

Summary of Our Results

Research Questions





Are short signatures against prepress attacks?

ex)

BSI-TR-03111

ISO/IEC 14888-3

Caveats (of *key-prefixed* signatures):

- Not a **standardized** implementation
- Preprocessing attacker is **time-bounded**
- Complex proof technique: **compression argument**

→ standardized!

→ unbounded!

→ much simpler proof!



Rest of the Talk:

- **Multi-User Signature Forgery Game**
- **Bridge-Finding Game** (in the Generic Group Model)
- Multi-User Security of Short Schnorr Signatures (**standardized implementations**)
against **Preprocessing Attacks (Bit-Fixing to Auxiliary-Input Technique)**

► **Answer 3: Yes, “short” version of standardized implementations of Schnorr signatures are secure!**

- 
- No key-prefixing
 - Disallow $e=0$ signatures!

Summary of Our Results

Research Questions



Are **short** Schnorr signatures secure against **preprocessing attacks**?

- ▷ **Answer 3:** Yes, “short” version of standardized implementations of Schnorr signatures are secure!

- No key-prefixing
- Disallow $e=0$ signatures!

ex)

BSI-TR-03111
ISO/IEC 14888-3

~~Caveats (of key prefixed signatures):~~ → Advantages:

- ~~Not a **standardized** implementation~~ → **standardized!**
- Preprocessing attacker is ~~**time bounded**~~ → **unbounded!**
- ~~Complex proof technique: **compression argument**~~ → **much simpler proof!**

Rest of the Talk:

- Multi-User Signature Forgery Game
- Bridge-Finding Game (in the Generic Group Model)
- Multi-User Security of Short Schnorr Signatures (**standardized implementations**) against **Preprocessing Attacks (Bit-Fixing to Auxiliary-Input Technique)**

Multi-User Signature Forgery Game

UF-CMA Security

$H(\cdot), \text{Mult}(\cdot, \cdot), \text{Inv}(\cdot)$



Signature Scheme: $\Pi = (\text{Kg}, \text{Sign}, \text{Vfy})$
 $(pk_i, sk_i) \leftarrow \text{Kg}(1^k), 1 \leq i \leq N$