

Summary of Our Results

Research Questions



Are short Schnorr signatures secure against preprocessing attacks?



Caveats (of key-prefixed signatures):

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

standardized!



much simpler proof!

Advantages:

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!
 BSI-TR-03111
 - · No key-prefixing
 - O Disallow e=0 signatures!

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!

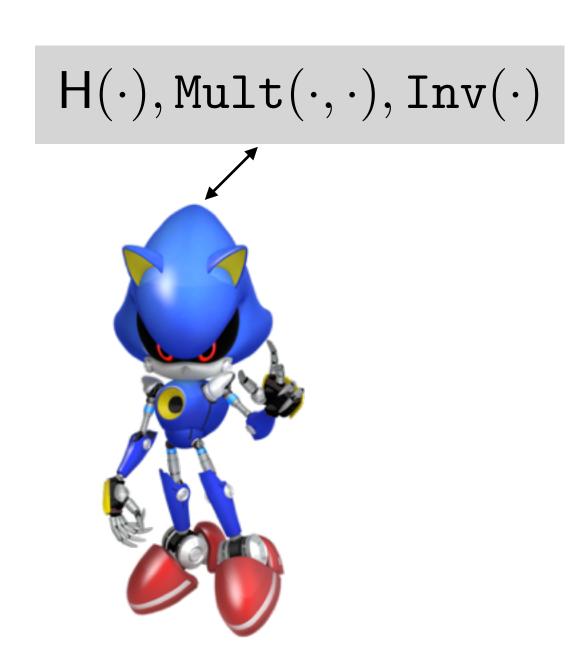
Rest of the Talk:

- 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)

ISO/IEC 14888-3

Multi-User Signature Forgery Game

UF-CMA Security





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