Hash-Based Signatures

Johannes Buchmann, Andreas Hülsung
Supported by DFG and DAAD

Part VI:
XMSS Secret Key

XMSS Secret Key Generation

CASED

Parameters: n, h, w, m, $\ell = \ell(w,m)$

Required:

- 2^h WOTS signature keys
- WOTS signature key: ℓ random strings in $\{0,1\}^n$

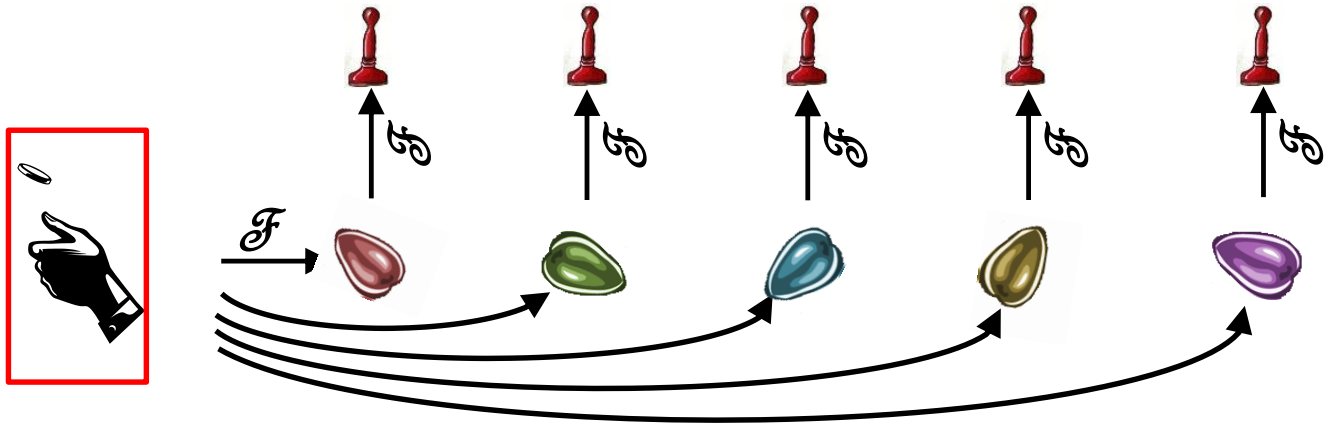
XMSS secret key generation:

- XMSS secret key is random seed in $\{0,1\}^n$
- WOTS signature keys generated using PRF

$$\mathcal{F} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$$

XMSS – Secret key

CASED



Secret Key Size: b

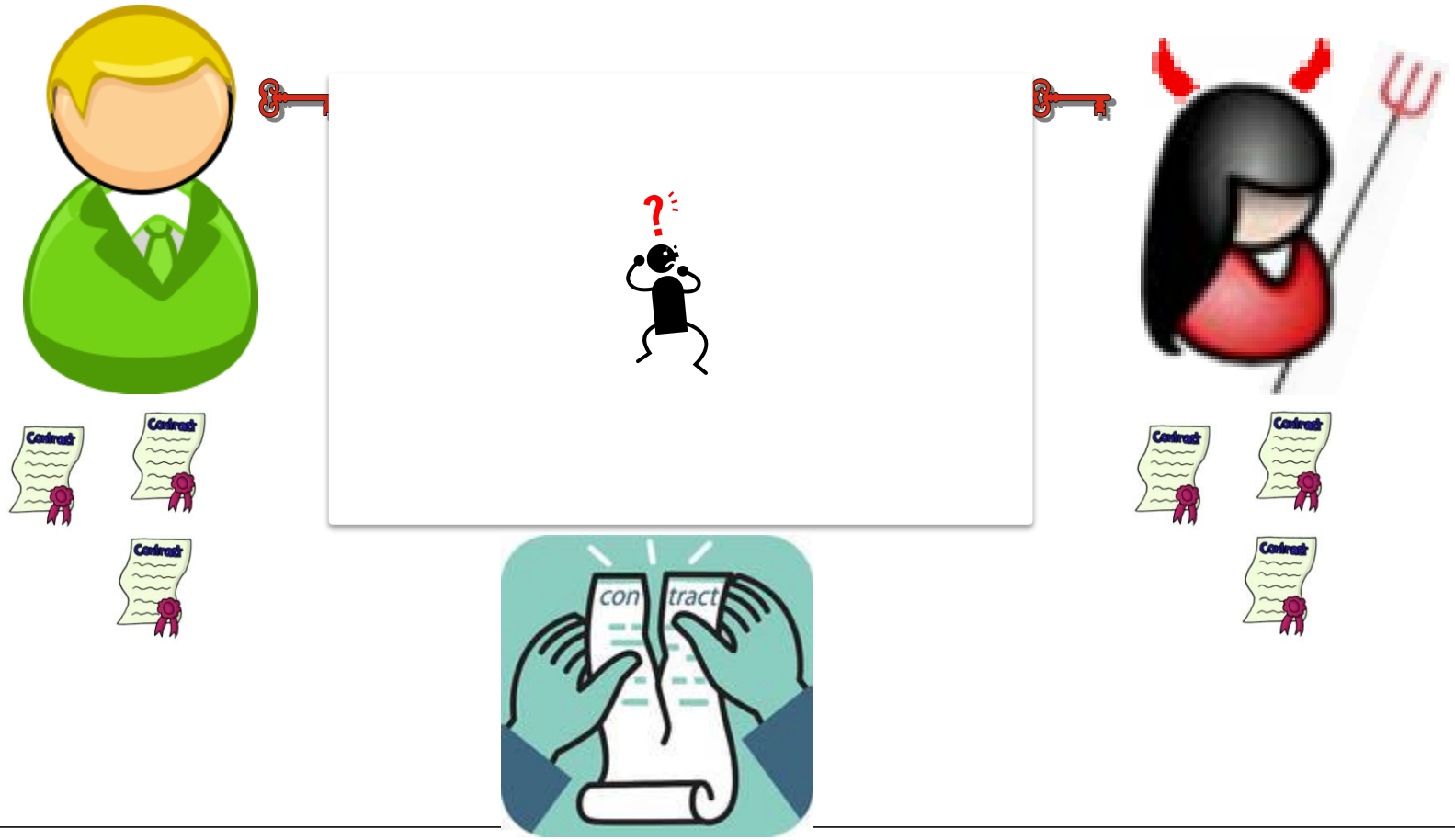
Hash-Based Signatures

Johannes Buchmann, Andreas Hülsung
Supported by DFG and DAAD

Part VII:
Forward secure variant of XMSS

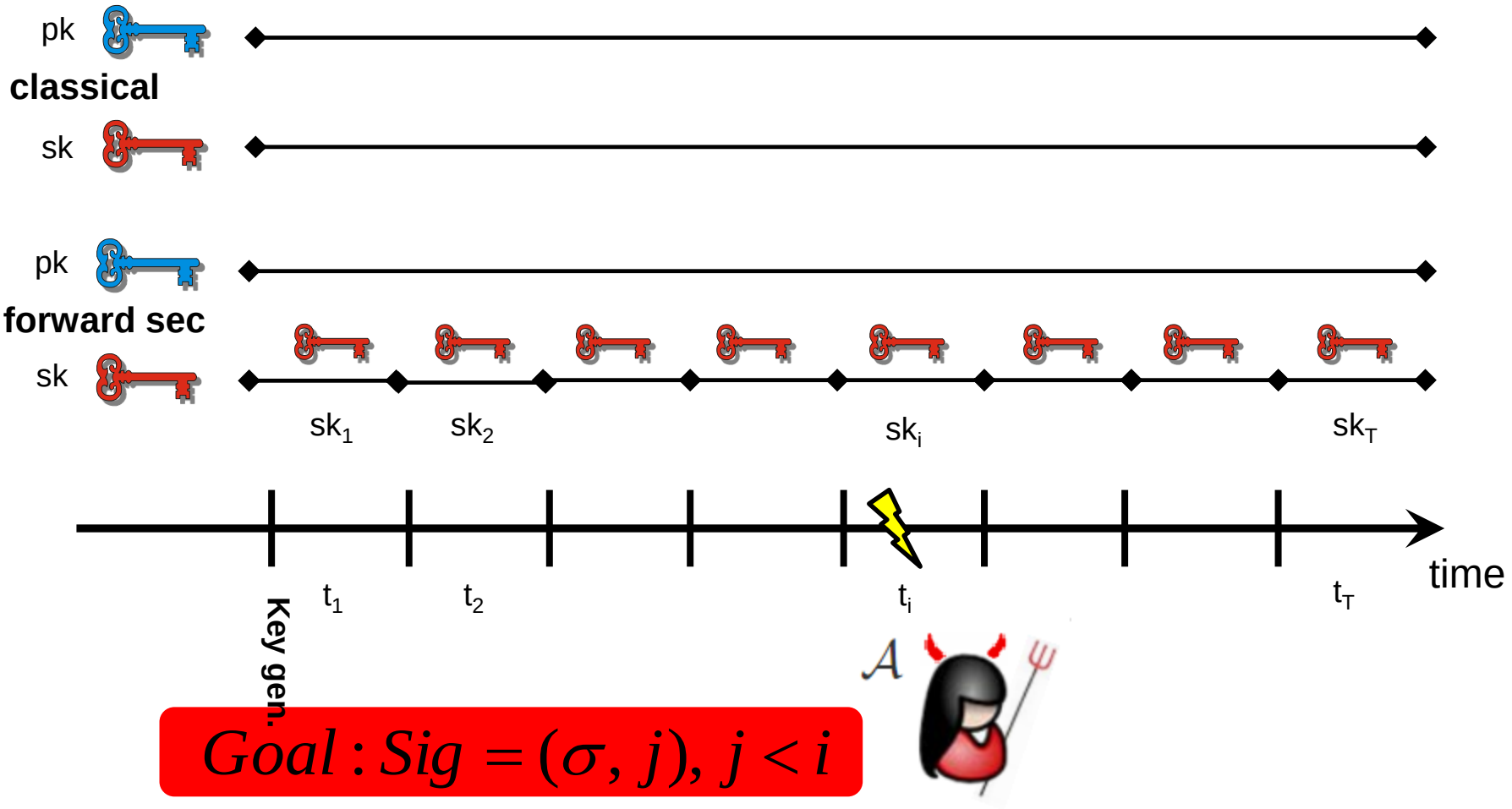
Forward Security

CASED



Forward Secure Signatures

CASED



XMSS forward secure

CASED