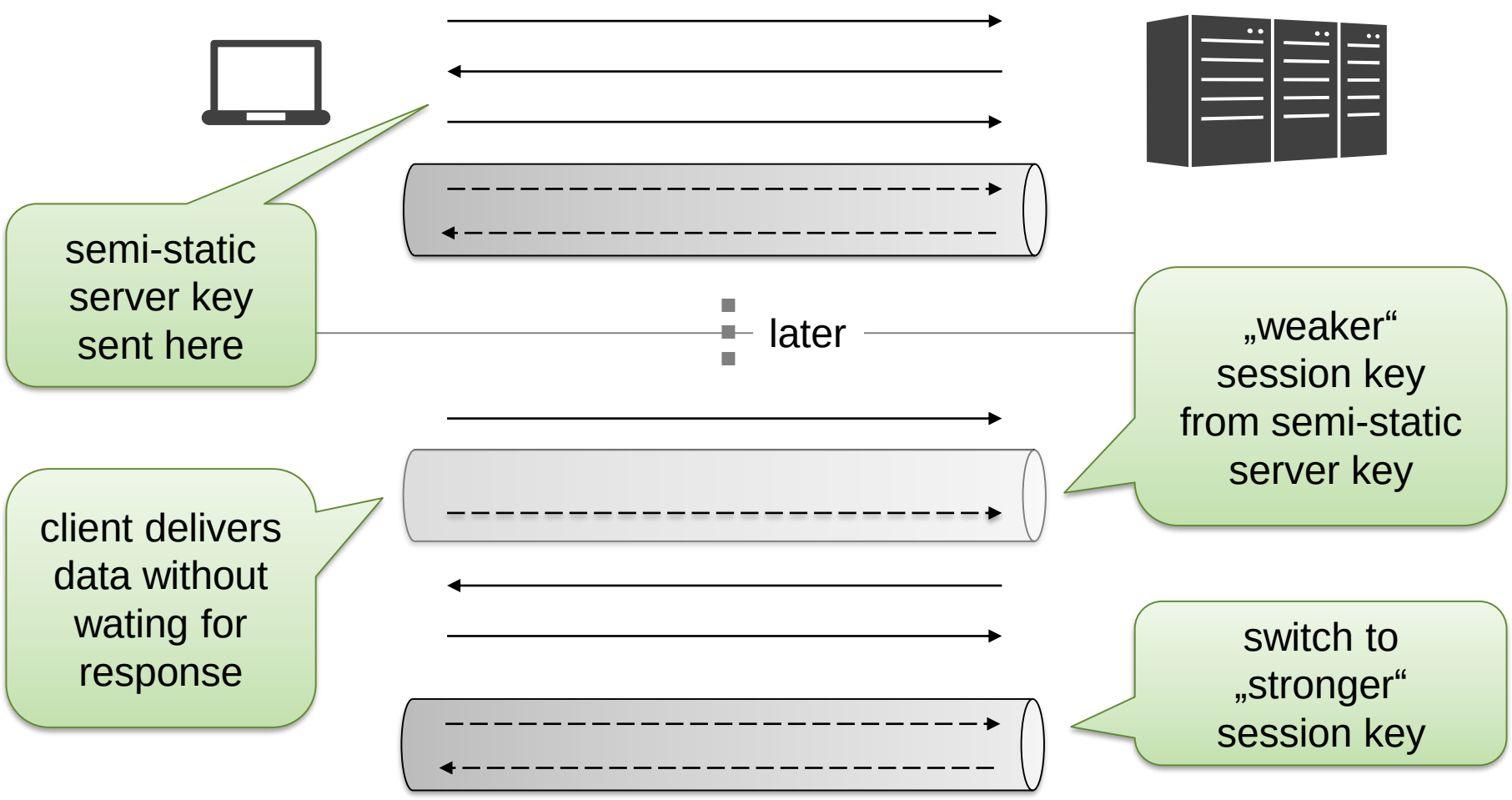
Part V
Zero Round-Trip Time (0RTT)

8th BIU Winter School on Key Exchange, 2018

Marc Fischlin

Zero Round-Trip Time

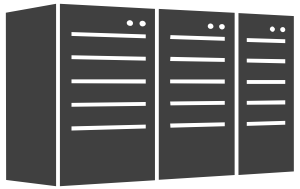


0RTT in QUIC

semi-static server key g^s

ephemeral key e, g^e

$K_1 = \mathrm{KDF}(\mathrm{DH}(e, g^s))$



semi-static server key s

g^e

$\{\mathrm{data}\}_{K_1}$

$\{g^t\}_{K_1}$

$K_1 = \mathrm{KDF}(\mathrm{DH}(g^e, s))$

ephemeral key t, g^t

$K_2 = \mathrm{KDF}(\mathrm{DH}(e, g^t))$

$K_2 = \mathrm{KDF}(\mathrm{DH}(g^e, t))$

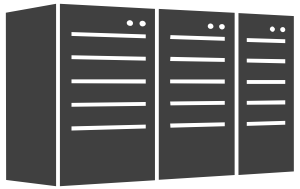
$\{\mathrm{data}\}_{K_2}$

Replay Attacks on QUIC?

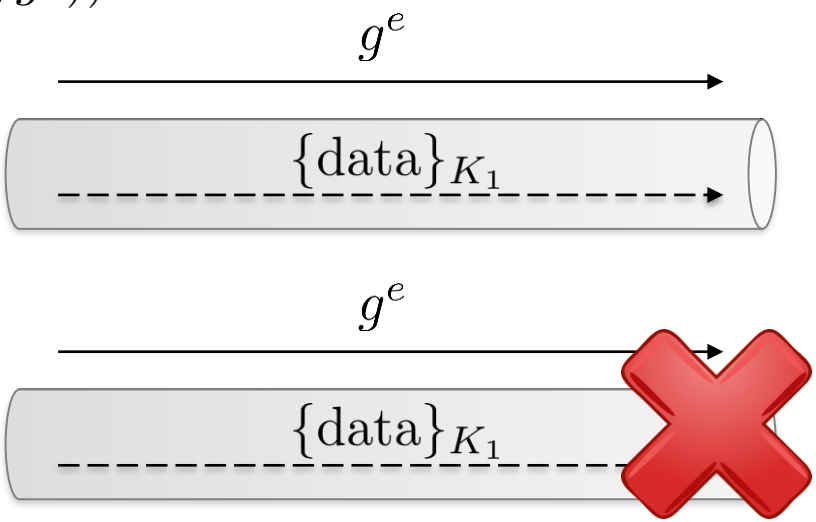
semi-static server key g^s

ephemeral key e, g^e

$K_1 = \mathrm{KDF}(\mathrm{DH}(e, g^s))$



semi-static server key s

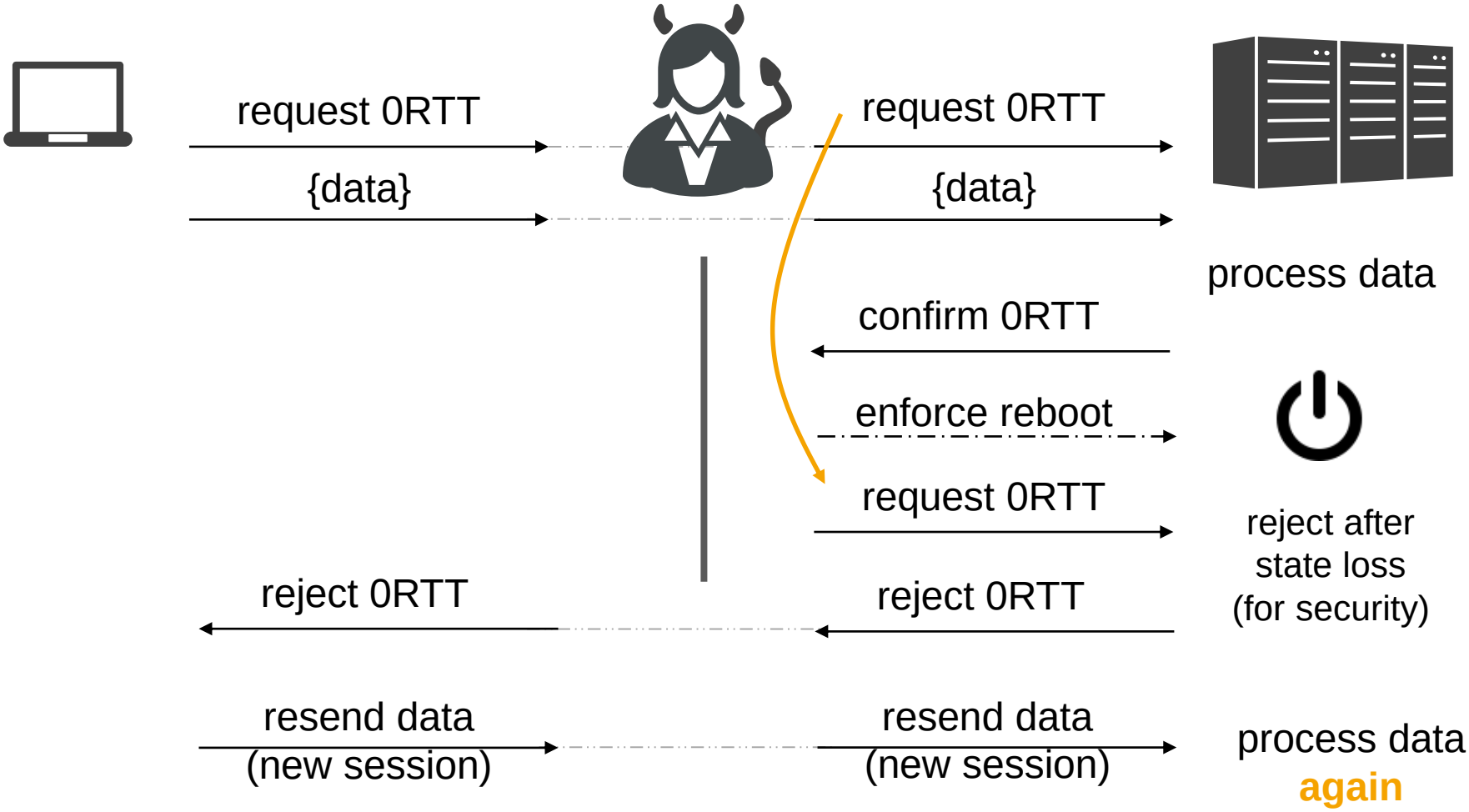


server stores previously received keys g^e

(not anymore in latest version of QUIC)

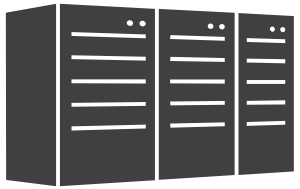
Replay Problems are Inherent (even with State)

Daniel Kahn Gillmor in IETF TLS 1.3 discussions



DH-0RTT in TLS 1.3 draft-12 (I)

switched to pre-shared-key 0RTT in later drafts



ClientHello
ClientKeyShare

ServerHello
ServerKeyShare

handshake key

handshake key

{ServerConfiguration*}
{ServerCertificate*}
{ServerCertificateVerify*}
{ServerFinished}

include semi-static key g^s here

{ClientCertificate*}
{ClientCertificateVerify*}
{ClientFinished}

channel key

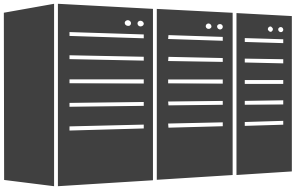
channel key

DH-0RTT in TLS 1.3 `draft-12` (II)

`CH` $r_c \leftarrow \{0,1\}^{256}$

`CKS` g^x

`ClientEarlyData`



semi-static server key g^s

`early_secret` $\leftarrow \mathrm{HKDF}(g^{sx}, \mathrm{trans})$

`{ClientCertificate0*}`

`{ClientCertificateVerify0*}`

`{ClientFinished0}`

`early_secret`

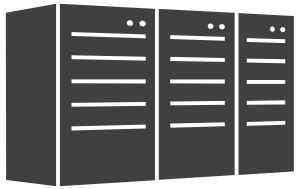
`{data}`

run full handshake from `ServerHello` onwards

...

0RTT-PSK since draft-19

only Pre-Shared-Key variant from draft 19 on



PSK

PSK

handshake key

ClientHello
ClientKeyShare*
early_data
psk_key_exchange_modes
pre_shared_key

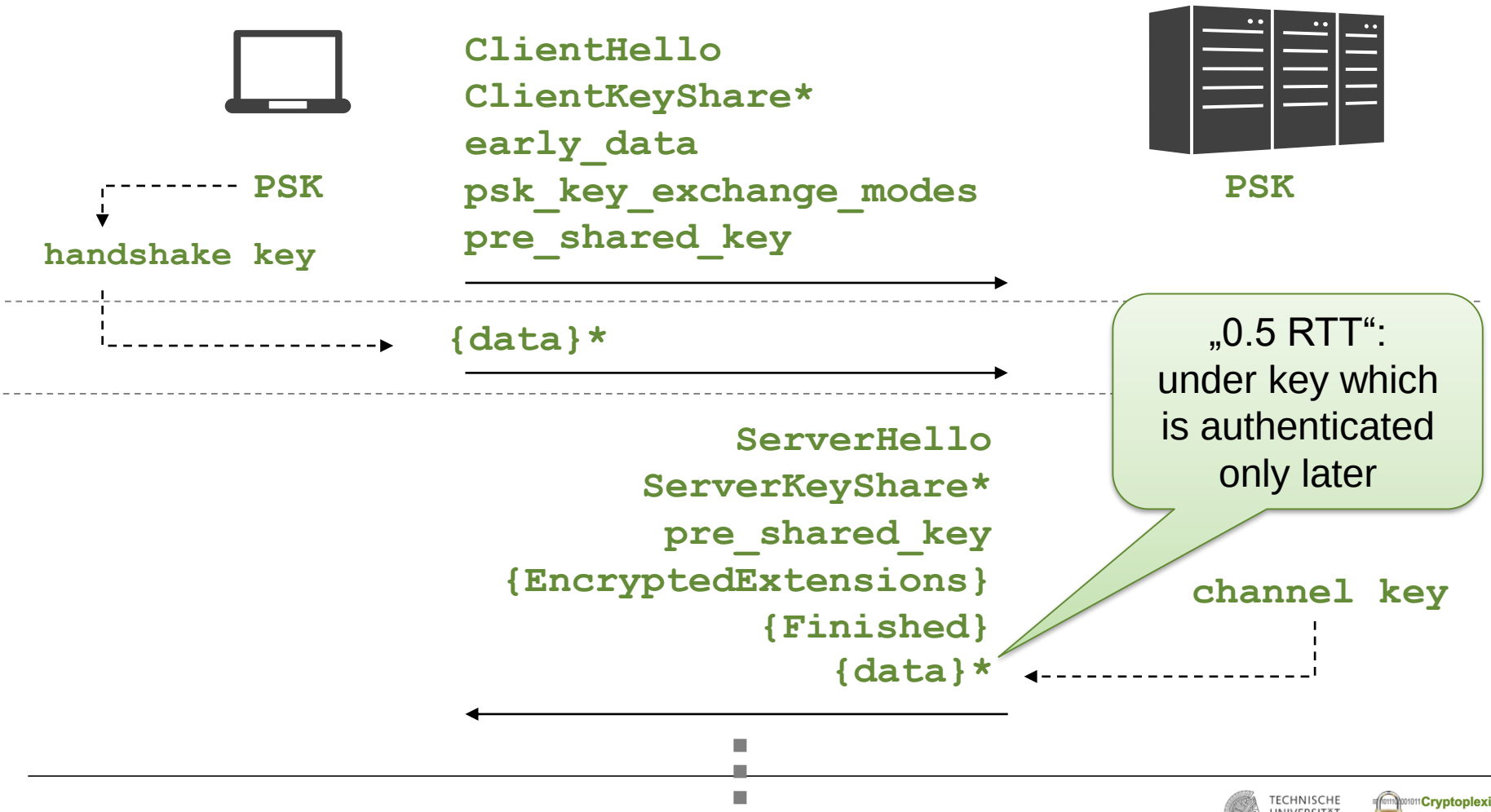
{data}*

no forward secrecy:
if PSK is comprised,
data is available

ServerHello
ServerKeyShare*
pre_shared_key
{EncryptedExtensions}
{Finished}

corresponds to resumption mode (except for data)

0.5RTT: Server Early-Data

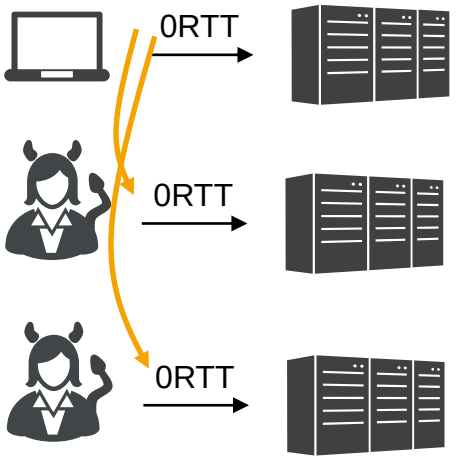


Security Results draft-12/14

Fischlin, Günther: Replay Attacks on Zero Round-Trip Time: The Case of the TLS 1.3 Handshake Candidates, EuroS&P 2017

Relax security model to replayable stages:

three (or more)
honest sessions can have
same sid in replayable stages



Then, handshake key in PSK-only mode is replayable
and all keys are non-forward secret
(under cryptographic assumptions)

Teaser for the Break

Can you give a (stateful)
0RTT-protocol
which is forward secret?