Modeling Advanced Security Aspects of Key Exchange and Secure Channel Protocols

TECHNISCHE UNIVERSITÄT DARMSTADT

Felix Günther

CAST/GI Promotionspreis IT-Sicherheit 2019

21. Mai 2019

TECHNISCHE UNIVERSITÄT DARMSTADT

Cryptoplexity

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

UC San Diego

Sichere Kommunikation

TECHNISCHE UNIVERSITÄT DARMSTADT

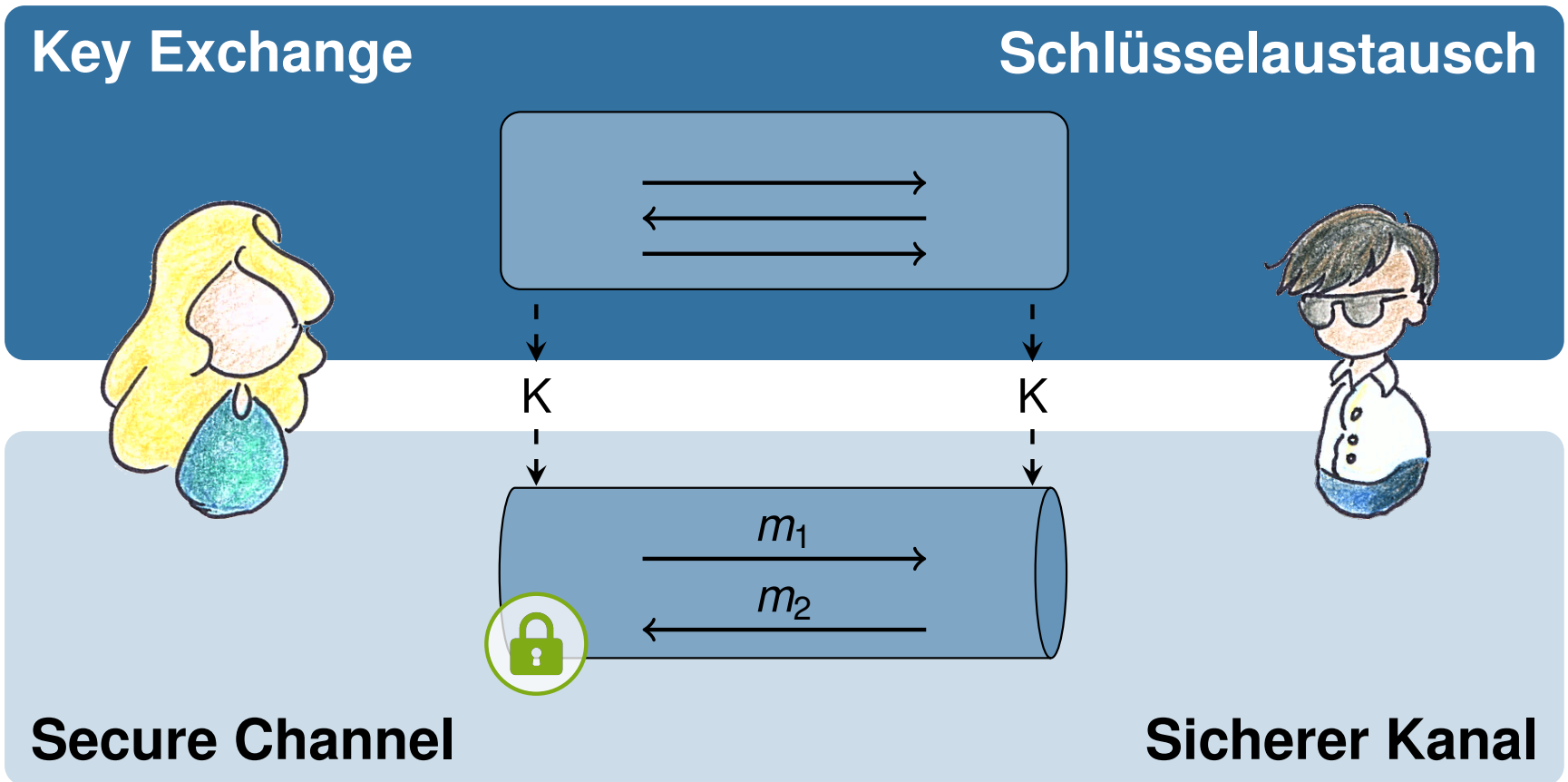
Sicherheitsziele:

- Vertraulichkeit
- Authentifikation
- Integritätsschutz

Sichere Kommunikation

Kryptographischer Kern

TECHNISCHE UNIVERSITÄT DARMSTADT



Zeichnungen: *Giorgia Azzurra Marson*

Schlüsselaustausch

Neuartige Designs

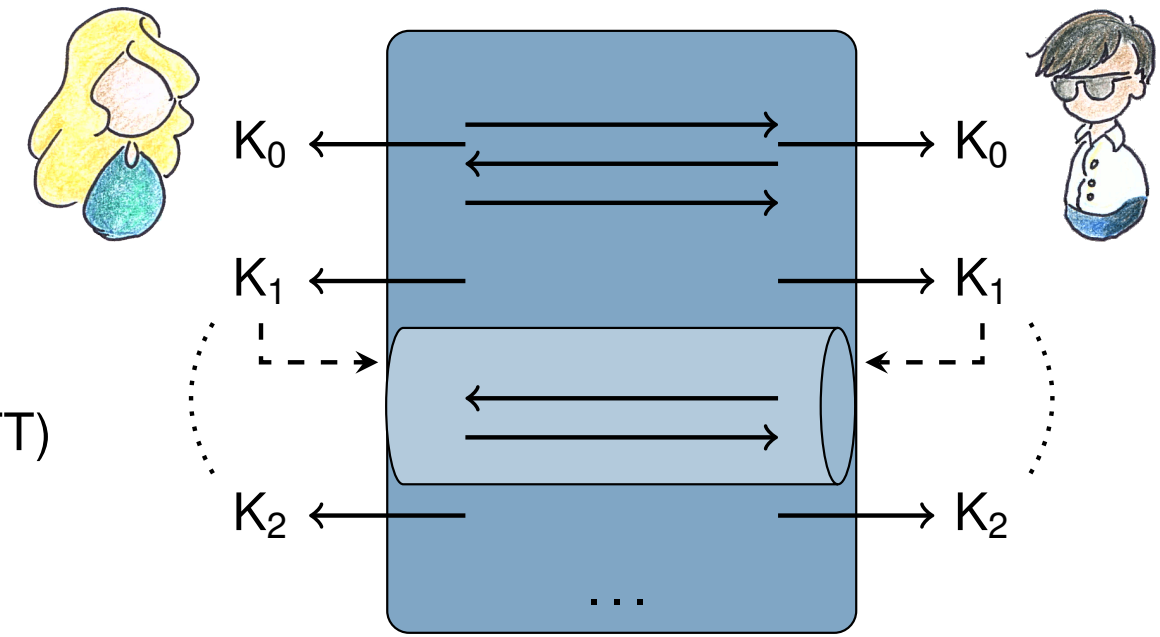
TECHNISCHE UNIVERSITÄT DARMSTADT

- klassisch: 1 Schlüssel ✓

Google QUIC

TLS 1.3

- neuartige Verfahren: gesteigerte Sicherheits- und Effizienzanforderungen

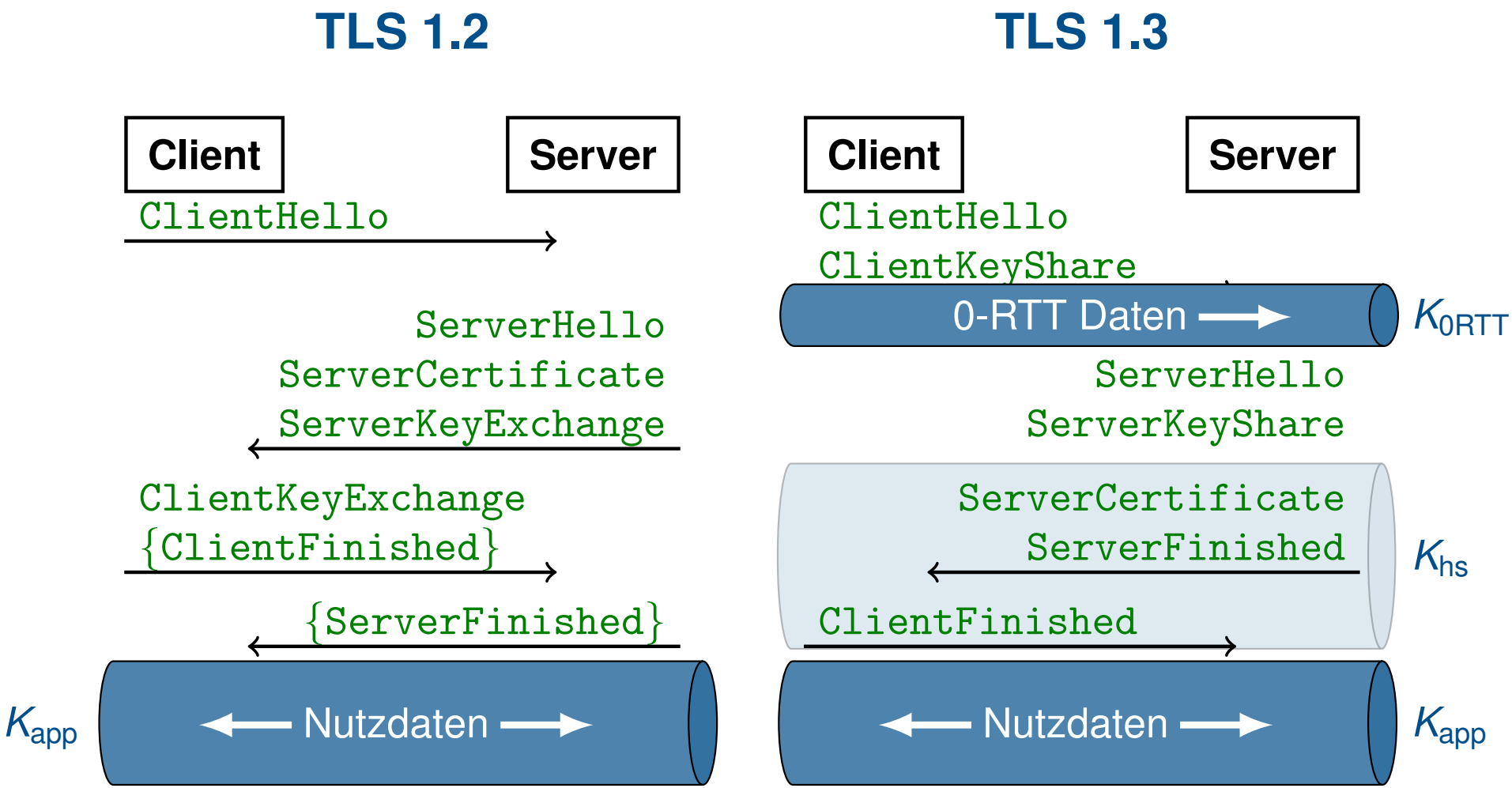


- mehrstufig
- verschachtelt
- minimale Latenzzeit (0-RTT)

Das Transport Layer Security Protokoll

Handshake – TLS 1.2 vs. TLS 1.3

TECHNISCHE UNIVERSITÄT DARMSTADT

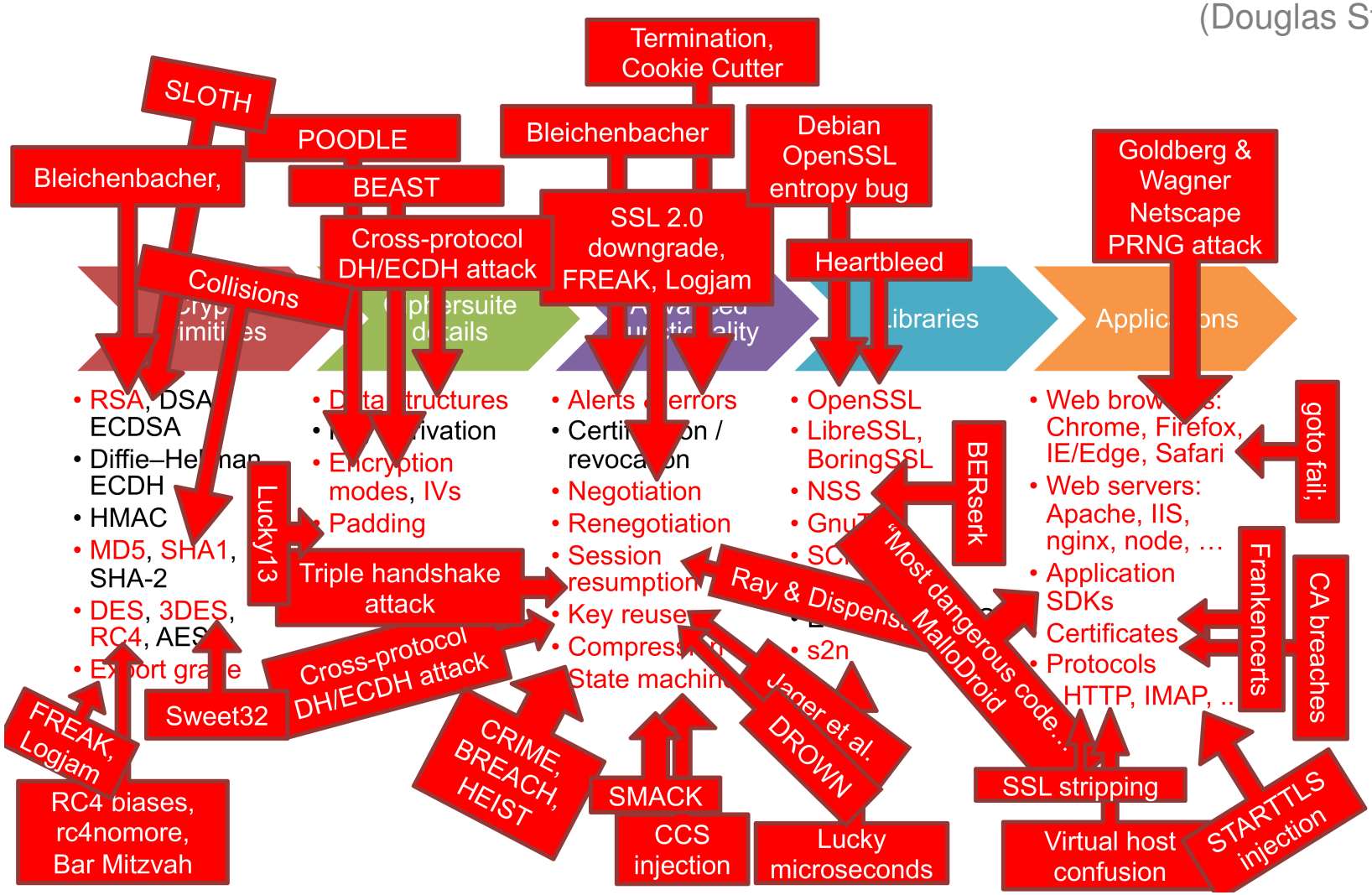


Sicherheitssituation vor TLS 1.3

oder: “Was kann schon schiefgehen?”

TECHNISCHE UNIVERSITÄT DARMSTADT

(Douglas Stebila)

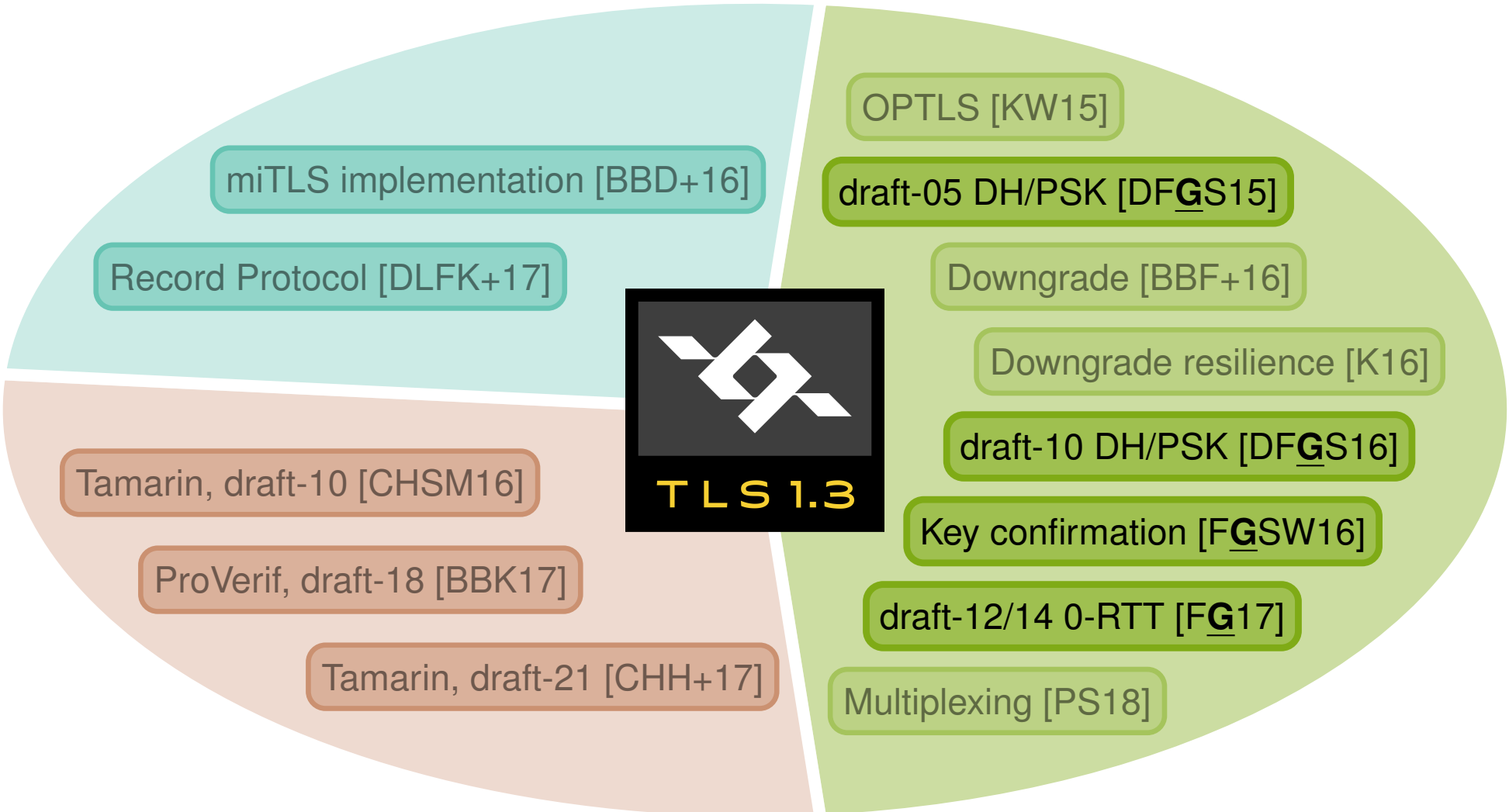


https://www.douglas.stebila.ca/research/presentations/tls-attacks/

TLS 1.3: Ein neuer Ansatz

IETF Standardisierungsprozess 2014–2018

TECHNISCHE UNIVERSITÄT DARMSTADT

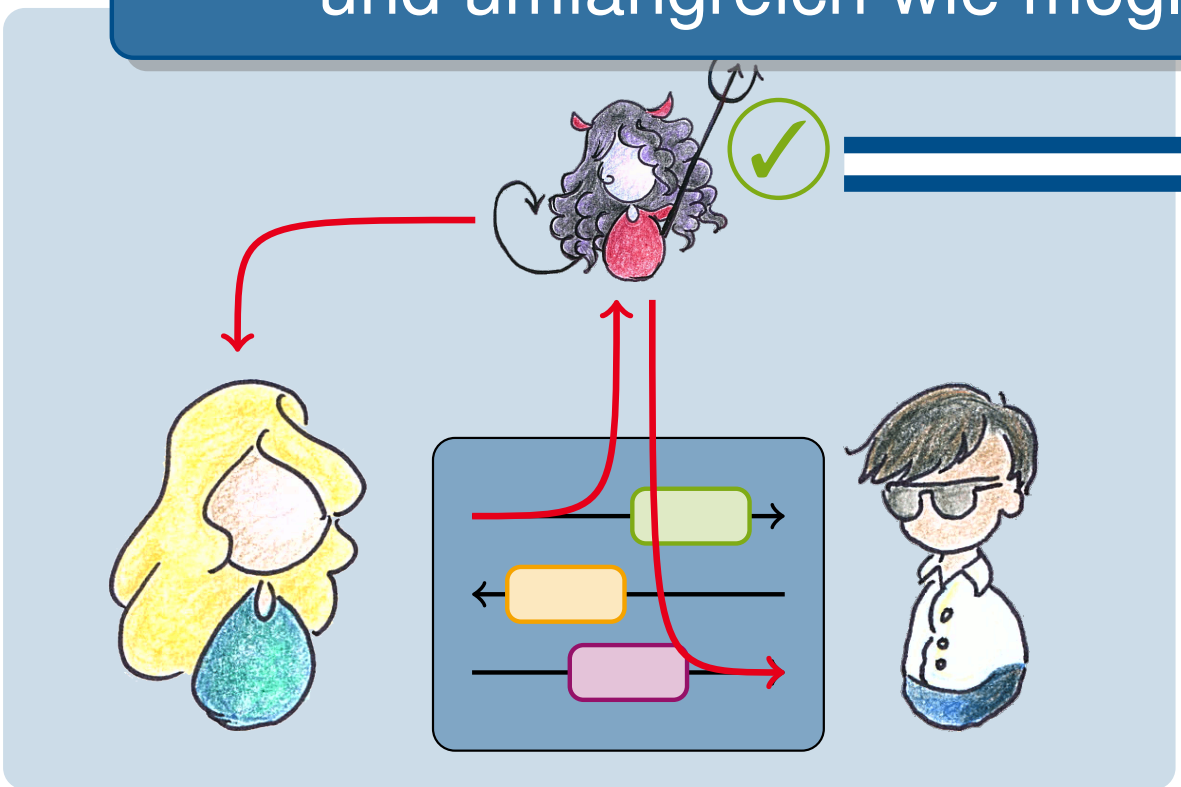


Was bedeutet kryptographische Sicherheit?

TECHNISCHE UNIVERSITÄT DARMSTADT

1. Abstraktes Protokoll
2. Sicherheitsdefinition
3. Sicherheitsbeweis

Ziel: Reales Protokollverhalten so präzise und umfangreich wie möglich erfassen.



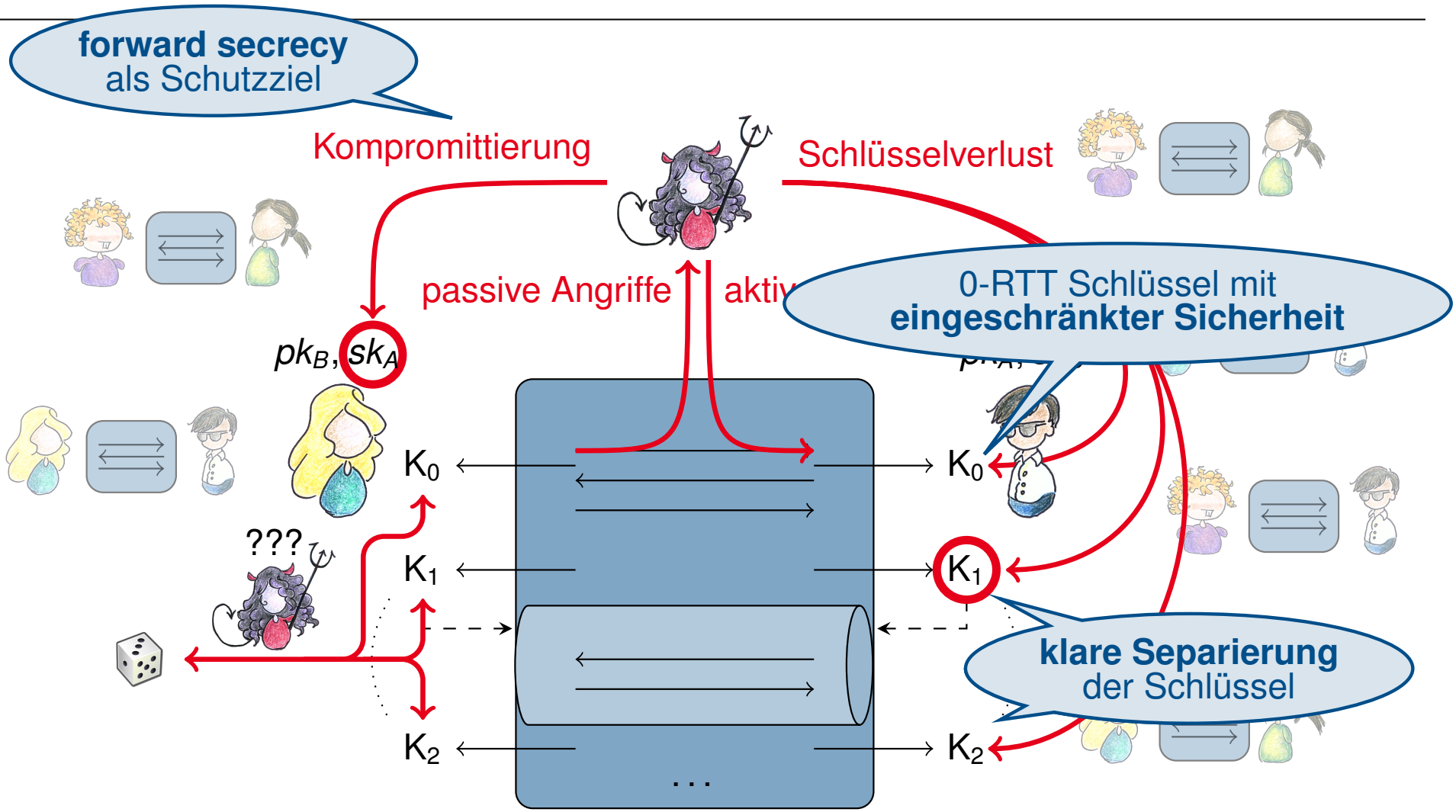
Komponente A

Komponente B

Komponente C

Neues Sicherheitsmodell für mehrstufigen Schlüsselaustausch

TECHNISCHE UNIVERSITÄT DARMSTADT

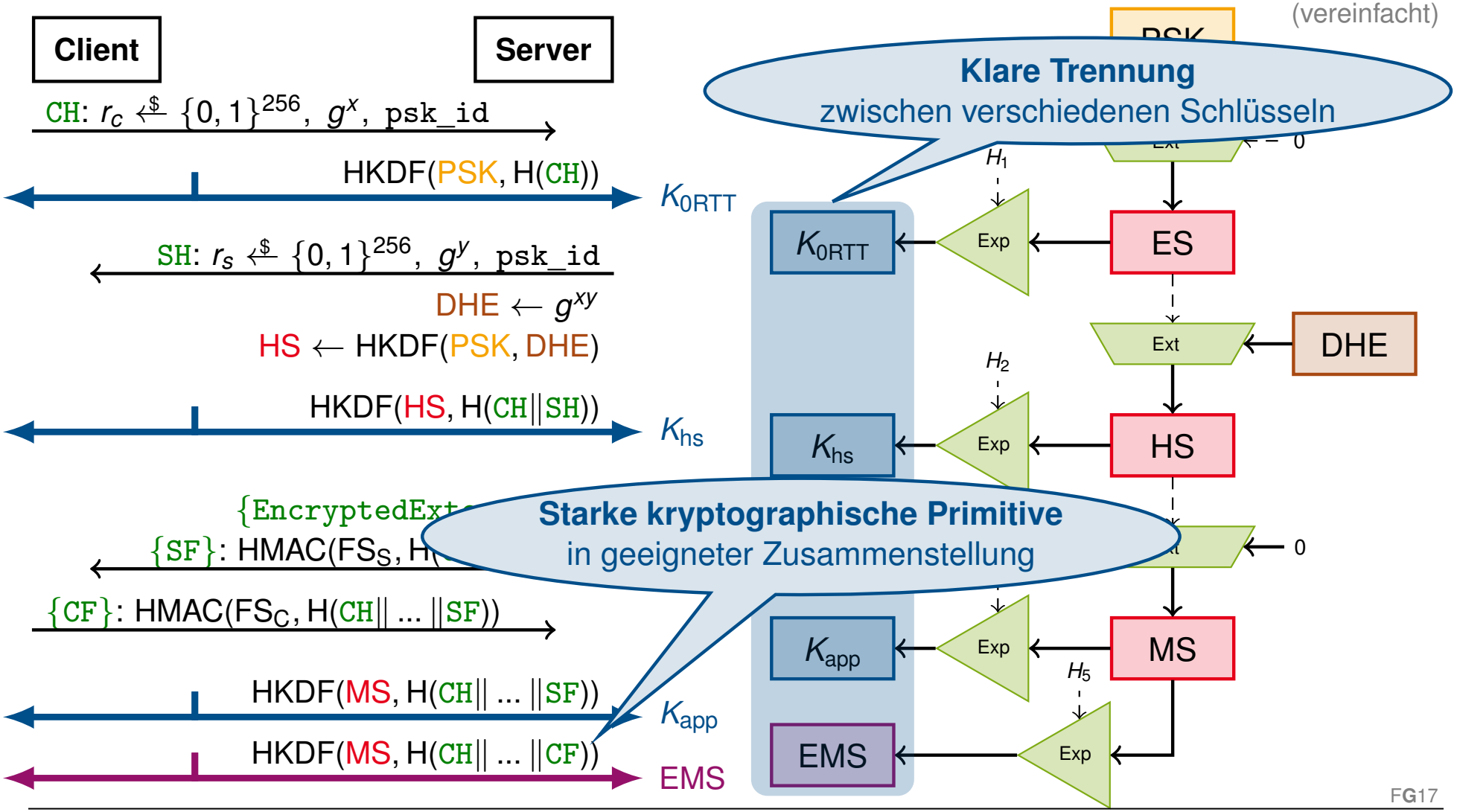


FG14, DFGS15, DFGS16, FG17

Sicherheitsanalyse von TLS 1.3

Beispiel: draft-14, Modus: PSK-(EC)DHE 0-RTT

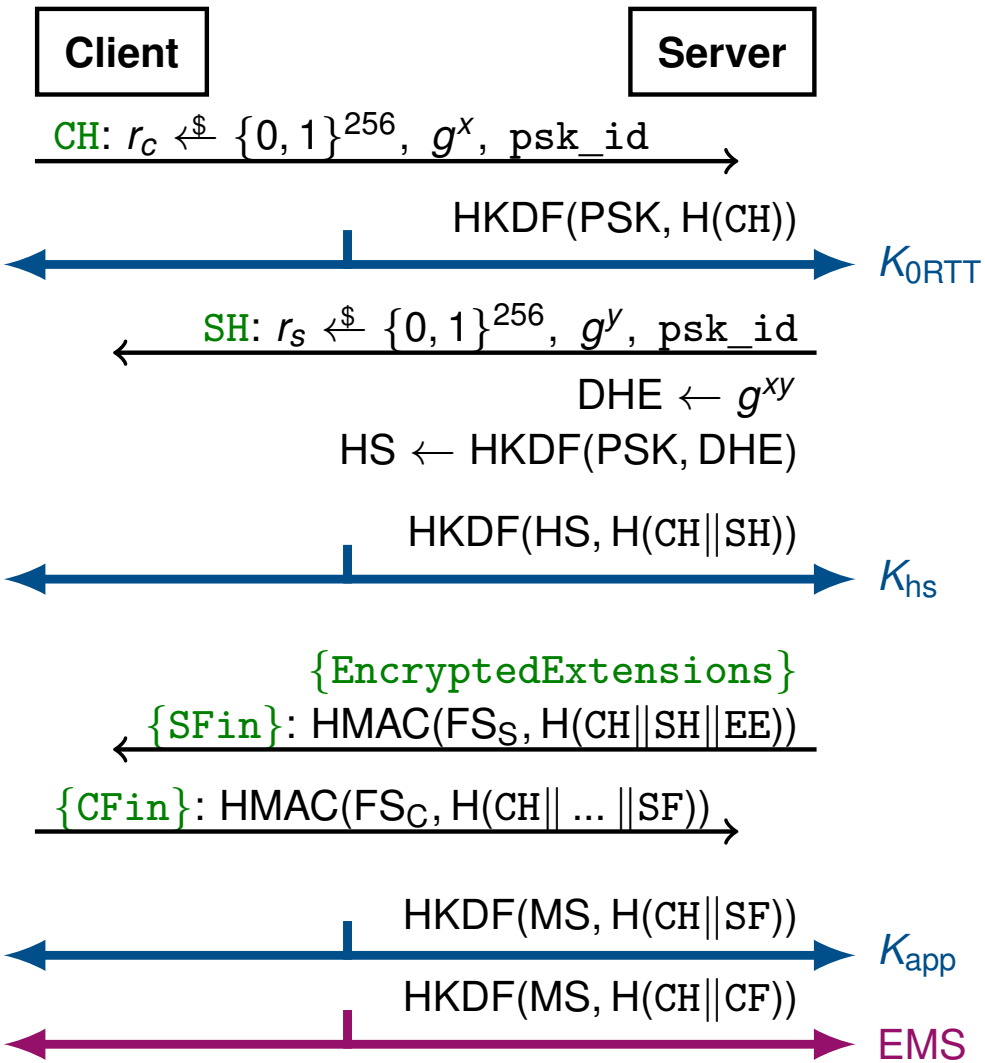
TECHNISCHE UNIVERSITÄT DARMSTADT



Sicherheitsanalyse von TLS 1.3

Beispiel: draft-14, Modus: PSK-(EC)DHE 0-RTT

TECHNISCHE UNIVERSITÄT DARMSTADT



Theorem 7.4. *The TLS 1.3* `draft-14` *PSK-(EC)DHE 0-RTT handshake is* **Multi-Stage**-*secure in a* ***key-independent*** *and* ***stage-3-forward-secret*** *manner with properties* (M, **AUTH**, USE, **REPLAY**).

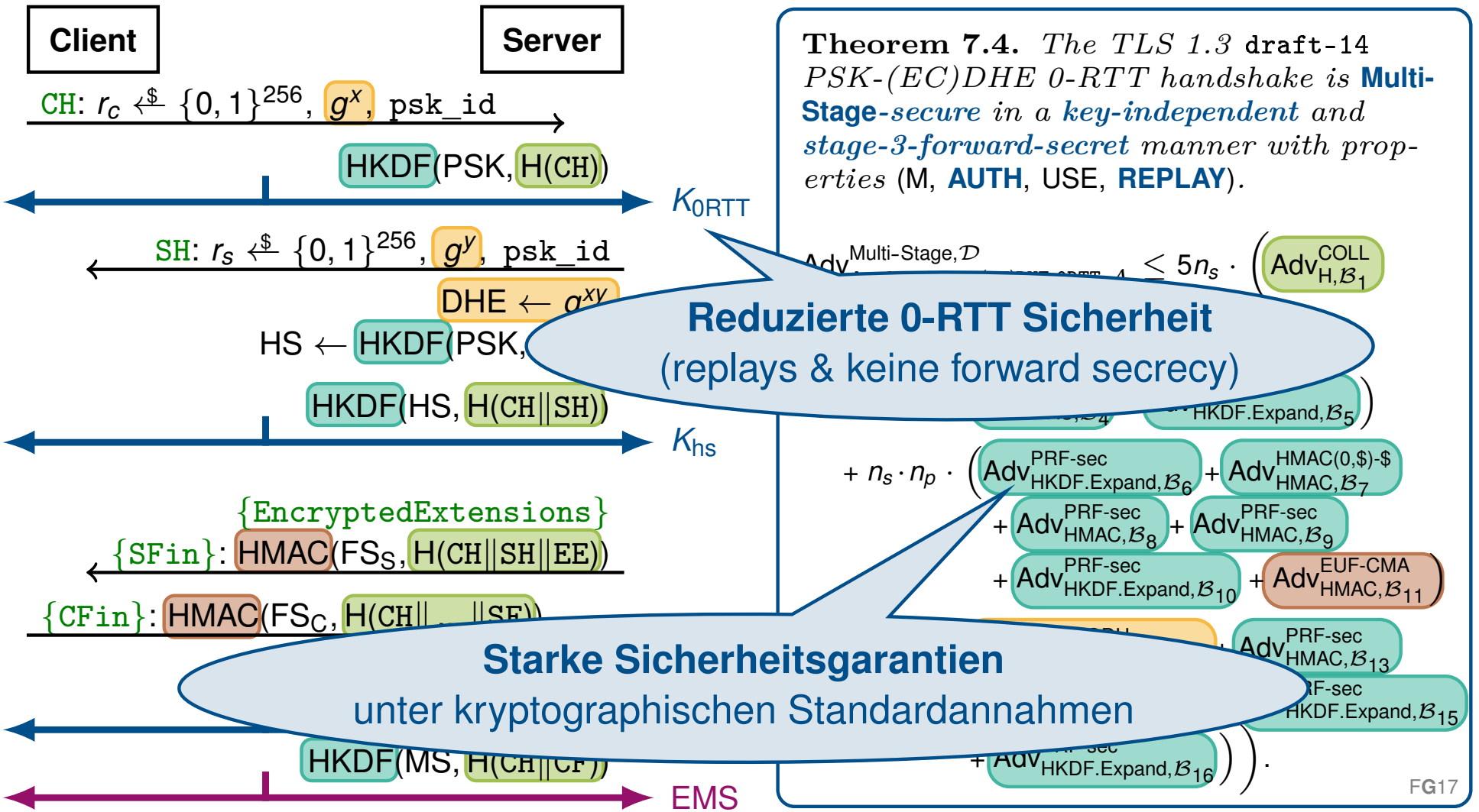
$$
\begin{aligned}
\mathrm{Adv}^{\text{Multi-Stage},\mathcal{D}}_{\texttt{draft-14-PSK-(EC)DHE-0RTT},\mathcal{A}} \leq 5n_s \cdot \Big(& \mathrm{Adv}^{\text{COLL}}_{\text{H},\mathcal{B}_1} \\
& + n_p \cdot \Big(\mathrm{Adv}^{\text{PRF-sec}}_{\text{HKDF.Expand},\mathcal{B}_2} + \mathrm{Adv}^{\text{HMAC(0,\$)-\$}}_{\text{HMAC},\mathcal{B}_3} \\
& \qquad + \mathrm{Adv}^{\text{PRF-sec}}_{\text{HMAC},\mathcal{B}_4} + \mathrm{Adv}^{\text{PRF-sec}}_{\text{HKDF.Expand},\mathcal{B}_5} \Big) \\
& + n_s \cdot n_p \cdot \Big(\mathrm{Adv}^{\text{PRF-sec}}_{\text{HKDF.Expand},\mathcal{B}_6} + \mathrm{Adv}^{\text{HMAC(0,\$)-\$}}_{\text{HMAC},\mathcal{B}_7} \\
& \qquad + \mathrm{Adv}^{\text{PRF-sec}}_{\text{HMAC},\mathcal{B}_8} + \mathrm{Adv}^{\text{PRF-sec}}_{\text{HMAC},\mathcal{B}_9} \\
& \qquad + \mathrm{Adv}^{\text{PRF-sec}}_{\text{HKDF.Expand},\mathcal{B}_{10}} + \mathrm{Adv}^{\text{EUF-CMA}}_{\text{HMAC},\mathcal{B}_{11}} \Big) \\
& + n_s \cdot n_p \cdot \Big(\mathrm{Adv}^{\text{snPRF-ODH}}_{\text{HKDF.Extract},\mathbb{G},\mathcal{B}_{12}} + \mathrm{Adv}^{\text{PRF-sec}}_{\text{HMAC},\mathcal{B}_{13}} \\
& \qquad + \mathrm{Adv}^{\text{PRF-sec}}_{\text{HKDF.Expand},\mathcal{B}_{14}} + \mathrm{Adv}^{\text{PRF-sec}}_{\text{HKDF.Expand},\mathcal{B}_{15}} \\
& \qquad + \mathrm{Adv}^{\text{PRF-sec}}_{\text{HKDF.Expand},\mathcal{B}_{16}} \Big) \Big).
\end{aligned}
$$

FG17

Sicherheitsanalyse von TLS 1.3

Beispiel: draft-14, Modus: PSK-(EC)DHE 0-RTT

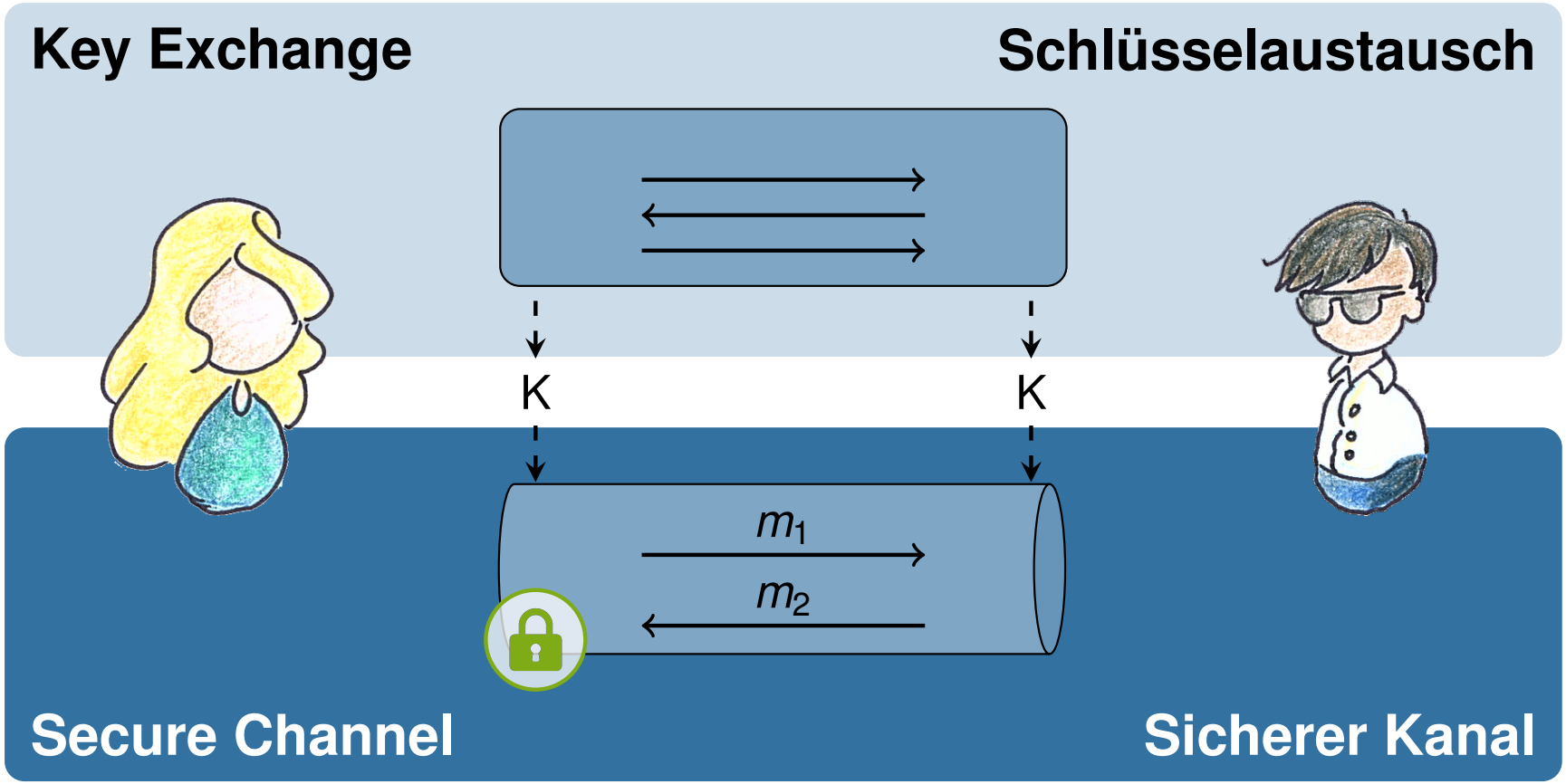
TECHNISCHE UNIVERSITÄT DARMSTADT



Sichere Kommunikation

Kryptographischer Kern

TECHNISCHE UNIVERSITÄT DARMSTADT



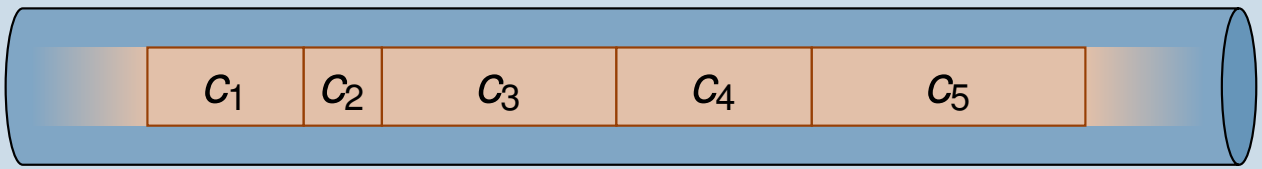
Sichere Kanäle

Präzisere Modelle & Neuartige Designs

TECHNISCHE UNIVERSITÄT DARMSTADT

Kanäle für Datenströme

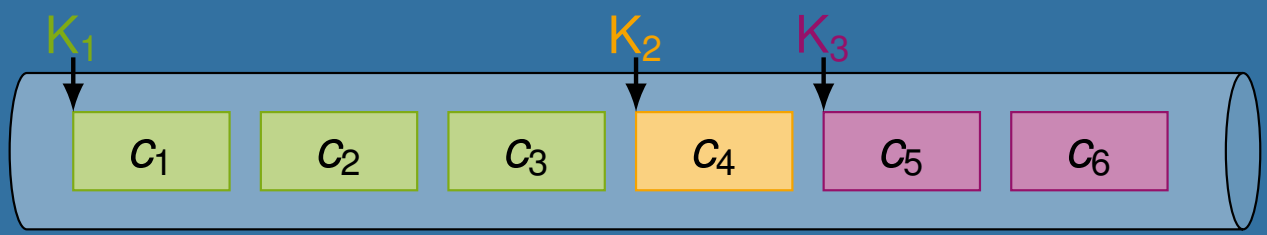
(TLS, SSH, QUIC, . . .)



[FGMP15]

Kanäle mit mehreren Schlüsseln

(TLS 1.3, Signal, . . .)

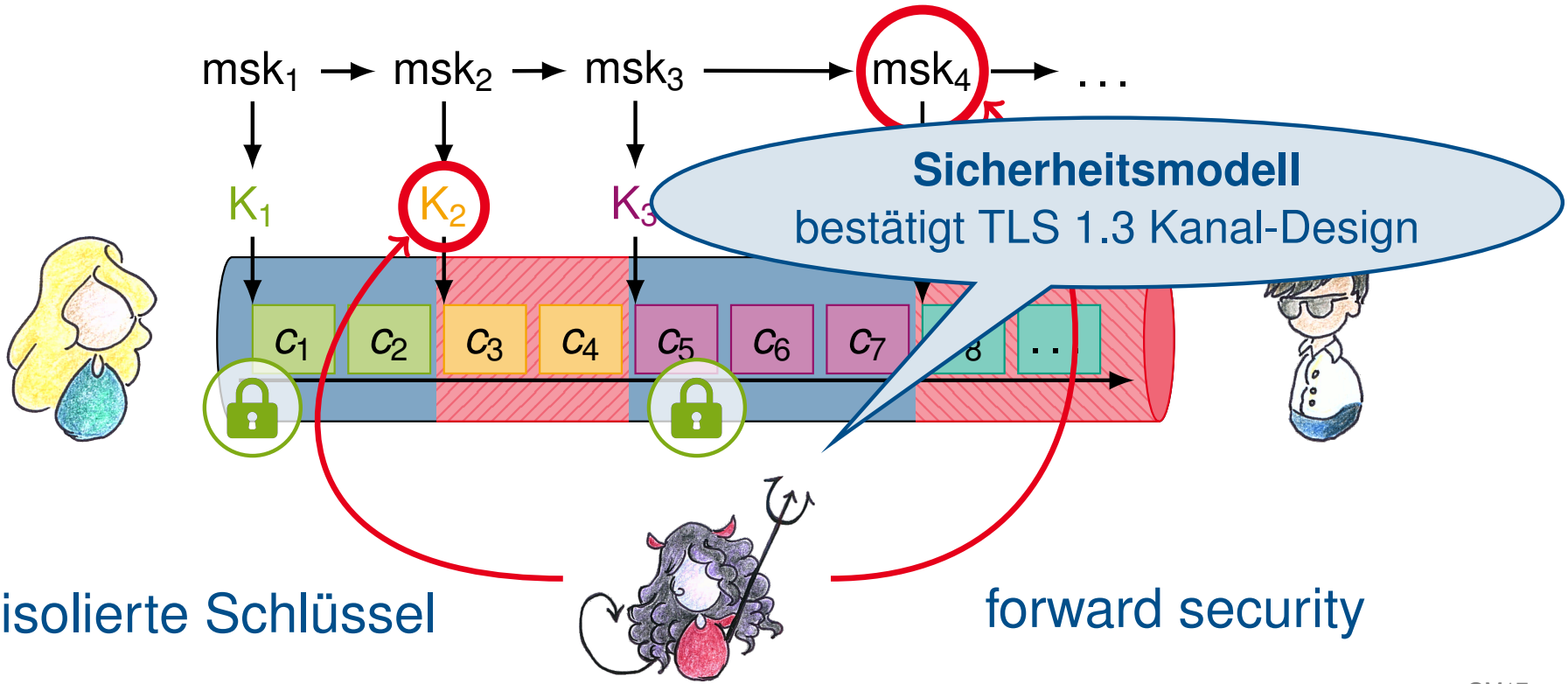


[GM17]

Kanäle mit mehreren Schlüssel

TECHNISCHE UNIVERSITÄT DARMSTADT

- klassisch: 1 Schlüssel ✓
- **TLS 1.3**, **Signal**, . . . : Kanal erlaubt Schlüssel-Updates



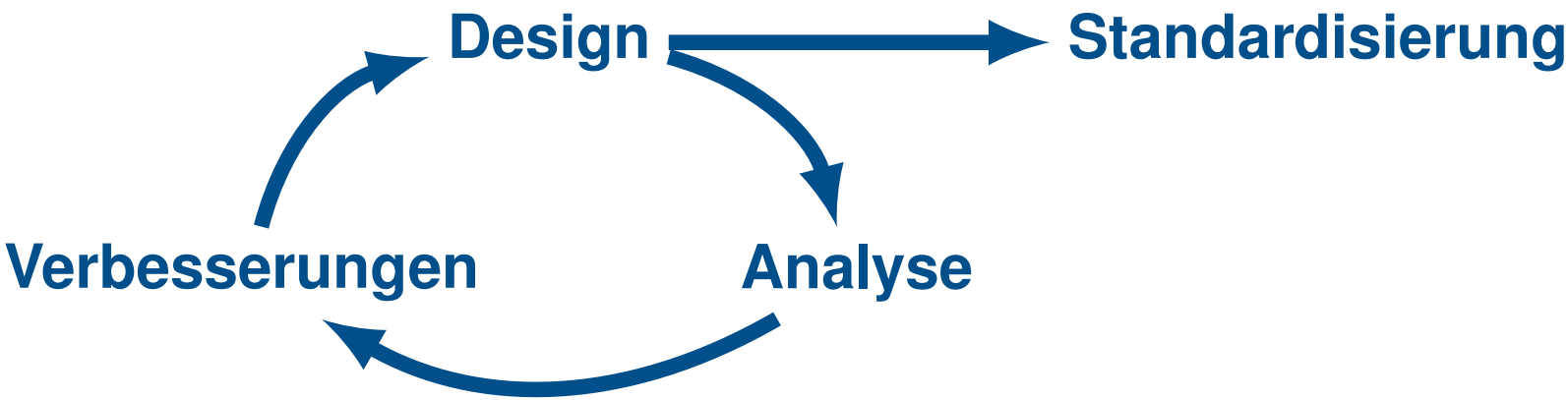
GM17

TLS 1.3 — Fazit

TLS 1.3

TECHNISCHE UNIVERSITÄT DARMSTADT

- höchst interaktiver Standardisierungsprozess nach neuem Schema:



- solides kryptographisches Design, viele Verbesserungen
- bereits heute (< 1 Jahr nach Standardisierung) weit verbreitet

Google CLOUDFLARE Java ...

- aber auch (sicherheits-)kritischere Komponenten, insb. 0-RTT replays

Bundesamt für Sicherheit in der Informationstechnik

Mindeststandard des BSI zur Verwendung von Transport Layer Security (TLS)

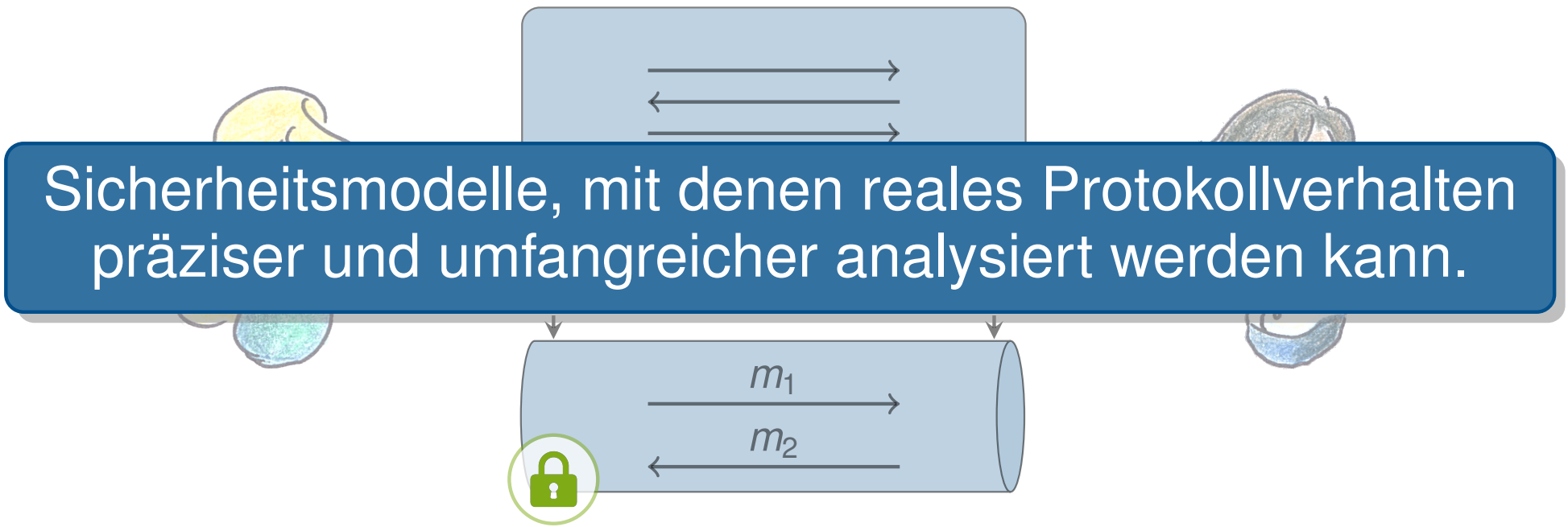
nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 05.04.2019

Meine Dissertation

Modeling Advanced Security Aspects of Key Exchange and Secure Channel Protocols

TECHNISCHE UNIVERSITÄT DARMSTADT

Grundlegende neue kryptographische Sicherheitsmodelle für Schlüsselaustausch und sichere Kanäle



Sicherheitsmodelle, mit denen reales Protokollverhalten präziser und umfangreicher analysiert werden kann.

TLS 1.3 Google QUIC

Vielen Dank!