ETH zürich

Two-Tier Authenticated Encryption

Nonce Hiding in QUIC

Mihir Bellare, **Felix Günther**, Björn Tackmann

UC San Diego

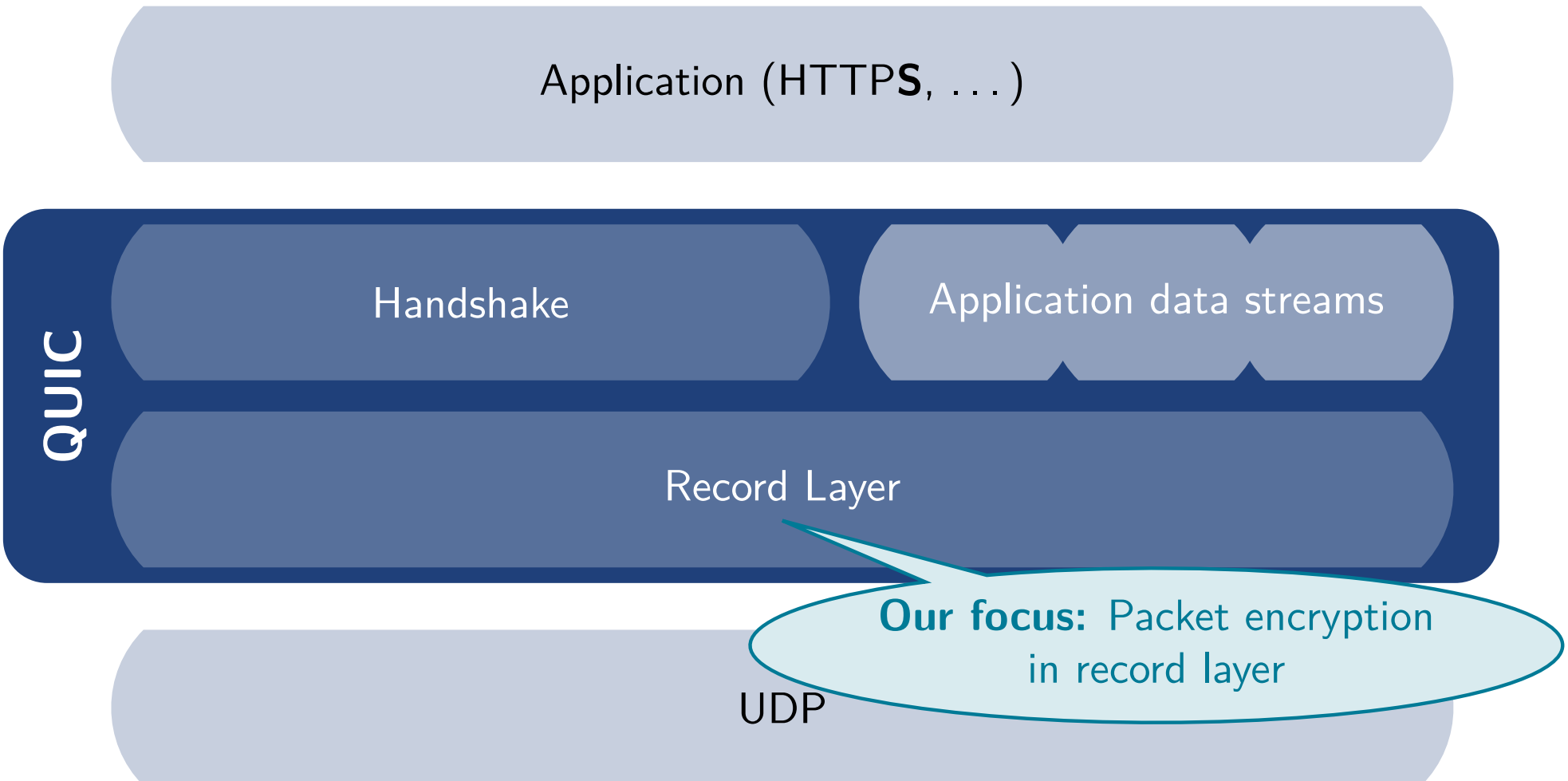
ETH zürich

DFG Deutsche Forschungsgemeinschaft German Research Foundation

DFINITY

QUIC within the Network Stack

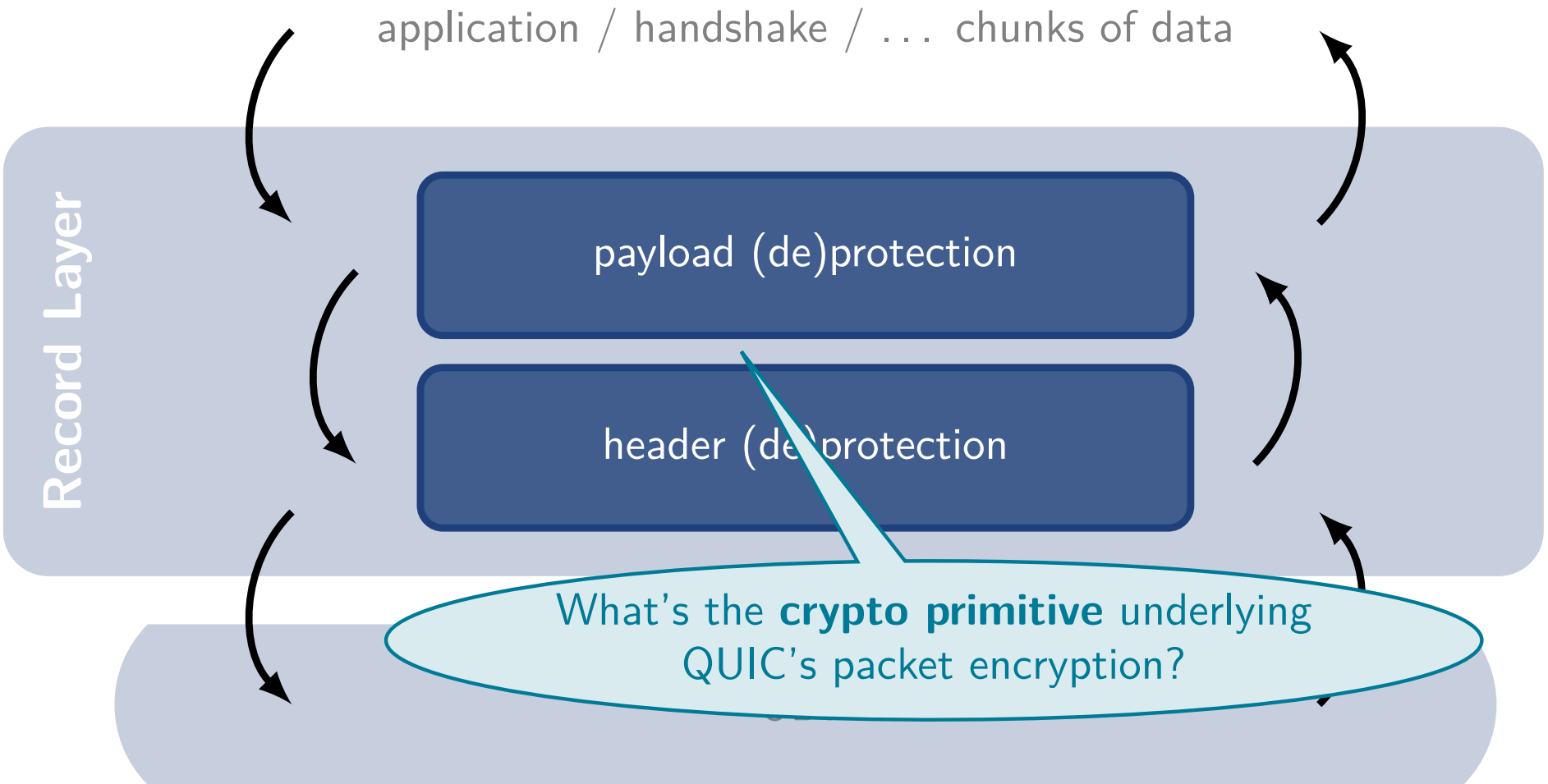
ETH zürich



The QUIC Record Layer

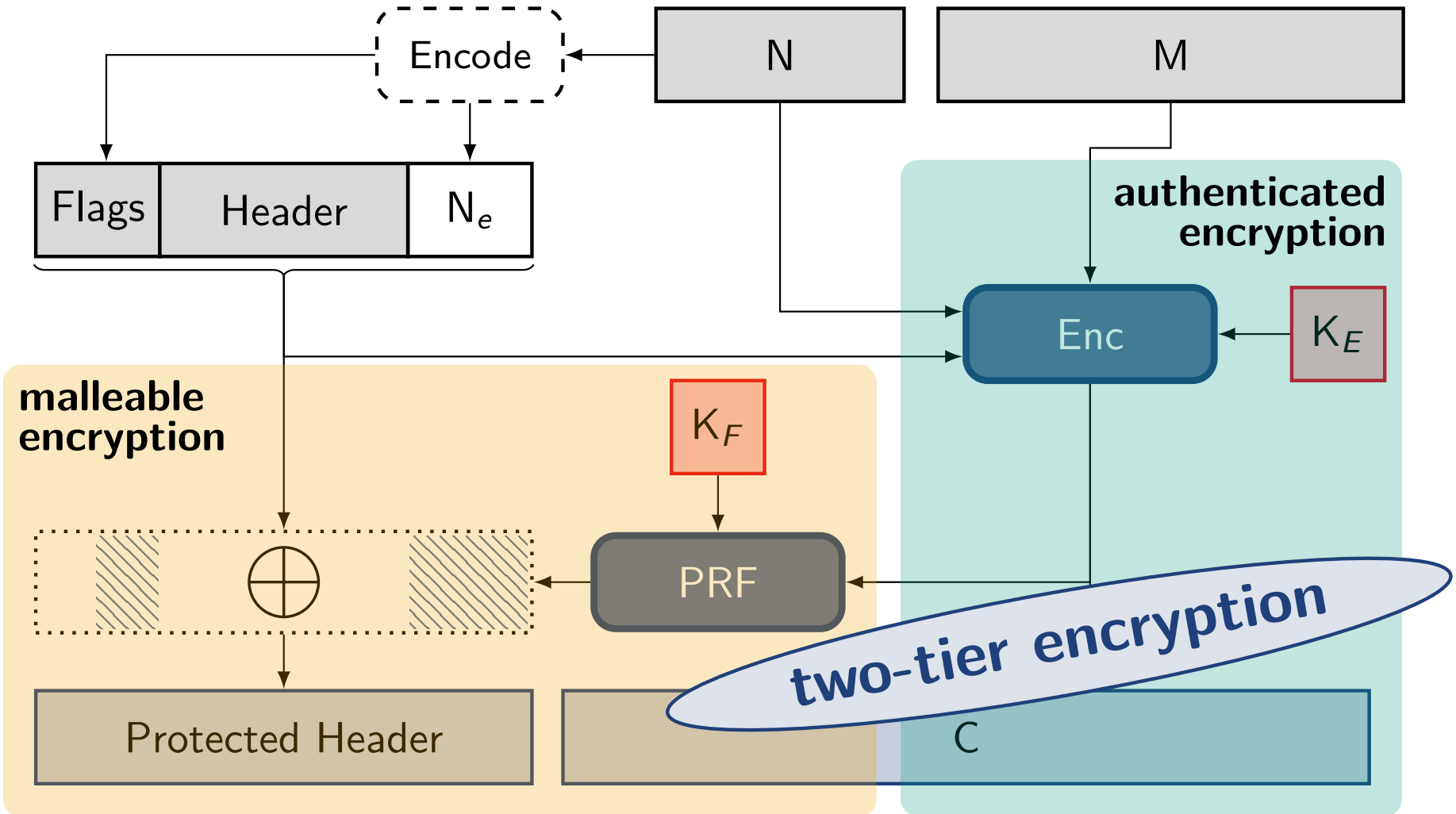
(highly simplified)

ETH zürich



QUIC Packet Encryption (QPE)

ETH zürich



Why a dedicated primitive?

ETH zürich

- formalize statements about expected properties of QPE
  - nonce-hiding [BNT19]
  - header-hiding *(new)*
  - forward secrecy through key updates (adopted from TLS 1.3 [GM17])
- explore variant constructions
  - potential for stronger security?
- establish a primitive that can be used elsewhere

Recap: Classical Nonce-based AE (NBE1)

[Rog02]

ETH zürich

$$C \leftarrow \mathsf{SE}_1.\mathsf{Enc}(K, N, M, H)$$
$$M \leftarrow \mathsf{SE}_1.\mathsf{Dec}(K, N, C, H)$$

- Enc **and** Dec get nonce N as input
- ... nonce has to travel with the ciphertext, somehow

- **What if you (QUIC) want to hide the nonce?**

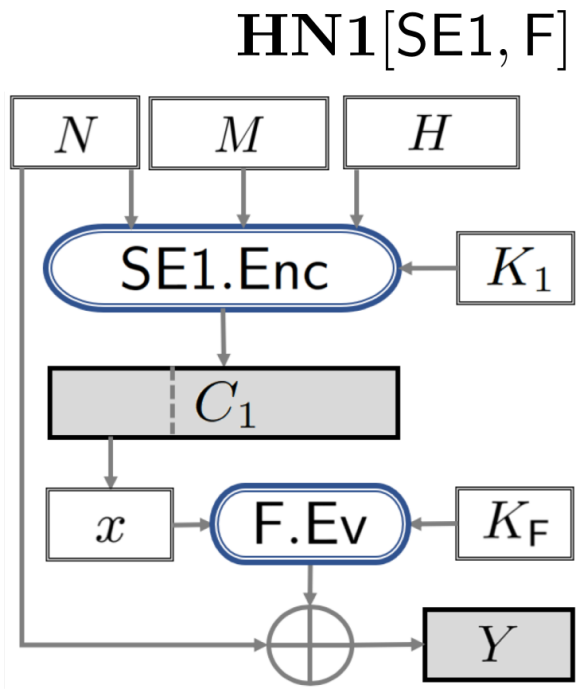
Nonce-hiding AE (NBE2)

[BNT19]

ETH zürich

$$C \leftarrow \mathsf{SE}_2.\mathsf{Enc}(K, N, M, H)$$
$$M \leftarrow \mathsf{SE}_2.\mathsf{Dec}(K, C, H)$$

- Dec no longer gets the nonce N
- Nonce needs to travel as part of (extended/full) ciphertext
- **HN1** transform: mask nonce via PRF
- **Still not quite what QUIC does...**
  - only partial nonce N_e gets transmitted
  - partial nonce length varies
  - further header bits masked



[BNT19]

Two-tier Authenticated Encryption

ETH zürich

$$(C_1, C_2) \leftarrow \mathsf{SE}_{\mathsf{tt}}.\mathsf{Enc}(K = (K_1, K_2), N, M = (M_1, M_2), H)$$

$$(M_1, st) \leftarrow \mathsf{SE}_{\mathsf{tt}}.\mathsf{Dec}_1(K_1, C_1)$$
$$M_2 \leftarrow \mathsf{SE}_{\mathsf{tt}}.\mathsf{Dec}_2(K_2, N, C_2, H, st)$$

- Encryption takes two keys and messages, produces two-part ciphertext
- Decryption in two steps/tiers:
  - Dec_1 recovers M_1 from C_1 (only)
  - Dec_2 recovers M_2 from C_2 **and** N, H (some of which may be derived from M_2)
- Idea (for QUIC): M_1 carries (partial) nonce / (to-be-)protected header

Two-tier Authenticated Encryption

Security

ETH zürich

$$(C_1, C_2) \approx (\$^{cl_1}, \$^{cl_2})$$

- Ciphertexts (both parts) look like random strings (of appropriate length cl_1, cl_2)

and

- Hard to come up with C_1^* for $(C_1, C_2) \leftarrow \mathsf{SE}_{\mathsf{tt}}.\mathsf{Enc}(.., (M_1, M_2), ..)$ s.t.

$$M_1 = M_1^* \leftarrow \mathsf{SE}_{\mathsf{tt}}.\mathsf{Dec}_1(.., C_1^*)$$

and

QUIC: leaks if decryption with decoded nonce is successful

classical **AE security**

- Hard to forge C_2^* which decrypts to non-error message $M_2^* \neq \perp$

QPE's Core: AEX

(Two-tier) Authenticated Encryption with XOR

ETH zürich

- based on (NBE1) nonce-based AE scheme SE and PRF F
- Keys: K_1 for F, K_2 for SE
- Encryption: M_2 via SE, then masking M_1 with sample of C_2

$\underline{\mathsf{AEX.Enc}((K_1, K_2), N, (M_1, M_2), H)}$

$s \| C_2 \leftarrow \mathsf{SE.Enc}(K_2, N, M_2, H)$

$C_1' \leftarrow M_1 \oplus \mathsf{F}(K_1, s)$

Return $(C_1 = (C_1' \| s), C_2)$

- Decryption: unmask M_1, pass sample onto Dec_2 in state

$\underline{\mathsf{AEX.Dec}_1(K_1, C_1)}$

$C_1' \| s \leftarrow C_1$

$M_1 \leftarrow C_1' \oplus \mathsf{F}(K_1, s)$

Return $(M_1, st = s)$

$\underline{\mathsf{AEX.Dec}_2(K_2, N, C_2, H, st)}$

$M_2 \leftarrow \mathsf{SE.Dec}(K_2, N, st \| C_2, H)$

Return M_2

QPE Is (Partially) Nonce-Hiding

ETH zürich

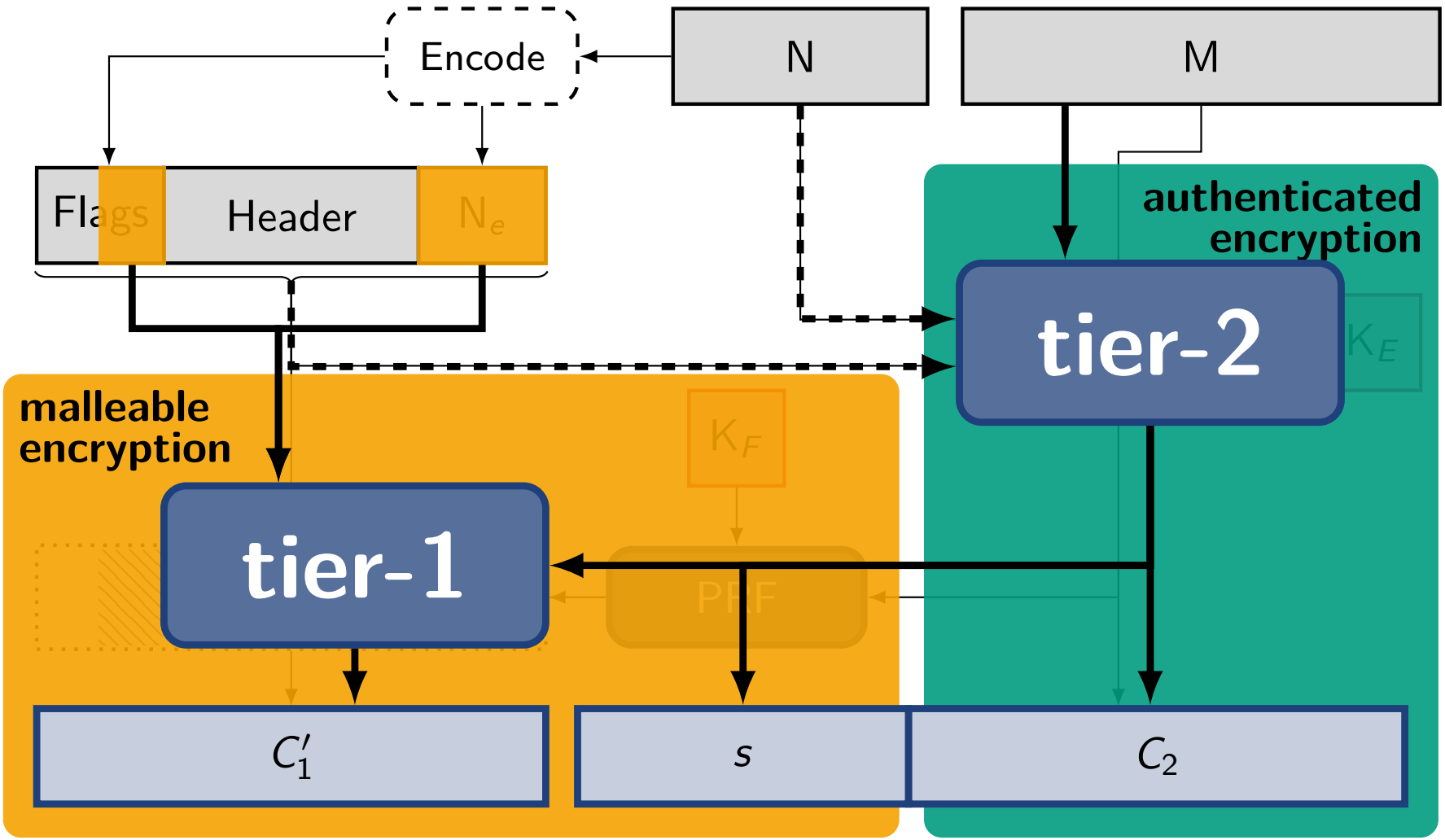
$$C \leftarrow \text{QPE.Enc}(K, (N_i, N_e), M, H)$$
$$M \leftarrow \text{QPE.Dec}(K, N_i, C, H)$$

- Dec is given N_i (based on expected sequence number) but not N_e
  - similar to AE5 notion (for CAESAR competition) of Namprempre, Rogaway, Shrimpton [NRS13]
  - likewise captured by Delignat-Lavaud et al. [DLFP+20]
- Generalizes NBE1 (omit N_e) and NBE2 (omit N_i)
- AEX internally:
  - Encrypt explicit nonce N_e part of inner scheme with the outer scheme
  - Recover N_e (and unprotected header) in two-tier decryption operation

QPE Is (Partially) Nonce-Hiding

Mapping Two-tier AEX to QPE

ETH zürich



Ongoing & Future Work

ETH zürich

- **Forward secrecy** through rotating AE encryption keys
  - two-tier AE notion modularly separates AE and masking (PRF) keys
  - tier-1 hiding QUIC's key-phase bit $\rightarrow$ lets tier-2 decide on which K_2 to use
- **Further instantiations** of two-tier AE
  - other nonce-hiding transforms from [BNT19]
  - stronger authenticity for tier-1 — what are the trade-offs?
- Application in **other settings**
  - **DTLS 1.3** adopted QUIC's header encryption
  - **Message Layer Security** (MLS) considers metadata encryption
  - ...

Summary

ETH zürich

- QUIC's Packet Encryption aims to hide packet numbers & more header
- We model its core as **two-tier authenticated encryption**

$$(C_1, C_2) \leftarrow \mathsf{SE}_{\mathsf{tt}}.\mathsf{Enc}(K = (K_1, K_2), N, M = (M_1, M_2), H)$$

$$(M_1, st) \leftarrow \mathsf{SE}_{\mathsf{tt}}.\mathsf{Dec}_1(K_1, C_1)$$
$$M_2 \leftarrow \mathsf{SE}_{\mathsf{tt}}.\mathsf{Dec}_2(K_2, N, C_2, H, st)$$

- We confirm that QPE is (partial) nonce-hiding via its core two-tier scheme AEX (AE-with-XOR)
- Two-tier AE as stepping stone:
  - forward security via key updates
  - variants with stronger security
  - applications beyond QUIC

Thank You!

mail@**felixguenther.info**

References I

ETH zürich

[BNT19] M. Bellare, R. Ng, and B. Tackmann. "Nonces Are Noticed: AEAD Revisited". In: *CRYPTO 2019, Part I*. Ed. by A. Boldyreva and D. Micciancio. Vol. 11692. LNCS. Springer, Heidelberg, Aug. 2019, pp. 235–265.

[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.

[GM17] F. Günther and S. Mazaheri. "A Formal Treatment of Multi-key Channels". In: *CRYPTO 2017, Part III*. Ed. by J. Katz and H. Shacham. Vol. 10403. LNCS. Springer, Heidelberg, Aug. 2017, pp. 587–618.

[NRS13] C. Namprempre, P. Rogaway, and T. Shrimpton. *AE5 Security Notions: Definitions Implicit in the CAESAR Call*. Cryptology ePrint Archive, Report 2013/242. `http://eprint.iacr.org/2013/242`. 2013.

[Rog02] P. Rogaway. "Authenticated-Encryption With Associated-Data". In: *ACM CCS 2002*. Ed. by V. Atluri. ACM Press, Nov. 2002, pp. 98–107.