A short tutorial on

ALGEBRAIC MANIPULATION DETECTION CODES

Abhinav Aggarwal

Cramer R, Dodis Y, Fehr S, Padró C, Wichs D. **Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors.** InAnnual International Conference on the Theory and Applications of Cryptographic Techniques 2008 Apr 13 (pp. 471-488). Springer Berlin Heidelberg.

BASIC IDEA

Adversary with write only access.
Knows x in advance.

Δ

x

Initial value
stored on the device

Store Device

$x + \Delta$

Final value read
from the device

Want to detect this tampering!!

[Enter AMD Codes.]

Adversary with write only access

Δ

We want to detect tampering with high probability!!

$$\Pr\left(dec\left(enc(x) + \Delta\right) \neq x\right) \leq \delta$$

AMD codes : $|enc(x)| = |x| + \mathcal{O}\left(1/\delta\right)$

DEFINITION

Definition 1. *An* (S, G, δ)-algebraic manipulation detection code, *or* (S, G, δ)-AMD code *for short, is a* probabilistic encoding *map* $\mathcal{E} : \mathcal{S} \to \mathcal{G}$ *from a set* $\mathcal{S}$ *of size* S *into an (additive) group* $\mathcal{G}$ *of order* G*, together with a (deterministic)* decoding *function* $D : \mathcal{G} \to \mathcal{S} \cup \{\perp\}$ *such that* $D(\mathcal{E}(s)) = s$ *with probability 1 for any* $s \in \mathcal{S}$*. The security of an AMD code requires that for any* $s \in \mathcal{S}, \Delta \in \mathcal{G}$, $\Pr[D(\mathcal{E}(s) + \Delta) \notin \{s, \perp\}] \leq \delta$.

An AMD code is called systematic *if* $\mathcal{S}$ *is a group, and the encoding is of the form*

$$\mathcal{E} : \mathcal{S} \to \mathcal{S} \times \mathcal{G}_1 \times \mathcal{G}_2, \; s \mapsto (s, x, f(x, s))$$

for some function f *and* $x \in_R \mathcal{G}_1$*. The decoding function of a systematic AMD code is naturally given by* $D(s', x', \sigma') = s'$ *if* $\sigma' = f(x', s')$ *and* $\perp$ *otherwise.*

EXISTENCE

Definition 2. *An AMD code* family *is a class of AMD codes such that for any* $\kappa, u \in \mathbb{N}$ *there exists an* (S, G, δ)*-AMD code in that class with* $S \geq 2^u$ *and* $\delta \leq 2^{-\kappa}$.

TAG SIZE

Definition 3. *The* effective tag size $\varpi^*(\kappa, u)$ *with respect to* $\kappa, u \in \mathbb{N}$ *of an AMD code family is defined as* $\varpi^*(\kappa, u) = \min\{\log(G)\} - u$ *where the minimum is over all* (S, G, δ)*-AMD codes in that class with* $S \geq 2^u$ *and* $\delta \leq 2^{-\kappa}$.

A LOWER BOUND

Theorem 1. *Any AMD code family has an affective tag size lower bounded by* $\varpi^*(\kappa, u) \geq 2\kappa - 2^{-u+1} \geq 2\kappa - 1$.

OPTIMAL CONSTRUCTION
ENCODING FUNCTION

$$\mathbb{F} = GF(p^n)$$
$$(d+2) \not\equiv 0 \ (mod\ p)$$

$$enc : \mathbb{F}^d \rightarrow \mathbb{F}^d \times \mathbb{F} \times \mathbb{F}$$
$$s \mapsto (s, x, f(x, s))$$

Can be a random string. Needs to hidden from the adversary.

Works perfectly for private channels!

OPTIMAL CONSTRUCTION
TAGGING FUNCTION

$$f(x,s) = x^{d+2} + \sum_{i=1}^{d} s_i x^i$$

Simple operations inside $\mathbb{F}$

Fast and efficient computation of codes!

OPTIMAL CONSTRUCTION
DECODING FUNCTION

$$dec((s,x,t)) = \begin{cases} s & \text{if } t = f(x,s) \\ \perp & \text{otherwise} \end{cases}$$

$$\Pr\left(dec(enc(s)) \notin \{s, \perp\}\right) \leq \frac{d+1}{p^n}$$

With p = 2 and d = 1, encoding overhead is at most $2\log\left(\frac{1}{\delta}\right)$

PROOF OF OPTIMALITY TAG SIZE

Recall ***enc*** : $GF(p^{\mathbf{n}})^{\mathbf{d}} \rightarrow GF(p^{\mathbf{n}})^{d+2}$

Hence, tag size = $\log_p (p^{n(d+2)}) - \log_p (p^{\mathbf{nd}}) = 2n$

PROOF OF OPTIMALITY GUARANTEE

We wish to show :

For any $s \in GF(p^n)$ and $\Delta \in GF(p^n)^{d+2}$, we have

$Pr\ (dec\ (\ enc(s) + \Delta\ ) \in \{\ s, \perp\ \}\ ) \geq 1 - \delta$

Enough to show :

Given $s \in GF(p^n)^d$ and $x \in GF(p^n)$, for any $s' \neq s$ and $\Delta_x , \Delta_f \in GF(p^n)^d$

we have, $Pr\ (\ f(x, s) + \Delta_x \neq f(x+ \Delta_f , s')\ ) \geq 1 - \delta$

Event of interest!

PROOF OF OPTIMALITY GUARANTEE

Let E be the event that $f(x, s) + \Delta_x = f(x+ \Delta_f, s')$.

Then, E is also the event that

$$x^{d+2} + \sum_{i=1}^{d} s_i x^i + \Delta_f = (x+ \Delta_x)^{d+2} + \sum_{i=1}^{d} s_i' (x+ \Delta_x)^i$$

By definition of f

Rearrange terms of the equation to get

$$-(d+2)\, \Delta_x\, x^{d+1} + \sum_{i=1}^{d} (s_i - s_i')\, x^i - \Delta_x\, p(x) + \Delta_f = 0$$

where p(x) is a polynomial of degree at most d in x.

PROOF OF OPTIMALITY GUARANTEE

Let $g(x) = -(d+2)\,\Delta_x\, x^{d+1} + \sum_{i=1}^{d} (s_i - s_i')\, x^i - \Delta_x\, p(x) + \Delta_f$

Claim I : g(x) is non zero and has degree at most (d+1)

Case I : ($\Delta x \neq 0$) Trivial, since (d+2) is non zero modulo p

Case II : ($\Delta x = 0$) For some i, we have $s_i \neq s_i'$

Claim II : g(x) has at most (d+1) roots

Claim III : g(x) = 0 with probability at most $(d+1)/p^n$

SOME APPLICATIONS

Robust Secret Sharing

Message Authentication Codes (With Key Manipulation Security)

Secure interactive communication (My talk!)

Questions??