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)

Algebraic Manipulation

$\mathcal{G} \ni x \quad \rightsquigarrow$

Algebraic Manipulation

$\mathcal{G} \ni x \quad \rightsquigarrow$

???

Algebraic Manipulation

$\mathcal{G} \ni x \quad \rightsquigarrow$

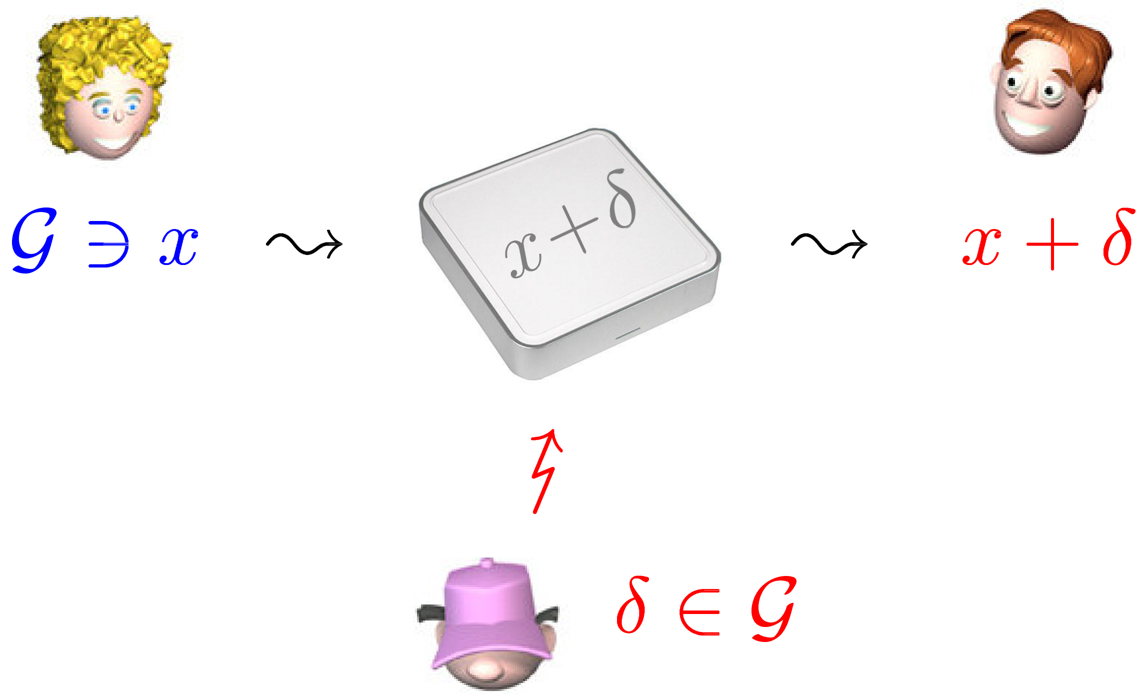
 $\delta \in \mathcal{G}$

Algebraic Manipulation

$\mathcal{G} \ni x \quad \rightsquigarrow$

$\delta \in \mathcal{G}$

Algebraic Manipulation



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

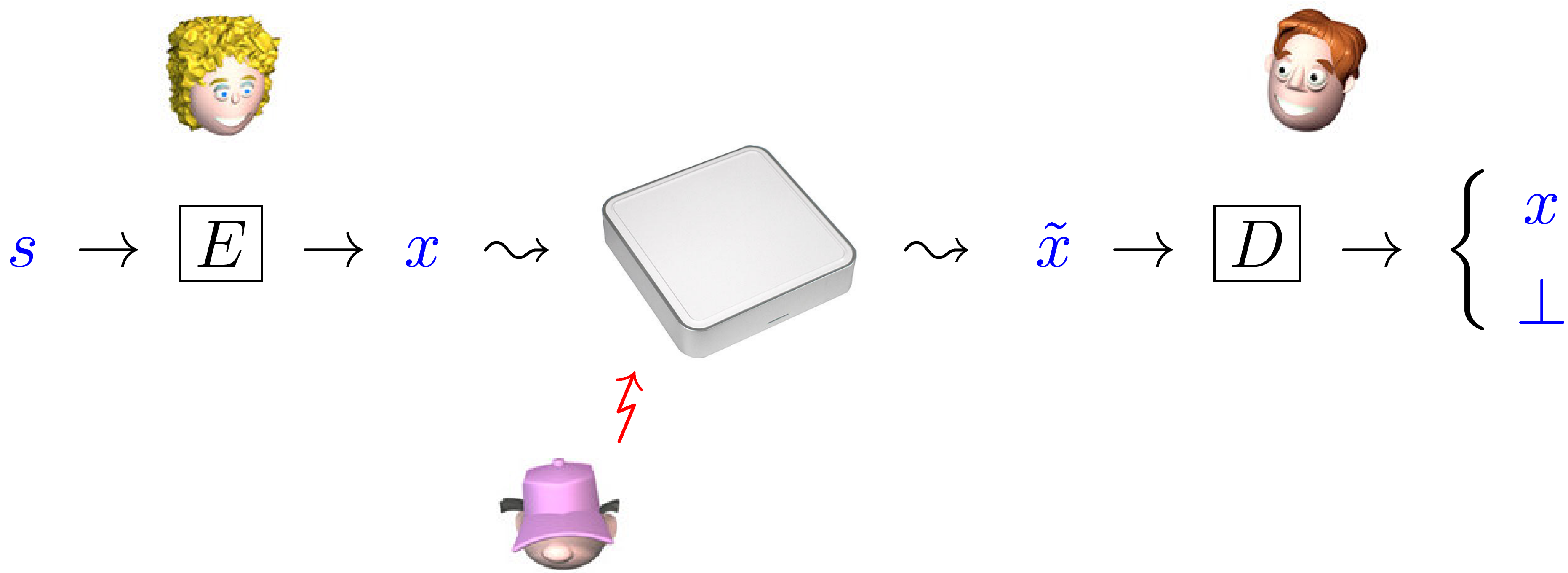
Algebraic-Manipulation Detection

Algebraic-manipulation detection (AMD) code:

$$s \rightarrow \boxed{E} \rightarrow x \rightsquigarrow$$

Algebraic-Manipulation Detection

Algebraic-manipulation detection (AMD) code:



Algebraic-Manipulation Detection

Algebraic-manipulation detection (AMD) code:

$$s \to \boxed{E} \to x \rightsquigarrow$$

$$\rightsquigarrow \tilde{x} \to \boxed{D} \to \begin{cases} x \\ \perp \end{cases}$$

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

Application

Recall: In a secret sharing scheme

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

Application

Recall: In a secret sharing scheme

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

Whereas in a robust secret sharing scheme

- fraud in the reconstruction phase is detected

Application

Recall: In a secret sharing scheme

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

AMD Codes - Formal Definition

Definition An (m, n)-*AMD code* is given by

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

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

AMD Codes - Formal Definition

Definition An (m, n)-*AMD code* is given by

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

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

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

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

Example I: Algebraic Construction

Cabello, Padró and Sáez, 2002:

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

$$\begin{array}{rccc} E: & \mathbb{F} & \to & \mathbb{F}\times\mathbb{F} \\ & s & \mapsto & (s, s^2) \end{array} \qquad \begin{array}{rccc} D: & \mathbb{F}\times\mathbb{F} & \to & \mathbb{F}\cup\{\perp\} \\ & (\tilde{s}, \tilde{p}) & \mapsto & \tilde{s} \text{ if } \tilde{s}^2 = \tilde{p}, \text{ else } \perp \end{array}$$

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

Example I: Algebraic Construction

Cabello, Padró and Sáez, 2002:

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

$$E: \quad \mathbb{F} \to \mathbb{F} \times \mathbb{F} \qquad\qquad D: \quad \mathbb{F} \times \mathbb{F} \to \mathbb{F} \cup \{\perp\}$$
$$\qquad s \mapsto (s, s^2) \qquad\qquad\qquad (\tilde{s}, \tilde{p}) \mapsto \tilde{s} \text{ if } \tilde{s}^2 = \tilde{p}, \text{ else } \perp$$

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 $1/|\mathbb{F}|$. $\square$

Example I: Algebraic Construction

Cabello, Padró and Sáez, 2002:

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

$$\begin{array}{rccc} E: & \mathbb{F} & \to & \mathbb{F} \times \mathbb{F} \\ & s & \mapsto & (s, s^2) \end{array} \qquad \begin{array}{rccl} D: & \mathbb{F} \times \mathbb{F} & \to & \mathbb{F} \cup \{\perp\} \\ & (\tilde{s}, \tilde{p}) & \mapsto & \tilde{s} \text{ if } \tilde{s}^2 = \tilde{p}, \text{ else } \perp \end{array}$$

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 $1/|\mathbb{F}|$. $\square$

Similarly

$$\begin{array}{rccc} E: & \mathbb{F} & \longrightarrow & \mathbb{F} \times \mathbb{F} \times \mathbb{F} \\ & s & \xmapsto{r \in \mathbb{F}} & (s, r, s \cdot r) \end{array} \qquad \begin{array}{rccl} D: & \mathbb{F} \times \mathbb{F} \times \mathbb{F} & \to & \mathbb{F} \cup \{\perp\} \\ & (\tilde{s}, \tilde{r}, \tilde{p}) & \mapsto & \tilde{s} \text{ if } \tilde{s} \cdot \tilde{r} = \tilde{p}, \text{ else } \perp \end{array}$$

is a strongly $1/q$-secure (q, q^3)-AMD code.

Example II: Combinatorial Construction

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

Example II: Combinatorial Construction

Definition $V \subset \mathcal{G}$ is a *t-difference-set*, if for every $0 \neq \delta \in \mathcal{G}$: $\delta = v - w$ for exactly t 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 $q + 1$.

Example II: Combinatorial Construction

Definition $V \subset \mathcal{G}$ is a *t-difference-set*, if for every $0 \neq \delta \in \mathcal{G}$: $\delta = v - w$ for exactly t 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:

$$\begin{array}{rrcl} E: & V & \to & \mathcal{G} \\ & s & \mapsto & s \end{array} \qquad \begin{array}{rrcl} D: & \mathcal{G} & \to & V \cup \{\perp\} \\ & \tilde{s} & \mapsto & \tilde{s} \text{ if } \tilde{s} \in V, \text{ else } \perp \end{array}$$

Example II: Combinatorial Construction

Definition $V \subset \mathcal{G}$ is a *t-difference-set*, if for every $0 \neq \delta \in \mathcal{G}$:
$\delta = v - w$ for exactly t 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:

$$\begin{array}{rccc} E: & V & \to & \mathcal{G} \\ & s & \mapsto & s \end{array} \qquad \begin{array}{rccc} D: & \mathcal{G} & \to & V \cup \{\perp\} \\ & \tilde{s} & \mapsto & \tilde{s} \text{ if } \tilde{s} \in V, \text{ else } \perp \end{array}$$

Proof. For any $\delta \in \mathcal{G}$, 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

Combinatorics of Weakly Secure Codes

Recall: $V \subset \mathcal{G}$ is a *t-difference-set*, if $\forall\, 0 \neq \delta \in \mathcal{G}$:
$\delta = v - w$ for **exactly** t pairs $v, w \in V$.

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

Combinatorics of Weakly Secure Codes

Recall: $V \subset \mathcal{G}$ is a *t-difference-set*, if $\forall\, 0 \neq \delta \in \mathcal{G}$:
$\delta = v - w$ for **exactly** t pairs $v, w \in V$.

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

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

$$E : V \ni s \mapsto s \in \mathcal{G}$$

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

Combinatorics of Weakly Secure Codes

Recall: $V \subset \mathcal{G}$ is a *t-difference-set*, if $\forall\, 0 \neq \delta \in \mathcal{G}$: $\delta = v - w$ for **exactly** t pairs $v, w \in V$.

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

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

$$E : V \ni s \mapsto s \in \mathcal{G}$$

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

And, if $E : \mathcal{S} \to \mathcal{G}$ is a **deterministic** weakly ε-secure AMD code, then $V = E(\mathcal{S}) \subset \mathcal{G}$ is a $\varepsilon|V|$-bounded-difference-set.

Combinatorics of Strongly Secure Codes

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

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

Combinatorics of Strongly Secure Codes

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

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

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

$$E : \{1, \ldots, m\} \ni s \stackrel{\hat{s} \leftarrow V_s}{\longmapsto} \hat{s} \in \mathcal{G}$$

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

Combinatorics of Strongly Secure Codes

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

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

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

$$E : \{1, \ldots, m\} \ni s \stackrel{\hat{s} \leftarrow V_s}{\longmapsto} \hat{s} \in \mathcal{G}$$

is a strongly ε-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 $s \in \mathcal{S}$, 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 $E : \mathcal{S} \to \mathcal{G}$ be (m, n)-AMD code. Recall: $m = |\mathcal{S}|$, $n = |\mathcal{G}|$.
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 $\varpi := \log(n) - \log(m)$.
(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

$$\varpi \geq \kappa - 2/m \qquad \text{resp.} \qquad \varpi \geq 2\kappa - 2/m$$

Lower Bounds

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

$$\varpi \geq \kappa - 2/m \qquad \text{resp.} \qquad \varpi \geq 2\kappa - 2/m$$

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

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

Lower Bounds

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

$$\varpi \geq \kappa - 2/m \qquad \text{resp.} \qquad \varpi \geq 2\kappa - 2/m$$

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

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

And thus

$$\varpi = \log(n) - \log(m) = \log \tfrac{n}{m-1}\tfrac{m-1}{m} = \log \underbrace{\tfrac{n}{m-1}}_{\geq 2^{\kappa}} + \log(1 - \tfrac{1}{m}) \geq \kappa - \tfrac{2}{m} .$$

Similarly for strongly secure AMD code. $\square$

Analysing the Examples

Cabello-Padró-Sáez constructions:

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

$$E: \quad s \quad \mapsto \quad (s, s^2) \qquad \text{resp.} \qquad E: \quad s \quad \xmapsto{r \in \mathbb{F}} \quad (s, r, s \cdot r)$$

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

Analysing the Examples

Cabello-Padró-Sáez constructions:

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

$$E: \quad s \quad \mapsto \quad (s, s^2) \qquad \text{resp.} \qquad E: \quad s \quad \xmapsto{r \in \mathbb{F}} \quad (s, r, s \cdot r)$$

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

Ogata-Kurosawa construction:

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

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

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

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

Scalability

All three constructions are (essentially) optimal...

Scalability

All three constructions are (essentially) optimal...

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

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

Example: $\kappa = 128$ and $\ell = 1\,\mathrm{MB}$. Then lower bound dictates $\varpi \geq 128$ for weak security whereas example codes have $\varpi = 8 \cdot 2^{20} = 8\,388\,608$.

Scalability

All three constructions are (essentially) optimal...

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

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

Example: $\kappa = 128$ and $\ell = 1\,\mathrm{MB}$. Then lower bound dictates $\varpi \geq 128$ for weak security whereas example codes have $\varpi = 8 \cdot 2^{20} = 8\,388\,608$.

Definition The *effective tag size* of a family of weakly/strongly secure AMD codes, with respect to κ and ℓ, is

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

where the min is over all weakly/strongly ε-secure (m, n)-AMD codes with $\varepsilon \leq 2^{-\kappa}$ 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

A-Code Based Construction

Theorem Let

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

Then

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

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

A-Code Based Construction

Theorem Let

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

Then

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

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

Using "good" A-codes:
strongly secure AMD-codes with effective tag size $\varpi^*(\kappa,\ell) \approx 4\kappa \;\; \forall \, \kappa, \ell$.

Proposition For any such A-code based AMD code: $\varpi^*(\kappa,\ell) \gtrsim 4\kappa$.

Recall: Lower bound would allow $\varpi^*(\kappa,\ell) \approx 2\kappa$.

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

Then

$$E : \mathbb{F}^k \to \mathbb{F}^k \times \mathbb{Z}_n \times \mathbb{F}, \ \mathbf{s} \xmapsto{x \leftarrow \mathbb{Z}_n} (\mathbf{s}, x, [\mathbf{C}(\mathbf{s})]_x)$$

is a strongly ε-secure AMD code with ε as follows:

- Extend $\mathcal{C}$ to multiset $\mathrm{cl}(\mathcal{C}) = \{(c_t, c_{t+1}, \ldots, c_{t-1}) \,|\, \mathbf{c} \in \mathcal{C}, t \in \mathbb{Z}_n\}$.
- If $\mathrm{cl}(\mathcal{C})$ contains doubles, then $\varepsilon = 1$ (i.e., no security).
- Else, let M be the max number of occurences of an entry within $\mathbf{c} - \mathbf{c}'$, quantified over $\mathbf{c} \neq \mathbf{c}' \in \mathrm{cl}(\mathcal{C})$.
  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

A Poly-Based Construction - First Try

Consider the code

$$\mathcal{C} = \{\mathbf{c}_{f(X)} \mid f(X) \in \mathbb{F}[X] \text{ with } \deg f(X) \leq k\}$$

where

$$\mathbf{c}_{f(X)} = \big(f(x)\big)_{x \in \mathbb{F}}$$

Obviously

$$\mathrm{rot}_t\big(c_{f(X)}\big) = c_{f(X+t)} \in \mathcal{C}$$

and thus gives **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

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

Theorem The resulting AMD code

$$E:\mathbb{F}^d \to \mathbb{F}^d \times \mathbb{F} \times \mathbb{F},\;\; \mathbf{s} \xmapsto{x \in \mathbb{F}} \big(\mathbf{s}, x, f_{\mathbf{s}}(x) = s_1x+\cdots+s_dx^d+x^{d+2}\big)$$

is strongly ε-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

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

Theorem The resulting AMD code

$$E : \mathbb{F}^d \to \mathbb{F}^d \times \mathbb{F} \times \mathbb{F}, \ \mathbf{s} \xmapsto{x \leftarrow \mathbb{F}} \big(\mathbf{s}, x, f_{\mathbf{s}}(x) = s_1 x + \cdots + s_d x^d + x^{d+2}\big)$$

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

Proof. • Attacker may transform $(\mathbf{s}, x, f_{\mathbf{s}}(x))$ to $(\mathbf{s}', x + \partial x, f_{\mathbf{s}}(x) + \partial e)$.

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

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

Theorem The resulting AMD code

$$E : \mathbb{F}^d \to \mathbb{F}^d \times \mathbb{F} \times \mathbb{F},\;\; \mathbf{s} \xmapsto{x \leftarrow \mathbb{F}} \big(\mathbf{s}, x, f_{\mathbf{s}}(x) = s_1 x + \cdots + s_d x^d + x^{d+2}\big)$$

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

Proof. • Attacker may transform $\big(\mathbf{s}, x, f_{\mathbf{s}}(x)\big)$ to $\big(\mathbf{s}', x + \partial x, f_{\mathbf{s}}(x) + \partial e\big)$.

- Define $g(X) := f_{\mathbf{s}'}(X + \partial x) - f_{\mathbf{s}}(X) - \partial e$.

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

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

Theorem The resulting AMD code

$$E : \mathbb{F}^d \to \mathbb{F}^d \times \mathbb{F} \times \mathbb{F}, \;\; \mathbf{s} \xmapsto{x \leftarrow \mathbb{F}} \big(\mathbf{s}, x, f_{\mathbf{s}}(x) = s_1 x + \cdots + s_d x^d + x^{d+2}\big)$$

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

Proof. • Attacker may transform $(\mathbf{s}, x, f_{\mathbf{s}}(x))$ to $(\mathbf{s}', x + \partial x, f_{\mathbf{s}}(x) + \partial e)$.

- Define $g(X) := f_{\mathbf{s}'}(X + \partial x) - f_{\mathbf{s}}(X) - \partial e$.
- Gets decoded to $s' \neq s$ if $f_{\mathbf{s}'}(x + \partial x) = f_{\mathbf{s}}(x) + \partial e$, i.e., if $g(x) = 0$.

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

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

Theorem The resulting AMD code

$$E : \mathbb{F}^d \to \mathbb{F}^d \times \mathbb{F} \times \mathbb{F},\;\; \mathbf{s} \xmapsto{x \in \mathbb{F}} \big(\mathbf{s}, x, f_{\mathbf{s}}(x) = s_1 x + \cdots + s_d x^d + x^{d+2}\big)$$

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

Proof. • Attacker may transform $\big(\mathbf{s}, x, f_{\mathbf{s}}(x)\big)$ to $\big(\mathbf{s}', x + \partial x, f_{\mathbf{s}}(x) + \partial e\big)$.

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

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

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

Theorem The resulting AMD code

$$E : \mathbb{F}^d \to \mathbb{F}^d \times \mathbb{F} \times \mathbb{F}, \; \mathbf{s} \xmapsto{x \leftarrow \mathbb{F}} \big(\mathbf{s}, x, f_{\mathbf{s}}(x) = s_1 x + \cdots + s_d x^d + x^{d+2}\big)$$

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

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

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

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?)

The End

“Thank you for your attention !!!”