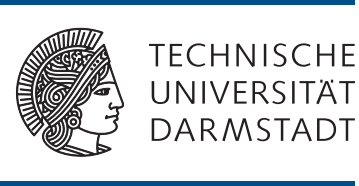
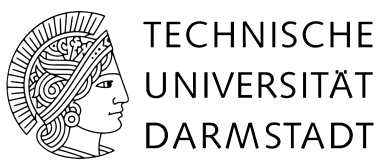
0-RTT Key Exchange with Full Forward Secrecy



Felix Günther

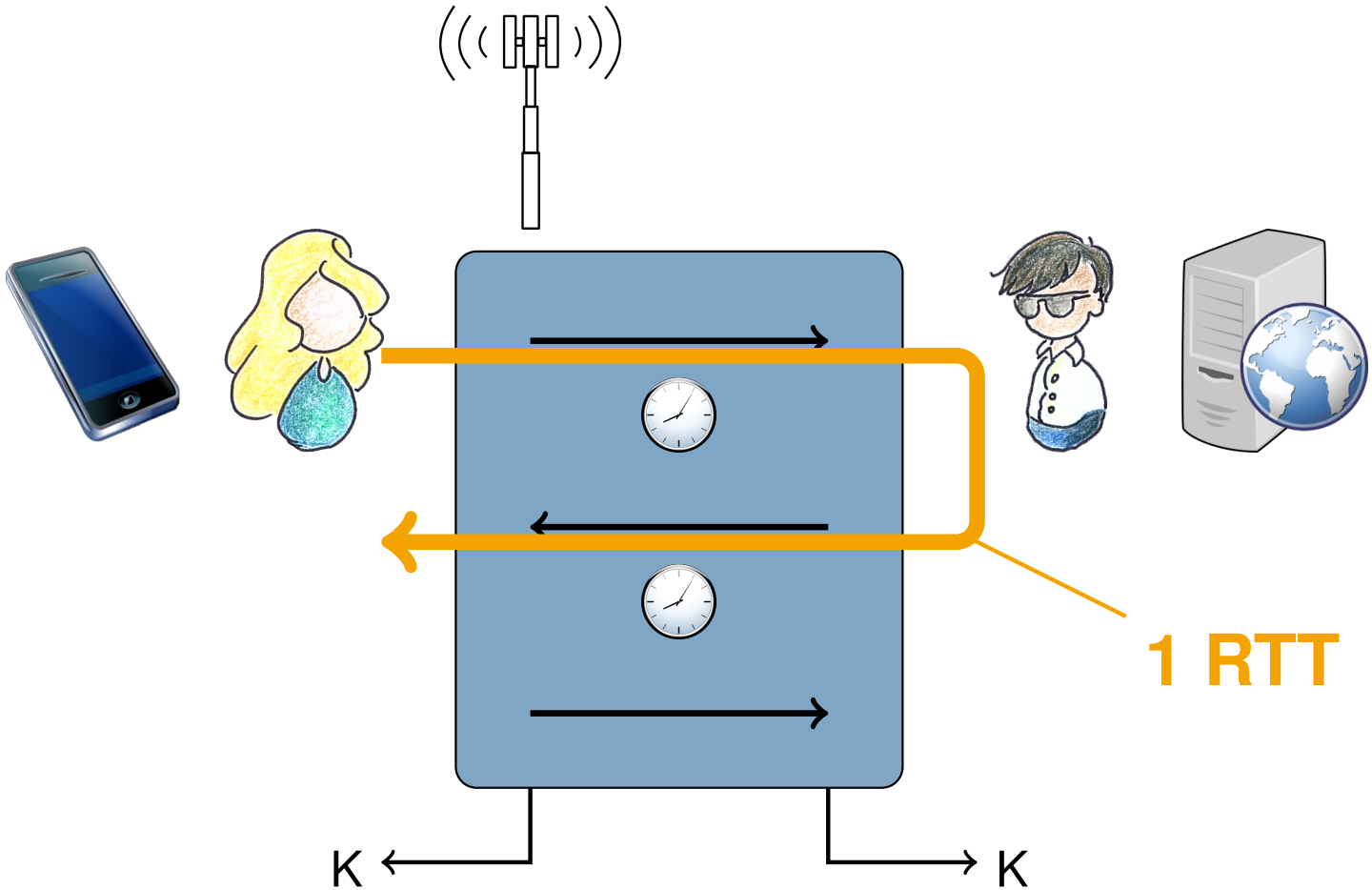
Technische Universität Darmstadt, Germany

joint work with Britta Hale, Tibor Jager, and Sebastian Lauer



Key Exchange
can be a bottleneck

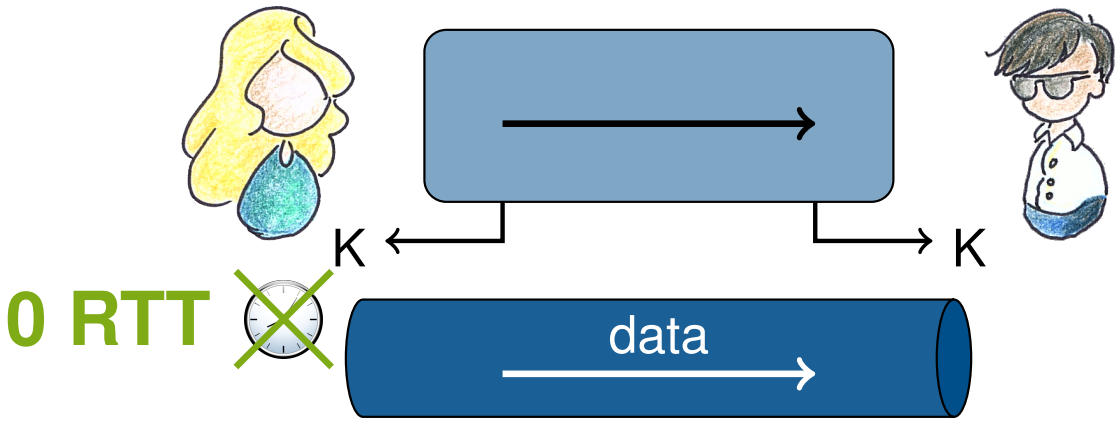
TECHNISCHE UNIVERSITÄT DARMSTADT



drawings by *Giorgia Azzurra Marson*

Solution: 0-RTT Key Exchange

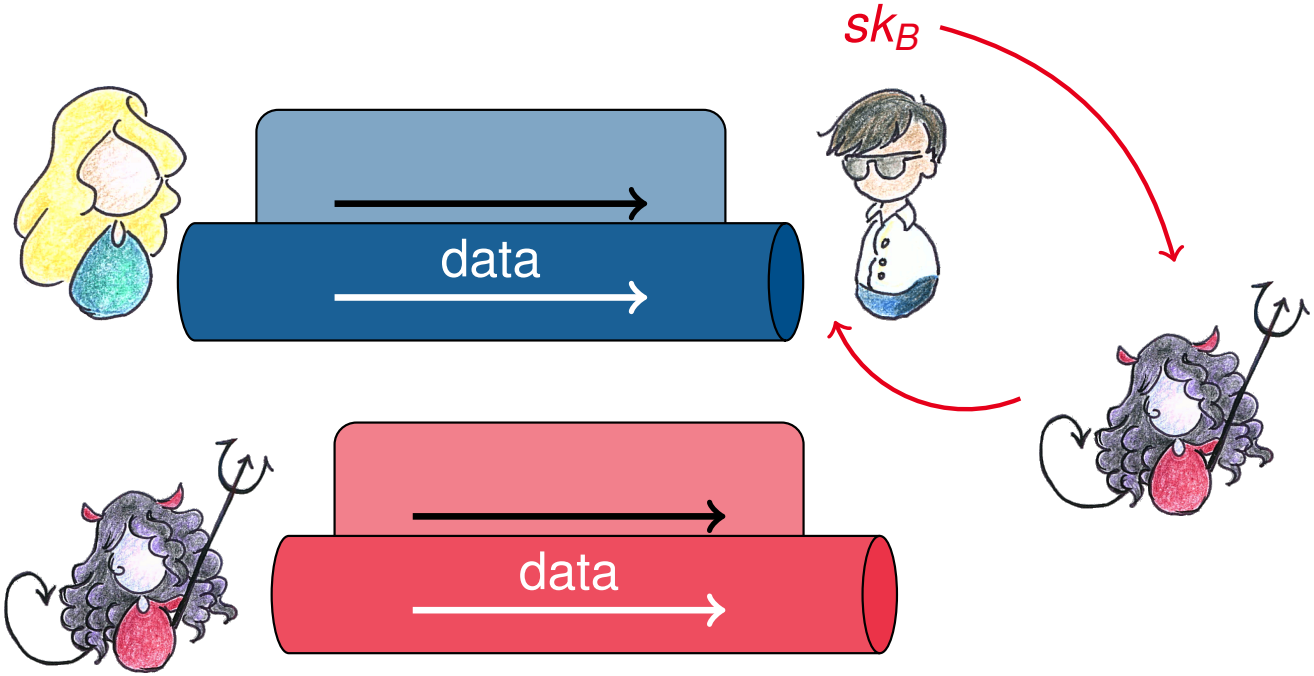
TECHNISCHE UNIVERSITÄT DARMSTADT



- theoretically not new
- in practice: **QUIC** (2013), **TLS 1.3** (2015+)

Problems with 0-RTT Key Exchange

TECHNISCHE UNIVERSITÄT DARMSTADT



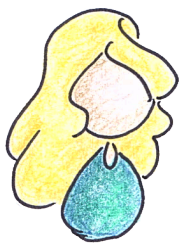
replays
(partially unavoidable)

no forward secrecy
(considered inherent)

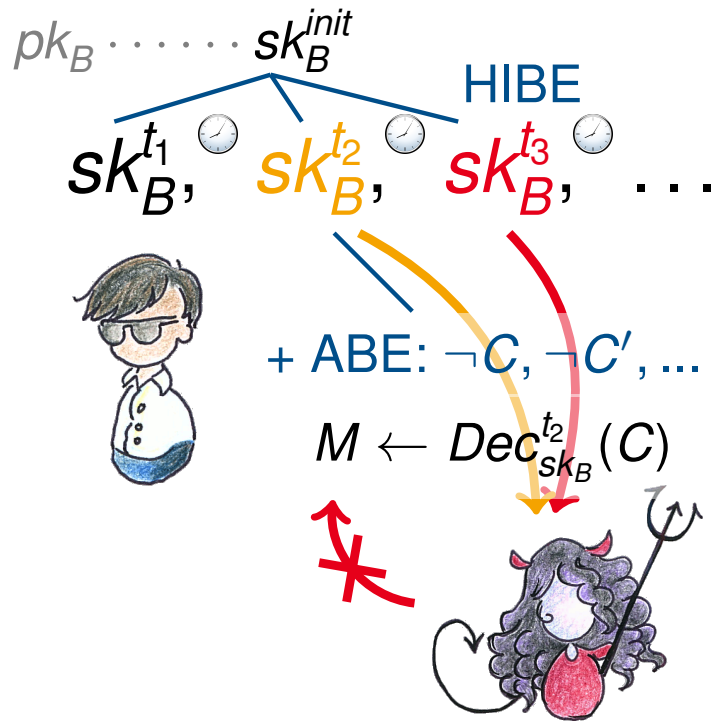
A Similar Scenario: Asynchronous Messaging

TECHNISCHE UNIVERSITÄT DARMSTADT

wants to send M



$C = Enc^{t_2}_{pk_B}(M)$

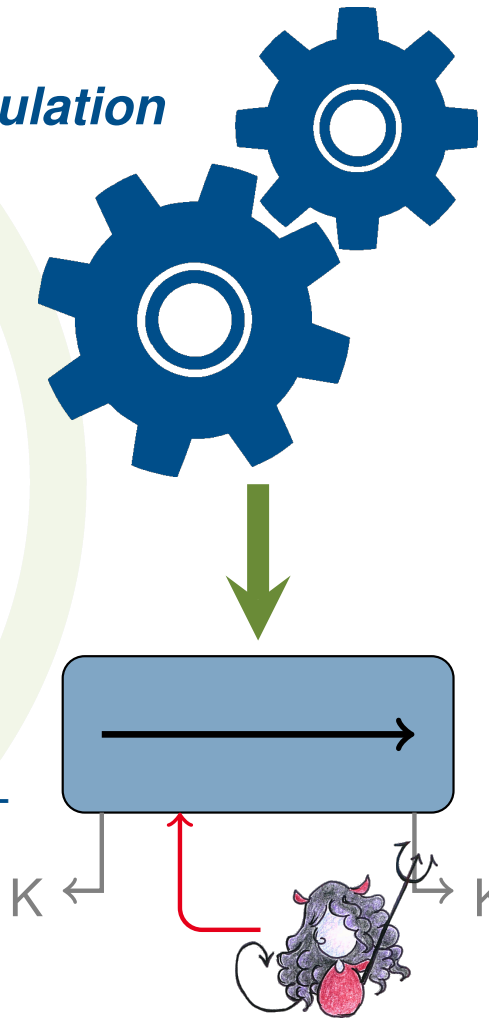


- public-key encryption with coarse **forward secrecy** (CHK'03)
- fine-grained **puncturable forward-secret encryption** (GM'15)

Puncturable Forward-Secret Encryption Yields Forward-Secret 0-RTT Key Exchange

TECHNISCHE UNIVERSITÄT DARMSTADT

- building block: **puncturable forward-secret key *encapsulation***
  - we build generically from any HIBKEM
  - can replace involved blend of HIBE+ABE [GM'15]
  - CCA-secure in the standard model

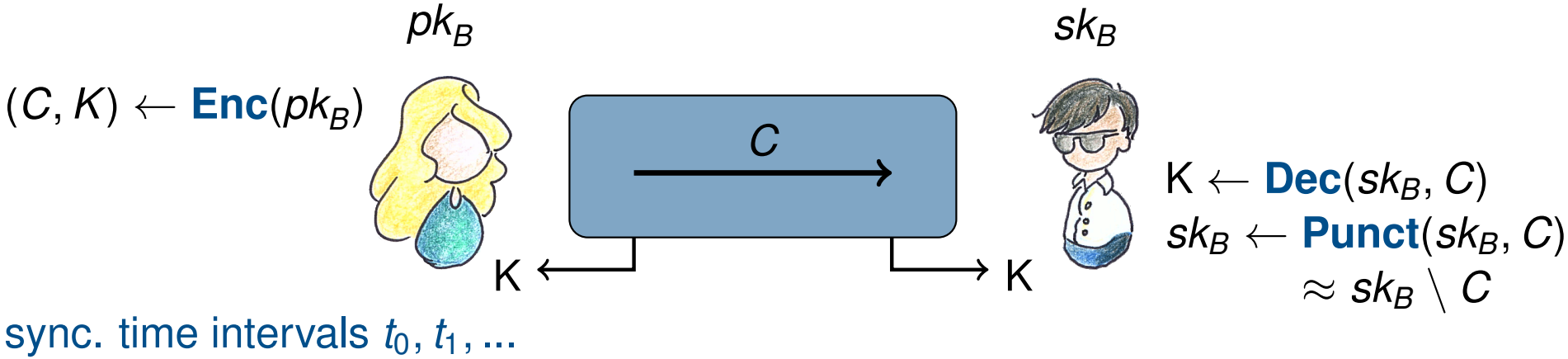


- **forward-secret 0-RTT key exchange**
  - we build from any PFSKEM
  - formalize key exchange security with forward-secret 0-RTT

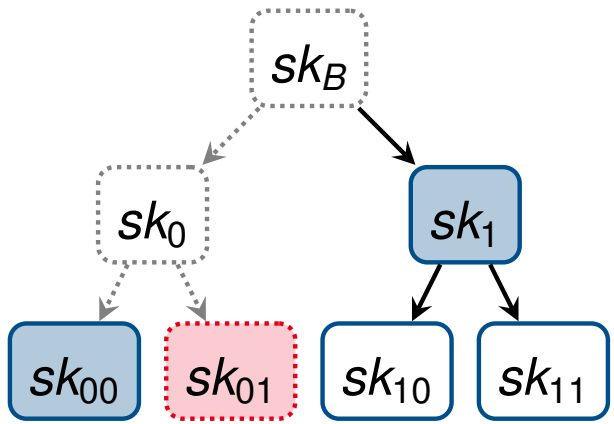
Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

TECHNISCHE UNIVERSITÄT DARMSTADT



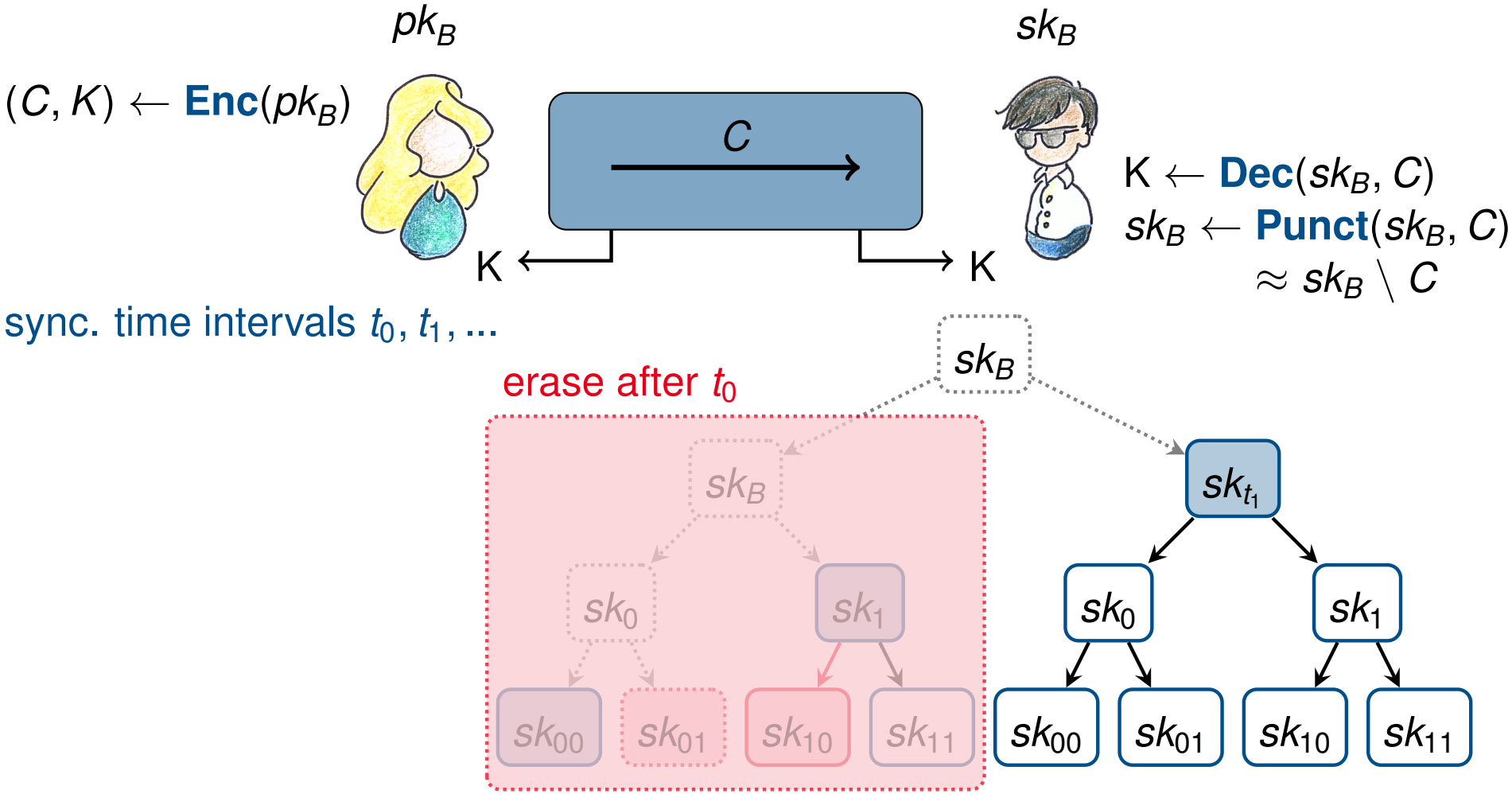
sync. time intervals $t_0, t_1, \ldots$



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

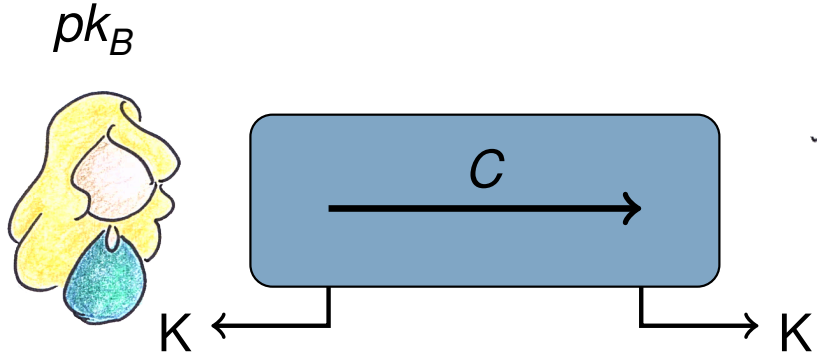
TECHNISCHE UNIVERSITÄT DARMSTADT



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

TECHNISCHE UNIVERSITÄT DARMSTADT

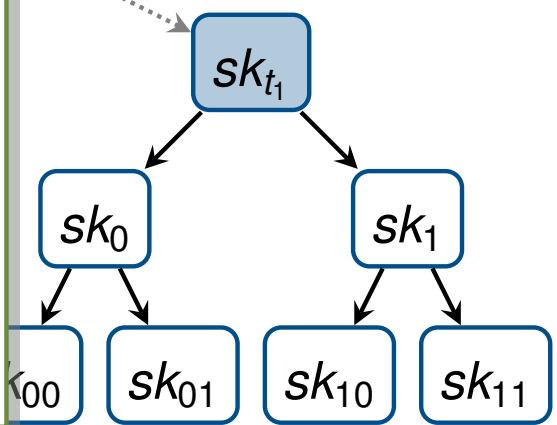


Evaluation (initial, based on BKP'14 HIBE)

- ✓ full forward secrecy
- ✓ replay protection
- time performance:
  - ✓ **Enc** few ms
  - ? **Dec** few seconds
  - ✗ **Punct** few minutes

hope: need only **selective security**

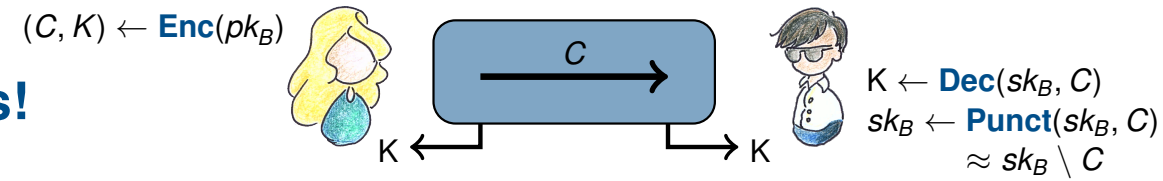
} expensive delegation



Summary

TECHNISCHE UNIVERSITÄT DARMSTADT

- **Fully forward-secret 0-RTT key exchange exists!**



- Generic construction and security proof
  - very simple single-message protocol
  - building block: puncturable forward-secret key encapsulation
  - from any HIBKEM

- Can we make this practical?

Thank You!

mail@**felixguenther.info**