ETH zürich

Cryptographic Parameters in TLS 1.3, QUIC, and Co.

Tighter Security and Robust Handling of Unreliable Networks

Felix Günther

based on joint work with Hannah Davis, Marc Fischlin, Christian Janson

ETH zürich | TECHNISCHE UNIVERSITÄT DARMSTADT | UC San Diego | DFG Deutsche Forschungsgemeinschaft German Research Foundation

Transport Layer Security (TLS)

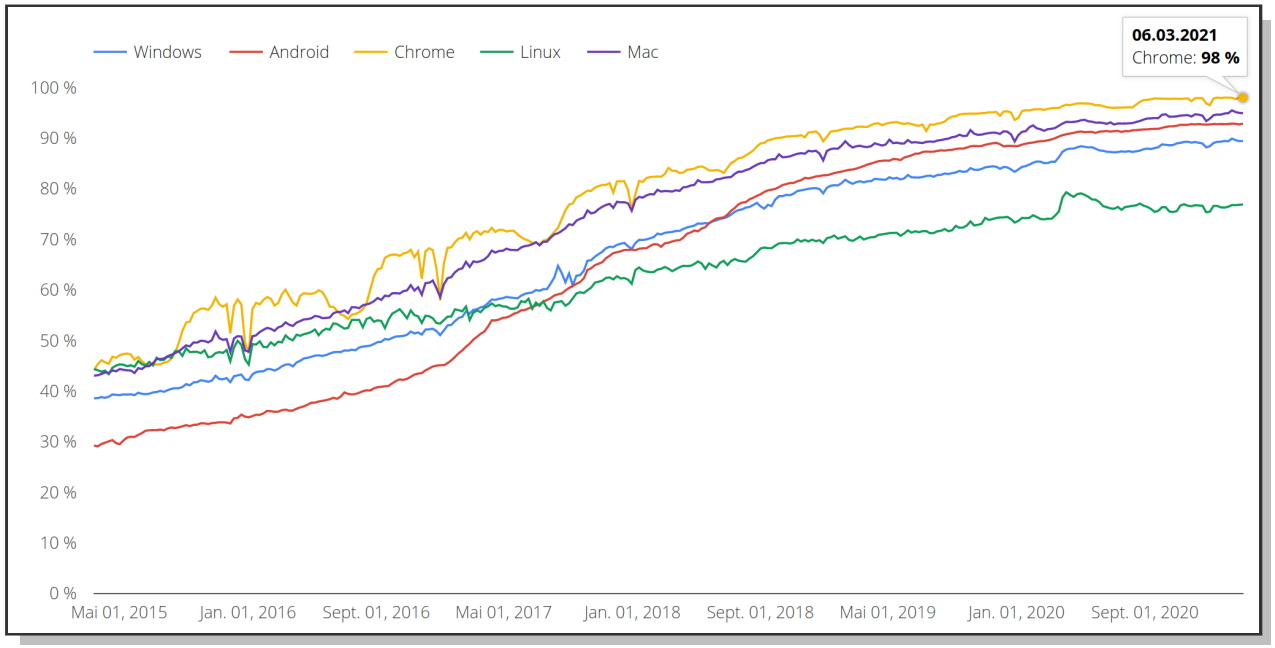
ETH zürich

TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.

TLS 1.3 [RFC 8446, Aug. 2018]

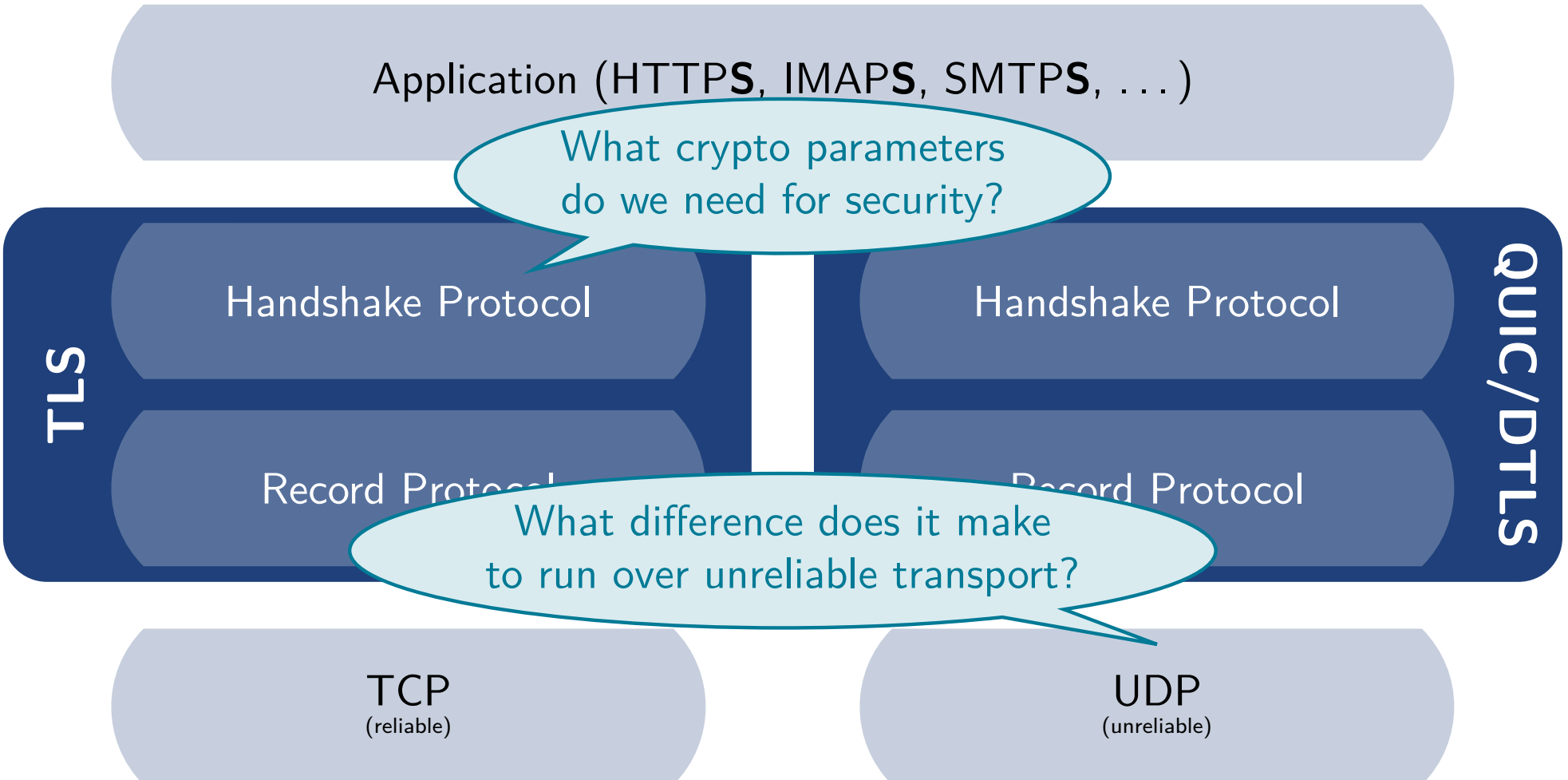
HTTPS-protected traffic

- 50%+ Sandvine (Oct 18)
- 72% Fortinet (Q3 18)
- 84% Firefox (Mar 21)
  (Telemetry)
- 77–98% Chrome (Mar 21)
  (Transparency Report)



Secure Transport within the Network Stack

ETH zürich

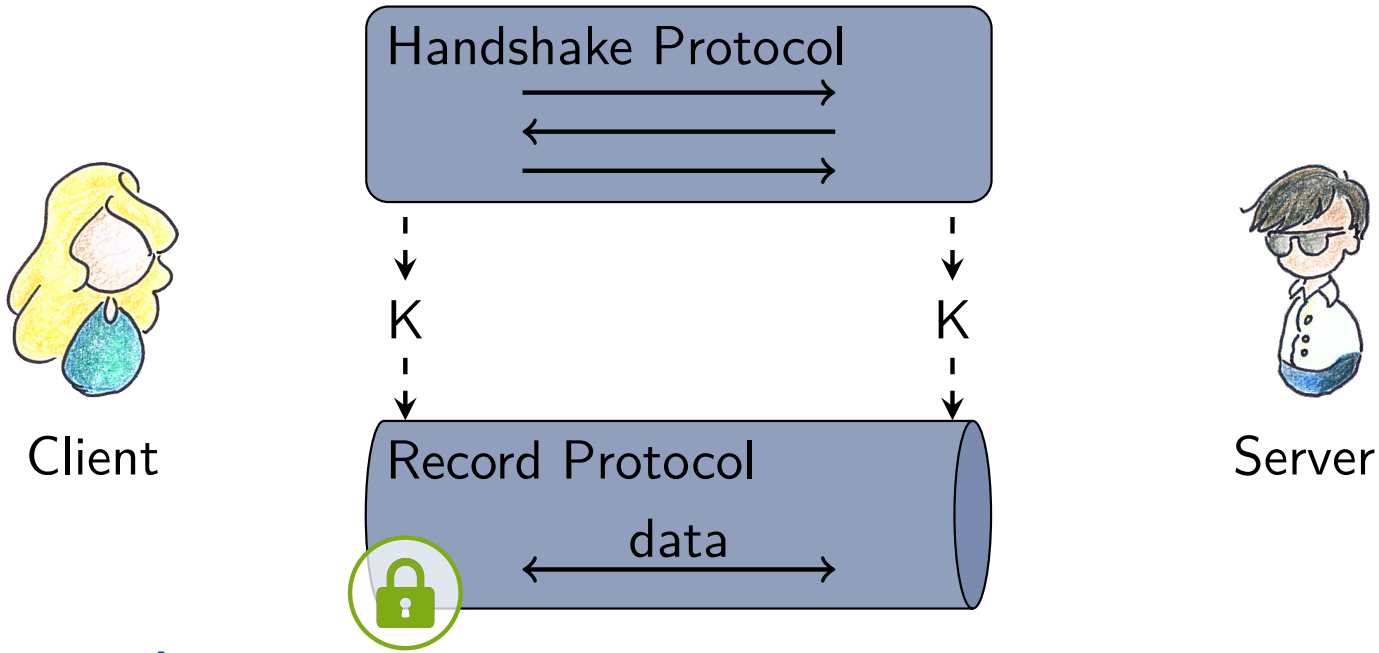


The Cryptographic Core

ETH zürich

Handshake Protocol:

- negotiate security parameters ("cipher suite")
- authenticate peers
- establish key material for data protection



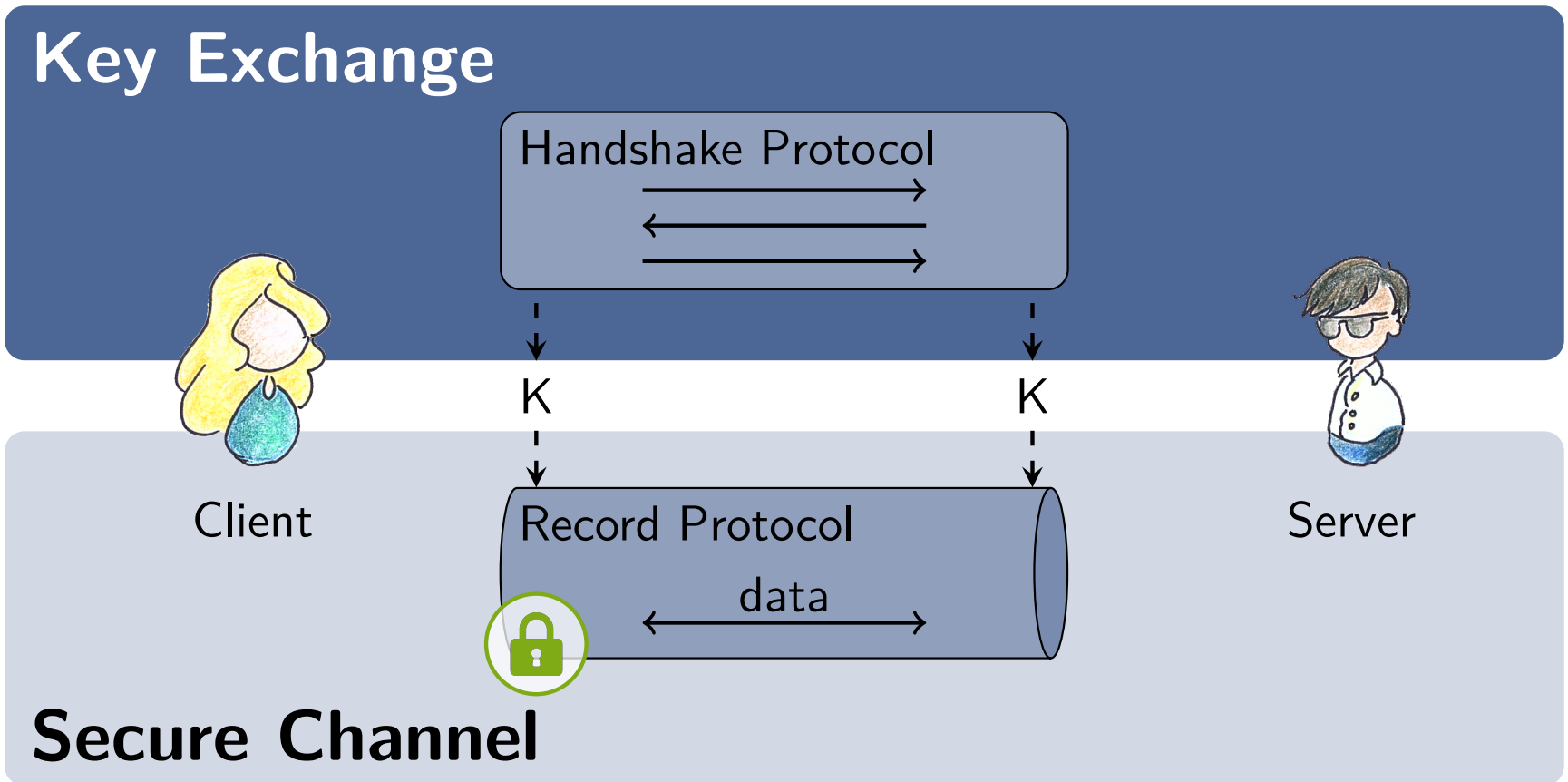
Record Protocol:

- protect data using key material from handshake
- ensuring confidentiality and integrity

drawings by *Giorgia Azzurra Marson*

The Cryptographic Core

ETH zürich



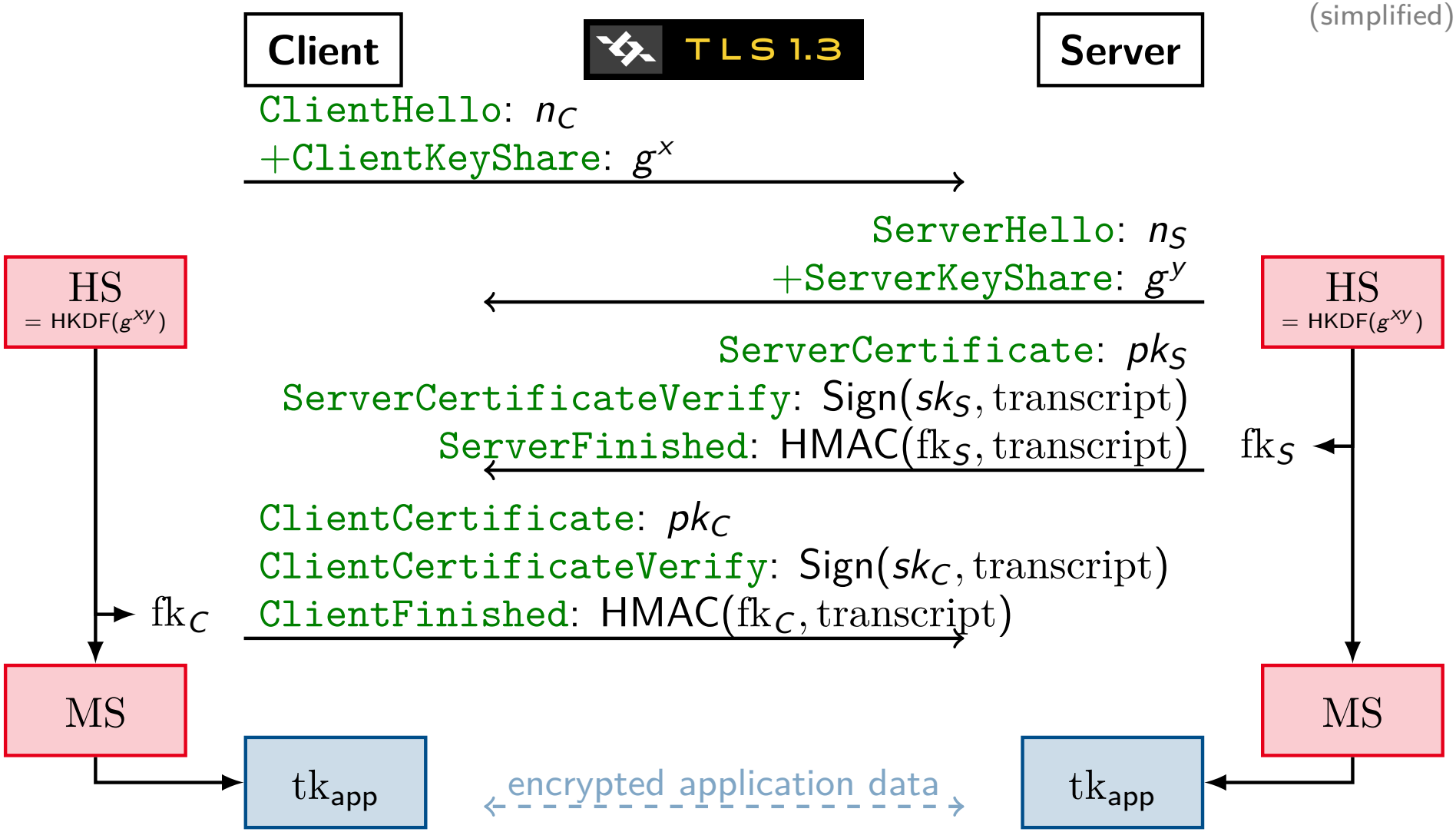
drawings by *Giorgia Azzurra Marson*

The TLS 1.3 Handshake

Full (EC)DHE Mode

ETH zürich

(simplified)

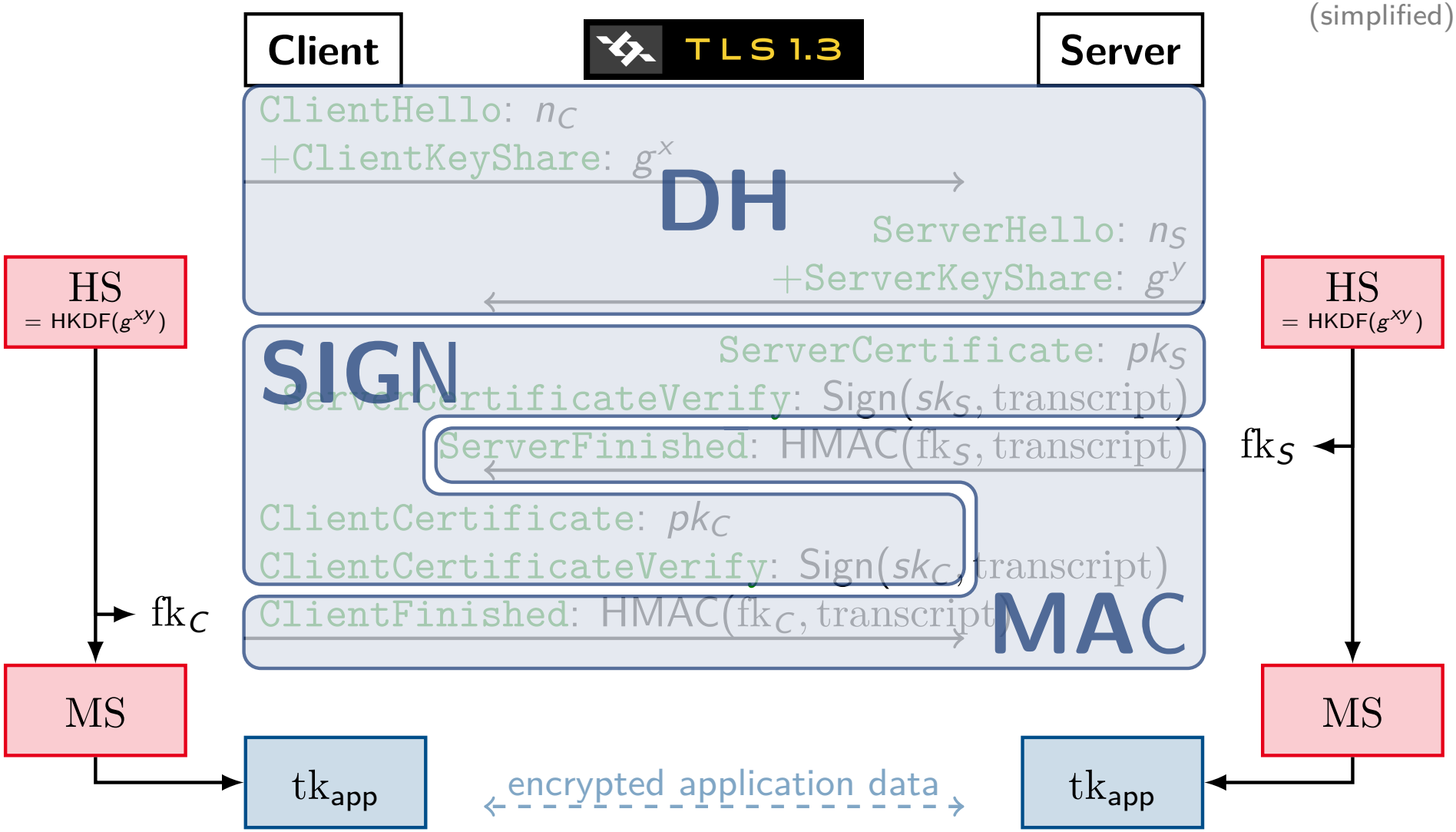


The TLS 1.3 Handshake

Full (EC)DHE Mode ≈ **SIGMA**: (DH w/) **SIG**n-and-**MA**c [Kra03]

ETH zürich

(simplified)



The TLS 1.3 Handshake

Secure in Principle (Only)

ETH zürich

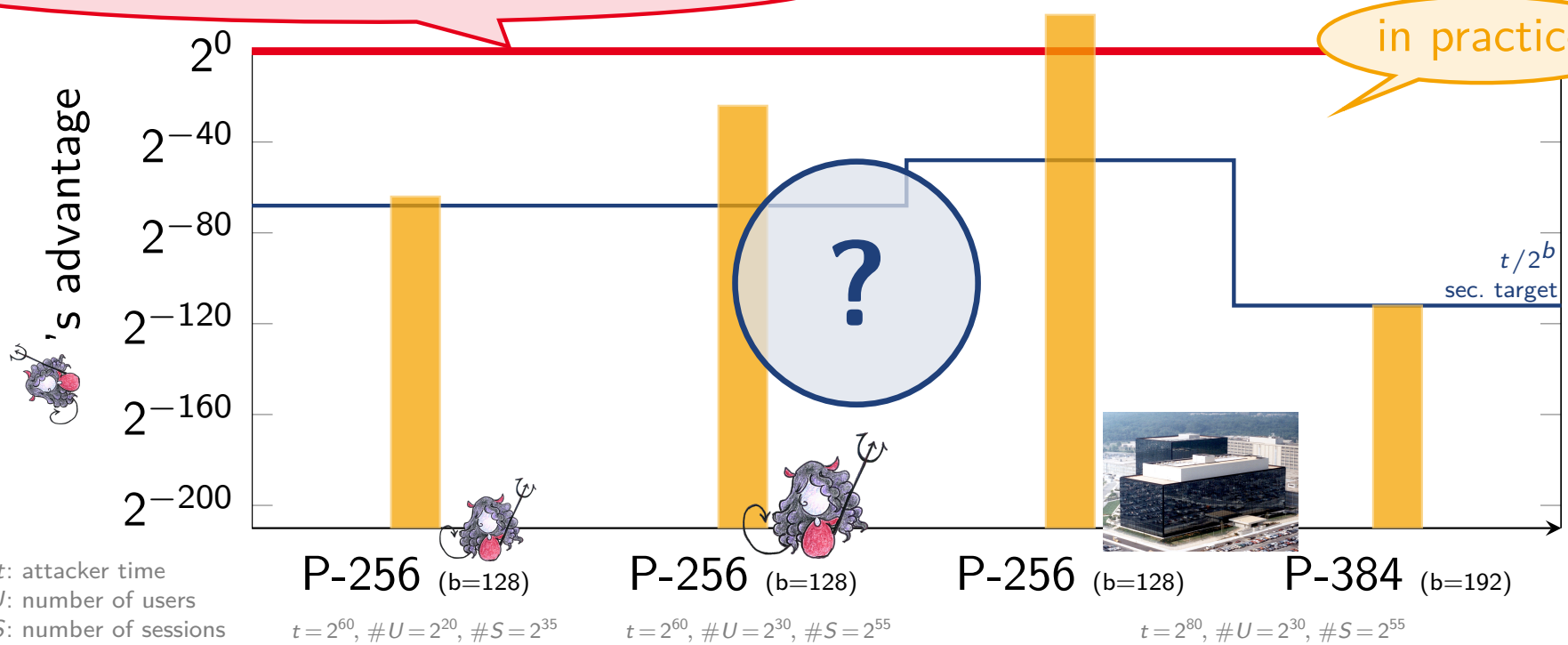
[DFGS21]:

$$\mathsf{Adv}^{\text{Multi-Stage},\mathcal{D}}_{\texttt{TLS1.3-full-1RTT},\mathcal{A}} \leq 6n_s \left(\begin{array}{l} \mathsf{Adv}^{\text{COLL}}_{\text{H},\mathcal{B}_1} + n_u \cdot \mathsf{Adv}^{\text{EUF-CMA}}_{\text{SIG},\mathcal{B}_2} \\ + n_s \left(\begin{array}{l} \mathsf{Adv}^{\text{dual-snPRF-ODH}}_{\text{HKDF.Extract},\mathbb{G},\mathcal{B}_3} + \mathsf{Adv}^{\text{PRF-sec}}_{\text{HKDF.Expand},\mathcal{B}_4} \\ + 2 \cdot \mathsf{Adv}^{\text{PRF-sec}}_{\text{HKDF.Expand},\mathcal{B}_5} + \mathsf{Adv}^{\text{PRF-sec}}_{\text{HKDF.Extract},\mathcal{B}_6} \\ + \mathsf{Adv}^{\text{PRF-sec}}_{\text{HKDF.Expand},\mathcal{B}_7} \end{array} \right) \end{array} \right)$$

in principle

this is Pr[breaks TLS 1.3] = 1!

in practice



t: attacker time
$\#U$: number of users
$\#S$: number of sessions

[DFGS21] Dowling, Fischlin, Günther, and Stebila: "A Cryptographic Analysis of the TLS 1.3 Handshake Protocol".

Key Exchange à la Diffie–Hellman

[DH76]

ETH zürich

knows x

g^x

g^y

knows y

$g^{xy} = (g^y)^x$

$K = \mathrm{KDF}(g^{xy})$

KDF: Key Derivation Function

$g^{xy} = (g^x)^y$

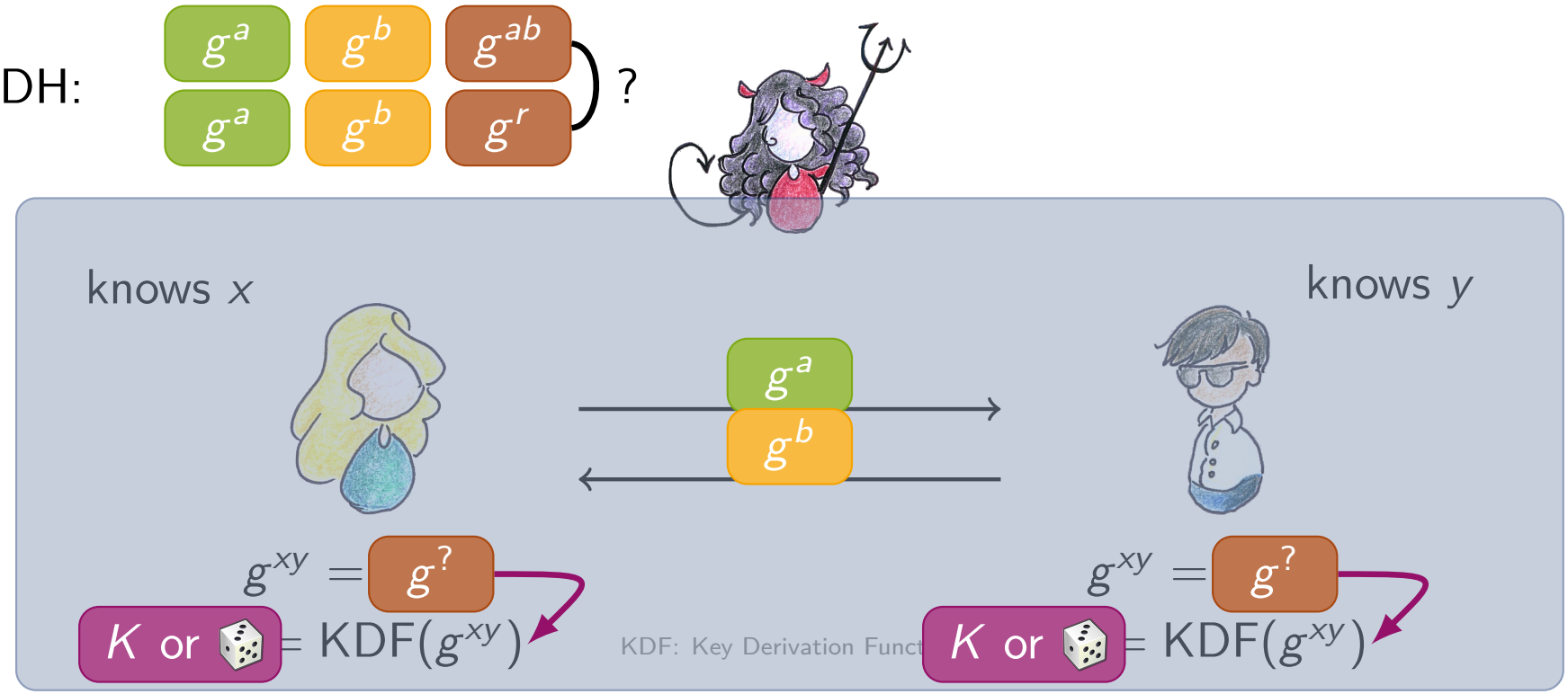
$K = \mathrm{KDF}(g^{xy})$

- key secrecy: given only g^x and g^y, key K remains secret (indist. from )

Key Exchange à la Diffie–Hellman

[DH76]

ETH zürich

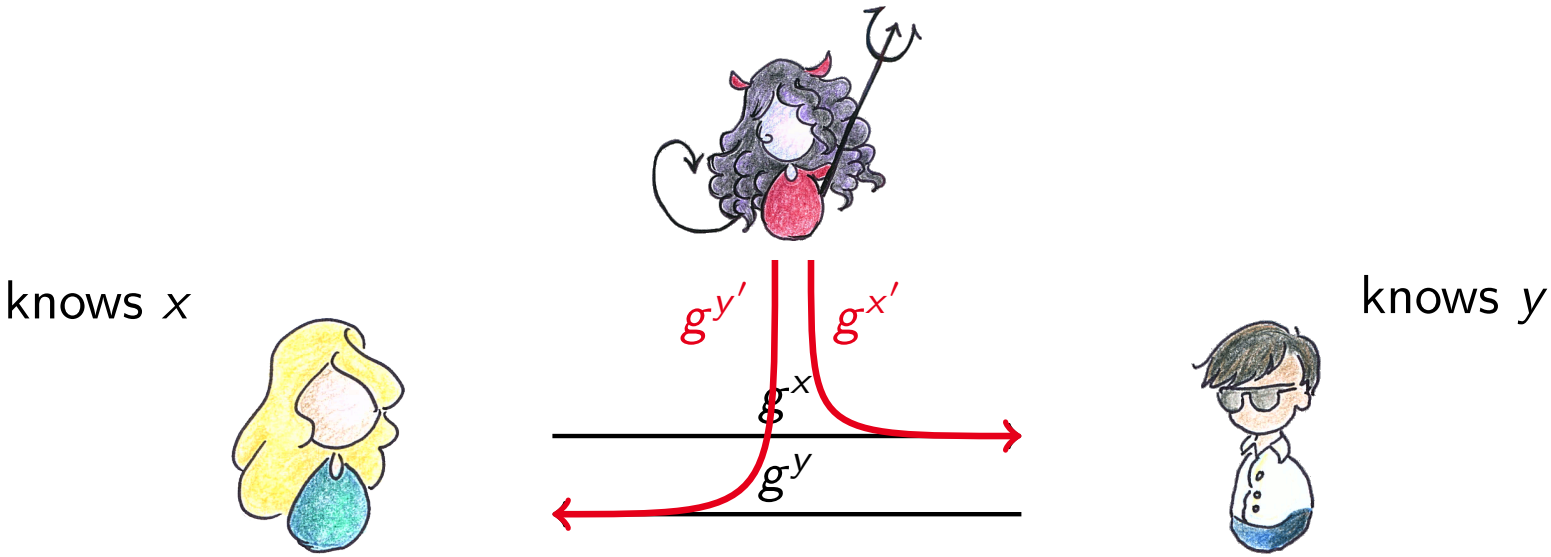


- key secrecy: given only g^x and g^y, key K remains secret (indist. from)

Key Exchange à la Diffie–Hellman

[DH76]

ETH zürich



$g^{xy} = (g^y)^x$

$K = \mathrm{KDF}(g^{xy})$

$K' = \mathrm{KDF}(g^{xy'})$

KDF: Key Derivation Function

$g^{xy} = (g^x)^y$

$K = \mathrm{KDF}(g^{xy})$

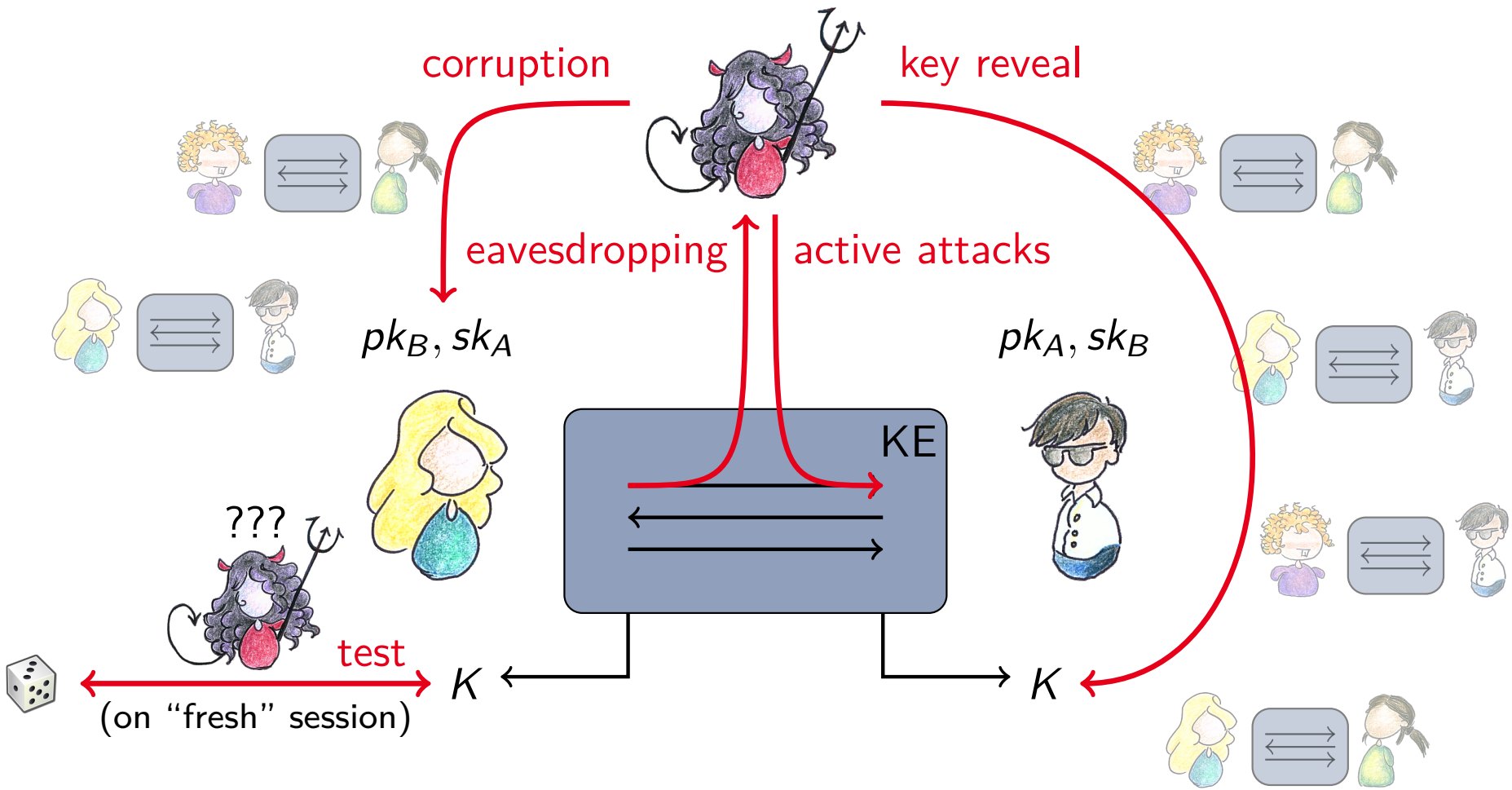
$K'' = \mathrm{KDF}(g^{x'y})$

- key secrecy: given only g^x and g^y, key K remains secret (indist. from )
- just one of many building blocks (no security against MitM, . . .)

Key Exchange Security

Bellare, Rogaway 1993 [BR94]

ETH zürich



Take Your Pick!

ETH zürich

- How do we handle all these parallel sessions in a reduction?
- We **guess**!

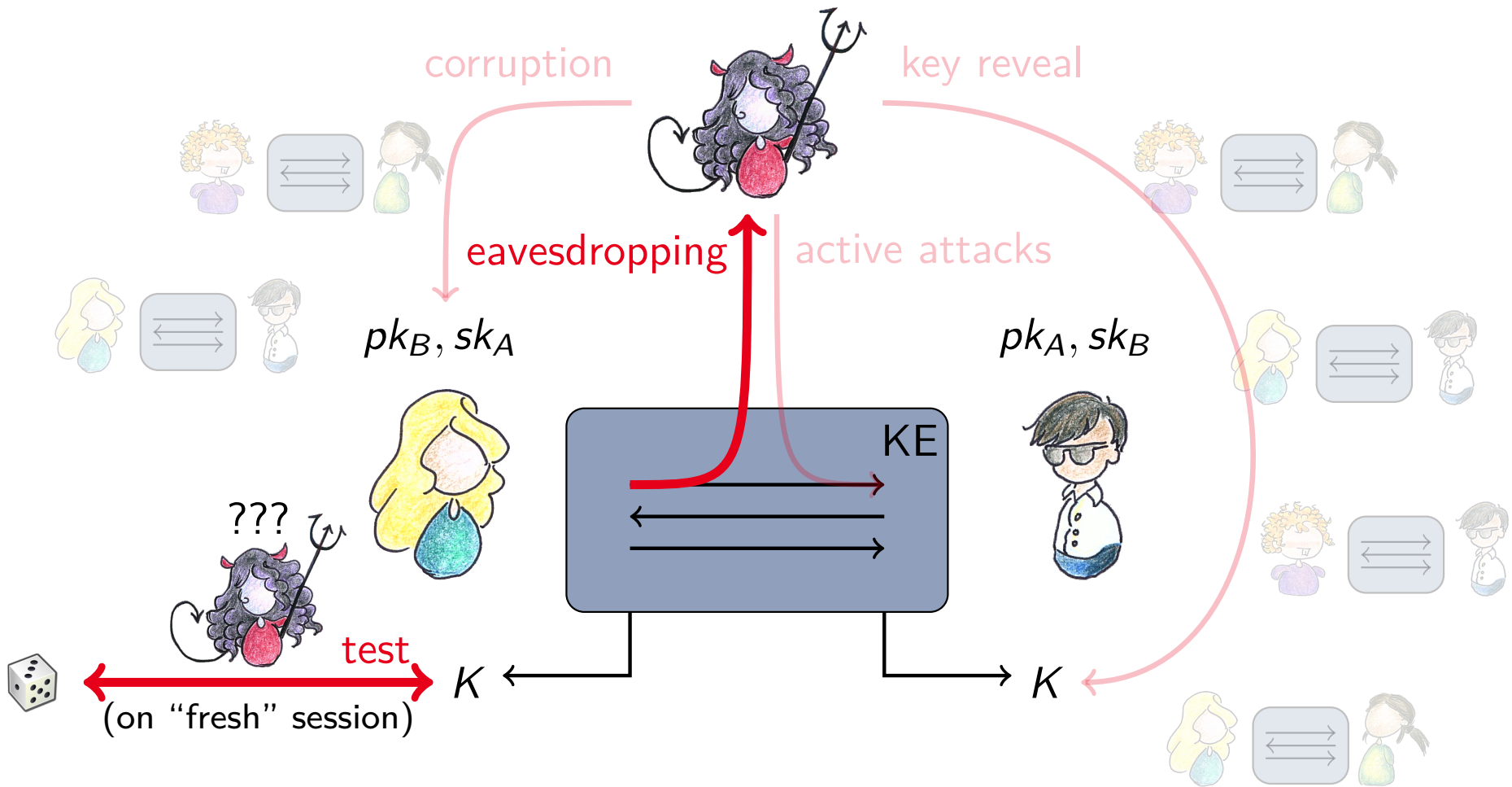
$$\mathsf{Adv}^{\text{Multi-Stage},\mathcal{D}}_{\texttt{TLS1.3-full-1RTT},\mathcal{A}} \leq 6n_s \left(\begin{array}{l} \mathsf{Adv}^{\text{COLL}}_{\text{H},\mathcal{B}_1} + n_u \cdot \mathsf{Adv}^{\text{EUF-CMA}}_{\text{SIG},\mathcal{B}_2} \\ + n_s \left(\begin{array}{l} \mathsf{Adv}^{\text{dual-snPRF-ODH}}_{\text{HKDF.Extract},\mathbb{G},\mathcal{B}_3} + \mathsf{Adv}^{\text{PRF-sec}}_{\text{HKDF.Expand},\mathcal{B}_4} \\ + 2 \cdot \mathsf{Adv}^{\text{PRF-sec}}_{\text{HKDF.Expand},\mathcal{B}_5} + \mathsf{Adv}^{\text{PRF-sec}}_{\text{HKDF.Extract},\mathcal{B}_6} \\ + \mathsf{Adv}^{\text{PRF-sec}}_{\text{HKDF.E} \end{array} \right) \end{array} \right)$$

in the real world, this is **bad**

. . . twice: for  and  — yielding factor #sessions^2

Let's Simplify...

ETH zürich



Let's Simplify... — Can We Do Better?

ETH zürich

- DDH is **rerandomizable**! (or "random self-reducible")
- Given a DDH tuple (g^a , g^b , g^c), where $c = ab$ or c random, we can generate new tuples

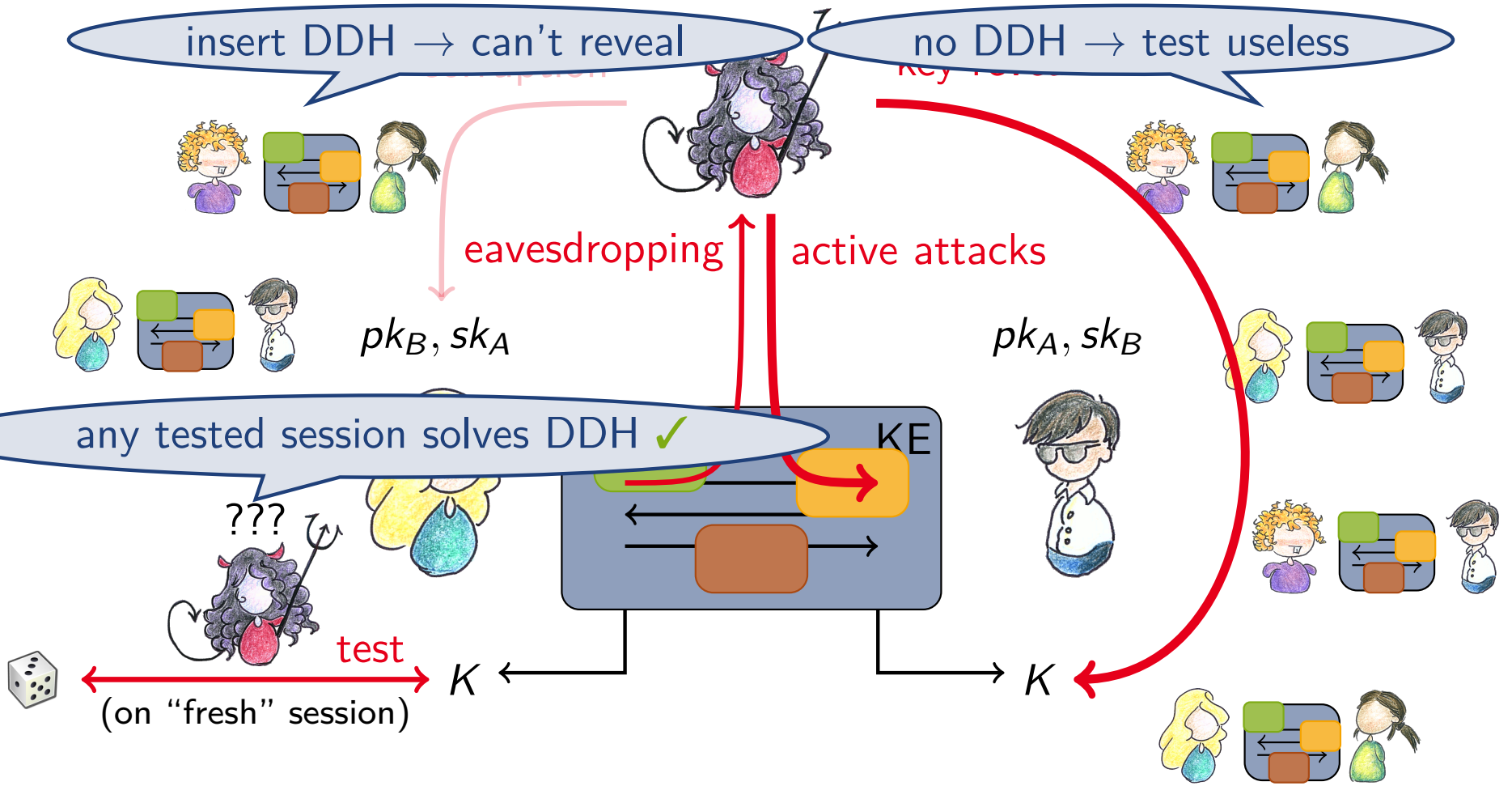
$$(g^{a'}, g^{b'}, g^{c'}) = \left(g^a \cdot g^{s_1},\ (g^b)^r \cdot g^{s_2},\ \underbrace{(g^c)^r \cdot (g^a)^{s_2} \cdot (g^b)^{r \cdot s_1} \cdot g^{s_1 s_2}}_{g^{a'b' + (c - ab)r \mod q}} \right)$$

  for random s_1, s_2, r.
- Deciding if $c' = a'b'$ or c' random for any of the $g^{c'}$ decides it for g^c
- Great — let's embed a DDH challenge into each connection!

[NR97] Naor and Reingold: "Number-theoretic Constructions of Efficient Pseudo-random Functions".
[BBM00] Bellare, Boldyreva, and Micali: "Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements".

The Commitment Problem

ETH zürich



Mind the Gap.

ETH zürich

- Employ the **Gap Diffie–Hellman** (GapDH) assumption.
- GapDH: Solving CDH ("given g^a, g^b, compute g^{ab}") is hard even when given a DDH oracle ("given (g^a, g^b, g^c), return $[ab == c]$")
  - More precisely: we'll use **StrongDH**, where g^a is fixed in the DDH oracle.
- Idea [Coh+19]:
  1. treat key derivation function $K = \mathrm{KDF}(g^{xy})$ as a **random oracle RO**
  2. embed (rerandomized) **StrongDH challenge** (g^a, g^b) in all sessions
  3. replace key K with random (while fresh)
  4.  can only compute the real K by querying $\mathrm{RO}(g^x, g^y, g^{xy}, \dots)$

  ... detect RO queries via DDH oracle ⇒ solve **StrongDH**
- NB: This means moving to the random oracle model.
  ... not a big issue: prior "standard-model" PRF-ODH assumption likely needs RO [BFGJ17]

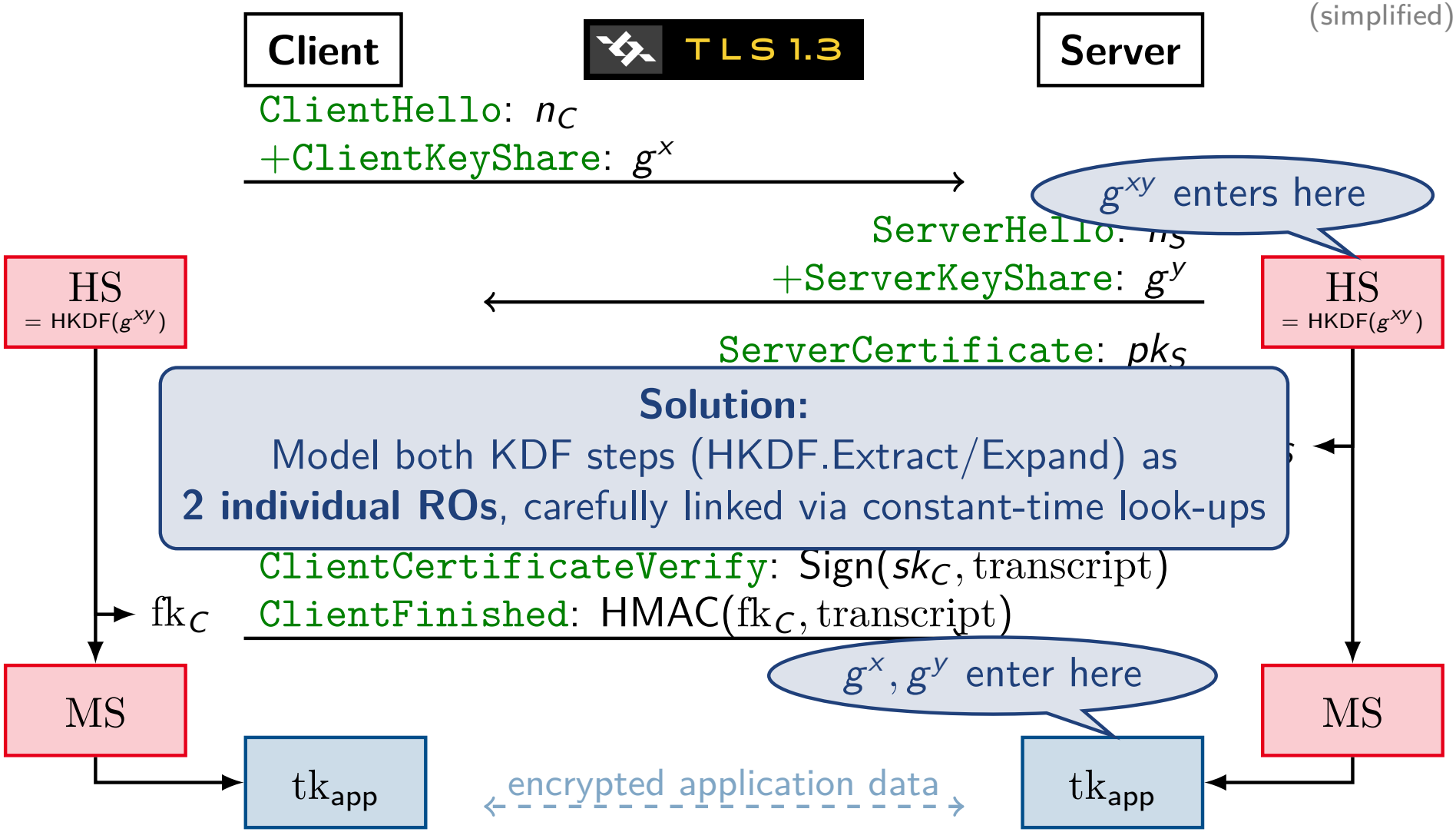
[Coh+19] Cohn-Gordon, Cremers, Gjøsteen, Jacobsen, and Jager: "Highly Efficient Key Exchange Protocols with Optimal Tightness".
[BFGJ17] Brendel, Fischlin, Günther, and Janson: "PRF-ODH: Relations, Instantiations, and Impossibility Results".

The TLS 1.3 Handshake

"Detect RO($g^x, g^y, g^{xy}, \dots$) queries via DDH oracle"

ETH zürich

(simplified)



The TLS 1.3 Handshake

Secure in Practice

ETH zürich

[DG21] Davis, G: "Tighter Proofs for the SIGMA and TLS 1.3 Key Exchange Protocols". ACNS 2021.

$$\mathsf{Adv}^{\text{KE-SEC}}_{\text{TLS 1.3}}(t, q_{\text{N}}, q_{\text{S}}, q_{\text{RS}}, q_{\text{RL}}, q_{\text{T}}) \leq \frac{2q_{\text{S}}^2}{2^{nl} \cdot p} + \mathsf{Adv}^{\text{CR}}_{\text{H}}(t_{\mathcal{B}_1})$$
$$+ 2 \cdot \mathsf{Adv}^{\text{stDH}}_{\mathbb{G}}(t_{\mathcal{B}_2}, q_{\text{RO}}) + \frac{q_{\text{RO}} \cdot q_{\text{S}}}{2^{kl-1}} + \mathsf{Adv}^{\text{mu-EUF-CMA}}_{\text{S}}(t_{\mathcal{B}_3}, q_{\text{N}}, q_{\text{S}}, q_{\text{S}}, q_{\text{RL}})$$
$$+ \mathsf{Adv}^{\text{mu-EUF-CMA}}_{\text{HMAC}}(t_{\mathcal{B}_4}, q_{\text{S}}, q_{\text{S}}, 1, q_{\text{S}}, 1, 0),$$

Core Improvement

StrongDH bound: $2 \cdot \mathsf{Adv}^{\text{stDH}}_{\mathbb{G}}(t_{\mathcal{B}_2}, q_{\text{RO}})$

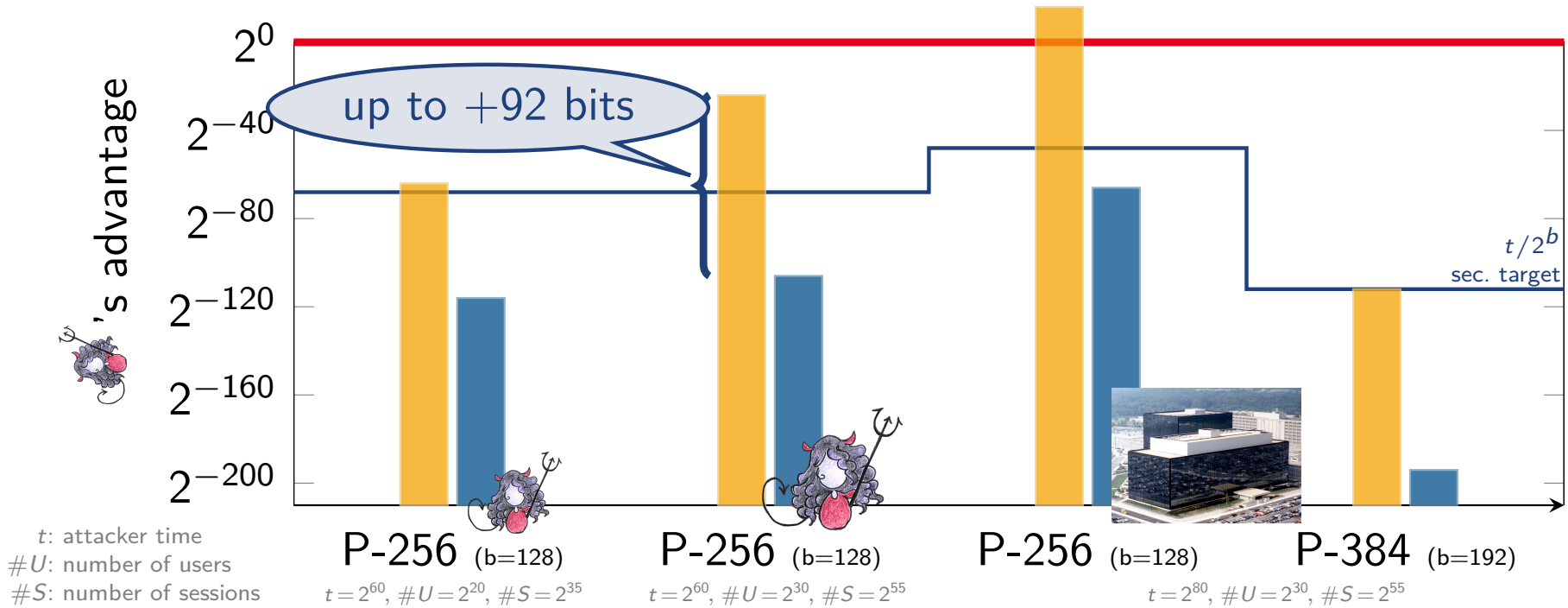
- constant factor / **no guessing** — core improvement by q_{S}^2 over [DFGS21]
- how hard is StrongDH?
  - we prove: $\mathsf{Adv}^{\text{stDH}}_{\mathbb{G}}(t, q) \leq 4t^2/p$ in the generic group model, like DDH
  - in particular, the $q = q_{\text{RO}}$ DDH queries don't deteriorate the GGM bound!
- concurrent & independent work confirms comparable bounds

  [DJ21] Diemert and Jager: "On the Tight Security of TLS 1.3: Theoretically-Sound Cryptographic Parameters for Real-World Deployments".

The TLS 1.3 Handshake

Secure in Practice

ETH zürich



Bottom line: TLS 1.3 (and SIGMA) parameters justified in practice.

They were all along, we just didn't know how to prove better bounds.

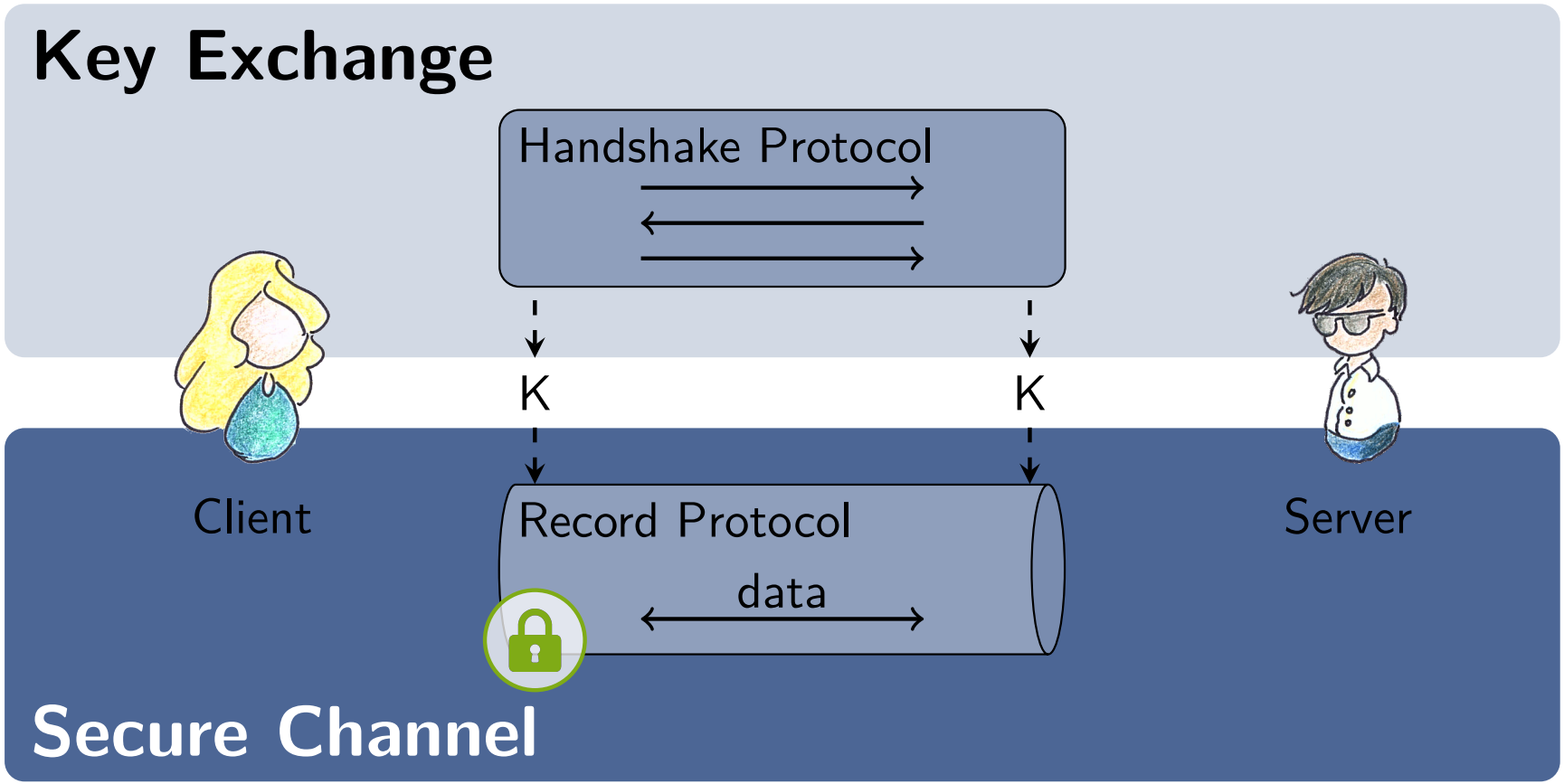
(And we still don't know how to do w/o random oracles. . .)

[DFGS21] Dowling, Fischlin, Günther, and Stebila: "A Cryptographic Analysis of the TLS 1.3 Handshake Protocol".

[DG21] Davis, G: "Tighter Proofs for the SIGMA and TLS 1.3 Key Exchange Protocols".

The Cryptographic Core

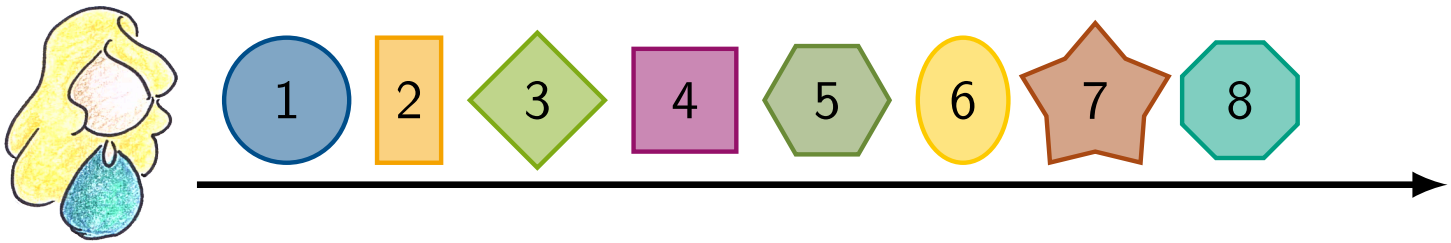
ETH zürich

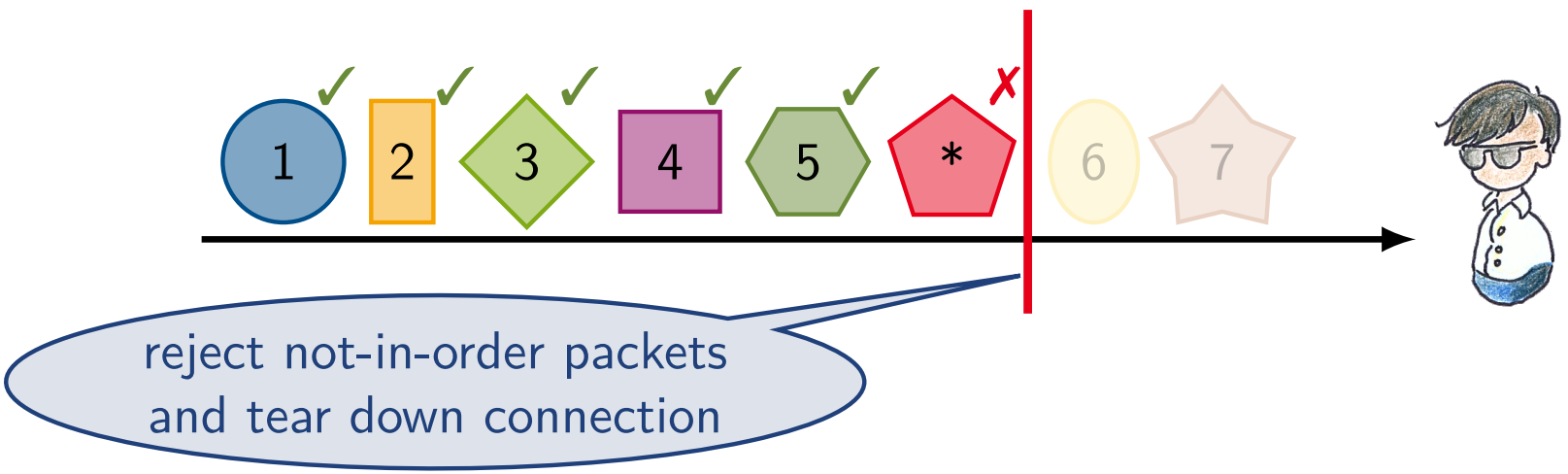


Recap: Secure Channels over TCP

. . . think: TLS

ETH zürich

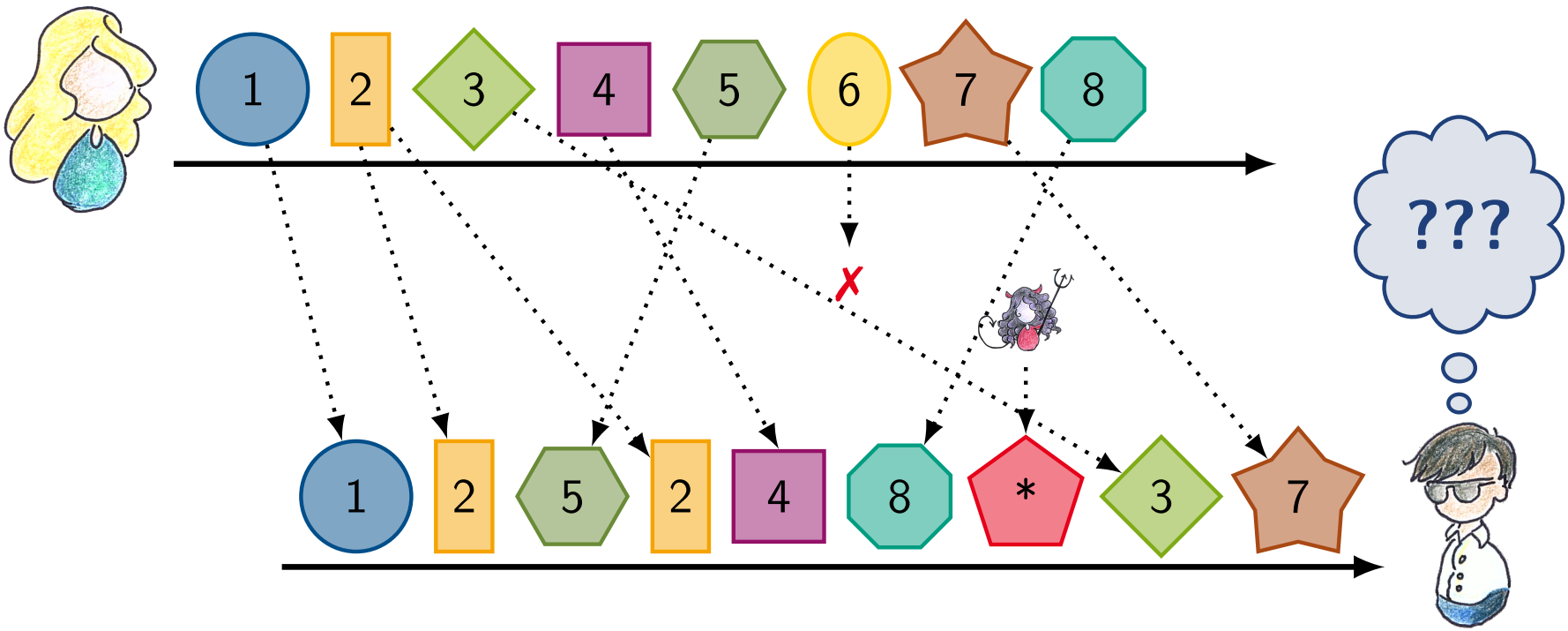




Handling Unreliable Transport

QUIC, DTLS, . . . over UDP

ETH zürich



Handling Unreliable Transport

Many choices. . .

ETH zürich

- **Replays / Duplicates**
  - prevent them?
  - check how far back?

QUIC	DTLS 1.3
MUST prevent	optional
e.g., anti-replay window (IPsec)	

- **Reordering**
  - permitted?
  - by how far max.?

QUIC	DTLS 1.3
. . . well, yes—it's UDP . . .	
dynamic 1–4B window	dynamic 1–2B window

- **Adversarial interaction**
  - Integrity: reject non-genuine packets

QUIC	DTLS 1.3
rely on AEAD	

- But how do you (formally) guarantee that replayed / reordered / adversarial packets don't affect others?

new notion: **Robustness**

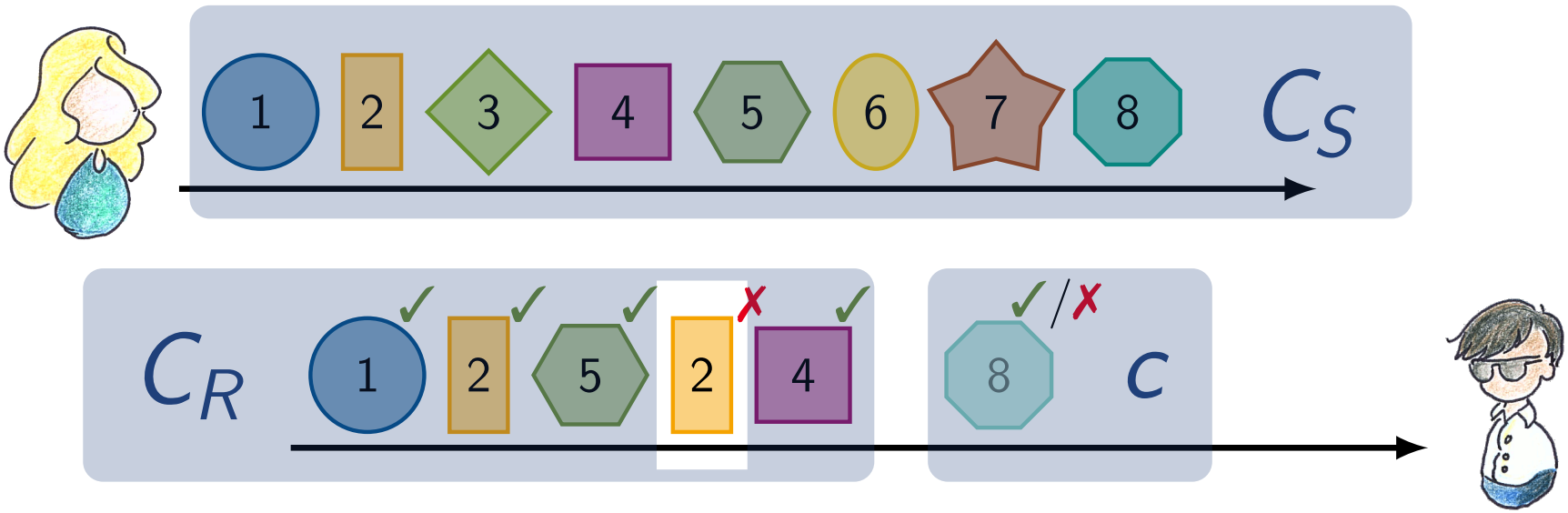
[FGJ20] Fischlin, G, Janson: "Robust Channels: Handling Unreliable Networks in the Record Layers of QUIC and DTLS 1.3".

Generalizing Channel Correctness

. . . beyond prior hierarchies [BKN02,KPB03,BHMS16,RZ18]

ETH zürich

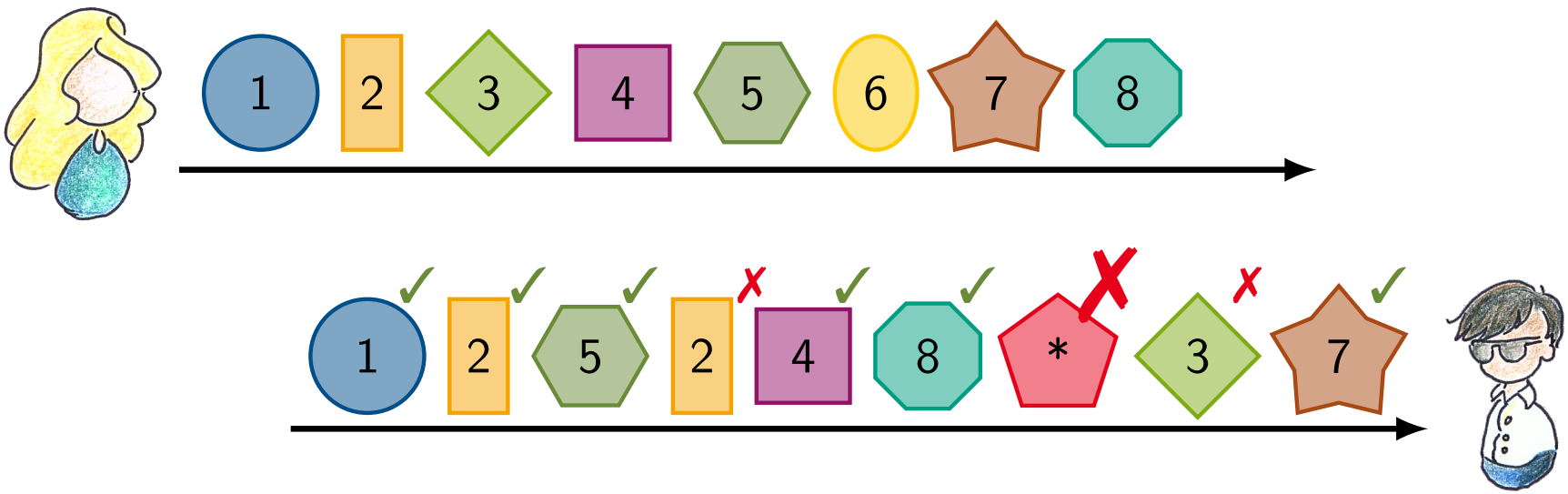
- parameterize what packet (ciphertext) reordering a channel **supports**
- predicate $\mathsf{supp}(C_S, C_R, c) = \checkmark \;/\; \times$ (simplified)
  - C_S: sequence of sent ciphertexts
  - C_R: sequence of *supported* ciphertexts received prior
  - c: next ciphertext to receive
- correctness (only) requires genuine, supported ctxts be correctly decrypted



Defining Robustness (ROB)

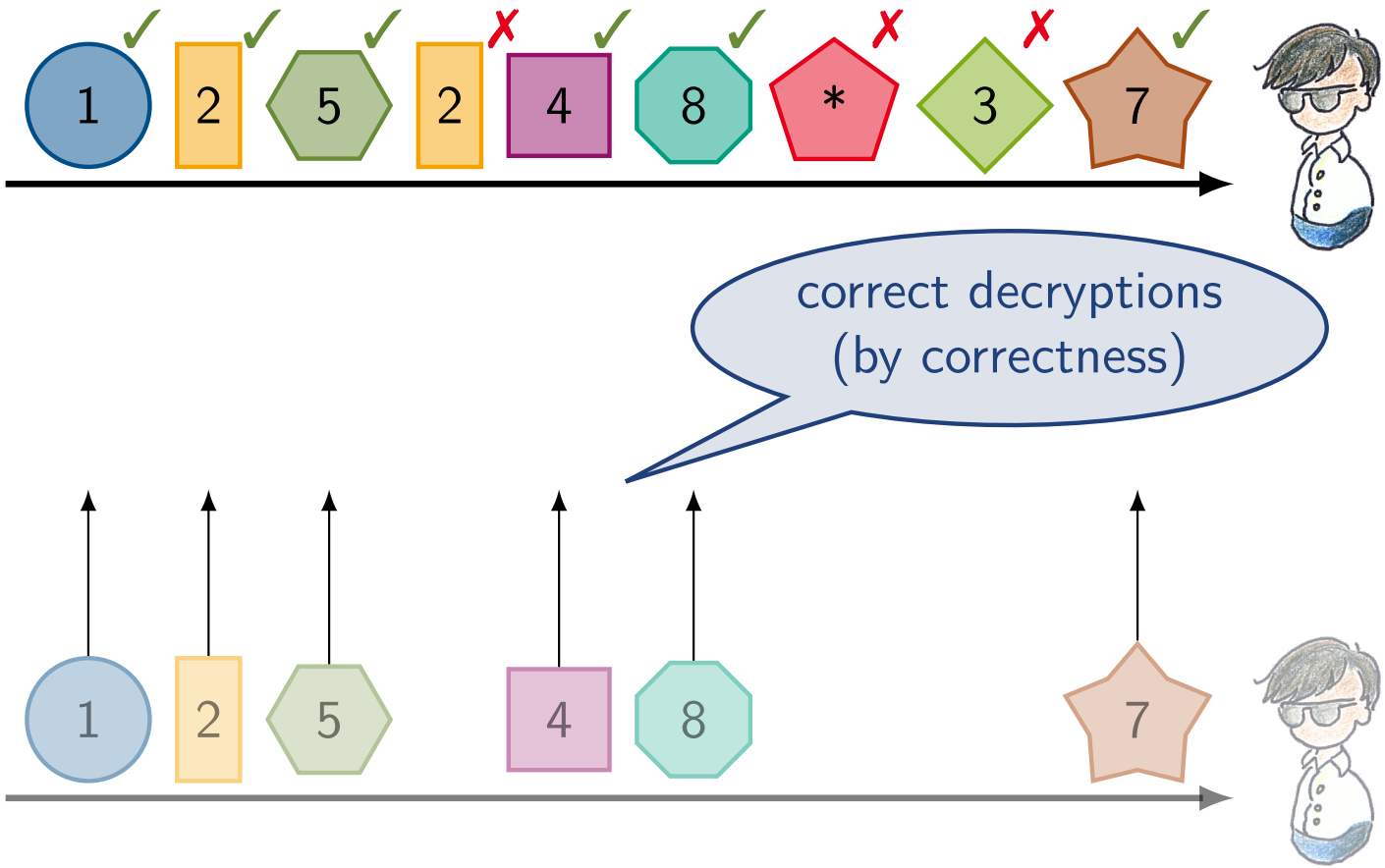
ETH zürich

"malicious packets cannot disturb expected channel behavior"



Defining Robustness (ROB)

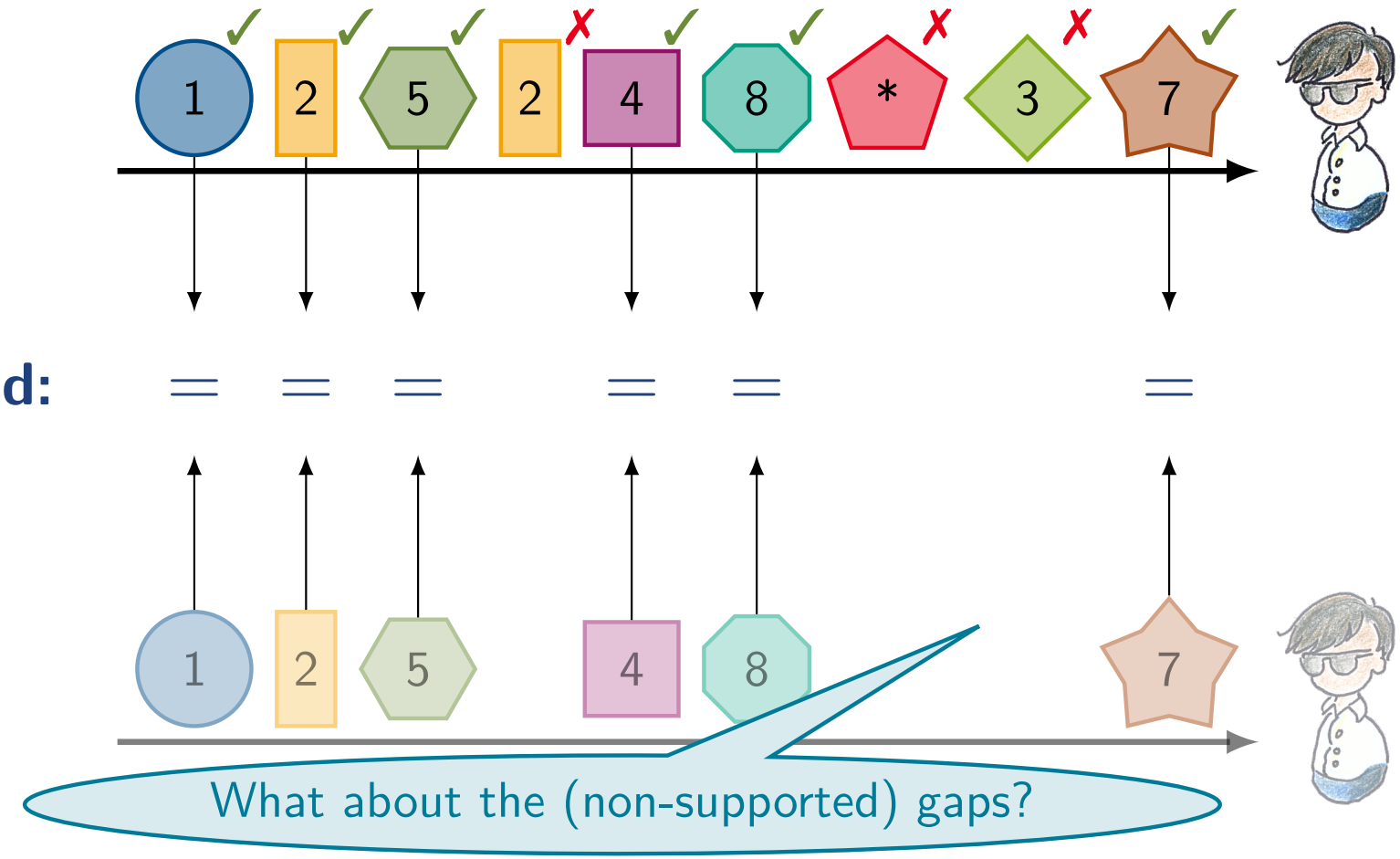
Idea: Compare with the supported, correct sub-trace



Defining Robustness (ROB)

Idea: Compare with the supported, correct sub-trace

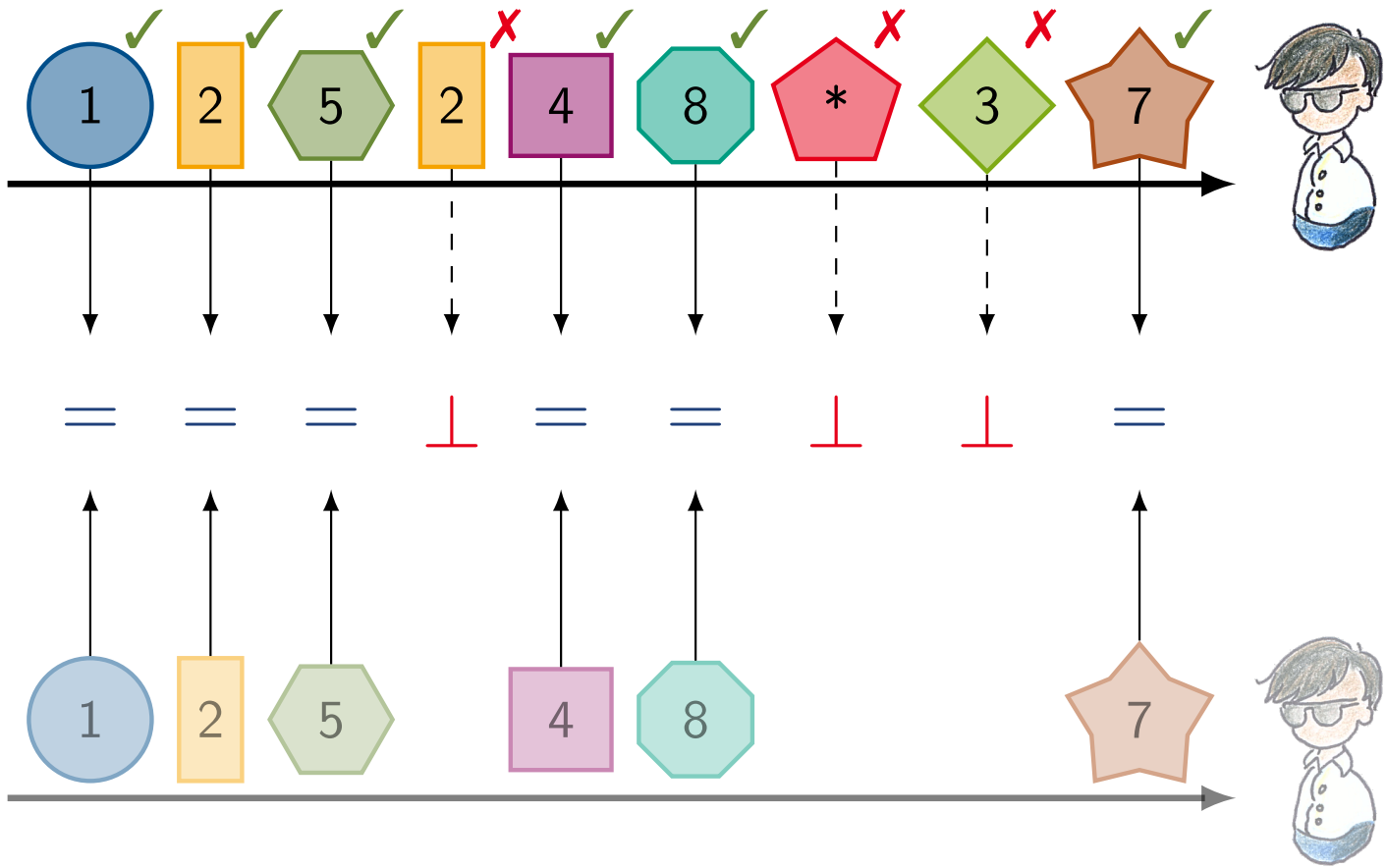
ETH zürich



Robust Integrity (ROB-INT)

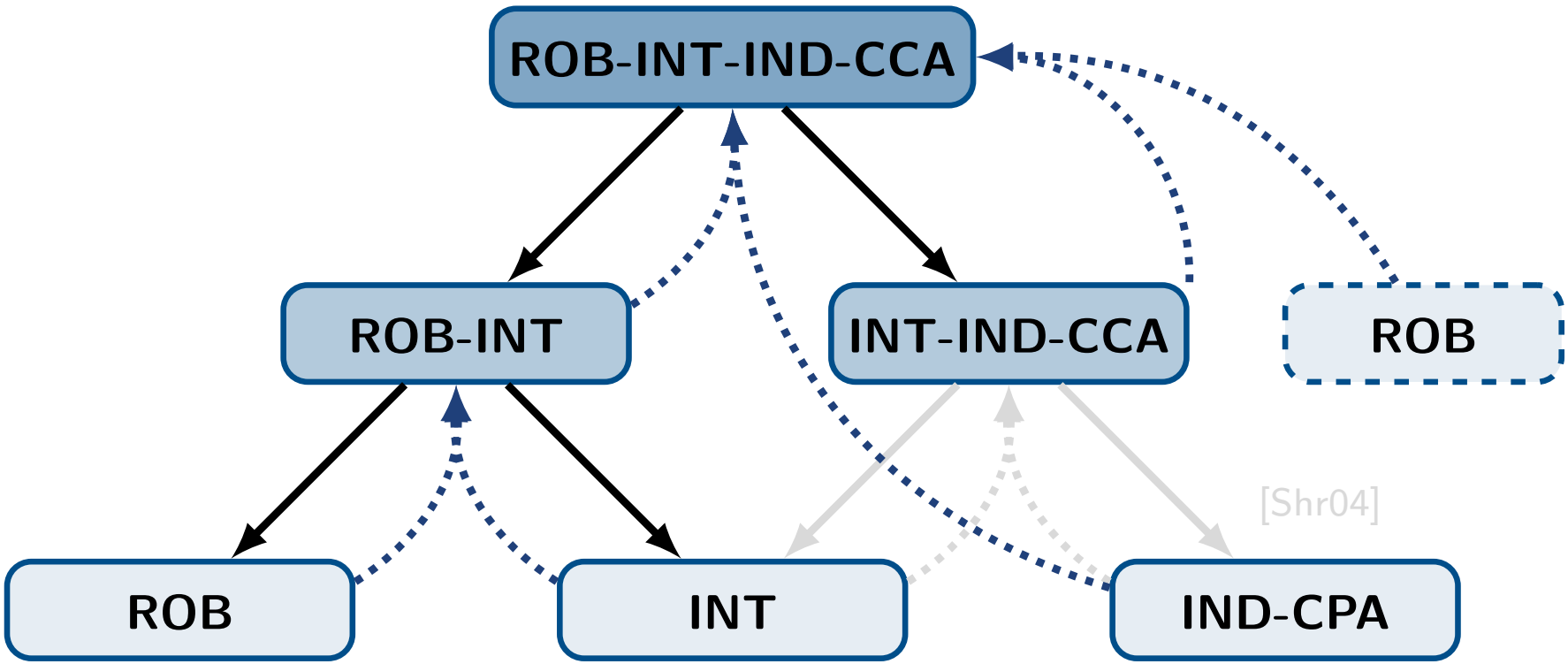
ETH zürich

- join **robustness** and **integrity** for desired property over unreliable transport

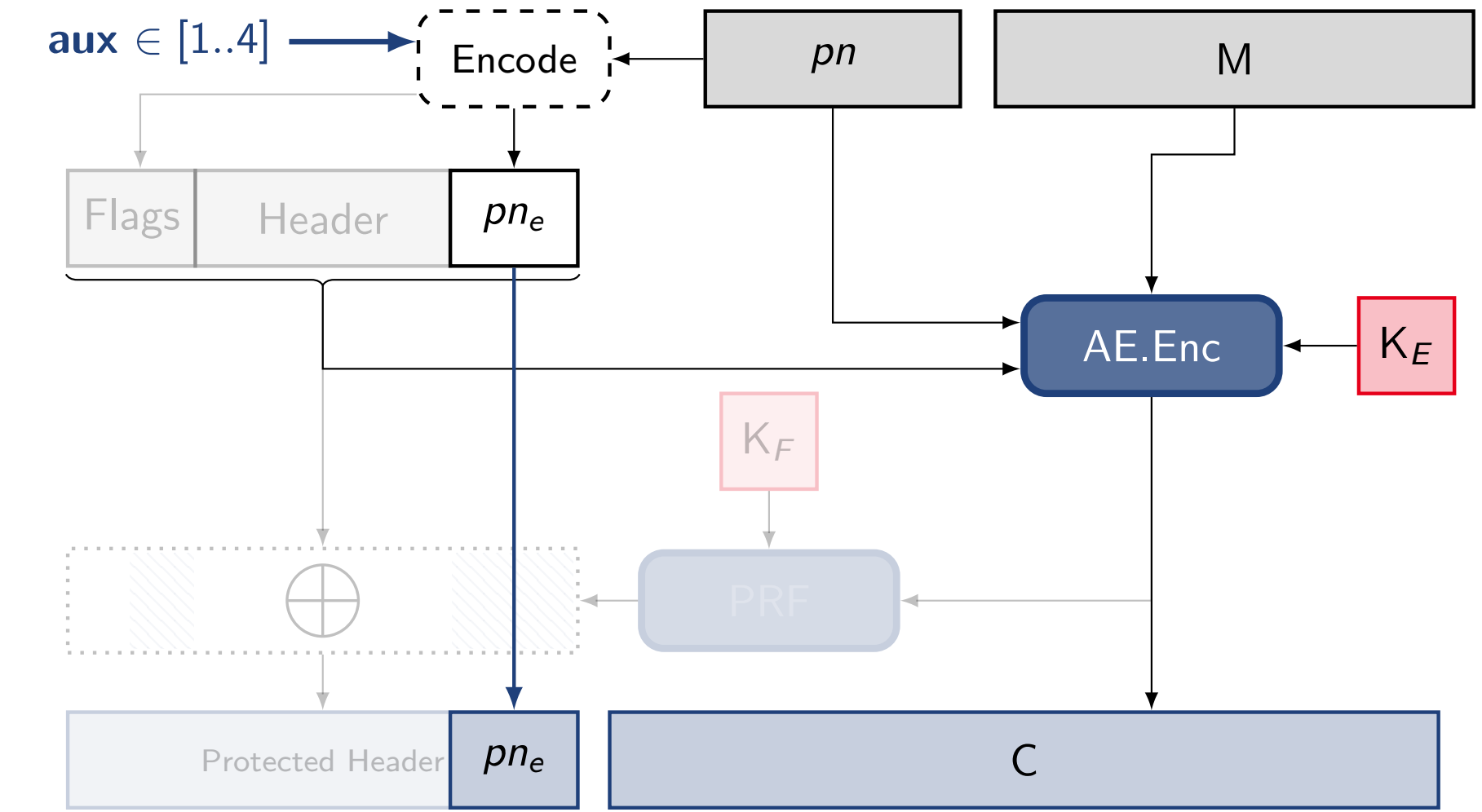


A Robust Hierarchy

ETH zürich



QUIC Payload Encryption

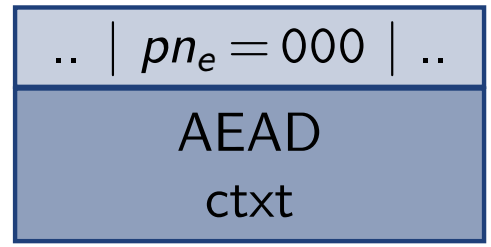


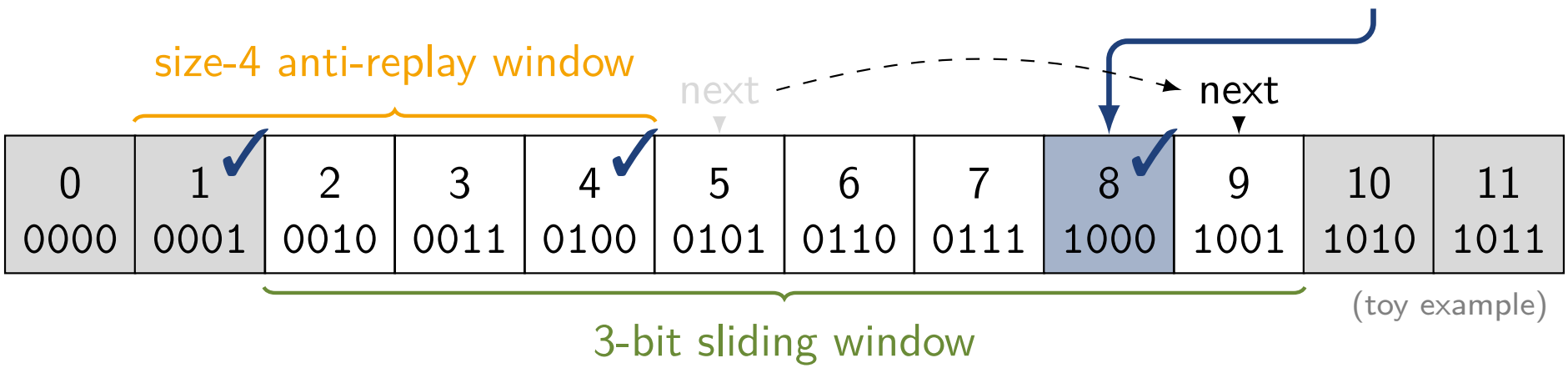
QUIC Channel

Correctness for Dynamic Sliding Windows

ETH zürich

- header (w/ partial packet no. pn_e) + AEAD ciphertext
- pn_e defines $|pn_e|$-**bit dynamic sliding window**
- check for **replays in w_r-sized window**





$$\mathsf{supp}_{dw\text{-}r[w_r]}(C_S, C_R, c) := \left[c \in C_S \wedge c \notin C_R \wedge \mathsf{index}(c, C_S) \in [\mathrm{n} - \min(w_b^c, w_r + 1), \mathrm{n} + w_f^c] \right]$$

supported if in sliding window (dynamic for c) **and** replay window

(simplified)

QUIC Channel

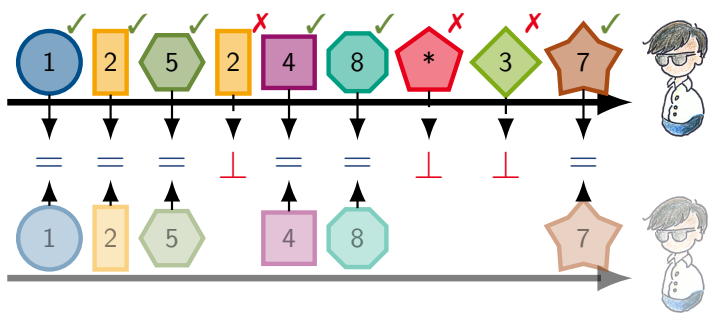
Robust Confidentiality and Integrity (ROB-INT-IND-CCA)

ETH zürich

- use hierarchy: **IND-CPA** + **ROB-INT** = **ROB-INT-IND-CCA**

$$\mathrm{Adv}^{\text{ROB-INT-IND-CCA}}_{\text{QUIC}} \leq \mathrm{Adv}^{\text{priv}}_{\text{AEAD}} + q_R \cdot \mathrm{Adv}^{\text{auth}}_{\text{AEAD}}$$

- important:  can make **multiple forgery attempts**
- factor q_R (#received ciphertexts) **non-tight loss** in security reduction, in contrast to **tight** reduction for TLS 1.3/reliable transport



Responses

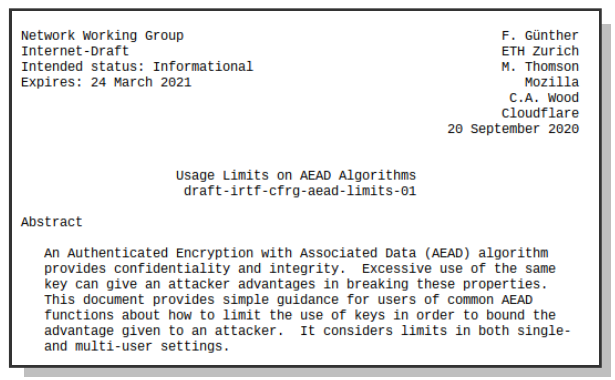
ETH zürich

- IETF WGs updated QUIC / DTLS 1.3 drafts
  to mandate **concrete forgery limits** (beyond confidentiality limits [LP17])

> The integrity protections ... depend on limiting the number of attempts to forge packets. ... QUIC ignores any packet that cannot be authenticated, allowing multiple forgery attempts.

  - QUIC: AES-GCM: 2^{52}, ChaCha20Poly1305: 2^{36}, AES-CCM: $2^{21.5}$
  - DTLS 1.3: AES-GCM, ChaCha20Poly1305: 2^{36}, AES-CCM: $2^{23.5}$

- **Usage Limits on AEAD Algorithms** `draft-irtf-cfrg-aead-limits`
  - new CFRG document draft
    (with Chris Wood, Martin Thomson)
  - provide user guidance on AEAD usage limits
  - confidentiality/integrity, single-/multi-key,
    AES-GCM/AES-CCM/ChaCha20Poly1305



Network Working Group — F. Günther, ETH Zurich
Internet-Draft — M. Thomson, Mozilla
Intended status: Informational — C.A. Wood, Cloudflare
Expires: 24 March 2021 — 20 September 2020

Usage Limits on AEAD Algorithms
draft-irtf-cfrg-aead-limits-01

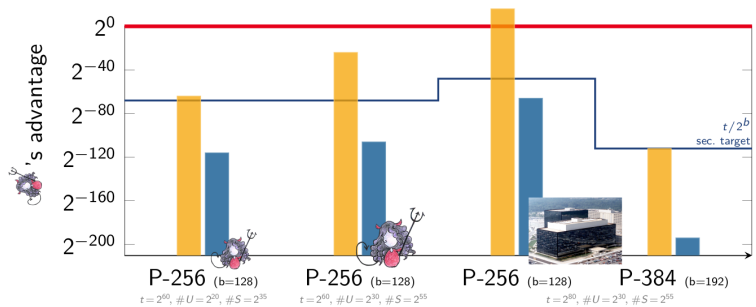
Abstract

An Authenticated Encryption with Associated Data (AEAD) algorithm provides confidentiality and integrity. Excessive use of the same key can give an attacker advantages in breaking these properties. This document provides simple guidance for users of common AEAD functions about how to limit the use of keys in order to bound the advantage given to an attacker. It considers limits in both single- and multi-user settings.

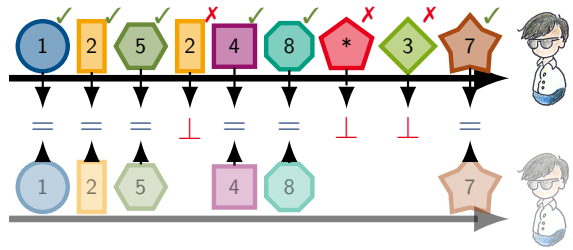
Summary

ETH zürich

- Real-world crypto parameters are often **hard to extract** from analyses
- We revisited (SIGMA and) TLS 1.3 and proved **tighter key exchange security**
  - ✓ confirming deployed parameters in practice



- We introduce new **channel robustness** property
  - ! our QUIC/DTLS 1.3 analysis led to **draft updates**, mandating forgery limits



full versions @ IACR ePrint:

- Tighter Security: `https://ia.cr/2020/1029`
- Robust Channels: `https://ia.cr/2020/718`

Thank You!

mail@**felixguenther.info**

References I

ETH zürich

[BBM00] M. Bellare, A. Boldyreva, and S. Micali. "Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements". In: *EUROCRYPT 2000*. Ed. by B. Preneel. Vol. 1807. LNCS. Springer, Heidelberg, May 2000, pp. 259–274.

[BKN02] M. Bellare, T. Kohno, and C. Namprempre. "Authenticated Encryption in SSH: Provably Fixing The SSH Binary Packet Protocol". In: *ACM CCS 2002*. Ed. by V. Atluri. ACM Press, Nov. 2002, pp. 1–11.

[BR94] M. Bellare and P. Rogaway. "Entity Authentication and Key Distribution". In: *CRYPTO'93*. Ed. by D. R. Stinson. Vol. 773. LNCS. Springer, Heidelberg, Aug. 1994, pp. 232–249.

[BHMS16] C. Boyd, B. Hale, S. F. Mjølsnes, and D. Stebila. "From Stateless to Stateful: Generic Authentication and Authenticated Encryption Constructions with Application to TLS". In: *CT-RSA 2016*. Ed. by K. Sako. Vol. 9610. LNCS. Springer, Heidelberg, 2016, pp. 55–71.

[BFGJ17] J. Brendel, M. Fischlin, F. Günther, and C. Janson. "PRF-ODH: Relations, Instantiations, and Impossibility Results". In: *CRYPTO 2017, Part III*. Ed. by J. Katz and H. Shacham. Vol. 10403. LNCS. Springer, Heidelberg, Aug. 2017, pp. 651–681.

[CK02] R. Canetti and H. Krawczyk. "Security Analysis of IKE's Signature-based Key-Exchange Protocol". In: *CRYPTO 2002*. Ed. by M. Yung. Vol. 2442. LNCS. `http://eprint.iacr.org/2002/120/`. Springer, Heidelberg, Aug. 2002, pp. 143–161.

[Coh+19] K. Cohn-Gordon, C. Cremers, K. Gjøsteen, H. Jacobsen, and T. Jager. "Highly Efficient Key Exchange Protocols with Optimal Tightness". In: *CRYPTO 2019, Part III*. Ed. by A. Boldyreva and D. Micciancio. Vol. 11694. LNCS. Springer, Heidelberg, Aug. 2019, pp. 767–797.

References II

ETH zürich

[DG21] H. Davis and F. Günther. "Tighter Proofs for the SIGMA and TLS 1.3 Key Exchange Protocols". In: *19th International Conference on Applied Cryptography and Network Security (ACNS 2021)*. Lecture Notes in Computer Science. To appear. Springer, June 2021.

[DJ21] D. Diemert and T. Jager. "On the Tight Security of TLS 1.3: Theoretically-Sound Cryptographic Parameters for Real-World Deployments". In: *Journal of Cryptology* (2021). To appear. Available as Cryptology ePrint Archive, Report 2020/726. `https://eprint.iacr.org/2020/726`.

[DH76] W. Diffie and M. E. Hellman. "New Directions in Cryptography". In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654.

[DFGS21] B. Dowling, M. Fischlin, F. Günther, and D. Stebila. "A Cryptographic Analysis of the TLS 1.3 Handshake Protocol". In: *Journal of Cryptology* (2021). To appear. Available as Cryptology ePrint Archive, Report 2020/1044. `https://eprint.iacr.org/2020/1044`.

[FGJ20] M. Fischlin, F. Günther, and C. Janson. "Robust Channels: Handling Unreliable Networks in the Record Layers of QUIC and DTLS 1.3". Cryptology ePrint Archive, Report 2020/718. `https://eprint.iacr.org/2020/718`. 2020.

[KPB03] T. Kohno, A. Palacio, and J. Black. "Building Secure Cryptographic Transforms, or How to Encrypt and MAC". Cryptology ePrint Archive, Report 2003/177. `http://eprint.iacr.org/2003/177`. 2003.

[Kra03] H. Krawczyk. "SIGMA: The "SIGn-and-MAc" Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols". In: *CRYPTO 2003*. Ed. by D. Boneh. Vol. 2729. LNCS. Springer, Heidelberg, Aug. 2003, pp. 400–425.

References III

ETH zürich

[LP17] A. Luykx and K. G. Paterson. "Limits on Authenticated Encryption Use in TLS". http://www.isg.rhul.ac.uk/~kp/TLS-AEbounds.pdf. Aug. 2017.

[NR97] M. Naor and O. Reingold. "Number-theoretic Constructions of Efficient Pseudo-random Functions". In: *38th FOCS*. IEEE Computer Society Press, Oct. 1997, pp. 458–467.

[RZ18] P. Rogaway and Y. Zhang. "Simplifying Game-Based Definitions - Indistinguishability up to Correctness and Its Application to Stateful AE". In: *CRYPTO 2018, Part II*. Ed. by H. Shacham and A. Boldyreva. Vol. 10992. LNCS. Springer, Heidelberg, Aug. 2018, pp. 3–32.

[Shr04] T. Shrimpton. "A Characterization of Authenticated-Encryption as a Form of Chosen-Ciphertext Security". Cryptology ePrint Archive, Report 2004/272. http://eprint.iacr.org/2004/272. 2004.