0-RTT Key Establishment with Full Forward Secrecy

Felix Günther[1] ***Britta Hale***[2] *Tibor Jager*[3] *Sebastian Lauer*[4]

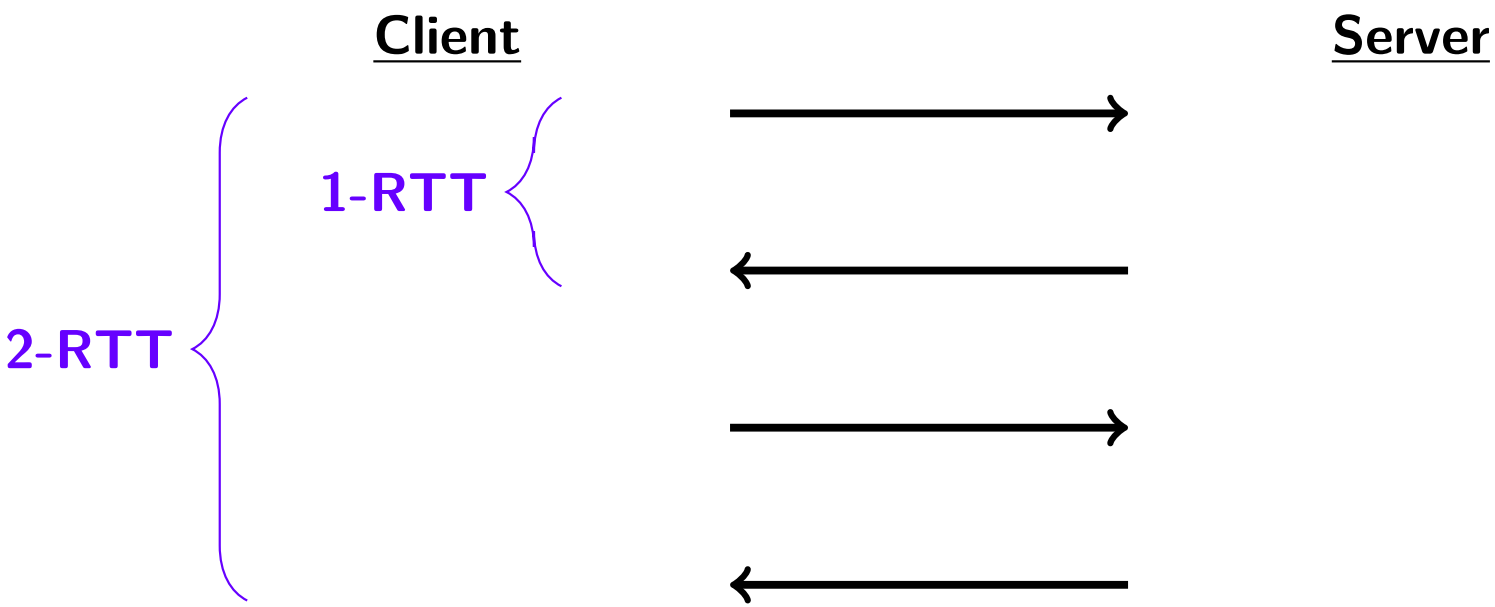
[1]Technischen Universität Darmstadt
[2]NTNU Norwegian University of Science and Technology
[3]Paderborn University
[4]Ruhr-Universität Bochum

Eurocrypt 2017

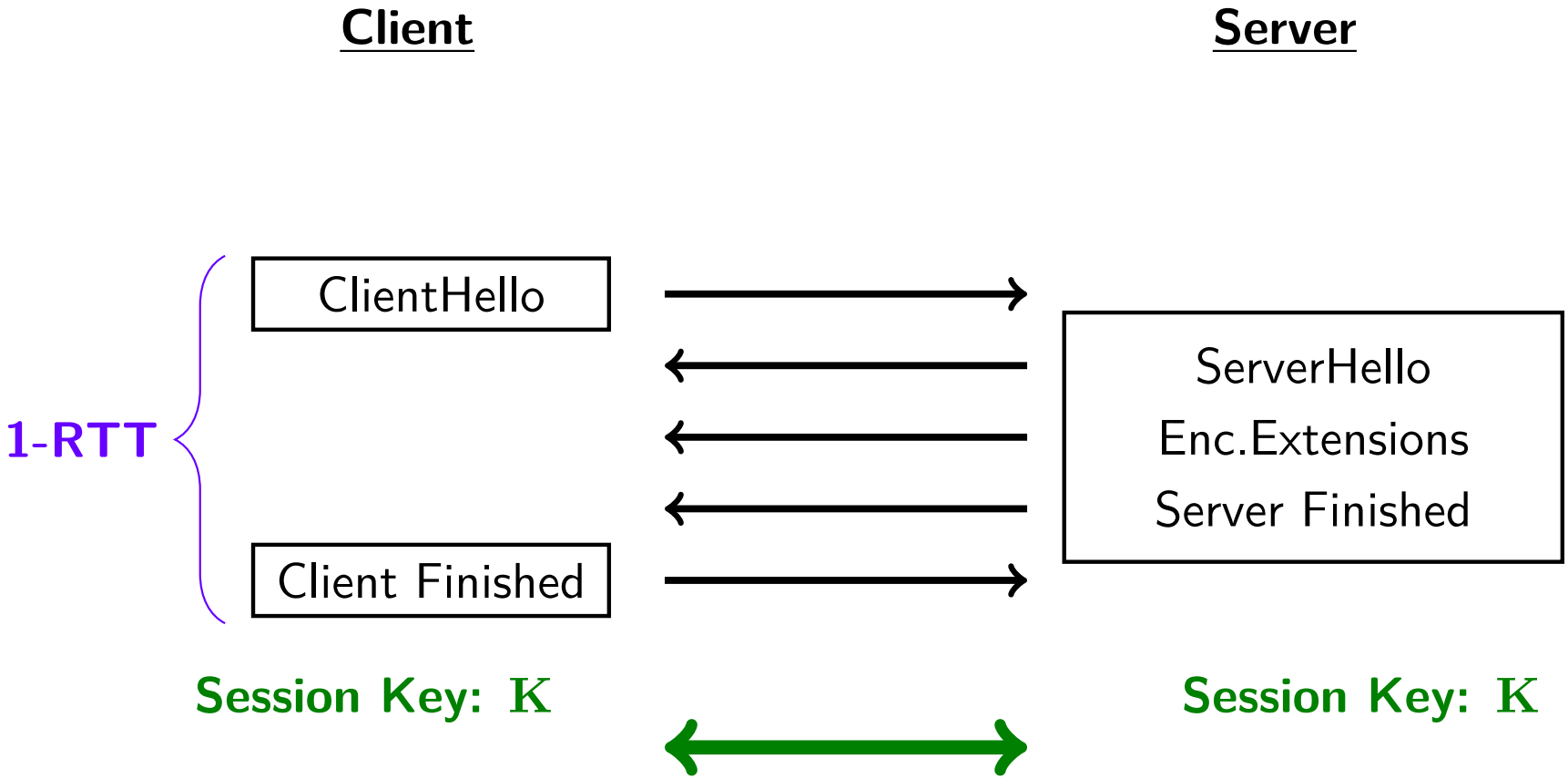
0-RTT with full forward secrecy

Yes, it is possible!

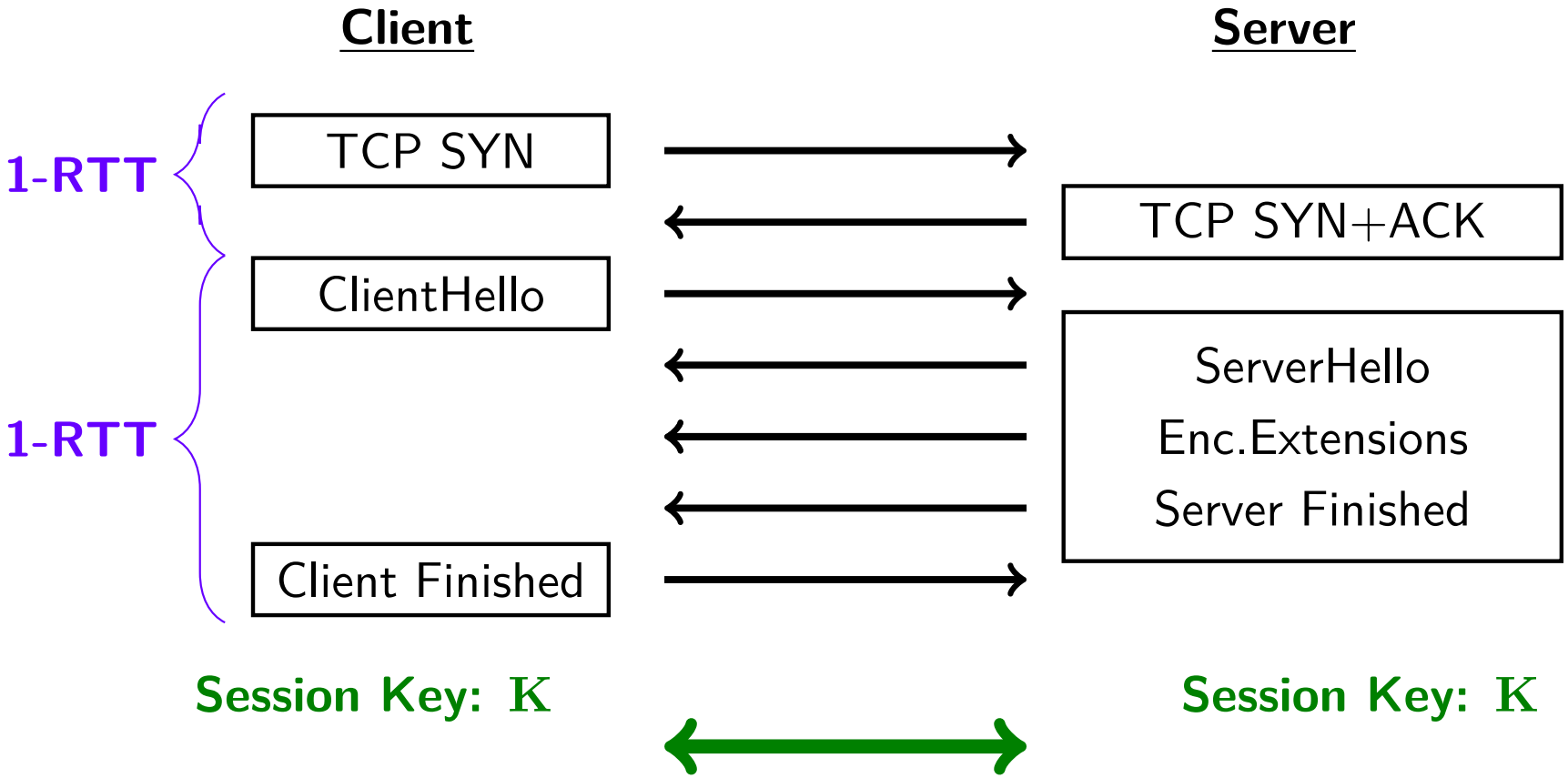
Round-Trip Time (RTT)



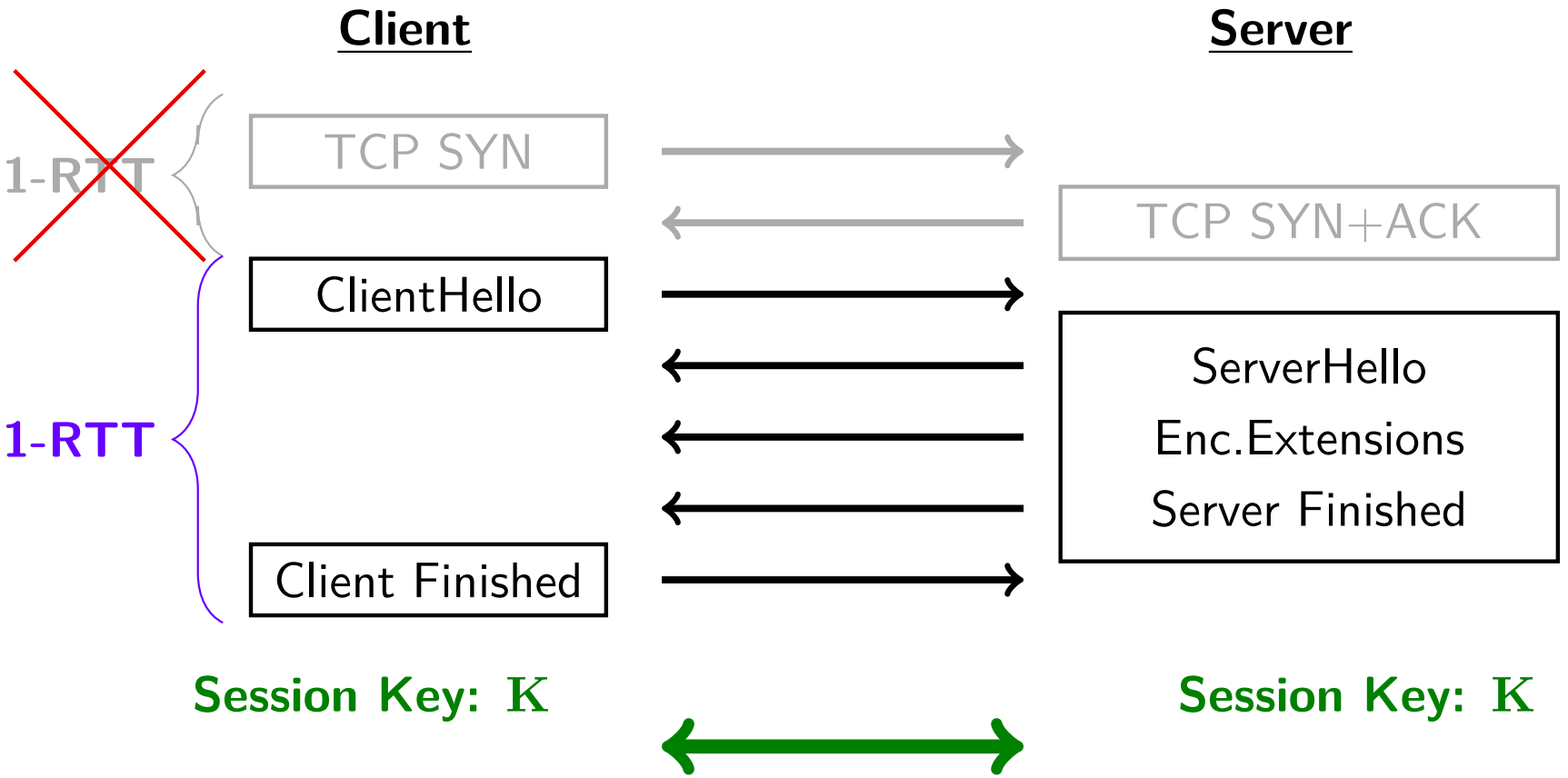
TLS+TCP:


Client
Server
ClientHello
ServerHello
Enc.Extensions
Server Finished
Client Finished
1-RTT
Session Key: K
Session Key: K

TLS+TCP:

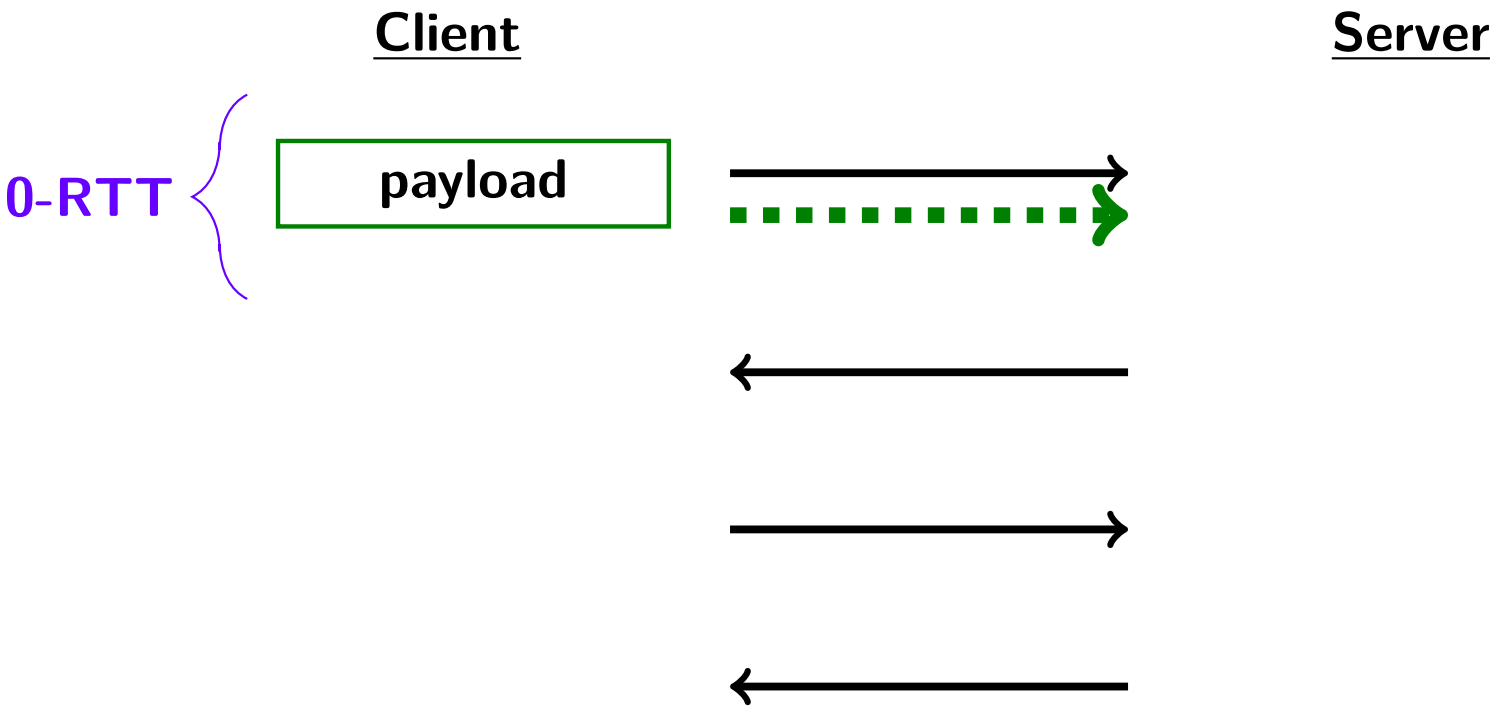

Client
Server
1-RTT
TCP SYN
TCP SYN+ACK
ClientHello
1-RTT
ServerHello
Enc.Extensions
Server Finished
Client Finished
Session Key: K
Session Key: K

TLS + UDP:


Client
Server
1-RTT
TCP SYN
TCP SYN+ACK
ClientHello
1-RTT
ServerHello
Enc.Extensions
Server Finished
Client Finished
Session Key: K
Session Key: K

Why not send cryptographically protected payload ***immediately***?

Zero Round-Trip Time (0-RTT)



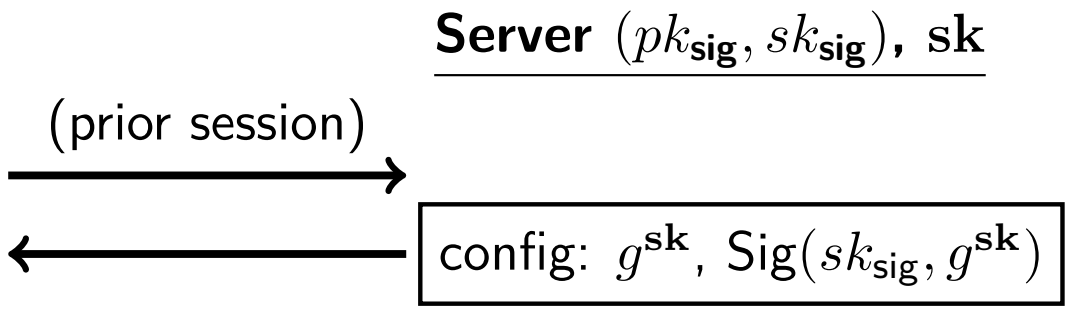
- **QUIC** by ...

- **QUIC** by ...

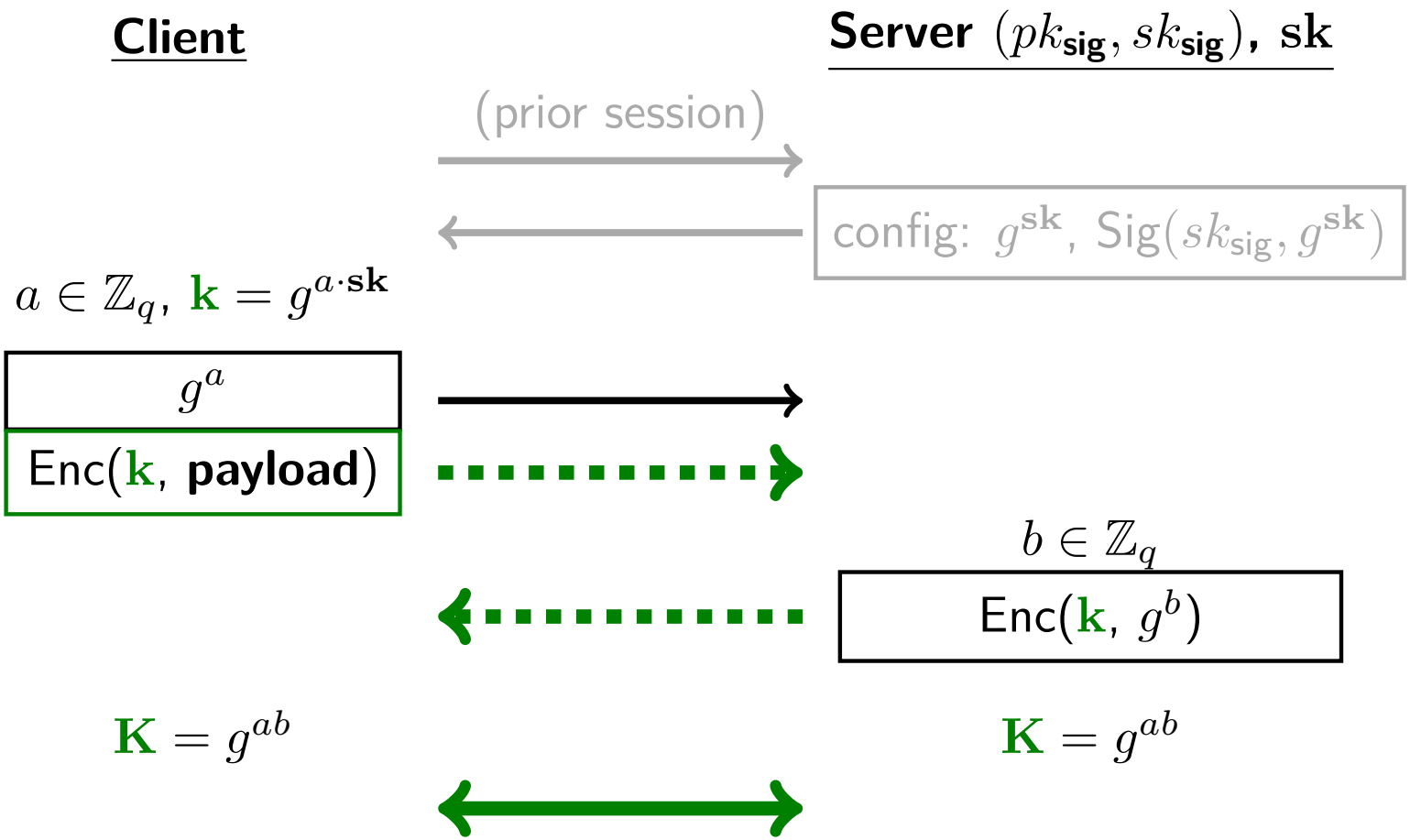
https://commons.wikimedia.org

(Quick UDP Internet Connections)

QUIC Protocol

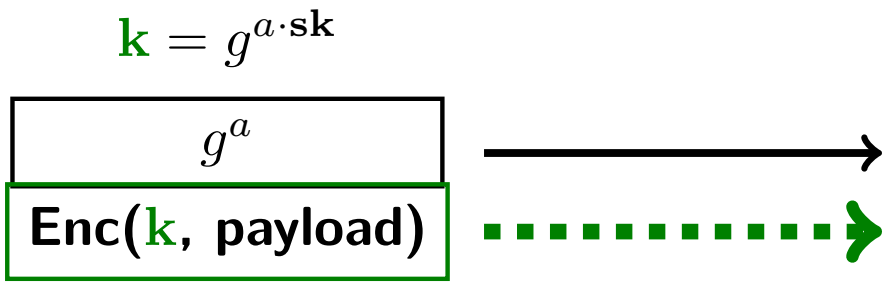


QUIC Protocol

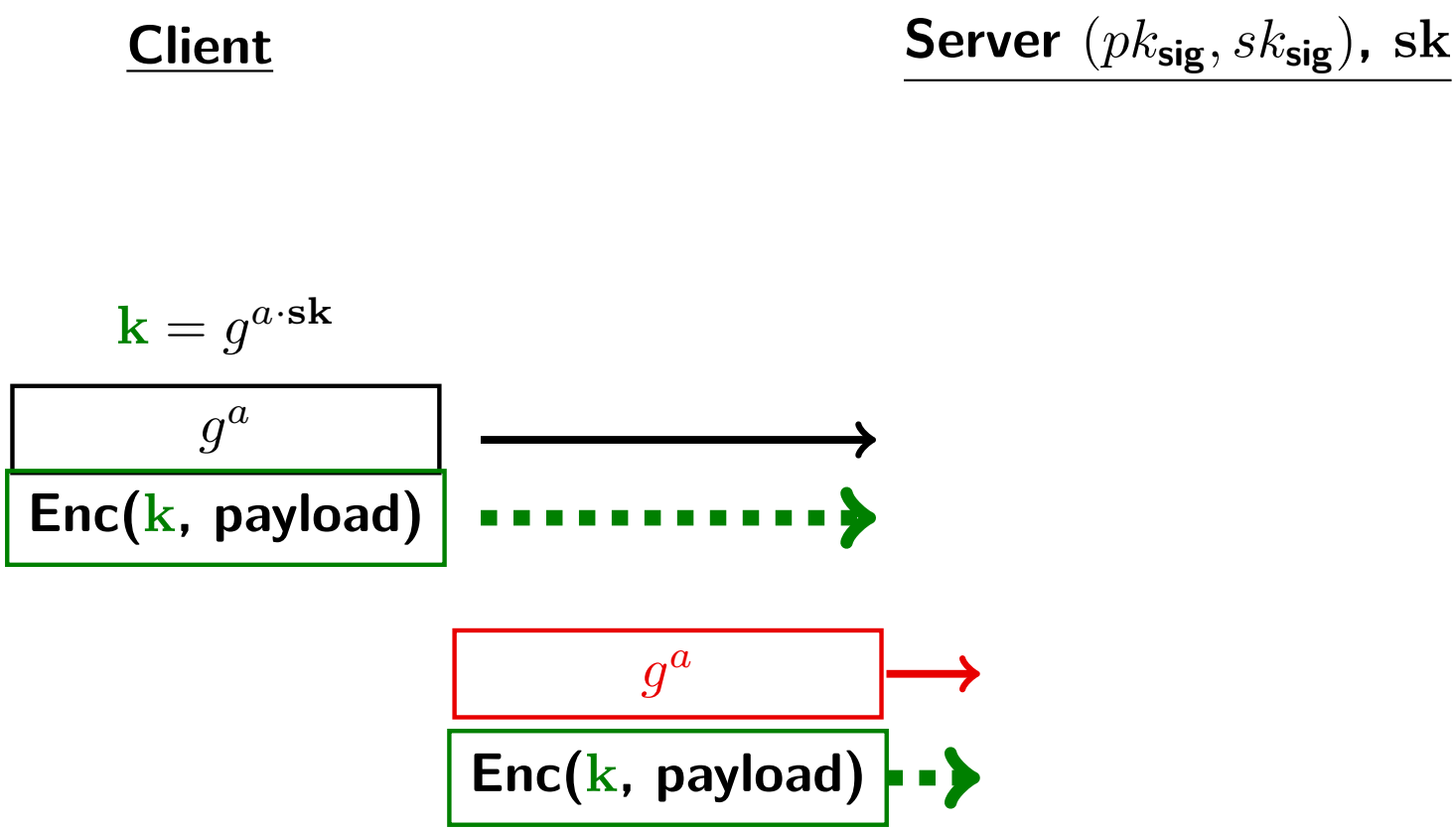


QUIC Protocol Issues: **Replay**

Client | **Server** $(pk_{\text{sig}}, sk_{\text{sig}})$, $\mathbf{sk}$



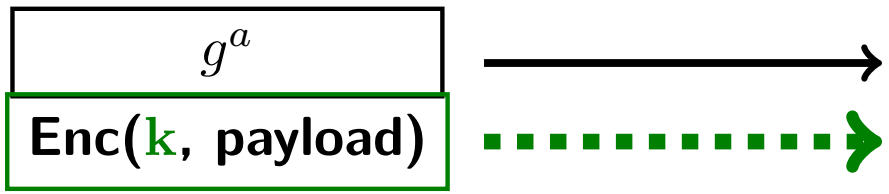
QUIC Protocol Issues: **Replay**



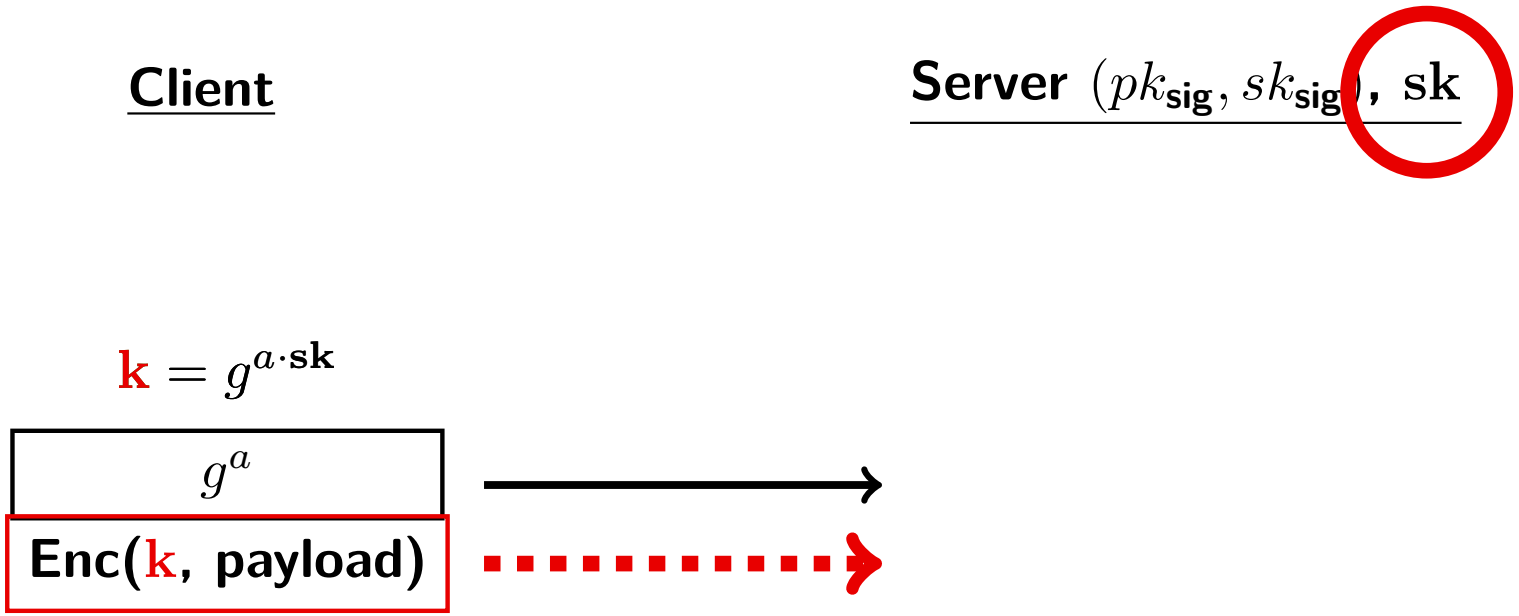
QUIC Protocol Issues: **Forward Secrecy**

Client

Server $(pk_{\text{sig}}, sk_{\text{sig}})$, $\mathbf{sk}$

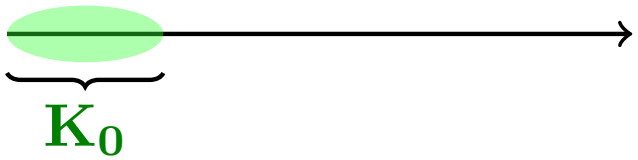


QUIC Protocol Issues: **Forward Secrecy**

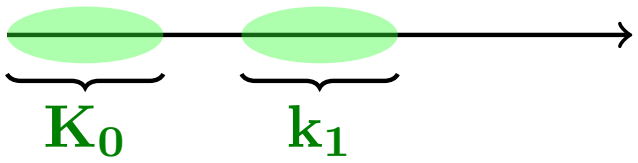


Forward Secrecy Threat Landscape:

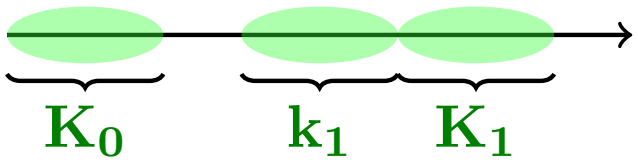
Forward Secrecy Threat Landscape:



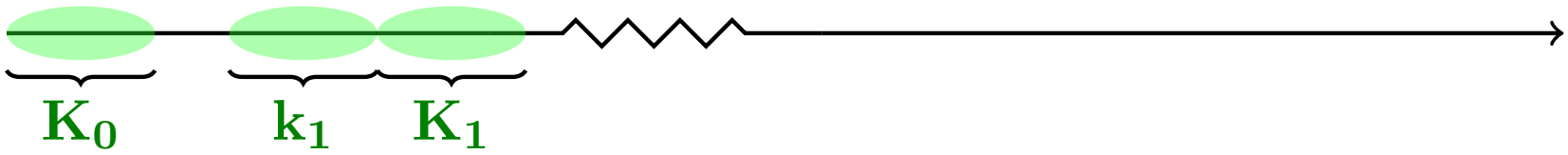
Forward Secrecy Threat Landscape:



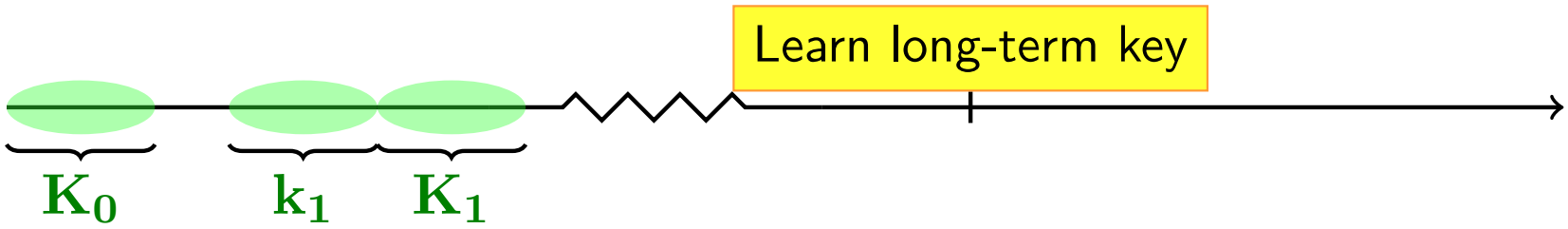
Forward Secrecy Threat Landscape:



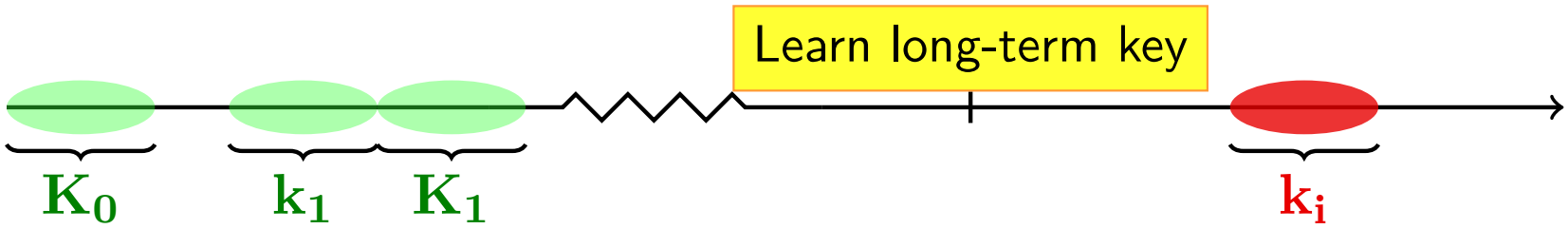
Forward Secrecy Threat Landscape:



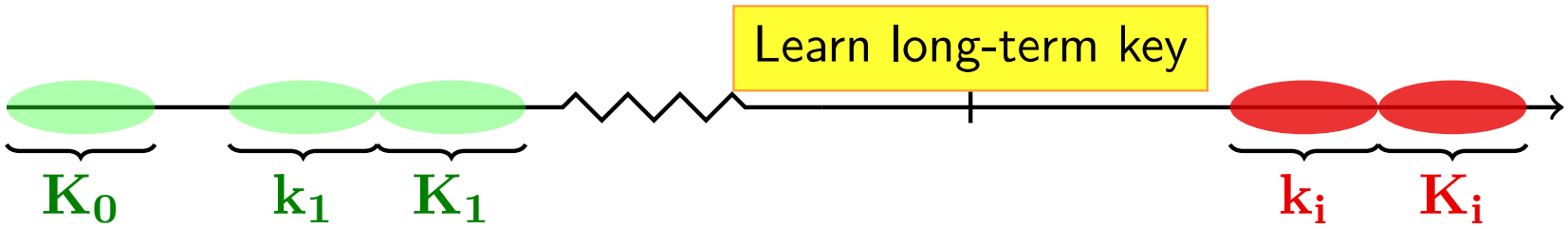
Forward Secrecy Threat Landscape:



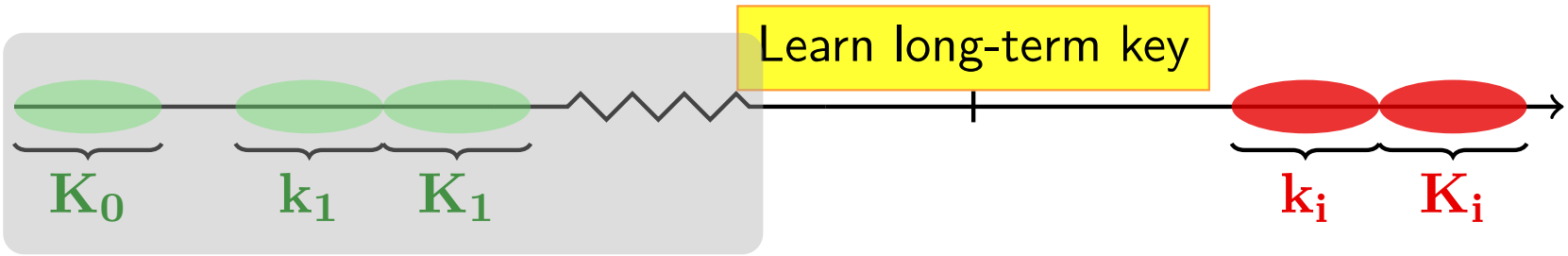
Forward Secrecy Threat Landscape:



Forward Secrecy Threat Landscape:

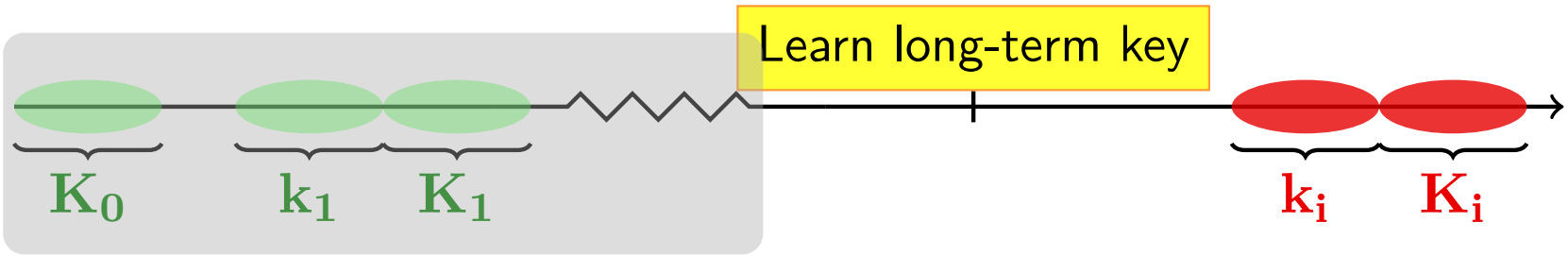


Forward Secrecy Threat Landscape:



Are past session keys secure?

Forward Secrecy Threat Landscape:



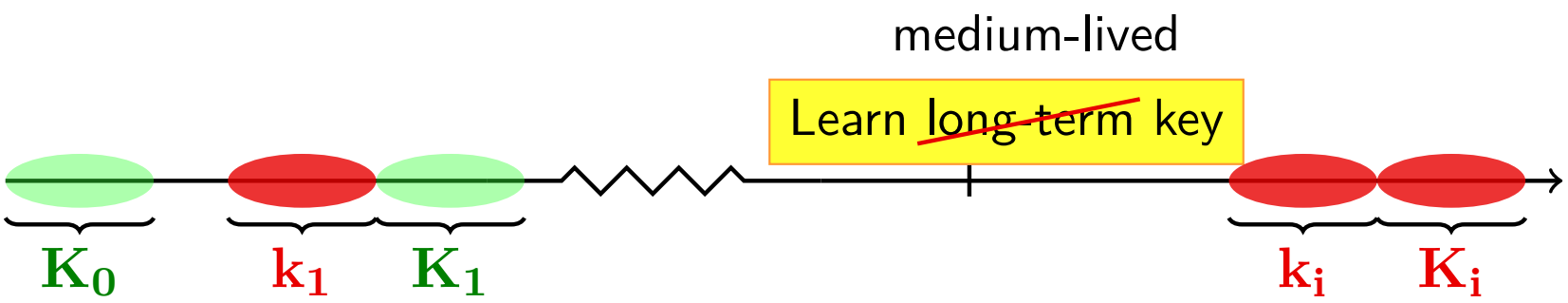
Are past session keys secure?

Perfect Forward Secrecy:

Long-term key compromised

Past session keys remain secure

QUIC



Is Perfect Forward Secrecy even possible for 0-RTT?

Yes!

Yes!

Our design:

- **Full Forward Secrecy**

Yes!

Our design:

- **Full Forward Secrecy**
- **Replay protection**

Yes!

Our design:

- **Full Forward Secrecy**
- **Replay protection**
- Based on hierarchical ID-based key encapsulation mechanism (with selective security)
  and one-time signatures

Yes!

Our design:

- **Full Forward Secrecy**
- **Replay protection**
- Based on hierarchical ID-based key encapsulation mechanism (with selective security) and one-time signatures
- Flexible to different instantiations/assumptions
  - post-quantum
  - pairings
  - etc...

Core idea:

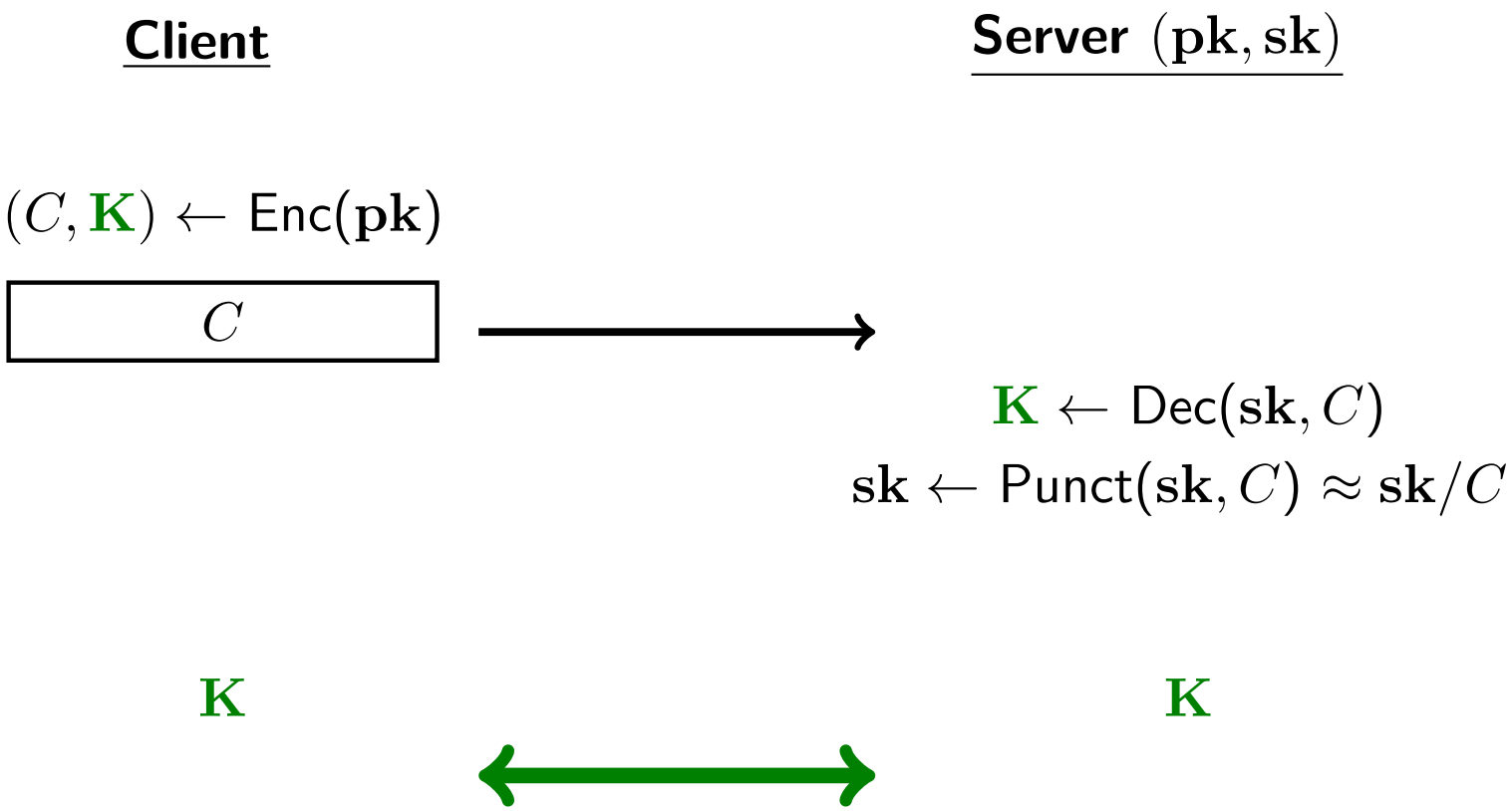
Server: static public key –
private key can be updated

$\rightarrow$ **Forward Secret KEM**

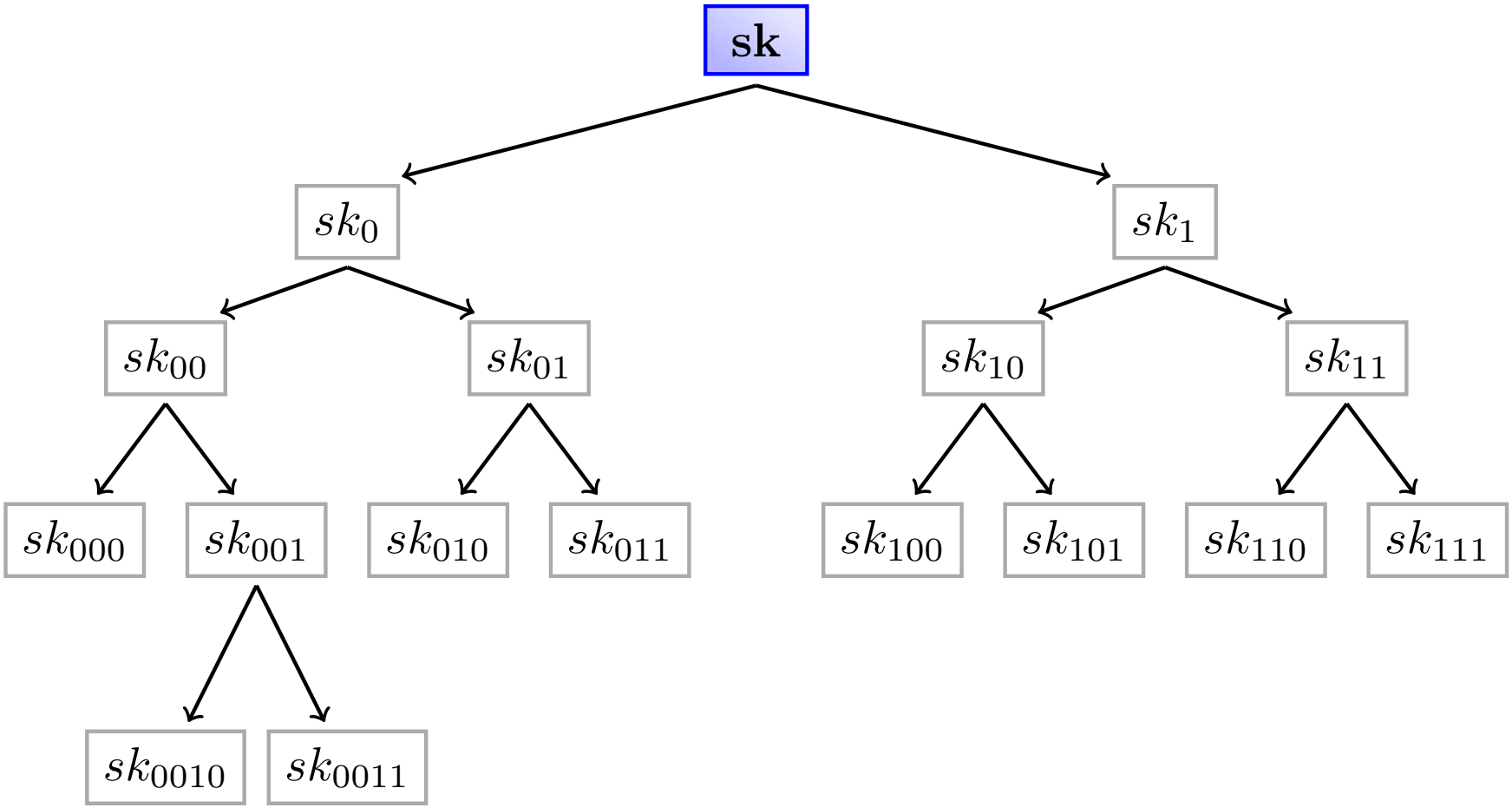
$\rightarrow$ **Forward Secret 0-RTT KE**

Forward Secure 0-RTT KE

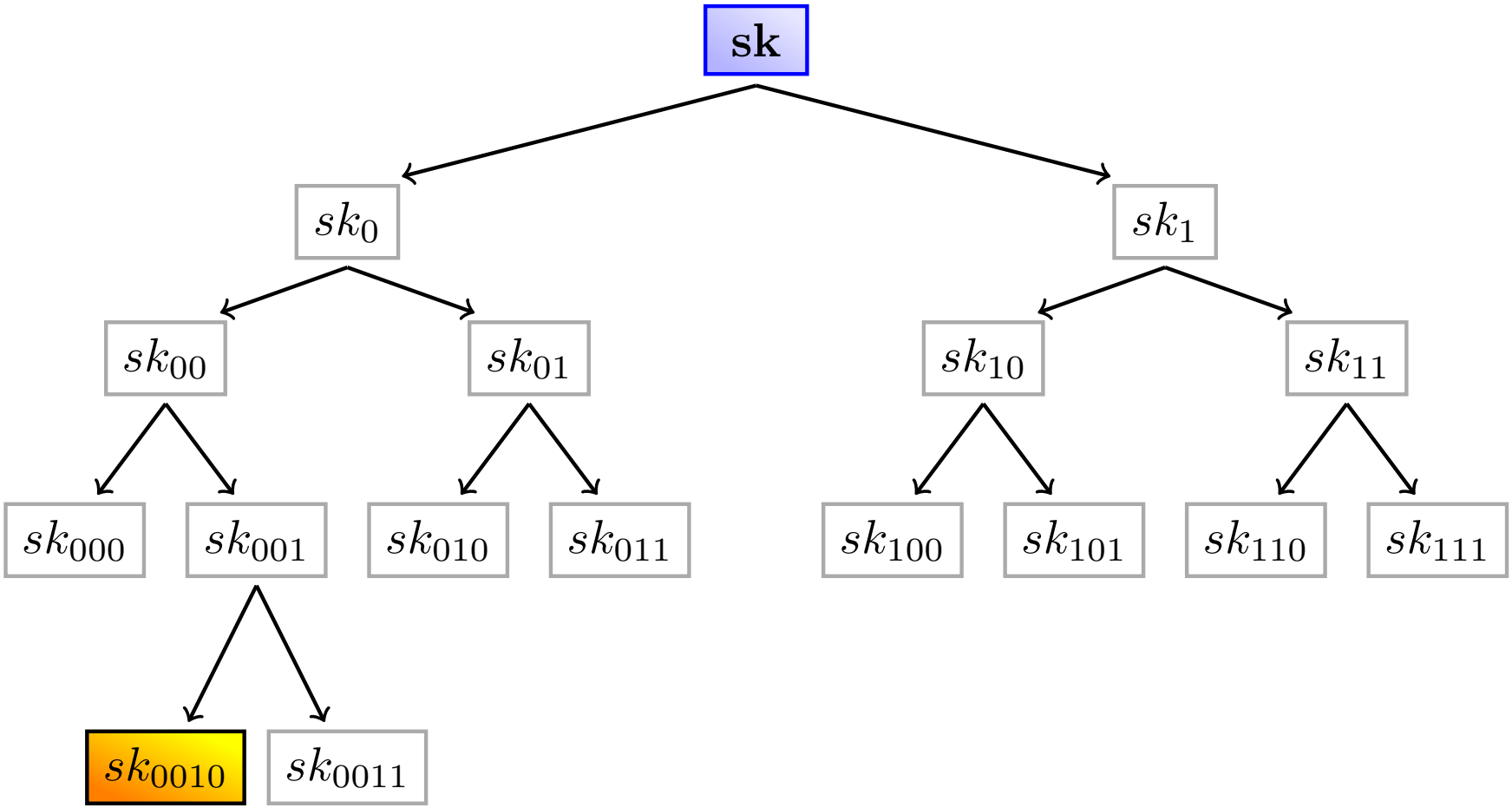
Core idea:



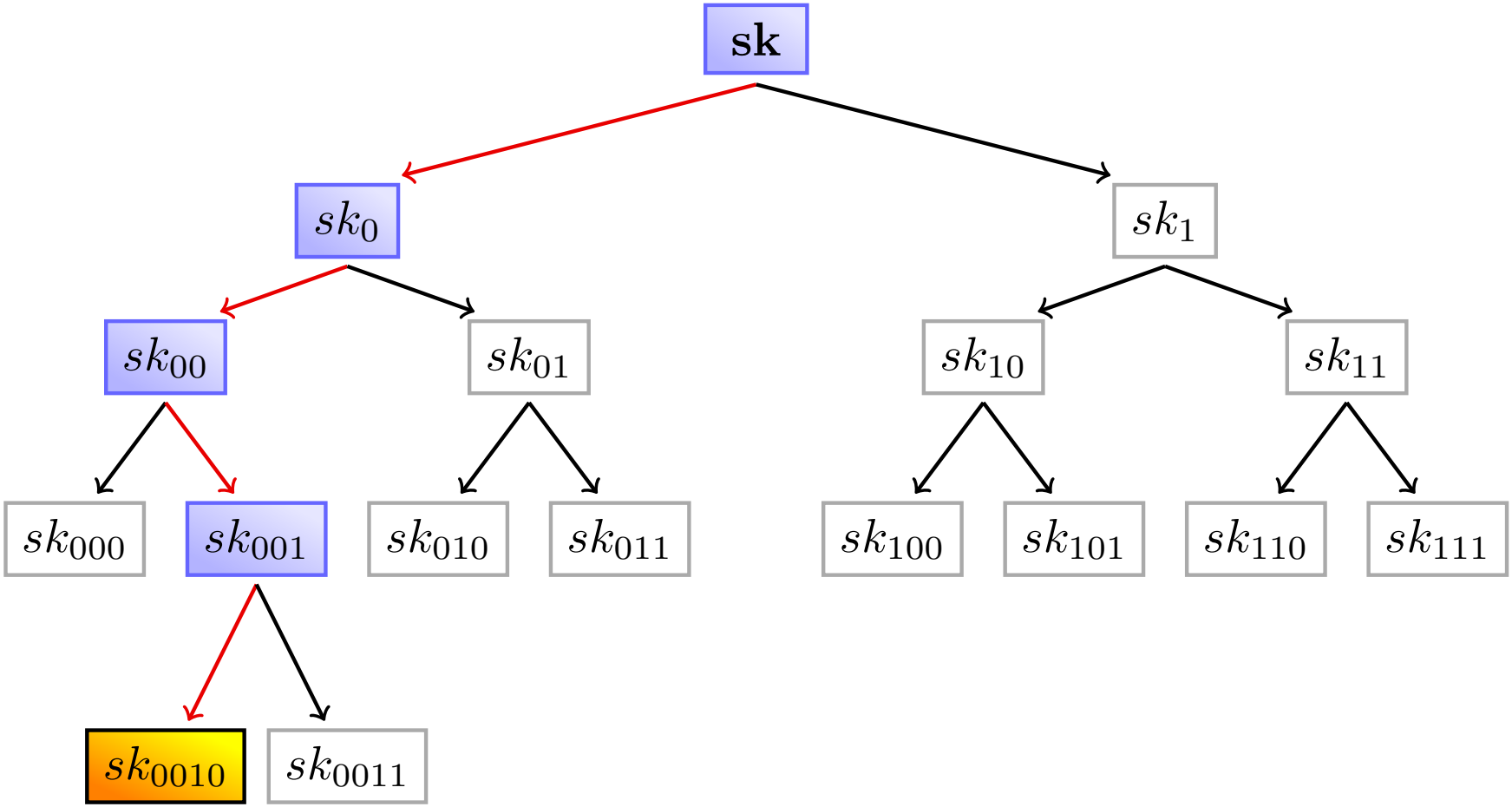
Hierarchical ID-Based KEM



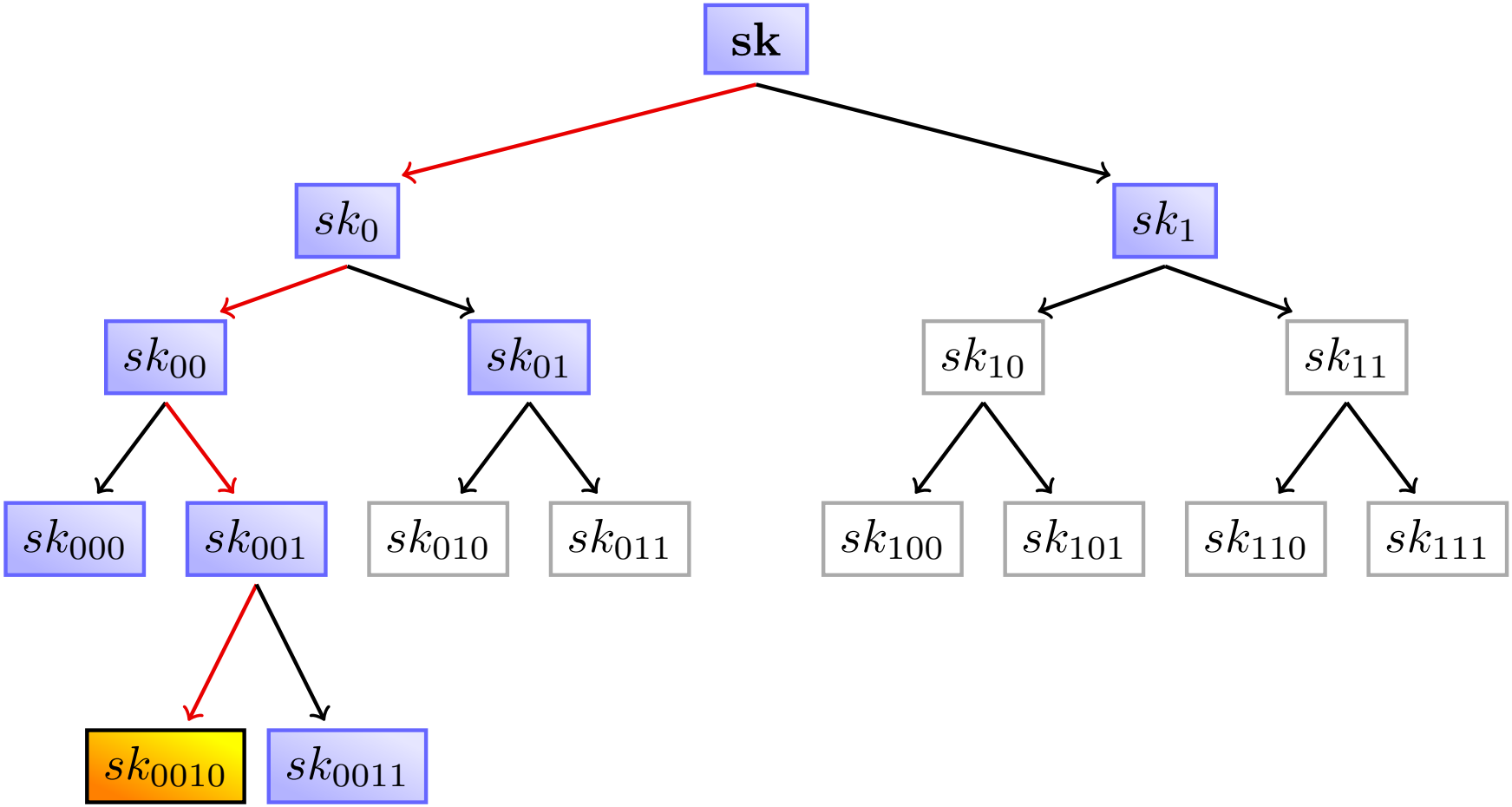
Hierarchical ID-Based KEM



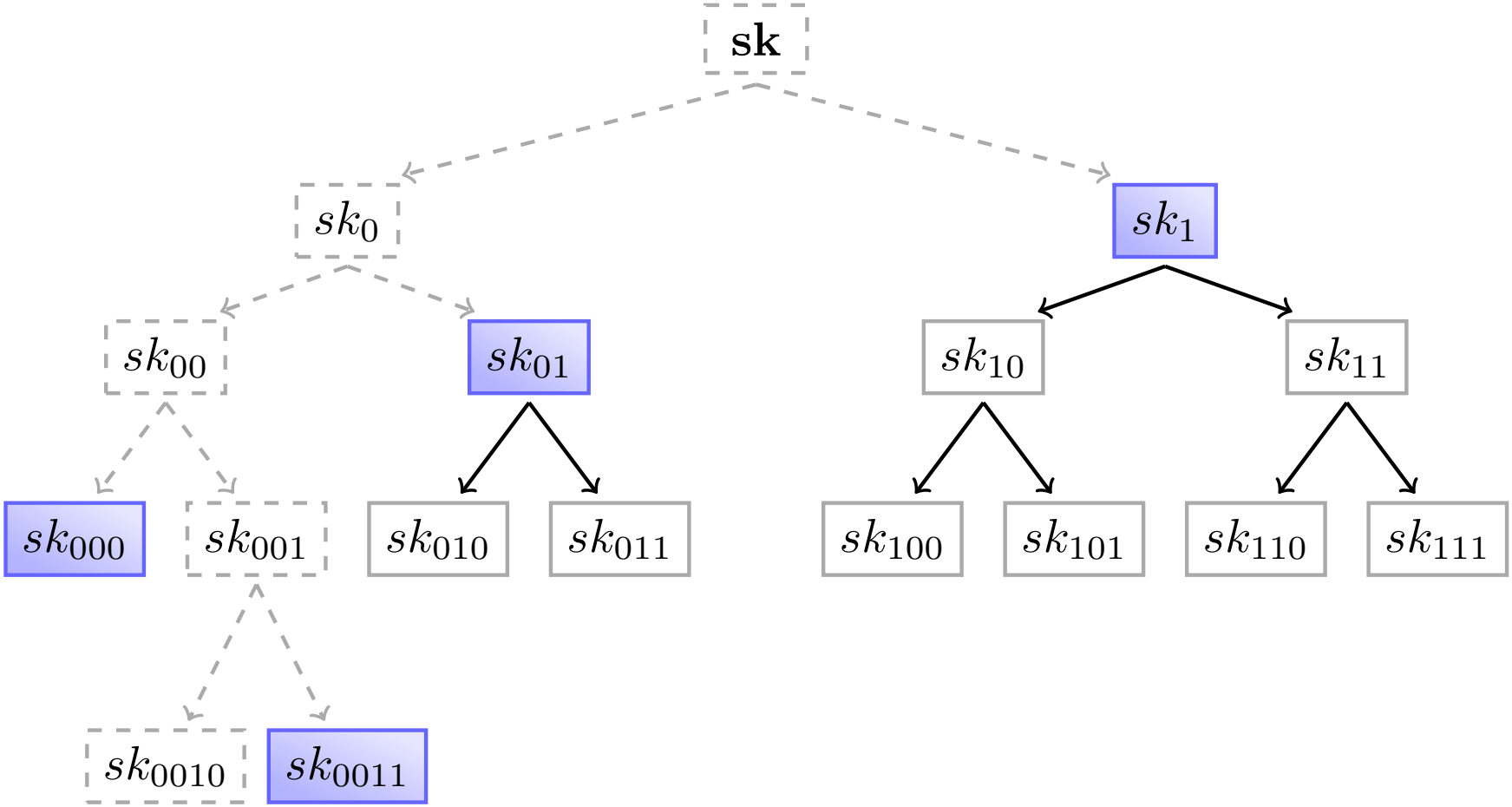
Puncturing private key $\mathbf{sk}$



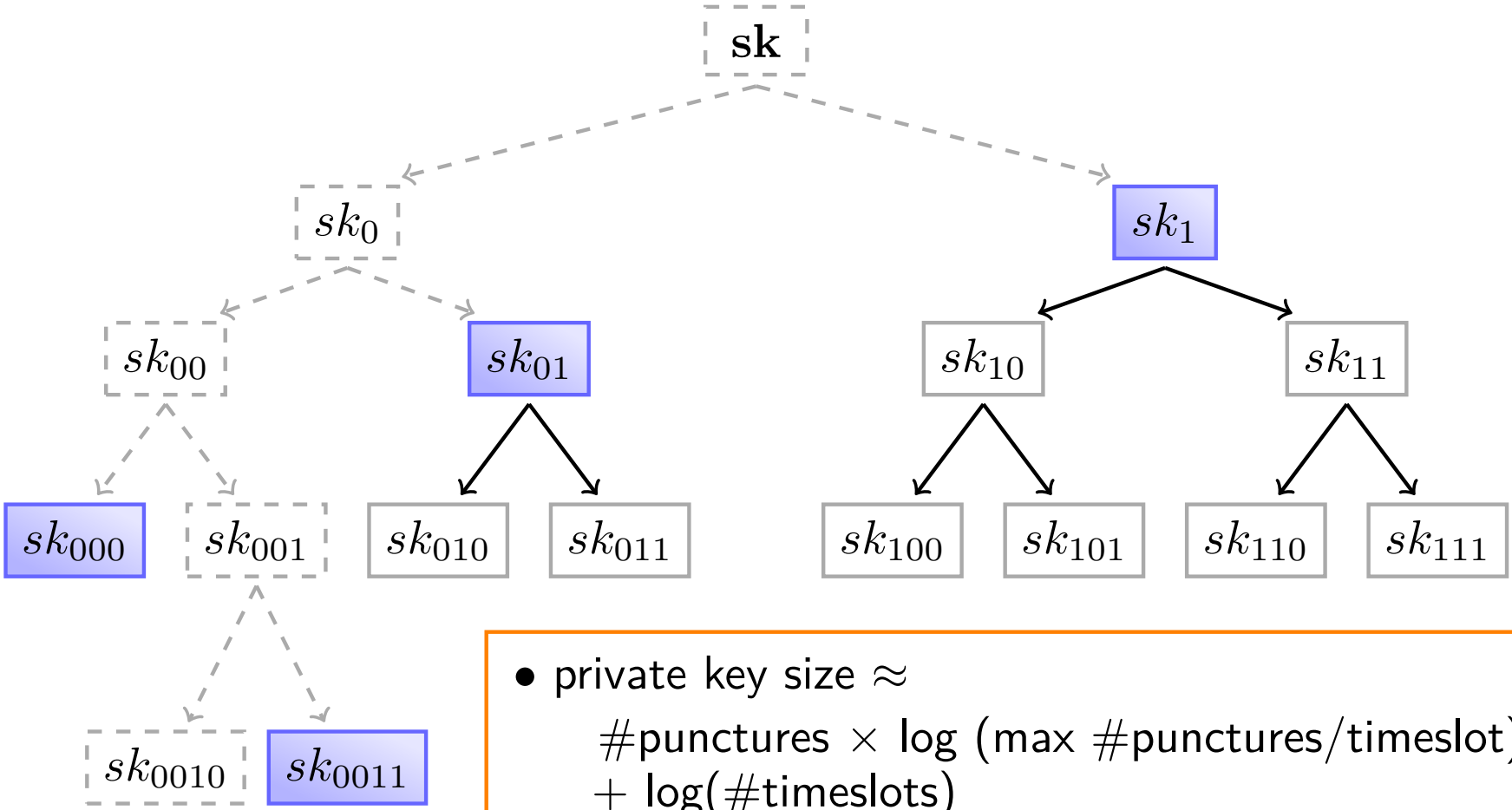
Puncturing private key $\mathbf{sk}$



Puncturing private key $\mathbf{sk}$

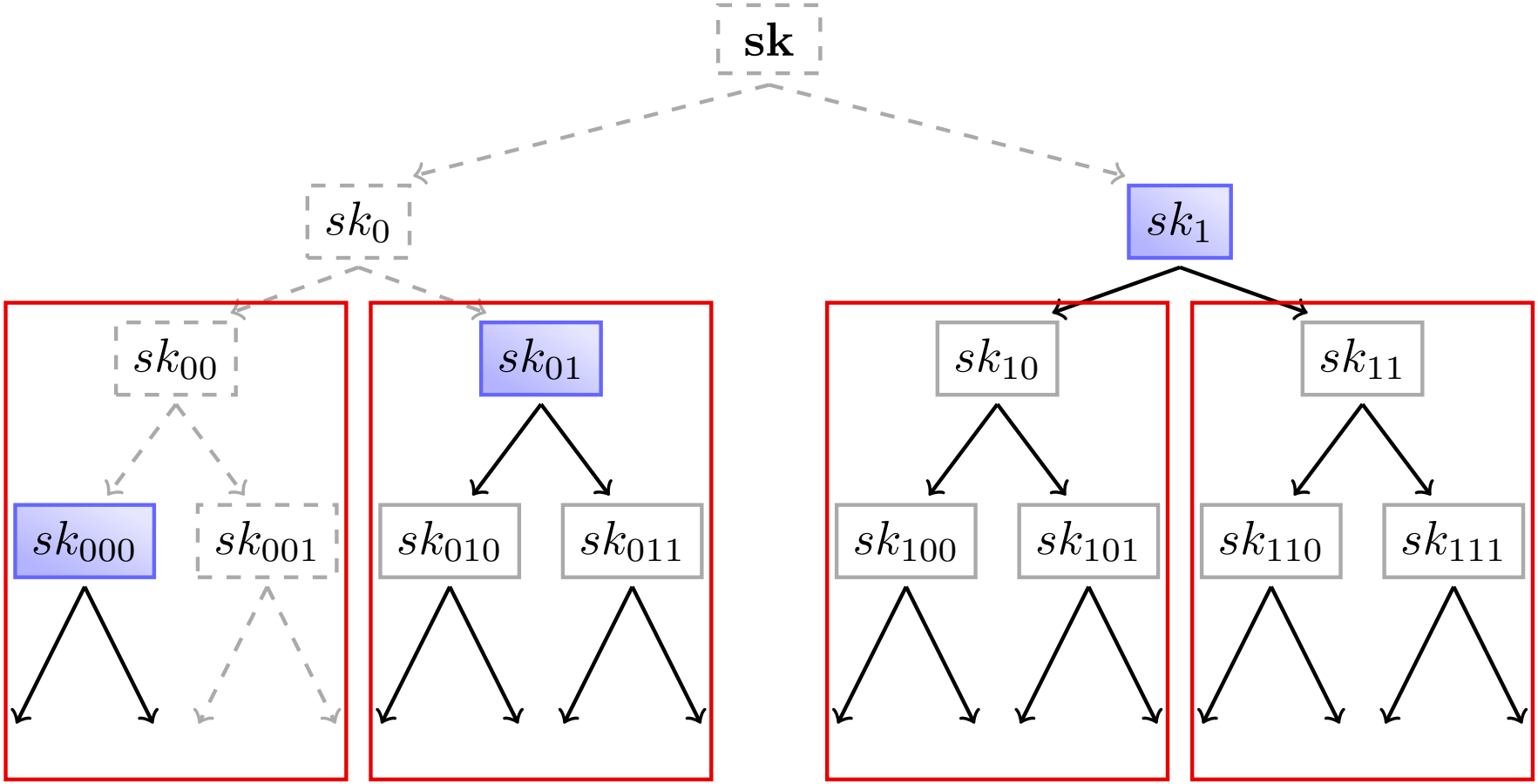


Puncturing private key $\mathbf{sk}$

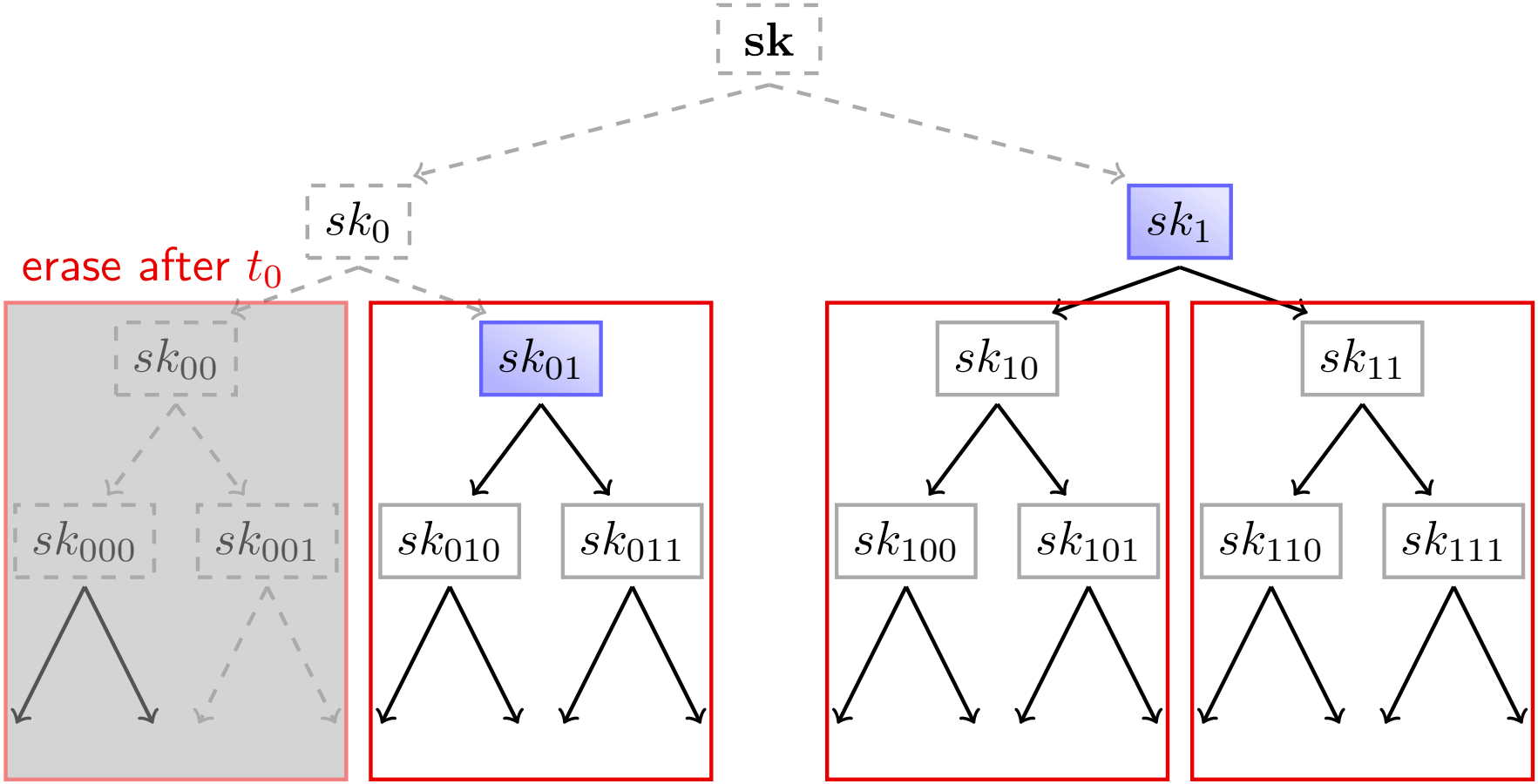


- private key size $\approx$
  #punctures $\times$ log (max #punctures/timeslot)
  $+$ log(#timeslots)
- #punctures $=$ #sessions

Purging the private key: time sync intervals $t_0, t_1, \ldots$



Purging the private key: time sync intervals $t_0, t_1, \ldots$



Evaluation:

Barreto-Naehrig elliptic curve P256, bilinear pairing, $\mathbf{pk}$ 128bits, one-time sig pk 256bits, timeslot length 30bits, avg. clock rate 3.2GHz

- Enc: ms
- Dec: seconds
- Puncturing: seconds

Evaluation:

Barreto-Naehrig elliptic curve P256, bilinear pairing, $\mathbf{pk}$ 128bits, one-time sig pk 256bits, timeslot length 30bits, avg. clock rate 3.2GHz

- Enc: ms
- Dec: seconds
- Puncturing: seconds $\rightarrow$ **need only selective security**

...Room for improvement?

Evaluation:

Barreto-Naehrig elliptic curve P256, bilinear pairing, $\mathbf{pk}$ 128bits, one-time sig pk 256bits, timeslot length 30bits, avg. clock rate 3.2GHz

- Enc: ms
- Dec: seconds
- Puncturing: seconds $\rightarrow$ **need only selective security**

...Room for improvement?

... vs. Green and Myers S&P '15:

- Any HIBE vs. specific bilinear groups
- CCA-secure in standard model vs. ROM

Now:

- FS 0-RTT key exchange + security model
- Generic construction + security proof
  (from one-time signatures and
  any hierarchical ID-based KEM with selective security)

Summary

Now:

- FS 0-RTT key exchange + security model
- Generic construction + security proof
  (from one-time signatures and
  any hierarchical ID-based KEM with selective security)

Future:

- Optimize KEM key delegation
- Make it practical!

Questions

?

ACKNOWLEDGEMENTS

Some slide designs are based on presentations of the same work by co-authors Felix Günther and Tibor Jager