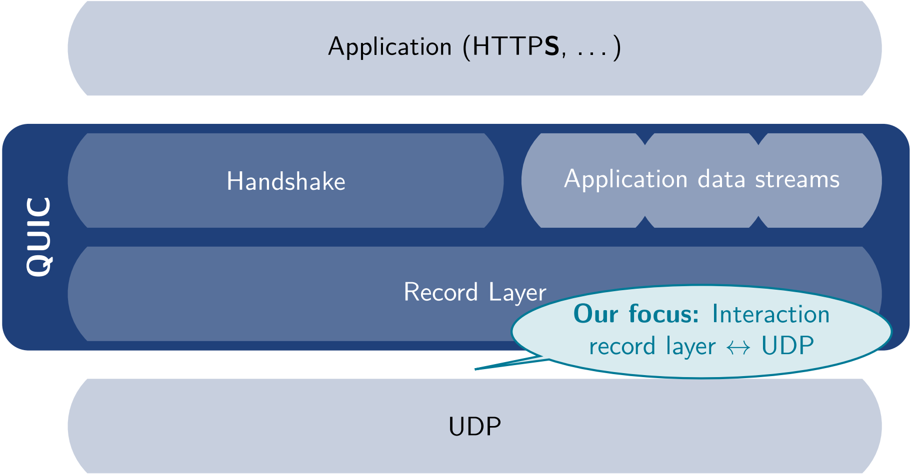
Robust Channels

Handling Unreliable Network Messages in QUIC's Record Layer

Marc Fischlin, **Felix Günther**, Christian Janson

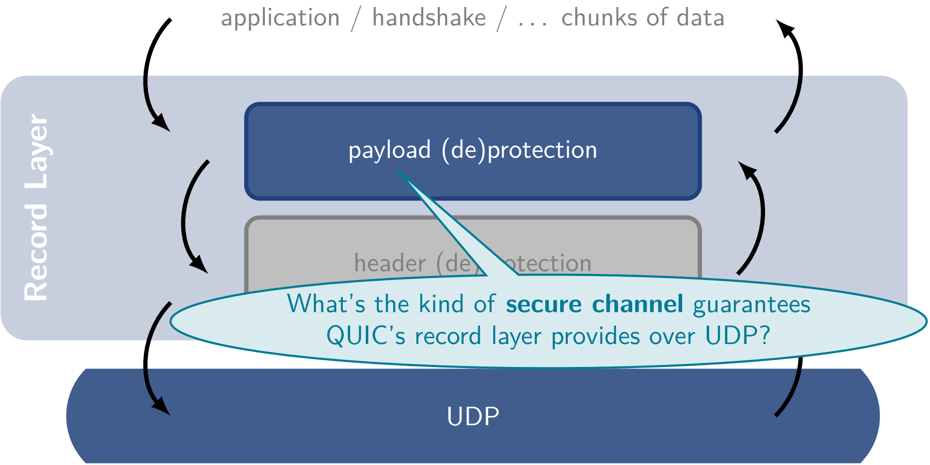
QUIC within the Network Stack



The QUIC Record Layer

(highly simplified)

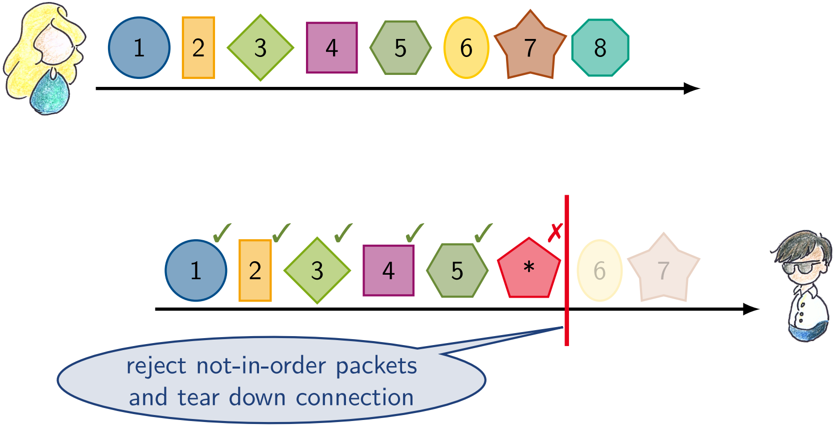
ETH zürich



Recap: Secure Channels over TCP

... think: TLS

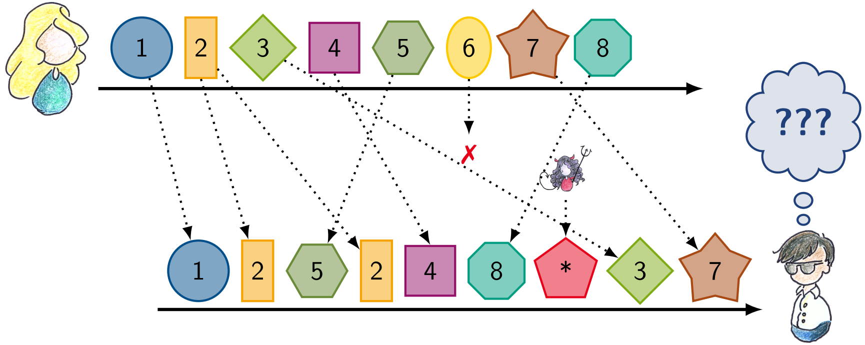
ETH zürich



drawings by *Giorgia Azzurra Marson*

Handling Unreliable Transport

QUIC, DTLS, ... over UDP



Handling Unreliable Transport

Many choices...

- **Replays / Duplicates**
  - prevent them? — **QUIC**: MUST prevent
  - check how far back? — **QUIC**: e.g., replay-check window (IPsec)
- **Reordering**
  - permitted? — **QUIC**: well, yes—it's UDP
  - by how far max.? — **QUIC**: dynamic sliding window
- **Adversarial interaction**
  - Integrity: always want to reject non-genuine packets — **QUIC**: use AEAD
  - But how do you (formally) guarantee that replayed / reordered / adversarial packets don't affect others?

Our Contributions

- **Generic channel model** capturing handling of unreliable transport
- New notion: **Robustness**
  — *"malicious packets cannot disturb expected channel behavior"*
- Assess **QUIC**'s packet encryption as [robust + secure?] channel
  - we also analyze the similar **DTLS 1.3** record layer

We're not the first to look at channels. . .

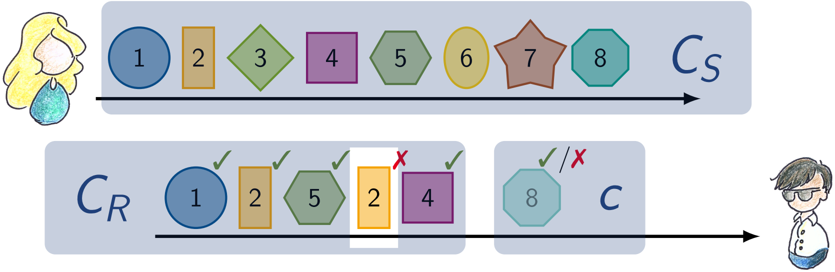
- initial (game-based security) formalization by [BKN02]
  - (stateful) confidentiality (IND-CCA) and integrity (INT-CTXT)
  - assuming reliable transport $\rightarrow$ reject upon/after first deviation
  - most cryptographic channel models follow this approach

- approaches towards a hierarchy of channels [KPB03,BHMS16,RZ18]
  - different levels of permissible reordering & replays
  - yet, these don't capture QUIC's sliding-window approach

- prior work on QUIC
  - don't consider the fine-grained reordering/replay protection [LJBN15,CJJ+19]
  - or remain on the AEAD-primitive level [DLFP+20,BGT20]

Generalizing Channel Correctness

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

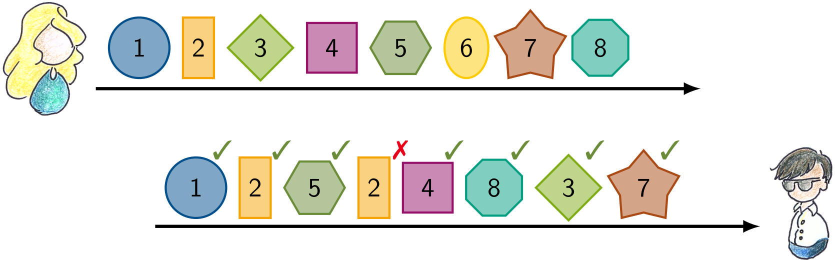


Generalizing Channel Correctness

Example support class: $\mathsf{supp}_{no\text{-}r}$ (no order, global anti-replay)

$$\mathsf{supp}_{no\text{-}r}(C_S, C_R, c) := \left[c \in C_S \wedge c \notin C_R\right]$$

- corresponds to level 2 of [BHMS16] $\neq$ DTLS (1.2)



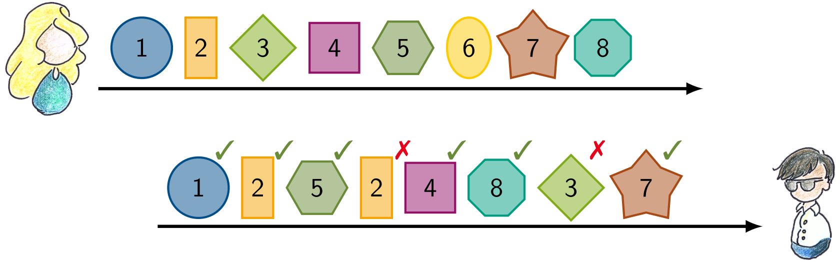
Generalizing Channel Correctness

Example support class: $\text{supp}_{\textit{no-r}[w_r]}$ (no order, anti-replay window)

$$\text{supp}_{\textit{no-r}[w_r]}(C_S, C_R, c) := \left[c \in C_S \wedge c \notin C_R \wedge \underline{\text{index}(c, C_S) \geq \text{m} - w_r} \right]$$

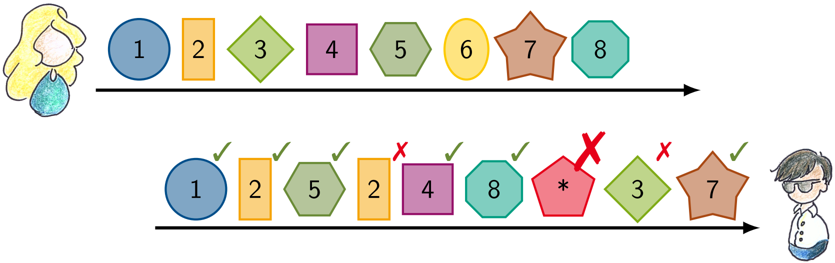
m: highest received index / packet number

- this is DTLS 1.2
- example below: $w_r = 4$



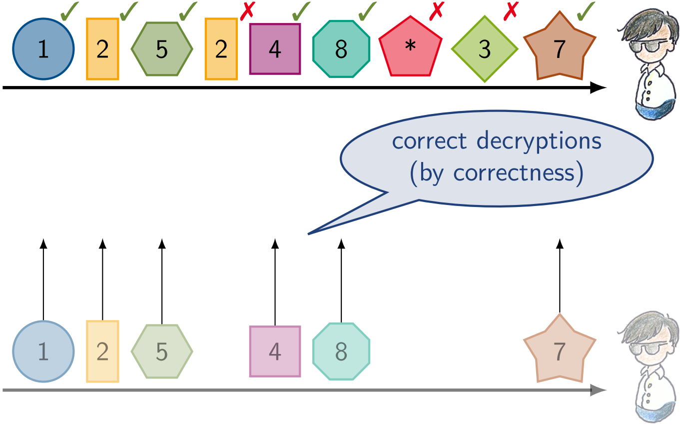
Defining Robustness (ROB)

"malicious packets cannot disturb expected channel behavior"



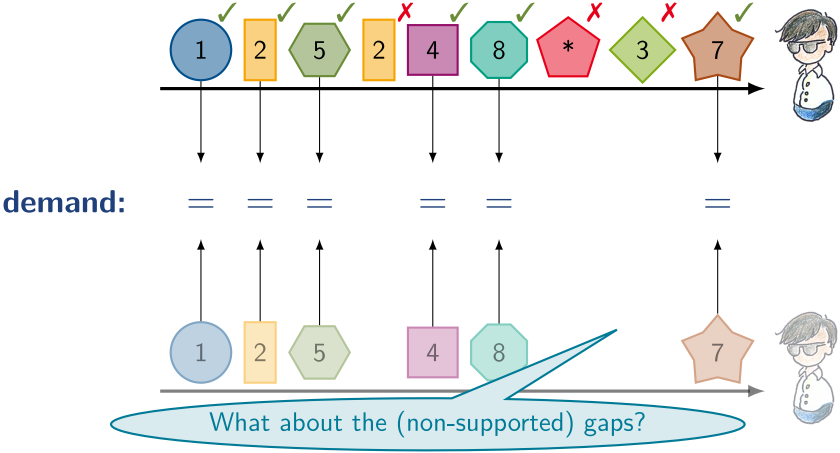
Defining Robustness (ROB)

Idea: Compare with the supported, correct sub-trace



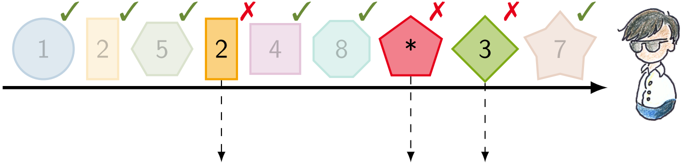
Defining Robustness (ROB)

Idea: Compare with the supported, correct sub-trace



Integrity (INT)

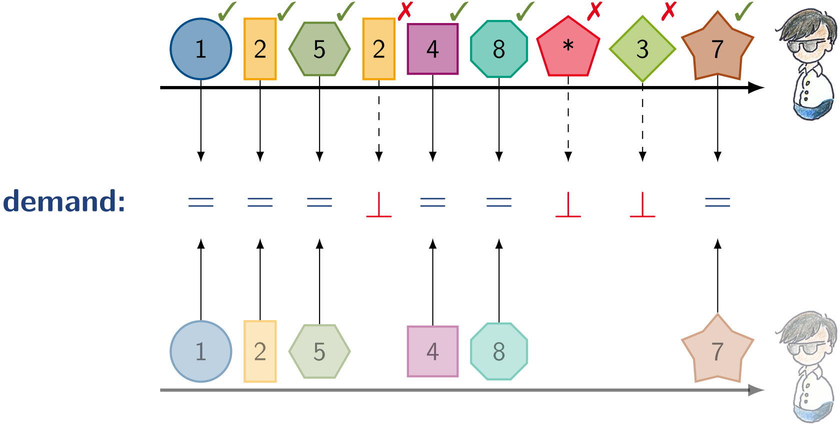
. . . wrt. supp predicate



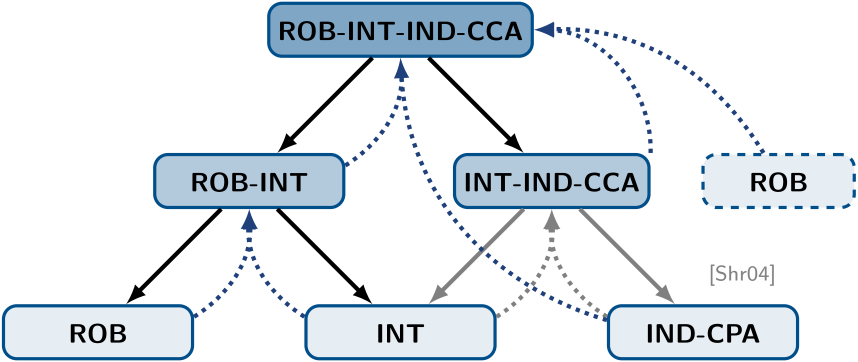
demand: $\perp$ $\perp$ $\perp$

Robust Integrity (ROB-INT)

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



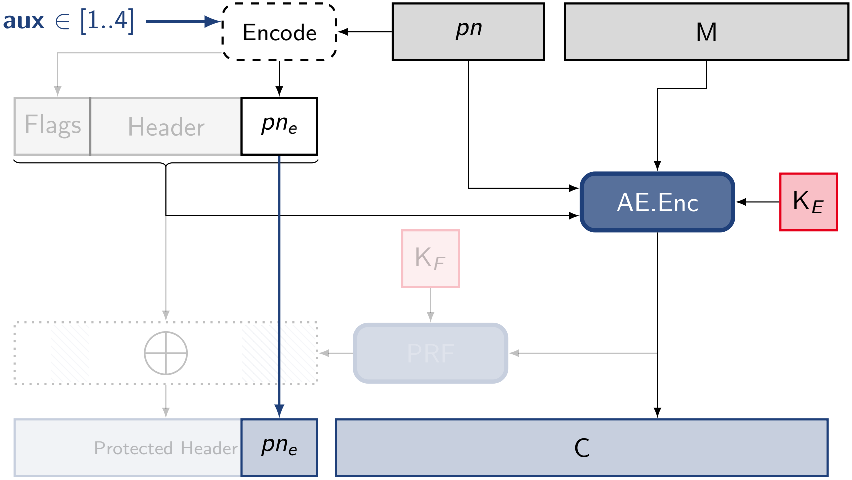
A Robust Hierarchy



all notions parameterized by same supp predicate

QUIC Payload Encryption

ETH zürich



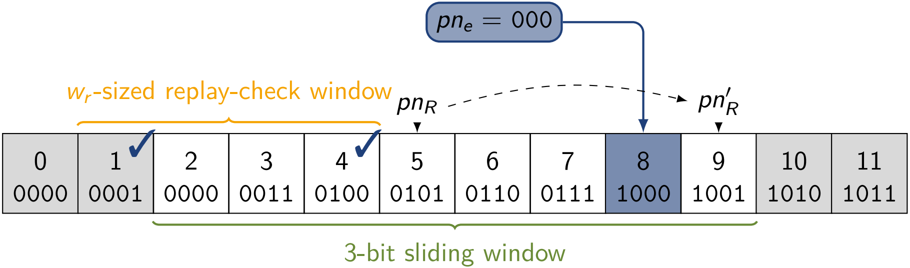
QUIC Channel

Dynamic Sliding Window

ETH zürich

- interpret pn_e in $|pn_e|$ **bit dynamic window** around next expected (pn_R)
- check for **replays in w_r sized window** back from pn_R

- **(toy) example:** 3-bit sliding window, replay window $w_r = 4$, $pn_R = 5$



QUIC Channel

Correctness

$$\mathsf{supp}_{dw\text{-}r[w_r]}(AC_S, C_R, c) :=$$

$$\Big[c \in C_S \wedge c \notin C_R \wedge \mathsf{index}(c, C_S) \in [\mathsf{n} - \min(w_b^c, w_r + 1), \mathsf{n} + w_f^c]\Big]$$

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

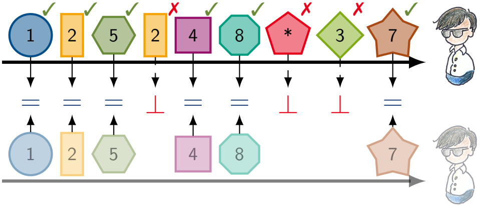
- **QUIC** matches this
  - based on correct decoding property when interpreting pn_e

QUIC Channel

Robust Integrity (ROB-INT)

Intuition:

- non-supported ctxts are rejected as AEAD error (or replays)
  - reordered out-of-window: pn_e decodes to different pn
  - or: actual adversarial forgery
- either would require **AEAD authenticity break** (via game-based reduction)
  - but:  can try multiple times
  - factor q_R (#received ciphertexts) loss in security reduction



QUIC Channel: Overall Security

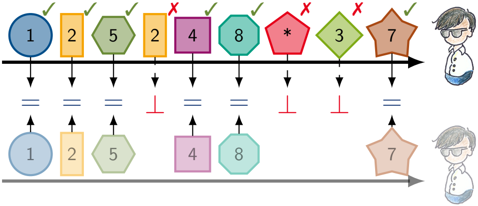
Robust Confidentiality and Integrity (ROB-INT-IND-CCA)

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

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

* for technical reasons (uniqueness of ciphertexts) there's an additional q_S^2 factor

- q_r loss matches that attacks become easier over unreliable transports [AP13]



Summary

- QUIC's channel construction ensures **robustness** over unreliable transport

- We establish this in a **generic channel model**
  - parameterized in what reordering / replay / ... is supported
  - introducing robustness as a first-class security property

- Our model captures **QUIC's dynamic sliding-window & replay-checking**
  - ... but also other settings like DTLS 1.2, DTLS 1.3, etc.
  - confirm QUIC achieves intended robust confidentiality and integrity

- Preliminary preprint for QUIPS 2020:
  `felixguenther.info/Q20_RC.pdf`

Thank You!

mail@**felixguenther.info**

References I

[AP13] N. J. AlFardan and K. G. Paterson. "Lucky Thirteen: Breaking the TLS and DTLS Record Protocols". In: *2013 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, May 2013, pp. 526–540.

[BGT20] M. Bellare, F. Günther, and B. Tackmann. *Two-Tier Authenticated Encryption: Nonce Hiding in QUIC*. QUIPS 2020 Workshop. 2020.

[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.

[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.

[CJJ+19] S. Chen, S. Jero, M. Jagielski, A. Boldyreva, and C. Nita-Rotaru. "Secure Communication Channel Establishment: TLS 1.3 (over TCP Fast Open) vs. QUIC". In: *ESORICS 2019, Part I*. Ed. by K. Sako, S. Schneider, and P. Y. A. Ryan. Vol. 11735. LNCS. Springer, Heidelberg, Sept. 2019, pp. 404–426.

[DLFP+20] A. Delignat-Lavaud, C. Fournet, B. Parno, J. Protzenko, T. Ramananandro, J. Bosamiya, J. Lallemand, I. Rakotonirina, and Y. Zhou. *A Security Model and Fully Verified Implementation for the IETF QUIC Record Layer*. Cryptology ePrint Archive, Report 2020/114. `https://eprint.iacr.org/2020/114`. 2020.

References II

[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.

[LJBN15] R. Lychev, S. Jero, A. Boldyreva, and C. Nita-Rotaru. "How Secure and Quick is QUIC? Provable Security and Performance Analyses". In: *2015 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, May 2015, pp. 214–231.

[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.