Rate 1 Non-malleable codes for polysize tampering

Svetlana Ivanova and Guillermo Gamboa

REU 2022, Rutgers University

This research is part of a project that has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No. 823748.

Coding schemes and tampering experiment

- Alice wants to send a message $m \in \{0,1\}^k$ to Bob using the coding scheme (Enc, Dec), where

  $Enc : \{0,1\}^k \to \{0,1\}^n$ is a randomized encoding function

  $Dec : \{0,1\}^n \to \{0,1\}^k \cup \{\perp\}$ is a deterministic decoding function

  and $\mathbb{P}[Dec(Enc(m)) = m] = 1$.

Coding schemes and tampering experiment

- Alice wants to send a message $m \in \{0,1\}^k$ to Bob using the coding scheme (Enc, Dec), where

  $$Enc : \{0,1\}^k \to \{0,1\}^n \text{ is a randomized encoding function}$$
  $$Dec : \{0,1\}^n \to \{0,1\}^k \cup \{\perp\} \text{ is a deterministic decoding function}$$

  and $\mathbb{P}[Dec(Enc(m)) = m] = 1$.
- Mallory gets into the channel and tampers with $Enc(m)$ using a function f from a set $\mathcal{F}$ of tampering functions.

Coding schemes and tampering experiment

- Alice wants to send a message $m \in \{0,1\}^k$ to Bob using the coding scheme (Enc, Dec), where

  $$Enc : \{0,1\}^k \to \{0,1\}^n \text{ is a randomized encoding function}$$
  $$Dec : \{0,1\}^n \to \{0,1\}^k \cup \{\perp\} \text{ is a deterministic decoding function}$$

  and $\mathbb{P}[Dec(Enc(m)) = m] = 1$.
- Mallory gets into the channel and tampers with $Enc(m)$ using a function f from a set $\mathcal{F}$ of tampering functions.
- Bob would want that $Dec(f(Enc(m)))$ is either m or completely unrelated to what Alice sent. Can we achieve this independent of the message m?

Non-malleable codes

The coding scheme (Enc, Dec) is **non-malleable w.r.t.** $\mathcal{F}$ if for each $f \in \mathcal{F}$ we can find a distribution D_f over $\{0,1\}^k \cup \{\perp\}$ such that the tampering experiment is "statistically indistinguishable" to the experiment $m' \leftarrow D_f$.

Examples of tampering

- Bit-Wise Independent Tampering - covers the majority of real-world tampering attacks that have been demonstrated in practice.
- Tampering By Polynomial Size Circuits - type of tampering we're focusing on.

The goal of our project

To construct a "rate compiler" that converts any non-malleable code resilient to tampering by size n^c circuits into a rate-1 non-malleable code resilient to tampering by size n^d (for constant $d < c$) circuits.