Modeling Preprocessing Attacks

Auxiliary-Input Model/Bit-Fixing Model

14

- Offline attacker $\mathcal{A}_{\mathsf{pre}}$ is unbounded and outputs an S-bit hint for online attacker $\mathcal{A}_{\mathsf{on}}$
- $\mathcal{A}_{\mathsf{on}}$ will try to win security games using the hint

Auxiliary-Input Model

Bit-Fixing Model (ROM)

- $\mathcal{A}_{\mathsf{pre}}$ fixes random oracle $\mathsf{H}(\cdot)$ at P locations
- $\mathcal{A}_{\mathsf{on}}$ initially knows nothing about remaining unfixed values (picked uniformly at random)


Realistic model


Proof can be difficult — we can no longer assume that RO H looks uniformly random to online attacker (due to hint)

- **Compression Argument:** if online attacker is too successful then we can “compress” H (compressing a random string is impossible)

multi-user security of **key-prefixed short** Schnorr signatures against preprocessing attacks **in ROM+GGM [EUROCRYPT 2022]**

multi-user security of **standardized implementations** of **short** Schnorr signatures against preprocessing attacks **in ROM+GGM [New Result]**

- Much easier to prove security
- Not a compelling model for preprocessing attacks!

- **Usage:** lower bound in Bit-Fixing Model $\Rightarrow$ lower bound in Auxiliary-Input Model [Coretti et al., EUROCRYPT 2018]

$$\varepsilon_{\mathsf{AI}}(S, q) \leq \varepsilon_{\mathsf{BF}}(P, q) + \mathcal{O}(Sq/P)$$

[Coretti et al., EUROCRYPT 2018]

Bit-Fixing ROM

Auxiliary-Input GGM

Auxiliary-Input ROM

[Coretti et al., CRYPTO 2018]

Bit-Fixing RPM

Bit-Fixing GGM

Bit-Fixing ICM

Auxiliary-Input ICM

Auxiliary-Input RPM

only showed in a single idealized model!