{1, \ldots, m\} \ni s \xrightarrow{\text{by} V_s} \hat{s} \in G
\]

is a strongly \( \varepsilon \)-secure AMD code with \( \varepsilon = \max_i t_i / |V_i| \).
**Combinatorics of Strongly Secure Codes**

**Definition** $V_1, \ldots, V_m \subset G$ is a $(t_1 \ldots t_m)$-differential-structure, if

- $V_i$'s are non-empty and disjoint, and
- $\forall i \in \{1, \ldots, m\}, 0 \neq \delta \in G: |(V_i + \delta) \cap \bigcup_{j \neq i} V_j| \leq t_i$.

**Theorem** If $V_1, \ldots, V_m \subset G$ is a $(t_1 \ldots t_m)$-differential-structure, then

$$E: \{1, \ldots, m\} \ni s \xrightarrow{V_i} \hat{s} \in G$$

is a strongly $\varepsilon$-secure AMD code with $\varepsilon = \max_i t_i / |V_i|$.

And, any strongly-secure AMD code with uniform selection implies a corresponding differential-structure.

**Definition** An AMD code is with uniform selection if for any $s \in S$, the encoding $E(s)$ is random over its possible values.
Road Map

- Introduction, definition, examples etc.
- The combinatorics of AMD codes
  - Measuring the quality of AMD codes, and lower bounds
  - A simple construction based on authentication codes
  - A construction based on error correcting codes
  - A near-optimal polynomial-based construction
The Tag Size

Let $E : S \rightarrow G$ be $(m,n)$-AMD code. Recall: $m = |S|$, $n = |G|$.

Clearly, $n \geq m$. We want $n$ to be as close to $m$ as possible.

Could measure this by the rate $\rho := \log(m)/\log(n)$.

More handy:

**Definition** The tag size is $\omega := \log(n) - \log(m)$.

(The number of bits added to the source $s$.)
Lower Bounds

**Theorem**  The tag size of a weakly/strongly $2^{-\kappa}$-secure $(m,n)$-AMD code is bounded by

\[ \omega \geq \kappa - 2/m \quad \text{resp.} \quad \omega \geq 2\kappa - 2/m \]
Lower Bounds

**Theorem** The tag size of a weakly/strongly $2^{-\kappa}$-secure $(m,n)$-AMD code is bounded by

$$\omega \geq \kappa - 2/m \quad \text{resp.} \quad \omega \geq 2\kappa - 2/m$$

**Proof.** Choose $\delta \in \mathcal{G}$ at random. For a random $s \in S$:

$$2^{-\kappa} \geq \Pr\left[E(s) + \delta \in \bigcup_{s' \neq s} D^{-1}(s')\right] = \frac{| \bigcup_{s' \neq s} D^{-1}(s') |}{n} \geq \frac{m - 1}{n}.$$
**Lower Bounds**

**Theorem** The tag size of a weakly/strongly $2^{-\kappa}$-secure $(m, n)$-AMD code is bounded by

$$\omega \geq \kappa - 2/m \quad \text{resp.} \quad \omega \geq 2\kappa - 2/m$$

**Proof.** Choose $\delta \in G$ at random. For a random $s \in S$:

$$2^{-\kappa} \geq \text{Prob}[E(s) + \delta \in \bigcup_{s' \neq s} D^{-1}(s')] = \left| \bigcup_{s' \neq s} D^{-1}(s') \right| \geq \frac{m - 1}{n}.$$ 

And thus

$$\omega = \log(n) - \log(m) = \log \frac{n}{m} \frac{m-1}{m} = \log \frac{n}{m} + \log \left(1 - \frac{1}{m}\right) \geq \kappa - \frac{2}{m}.$$ 

Similarly for strongly secure AMD code. \qed
Analysing the Examples

Cabello-Padró-Sáez constructions:

The weakly/strongly $1/q$-secure AMD codes

$$E : s \mapsto (s, s^2) \quad \text{resp.} \quad E : s \mapsto (s, r, s \cdot r)$$

have tag size $\log(q)$ resp. $2\log(q)$. 
Analysing the Examples

Cabello-Padró-Sáez constructions:

The weakly/strongly $1/q$-secure AMD codes

$$E : s \mapsto (s, s^2) \quad \text{resp.} \quad E : s \mapsto^r (s, r, s \cdot r)$$

have tag size $\log(q)$ resp. $2\log(q)$.

Ogata-Kurosawa construction:

The weakly $1/(q + 1)$-secure AMD code

$$E : V \ni s \mapsto s \in G = \mathbb{Z}_p$$

where $|V| = q + 1$ with $p = q^2 + q + 1$, has tag size

$$\log(p) - \log(q + 1) = \log(q^2 + q + 1) - \log(q + 1) = \log(q + \frac{1}{q + 1}).$$
Scalability

All three constructions are (essentially) optimal...
Scalability

All three constructions are (essentially) optimal...

... but they are all not scalable: $|S| = 1/\varepsilon = 1/q$.

May want to choose $|S| = 2^\ell$ and $\varepsilon = 2^{-\kappa}$ independently.

Example: $\kappa = 128$ and $\ell = 1$ MB. Then lower bound dictates $\varpi \geq 128$ for weak security whereas example codes have $\varpi = 8 \cdot 2^{20} = 8388608$. 
Scalability

All three constructions are (essentially) optimal...

... but they are all not scalable: \(|S| = 1/\epsilon = 1/q\).

May want to choose \(|S| = 2^\ell\) and \(\epsilon = 2^{-\kappa}\) independently.

Example: \(\kappa = 128\) and \(\ell = 1\) MB. Then lower bound dictates \(\varpi \geq 128\) for weak security whereas example codes have \(\varpi = 8 \cdot 2^{20} = 8388608\).

Definition  The effective tag size of a family of weakly/strongly secure AMD codes, with respect to \(\kappa\) and \(\ell\), is

\[
\varpi^*(\kappa, \ell) := \min\{n\} - \ell
\]

where the min is over all weakly/strongly \(\epsilon\)-secure \((m, n)\)-AMD codes with \(\epsilon \leq 2^{-\kappa}\) and \(m \geq 2^\ell\).

Known AMD codes are optimal (wrt. to effective tag size) only for \(\ell \approx \kappa\).
Road Map

- Introduction, definition, examples etc.
- The combinatorics of AMD codes
- Measuring the quality of AMD codes, and lower bounds
  - A simple construction based on authentication codes
  - A construction based on error correcting codes
  - A near-optimal polynomial-based construction
**Theorem** Let

- $A : \mathcal{K} \times S \to T$ an A-code with substitution probability $p_S$
- $E' : \mathcal{K} \to \mathcal{G}'$ be a weakly $\varepsilon'$-secure AMD code.

Then

$$E : S \longrightarrow S \times \mathcal{G}' \times T, \ s \xrightarrow{K} (s, E'(k), A(k, s))$$

is a strongly $\varepsilon$-secure AMD-code with $\varepsilon = \varepsilon' + p_S$. 
A-Code Based Construction

**Theorem** Let

- $A : \mathcal{K} \times \mathcal{S} \rightarrow \mathcal{T}$ an A-code with substitution probability $p_S$
- $E' : \mathcal{K} \rightarrow \mathcal{G}'$ be a **weakly** $\varepsilon'$-secure AMD code.

Then

$$E : \mathcal{S} \rightarrow \mathcal{S} \times \mathcal{G}' \times \mathcal{T}, \quad s \overset{k_S}{\mapsto} (s, E'(k), A(k, s))$$

is a strongly $\varepsilon$-secure AMD-code with $\varepsilon = \varepsilon' + p_S$.

Using “good” A-codes:

strongly secure AMD-codes with effective tag size $\overline{\omega}^*(\kappa, \ell) \approx 4\kappa$ \forall $\kappa, \ell$.

**Proposition** For any such A-code based AMD code: $\overline{\omega}^*(\kappa, \ell) \succeq 4\kappa$.

Recall: Lower bound would allow $\overline{\omega}^*(\kappa, \ell) \approx 2\kappa$. 

---
Road Map

- Introduction, definition, examples etc.
- The combinatorics of AMD codes
- Measuring the quality of AMD codes, and lower bounds
- A simple construction based on authentication codes
- A construction based on error correcting codes
- A near-optimal polynomial-based construction
Based on Error Correcting Codes

Let \( C \subset \mathbb{F}^n \) be a (not necessarily linear) error correcting code, and \( C : \mathbb{F}^k \rightarrow C \) the encoding function.

Then
\[
E : \mathbb{F}^k \rightarrow \mathbb{F}^k \times \mathbb{Z}_n \times \mathbb{F}, \ s \xmapsto{\mathbb{Z}_n} \left( s, x, [C(s)]_x \right)
\]
is a strongly \( \varepsilon \)-secure AMD code with \( \varepsilon \) as follows:

- Extend \( C \) to multiset \( \text{cl}(C) = \{(c_t, c_{t+1}, \ldots, c_{t-1}) \mid c \in C, t \in \mathbb{Z}_n\} \).
- If \( \text{cl}(C) \) contains doubles, then \( \varepsilon = 1 \) (i.e., no security).
- Else, let \( M \) be the max number of occurrences of an entry within \( c - c' \), quantified over \( c \neq c' \in \text{cl}(C) \).
  Then \( \varepsilon = M/n \).
Road Map

- Introduction, definition, examples etc.
- The combinatorics of AMD codes
- Measuring the quality of AMD codes, and lower bounds
- A simple construction based on authentication codes
- A construction based on error correcting codes
- A near-optimal polynomial-based construction
Consider the code

\[ \mathcal{C} = \{c_{f(x)} \mid f(X) \in \mathbb{F}[X] \text{ with } \deg f(X) \leq k \} \]

where

\[ c_{f(x)} = (f(x))_{x \in \mathbb{F}} \]

Obviously

\[ \text{rot}_t(c_{f(x)}) = c_{f(x+t)} \in \mathcal{C} \]

and thus gives \textbf{no (good) AMD code}. 
A Near-Optimal Poly-Based Construction

Let $\mathbb{F}$ be finite field of size $q$, and let $d < q - 2$. Use polys of the form

$$f_s(X) = 0 + s_1X + \cdots + s_dX^d + 0 \cdot X^{d+1} + + X^{d+2} \in \mathbb{F}[X].$$

**Theorem** The resulting AMD code

$$E : \mathbb{F}^d \to \mathbb{F}^d \times \mathbb{F} \times \mathbb{F}, \ s \mapsto (s, x, f_s(x) = s_1 x + \cdots + s_d x^d + x^{d+2})$$

is strongly $\varepsilon$-secure with $\varepsilon = (d + 1)/q$.

**Proof.**
A Near-Optimal Poly-Based Construction

Let $\mathbb{F}$ be finite field of size $q$, and let $d < q - 2$. Use polys of the form

$$f_s(X) = 0 + s_1 X + \cdots + s_d X^d + 0 \cdot X^{d+1} + X^{d+2} \in \mathbb{F}[X].$$

**Theorem** The resulting AMD code

$$E : \mathbb{F}^d \to \mathbb{F} \times \mathbb{F} \times \mathbb{F}, \; s \xmapsto{\epsilon^{-}} (s, x, f_s(x) = s_1 x + \cdots + s_d x^d + x^{d+2})$$

is strongly $\epsilon$-secure with $\epsilon = (d + 1)/q$.

**Proof.** Attacker may transform $(s, x, f_s(x))$ to $(s', x + ax, f_s(x) + ax)$.
Let $\mathbb{F}$ be finite field of size $q$, and let $d < q - 2$. Use polys of the form
\[
f_s(X) = 0 + s_1 X + \cdots + s_d X^d + 0 \cdot X^{d+1} + X^{d+2} \in \mathbb{F}[X].
\]

**Theorem** The resulting AMD code
\[
E : \mathbb{F}^d \rightarrow \mathbb{F}^d \times \mathbb{F} \times \mathbb{F}, \quad s \xrightarrow{\mathcal{E}} (s, x, f_s(x) = s_1 x + \cdots + s_d x^d + x^{d+2})
\]
is strongly $\varepsilon$-secure with $\varepsilon = (d + 1)/q$.

**Proof.**
- Attacker may transform $(s, x, f_s(x))$ to $(s', x + \alpha x, f_s(x) + \alpha x)$.
- Define $g(X) := f_{s'}(X + \alpha x) - f_s(X) - \alpha e$. 

---

**Corollary** The effectivetagsize of this AMD code family ranges within $\mathcal{O}(\mathcal{E})$ on the LHS (i.e. near-optimality) if $\varepsilon = (d + 1)/q$. 

---

**Centrum voor Wiskunde en Informatica**

Combinatorial Codes for Detection of Algebraic Manipulation – p.23/25
Let $\mathbb{F}$ be finite field of size $q$, and let $d < q - 2$. Use polys of the form

$$f_s(X) = 0 + s_1X + \cdots + s_dX^d + 0 \cdot X^{d+1} + + X^{d+2} \in \mathbb{F}[X].$$

**Theorem** The resulting AMD code

$$E: \mathbb{F}^d \to \mathbb{F}^d \times \mathbb{F} \times \mathbb{F}, \ s \xmapsto{\sigma} (s, x, f_s(x) = s_1x + \cdots + s_dx^d + x^{d+2})$$

is strongly $\varepsilon$-secure with $\varepsilon = (d + 1)/q$.

**Proof.** • Attacker may transform $(s, x, f_s(x))$ to $(s', x + \alpha x, f_s(x) + \alpha e)$.

• Define $g(X) := f_{s'}(X + \alpha x) - f_s(X) - \alpha e$.

• Gets decoded to $s' \neq s$ if $f_{s'}(x + \alpha x) = f_s(x) + \alpha e$, i.e., if $g(x) = 0$. 

**Corollary** The effectivetagsize of this AMD codefamilyranges within

\[\text{with } \varepsilon \text{ on the LHS (i.e. near-optimality) if } \varepsilon \text{ for a} \]
Let $\mathbb{F}$ be finite field of size $q$, and let $d < q - 2$. Use polys of the form

$$f_s(X) = 0 + s_1X + \cdots + s_dX^d + 0 \cdot X^{d+1} + X^{d+2} \in \mathbb{F}[X].$$

**Theorem** The resulting AMD code

$$E : \mathbb{F}^d \rightarrow \mathbb{F}^d \times \mathbb{F} \times \mathbb{F}, \quad s \xrightarrow{x \in \mathbb{F}} (s, x, f_s(x) = s_1x + \cdots + s_dx^d + x^{d+2})$$

is strongly $\varepsilon$-secure with $\varepsilon = (d + 1)/q$.

**Proof.**

- Attacker may transform $(s, x, f_s(x))$ to $(s', x + \alpha x, f_s(x) + \alpha)$.
- Define $g(X) := f_{s'}(X + \alpha x) - f_s(X) - \alpha$.
- Gets decoded to $s' \neq s$ if $f_{s'}(x + \alpha x) = f_s(x) + \alpha$, i.e., if $g(x) = 0$.
- Easy to see: $1 \leq \deg g(X) \leq d$. Thus, $\varepsilon \leq (d + 1)/q$.

□
A Near-Optimal Poly-Based Construction

Let $\mathbb{F}$ be finite field of size $q$, and let $d < q - 2$. Use polys of the form

$$f_s(X) = 0 + s_1 X + \cdots + s_d X^d + 0 \cdot X^{d+1} + + X^{d+2} \in \mathbb{F}[X].$$

**Theorem** The resulting AMD code

$$E : \mathbb{F}^d \rightarrow \mathbb{F}^d \times \mathbb{F} \times \mathbb{F}, \quad s \xrightarrow{x \mapsto} (s, x, f_s(x) = s_1 x + \cdots + s_d x^d + x^{d+2})$$

is strongly $\varepsilon$-secure with $\varepsilon = (d + 1)/q$.

**Corollary** The effective tag size of this AMD code family ranges within

$$2\kappa + 2 \log(\ell) \lesssim \omega^*(\kappa, \ell) \leq 3\kappa + 3 \log(\ell)$$

with $\approx$ on the LHS (i.e. near-optimality) if $\ell \approx d(\kappa + \log(d))$ for a $d \in \mathbb{N}$. 
Summary and Open Problem

- Notion of algebraic-manipulation and of AMD codes
- Combinatorial understanding of AMD codes
- Lower bounds
- Constructions: - based on A-codes
  - based on error-correcting codes
  - based on polynomials

Open problem:

Even better constructions
(based on algebraic curves, or on results from combinatorics?)
“Thank you for your attention!!!”