

0-RTT Key Exchange with Full Forward Secrecy



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Felix Günther

Technische Universität Darmstadt, Germany

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



TECHNISCHE
UNIVERSITÄT
DARMSTADT



Cryptoplexity

Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de



CROSSING

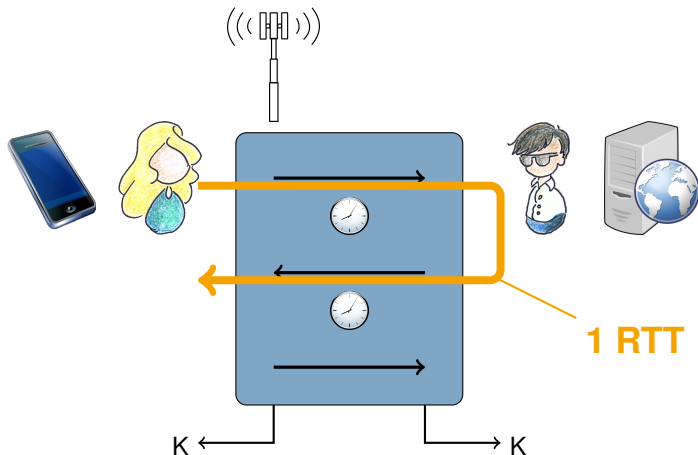
 **NTNU**



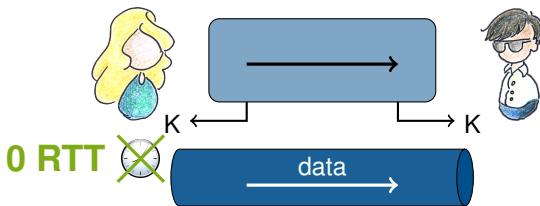
**PADERBORN
UNIVERSITY**


RUB

Key Exchange can be a bottleneck

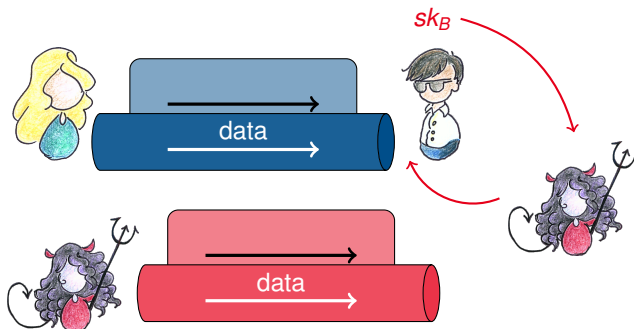


Solution: 0-RTT Key Exchange



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

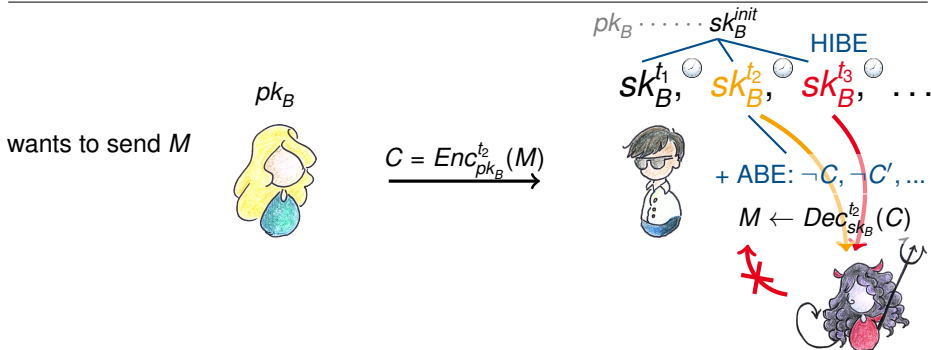
Problems with 0-RTT Key Exchange



replays
(partially unavoidable)

no forward secrecy
(considered inherent)

A Similar Scenario: Asynchronous Messaging



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



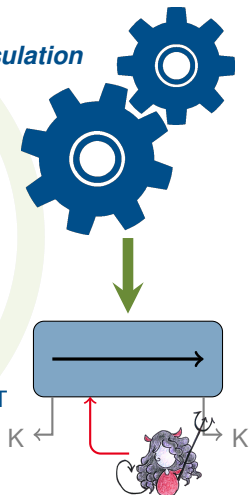
Puncturable Forward-Secret Encryption Yields Forward-Secret 0-RTT Key Exchange

▶ building block: **puncturable forward-secret key encapsulation**

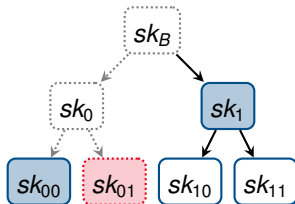
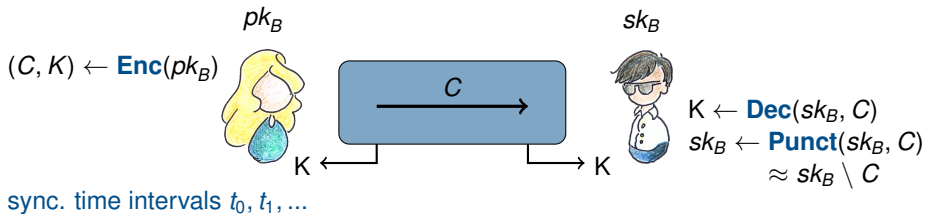
- ▶ we build generically from any HIBKEM
- ▶ can replace involved blend of HIBE+ABE [GM'15]
- ▶ CCA-secure in the standard model

▶ **forward-secret 0-RTT key exchange**

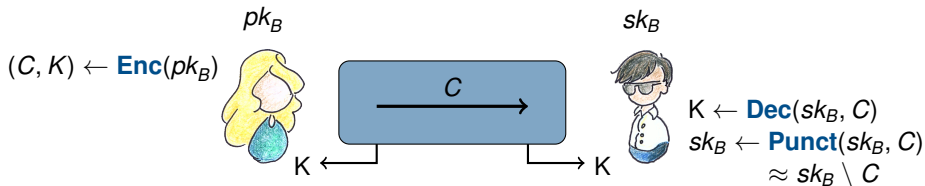
- ▶ we build from any PFSKEM
- ▶ formalize key exchange security with forward-secret 0-RTT



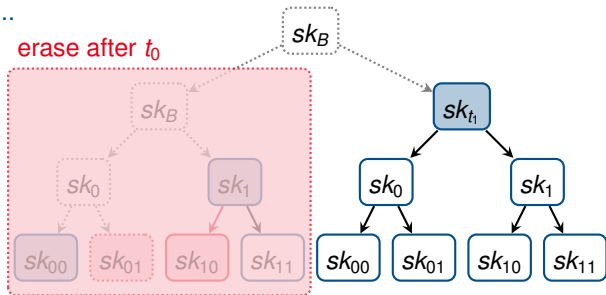
Our Forward-Secret 0-RTT Key Exchange In a Nutshell



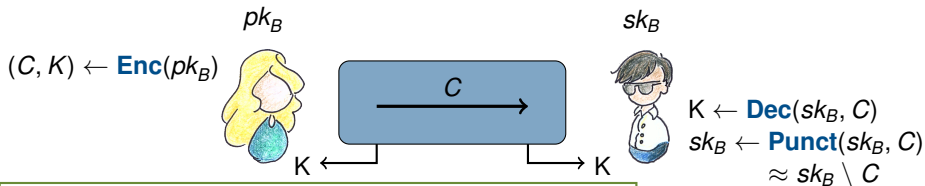
Our Forward-Secret 0-RTT Key Exchange In a Nutshell



sync. time intervals t_0, t_1, \dots



Our Forward-Secret 0-RTT Key Exchange In a Nutshell



Evaluation (initial, based on BKP'14 HIBE)

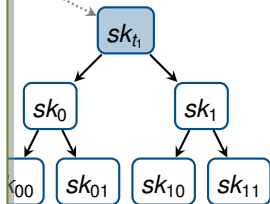
- ✓ full forward secrecy
- ✓ replay protection

▶ time performance:

✓	Enc	few ms
?	Dec	few seconds
✗	Punct	few minutes

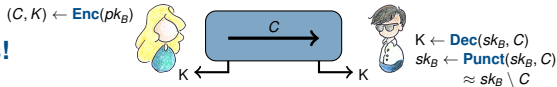
hope: need only selective security

expensive delegation



Summary

- ▶ **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