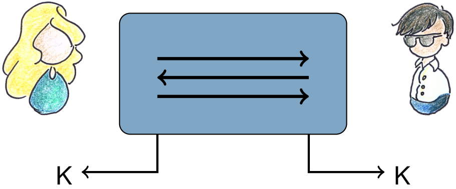
0-RTT Key Exchange with Full Forward Secrecy

Felix Günther

Technische Universität Darmstadt, Germany

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

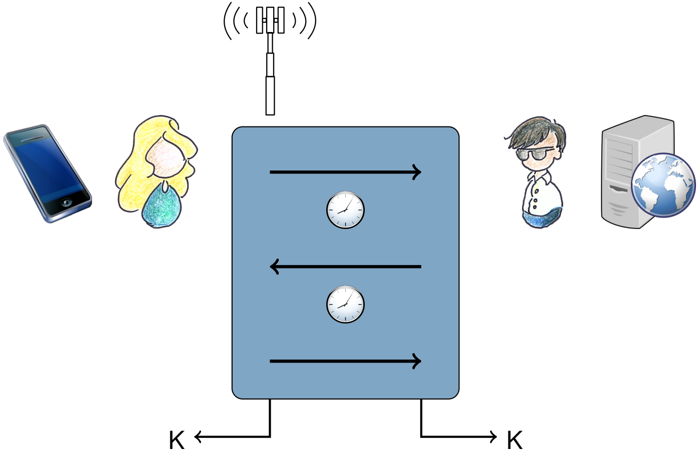
Key Exchange



drawings by *Giorgia Azzurra Marson*

Key Exchange

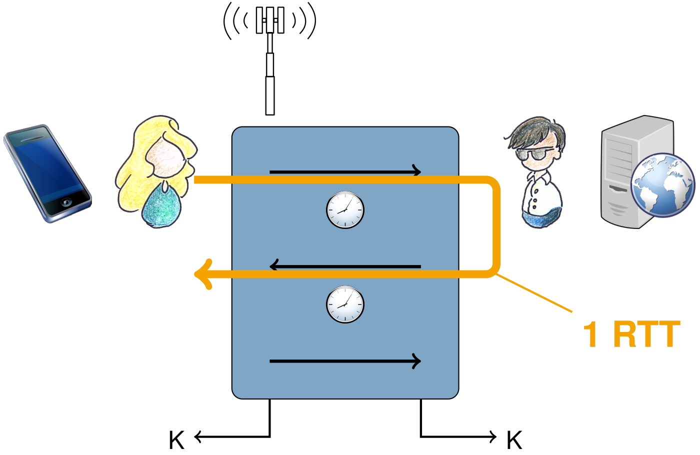
can be a bottleneck



drawings by *Giorgia Azzurra Marson*

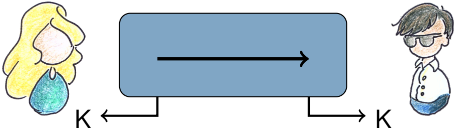
Key Exchange

can be a bottleneck

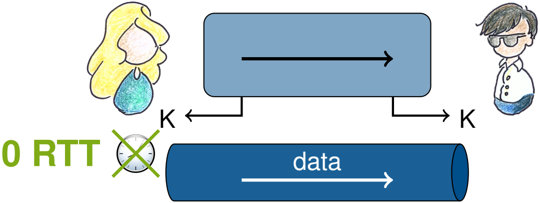


drawings by *Giorgia Azzurra Marson*

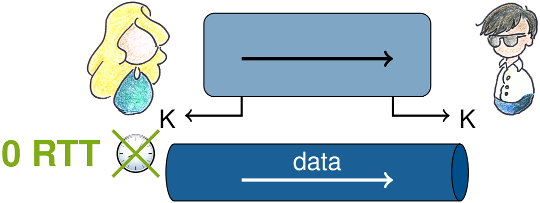
Solution: 0-RTT Key Exchange



Solution: 0-RTT Key Exchange

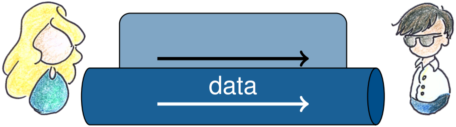


Solution: 0-RTT Key Exchange

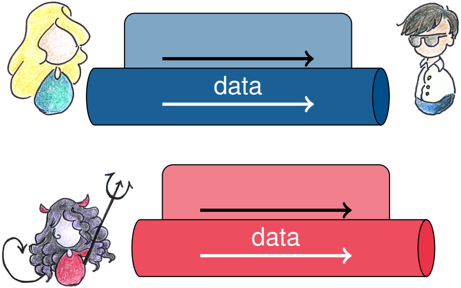


- theoretically not new
- in practice: **QUIC** (2013), **TLS 1.3** (2015+)

Problems with 0-RTT Key Exchange



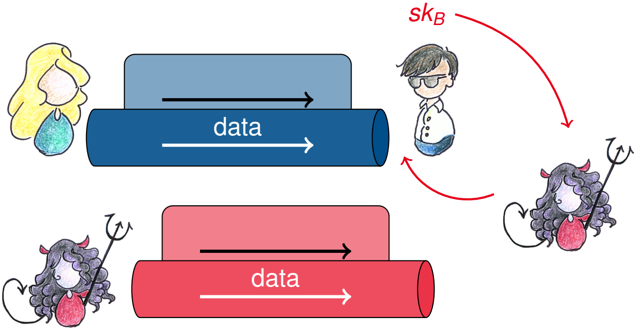
Problems with 0-RTT Key Exchange



replays

(partially unavoidable)

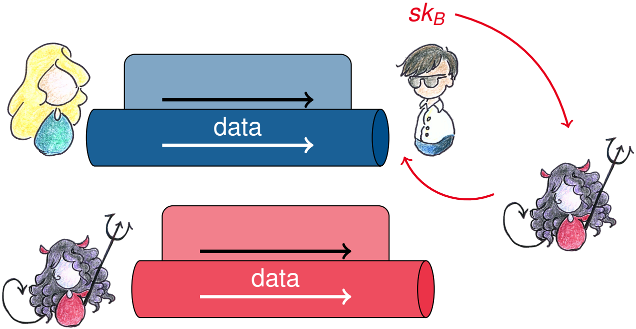
Problems with 0-RTT Key Exchange



replays
(partially unavoidable)

no forward secrecy
(considered inherent)

Problems with 0-RTT Key Exchange

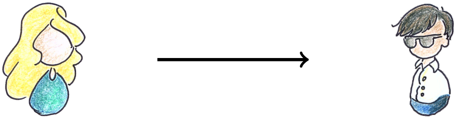


replays
(partially unavoidable)

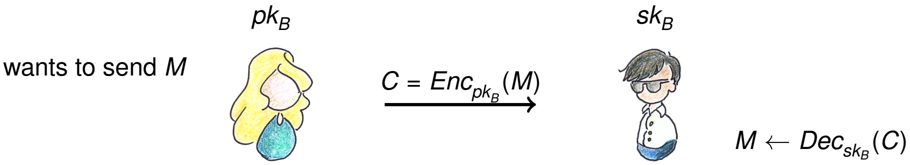
no forward secrecy
(considered inh✗rent)

A Similar Scenario: Asynchronous Messaging

wants to send M



A Similar Scenario: Asynchronous Messaging



pk_B

wants to send M

$C = Enc_{pk_B}(M)$ $\xrightarrow{\quad}$

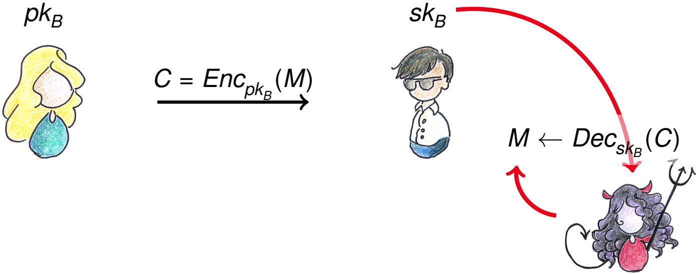
sk_B

$M \leftarrow Dec_{sk_B}(C)$

- public-key encryption

A Similar Scenario: Asynchronous Messaging

wants to send M



pk_B

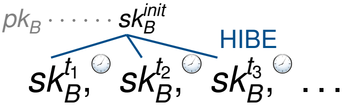
$C = Enc_{pk_B}(M)$

sk_B

$M \leftarrow Dec_{sk_B}(C)$

- public-key encryption

A Similar Scenario: Asynchronous Messaging

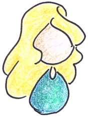

$pk_B \cdots\cdots sk_B^{init}$

HIBE

$sk_B^{t_1}, \; sk_B^{t_2}, \; sk_B^{t_3}, \; \ldots$

pk_B

wants to send M

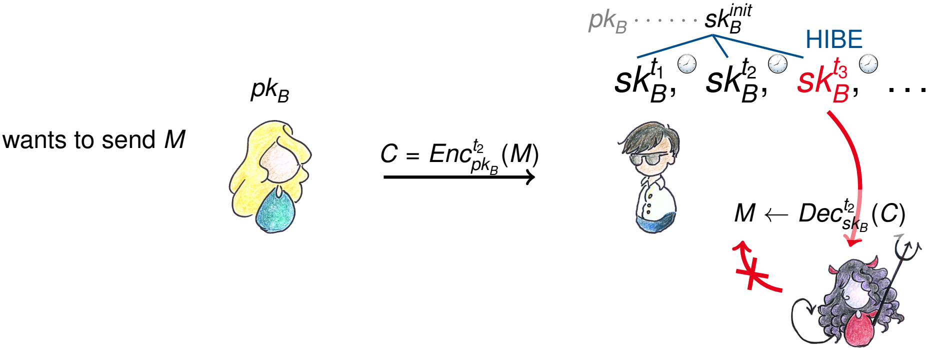


$\xrightarrow{C = Enc^{t_2}_{pk_B}(M)}$

$M \leftarrow Dec^{t_2}_{sk_B}(C)$

- public-key encryption with coarse **forward secrecy** (CHK'03)

A Similar Scenario: Asynchronous Messaging



$pk_B \cdots\cdots sk_B^{init}$

HIBE

$sk_B^{t_1},\ sk_B^{t_2},\ sk_B^{t_3},\ \ldots$

pk_B

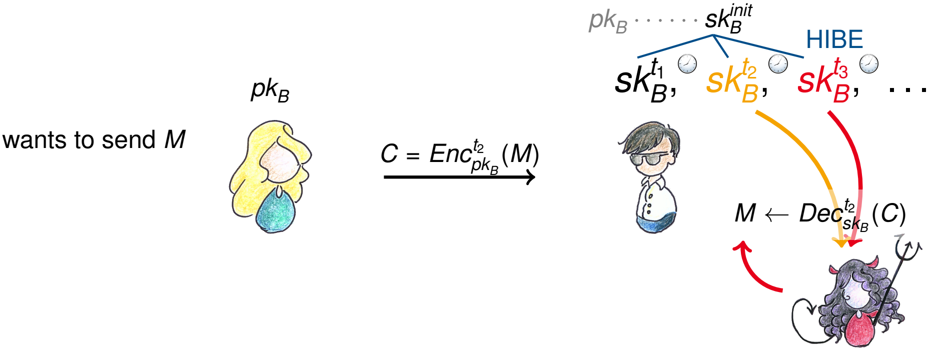
wants to send M

$C = Enc_{pk_B}^{t_2}(M)$

$M \leftarrow Dec_{sk_B}^{t_2}(C)$

- public-key encryption with coarse **forward secrecy** (CHK’03)

A Similar Scenario: Asynchronous Messaging



wants to send M

pk_B

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

$pk_B \cdots\cdots sk_B^{init}$

HIBE

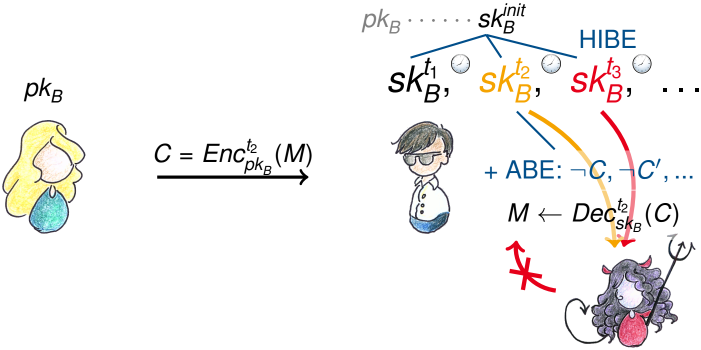
$sk_B^{t_1}, \; sk_B^{t_2}, \; sk_B^{t_3}, \; \ldots$

$M \leftarrow Dec^{t_2}_{sk_B}(C)$

- public-key encryption with coarse **forward secrecy** (CHK'03)

A Similar Scenario: Asynchronous Messaging

wants to send M



pk_B

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

$pk_B \cdots\cdots sk_B^{init}$

HIBE

$sk_B^{t_1}, \; sk_B^{t_2}, \; sk_B^{t_3}, \; \ldots$

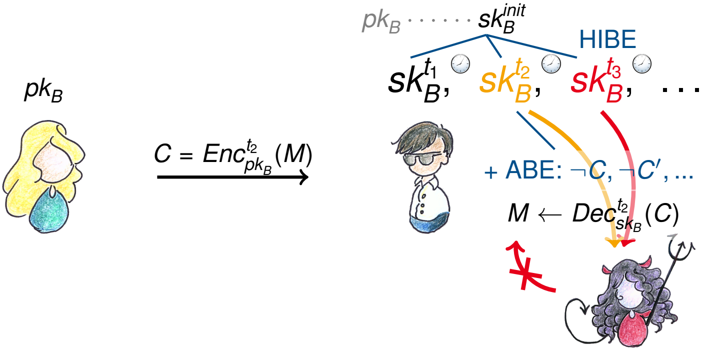
+ ABE: $\neg C, \neg C', \ldots$

$M \leftarrow Dec^{t_2}_{sk_B}(C)$

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

A Similar Scenario: Asynchronous Messaging

wants to send M



pk_B

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

$pk_B \cdots\cdots sk^{init}_B$

HIBE

$sk^{t_1}_B, \; sk^{t_2}_B, \; sk^{t_3}_B, \; \ldots$

$+$ ABE: $\neg C, \neg C', \ldots$

$M \leftarrow Dec^{t_2}_{sk_B}(C)$

- 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

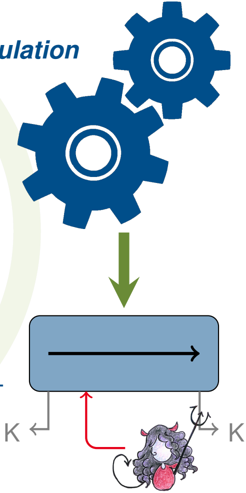
Puncturable Forward-Secret Encryption Yields Forward-Secret 0-RTT Key Exchange

- 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

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

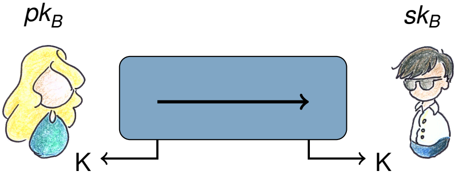
TECHNISCHE UNIVERSITÄT DARMSTADT

- 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

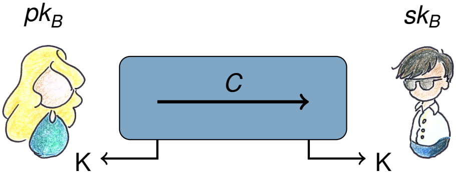
In a Nutshell



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

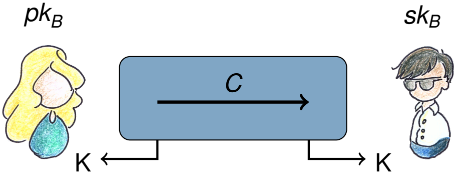
$(C, K) \leftarrow \mathbf{Enc}(pk_B)$



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

$(C, K) \leftarrow \textbf{Enc}(pk_B)$



$$K \leftarrow \textbf{Dec}(sk_B, C)$$

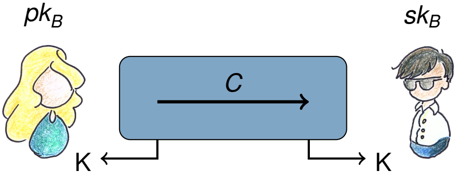
$$sk_B \leftarrow \textbf{Punct}(sk_B, C)$$

$$\approx sk_B \setminus C$$

Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

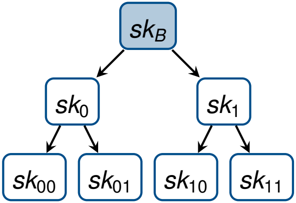
$(C, K) \leftarrow$ **Enc**(pk_B)



K $\leftarrow$ **Dec**(sk_B, C)

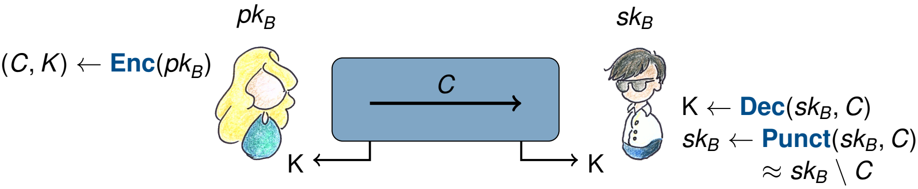
$sk_B \leftarrow$ **Punct**(sk_B, C)

$\approx sk_B \setminus C$



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell



pk_B

$(C, K) \leftarrow \textbf{Enc}(pk_B)$

$\xrightarrow{C}$

K

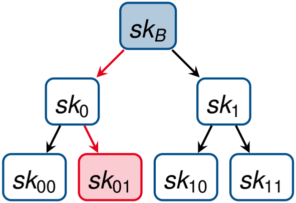
K

sk_B

$K \leftarrow \textbf{Dec}(sk_B, C)$

$sk_B \leftarrow \textbf{Punct}(sk_B, C)$

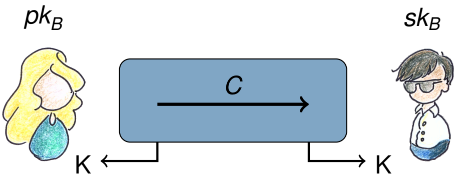
$\approx sk_B \setminus C$



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

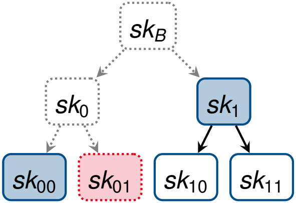
$(C, K) \leftarrow$ **Enc**(pk_B)



$K \leftarrow$ **Dec**(sk_B, C)

$sk_B \leftarrow$ **Punct**(sk_B, C)

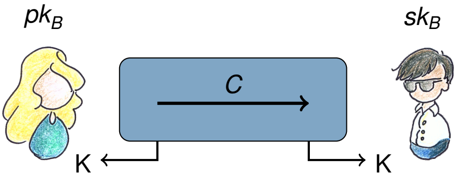
$\approx sk_B \setminus C$



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

$(C, K) \leftarrow \mathbf{Enc}(pk_B)$



pk_B

sk_B

C

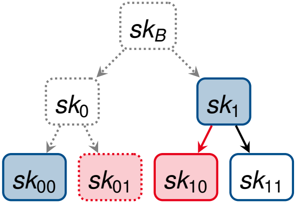
K

K

$K \leftarrow \mathbf{Dec}(sk_B, C)$

$sk_B \leftarrow \mathbf{Punct}(sk_B, C)$

$\approx sk_B \setminus C$



sk_B

sk_0

sk_1

sk_{00}

sk_{01}

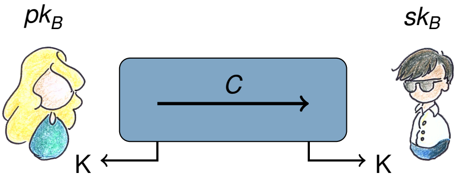
sk_{10}

sk_{11}

Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

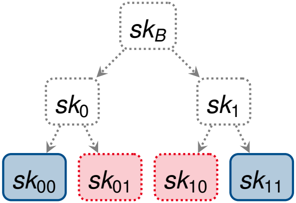
$(C, K) \leftarrow$ **Enc**(pk_B)



$K \leftarrow$ **Dec**(sk_B, C)

$sk_B \leftarrow$ **Punct**(sk_B, C)

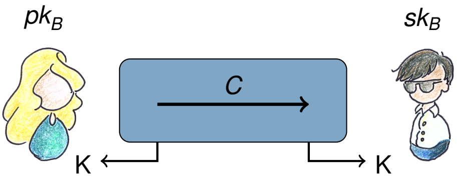
$\approx sk_B \setminus C$



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

$(C, K) \leftarrow$ **Enc**(pk_B)

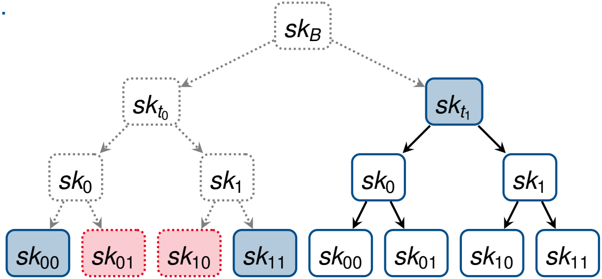


$K \leftarrow$ **Dec**(sk_B, C)

$sk_B \leftarrow$ **Punct**(sk_B, C)

$\approx sk_B \setminus C$

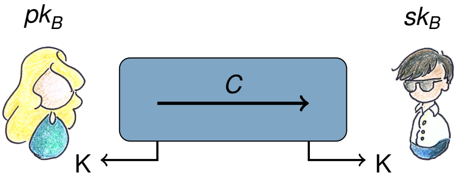
sync. time intervals $t_0, t_1, \ldots$



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

$(C, K) \leftarrow$ **Enc**(pk_B)

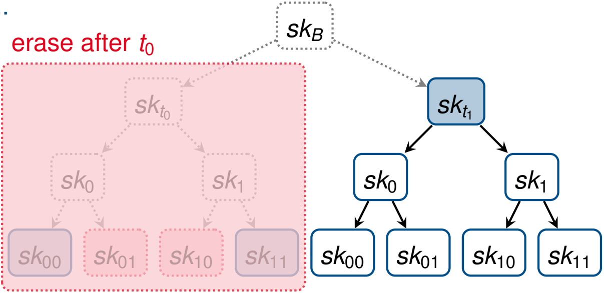


K $\leftarrow$ **Dec**(sk_B, C)

$sk_B \leftarrow$ **Punct**(sk_B, C)

$\approx sk_B \setminus C$

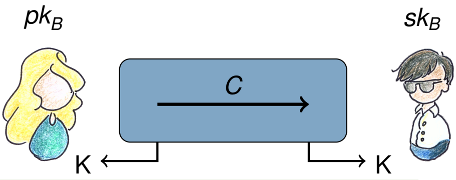
sync. time intervals $t_0, t_1, \ldots$



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

$(C, K) \leftarrow$ **Enc**(pk_B)

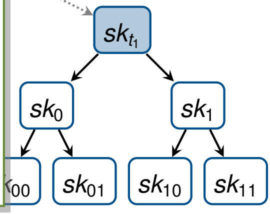


$K \leftarrow$ **Dec**(sk_B, C)

$sk_B \leftarrow$ **Punct**(sk_B, C)

$\approx sk_B \setminus C$

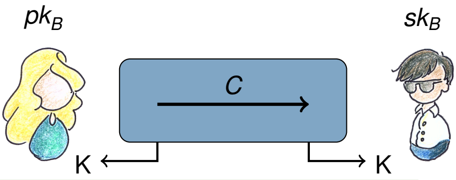
Evaluation



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

$(C, K) \leftarrow$ **Enc**(pk_B)



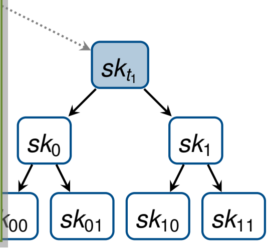
$K \leftarrow$ **Dec**(sk_B, C)

$sk_B \leftarrow$ **Punct**(sk_B, C)

$\approx sk_B \setminus C$

Evaluation

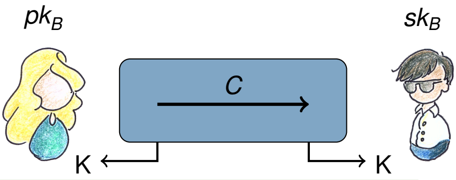
✓ full forward secrecy



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

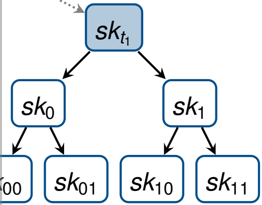
$(C, K) \leftarrow$ **Enc**(pk_B)



$K \leftarrow$ **Dec**(sk_B, C)
$sk_B \leftarrow$ **Punct**(sk_B, C)
$\approx sk_B \setminus C$

Evaluation

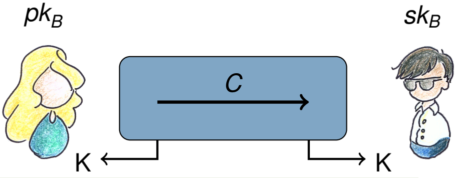
- ✓ full forward secrecy
- ✓ replay protection



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

$(C, K) \leftarrow$ **Enc**(pk_B)



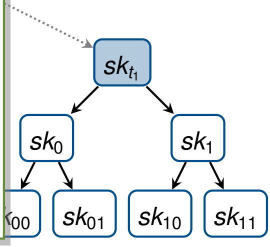
$K \leftarrow$ **Dec**(sk_B, C)

$sk_B \leftarrow$ **Punct**(sk_B, C)

$\approx sk_B \setminus C$

Evaluation (initial, based on BKP'14 HIBE)

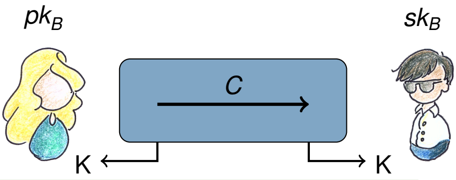
- ✓ full forward secrecy
- ✓ replay protection



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

$(C, K) \leftarrow$ **Enc**(pk_B)



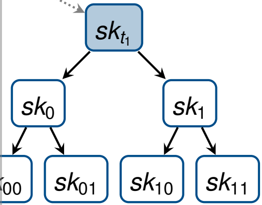
$K \leftarrow$ **Dec**(sk_B, C)
$sk_B \leftarrow$ **Punct**(sk_B, C)
$\approx sk_B \setminus C$

Evaluation (initial, based on BKP'14 HIBE)

✓ full forward secrecy

✓ replay protection

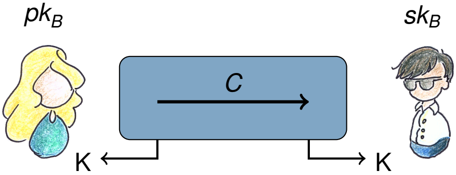
- time performance:
  ✓ **Enc** few ms



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

$(C, K) \leftarrow$ **Enc**(pk_B)



$K \leftarrow$ **Dec**(sk_B, C)

$sk_B \leftarrow$ **Punct**(sk_B, C)

$\approx sk_B \setminus C$

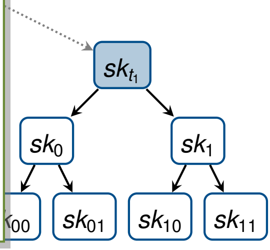
Evaluation (initial, based on BKP'14 HIBE)

✓ full forward secrecy

✓ replay protection

- time performance:

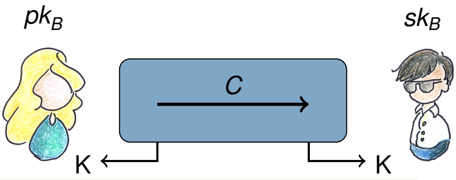
✓	**Enc**	few ms
?	**Dec**	few seconds



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

$(C, K) \leftarrow$ **Enc**(pk_B)



K $\leftarrow$ **Dec**(sk_B, C)

$sk_B \leftarrow$ **Punct**(sk_B, C)

$\approx sk_B \setminus C$

Evaluation (initial, based on BKP'14 HIBE)

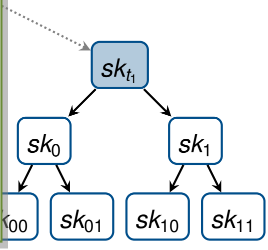
✓ full forward secrecy

✓ replay protection

- time performance:

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

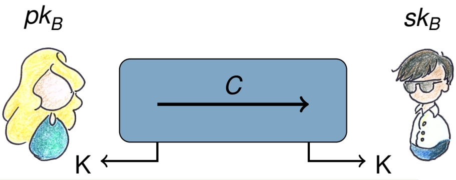
$\left.\right\}$ expensive delegation



Our Forward-Secret 0-RTT Key Exchange

In a Nutshell

$(C, K) \leftarrow \textbf{Enc}(pk_B)$



$K \leftarrow \textbf{Dec}(sk_B, C)$

$sk_B \leftarrow \textbf{Punct}(sk_B, C)$

$\approx sk_B \setminus C$

Evaluation (initial, based on BKP'14 HIBE)

✓ full forward secrecy

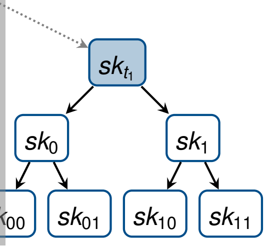
✓ replay protection

- time performance:

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

expensive delegation

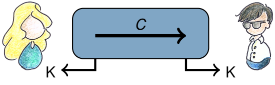
hope: need only **selective security**



Summary

Summary

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



$(C, K) \leftarrow \textbf{Enc}(pk_B)$

$K \leftarrow \textbf{Dec}(sk_B, C)$

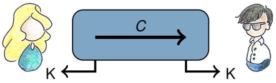
$sk_B \leftarrow \textbf{Punct}(sk_B, C)$

$\approx sk_B \setminus C$

Summary

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

$(C, K) \leftarrow \textbf{Enc}(pk_B)$



$K \leftarrow \textbf{Dec}(sk_B, C)$

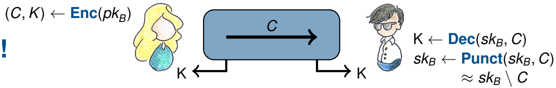
$sk_B \leftarrow \textbf{Punct}(sk_B, C)$

$\approx sk_B \setminus C$

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

Summary

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



$(C, K) \leftarrow$ **Enc**(pk_B)

C

K

K

$K \leftarrow$ **Dec**(sk_B, C)
$sk_B \leftarrow$ **Punct**(sk_B, C)
$\approx sk_B \setminus C$

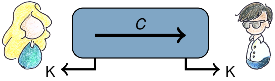
- Generic construction and security proof
  - very simple single-message protocol
  - building block: puncturable forward-secret key encapsulation
  - from any HIBKEM

- Can we make this practical?

Summary

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

$(C, K) \leftarrow \textbf{Enc}(pk_B)$



$K \leftarrow \textbf{Dec}(sk_B, C)$
$sk_B \leftarrow \textbf{Punct}(sk_B, C)$
$\approx sk_B \setminus C$

- 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**

P.S. Britta and Felix plan on finishing their Ph.D. in the next year resp. months and interesting job offers are always welcome.