Computational analysis of EDHOC SIG-SIG

Marc Ilunga and Felix Günther

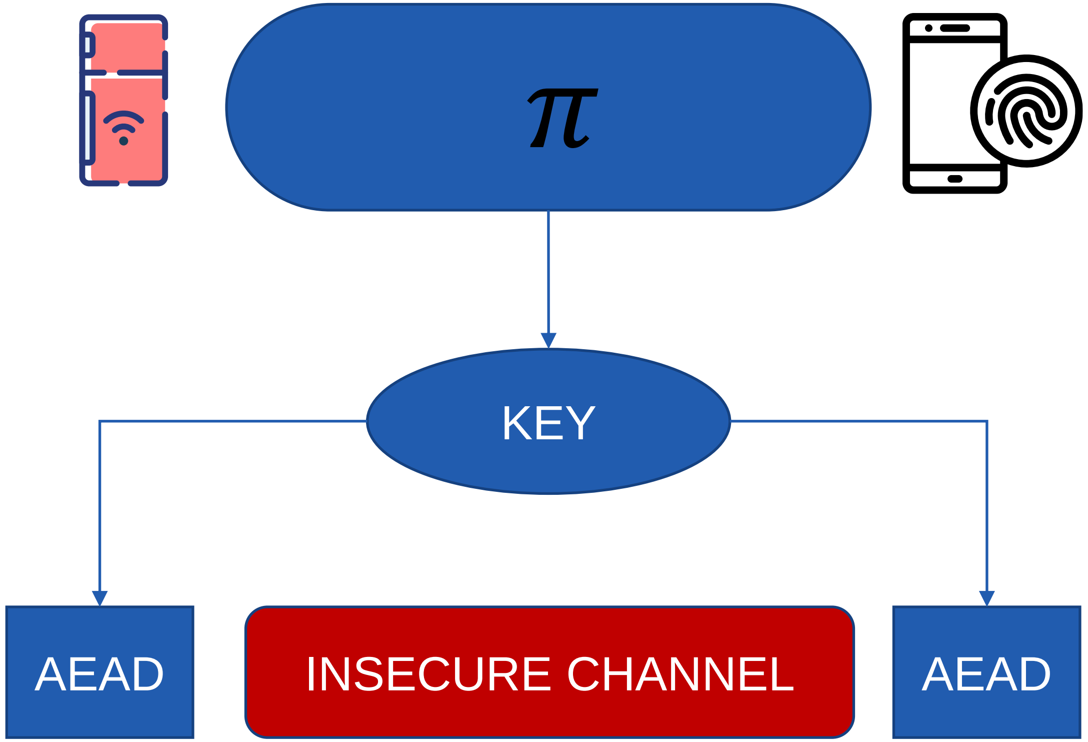
22.07.2022

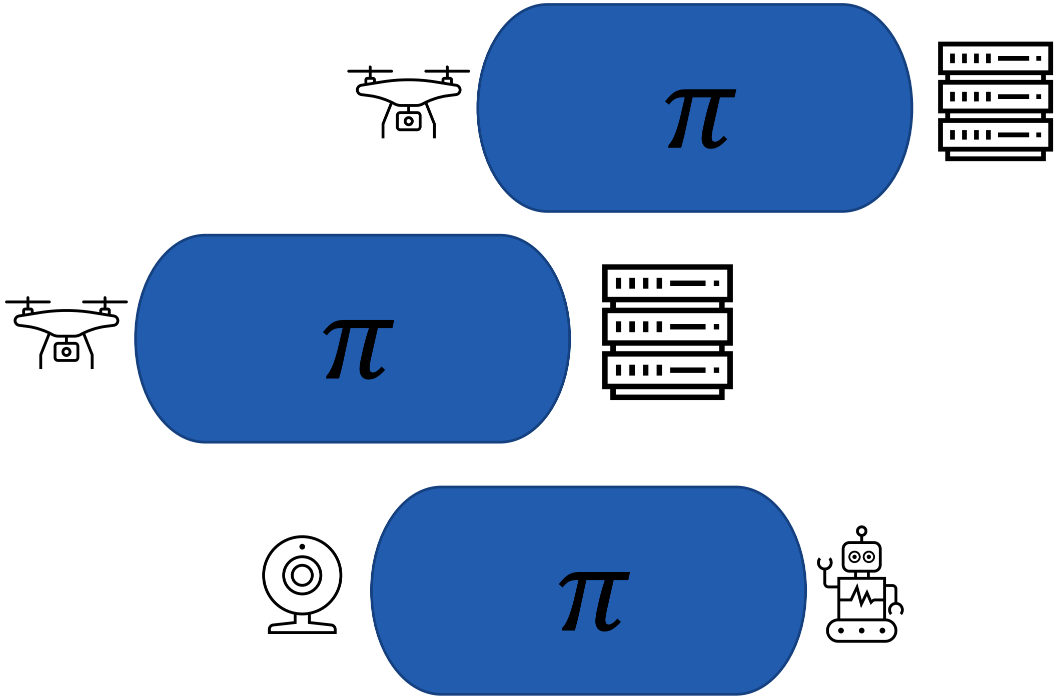
EDHOC SIG-SIG is structurally sound and secure

Security goals	Key secrecy, explicit authentication, and forward secrecy
Security Model	Multi-Stage Key Exchange Model • Carefully adapted to analyze explicit authentication
Main result	Security proof for EDHOC SIG-SIG • Limitation: loose security bounds • Opportunity for future work: Davis *et al.* on tight analysis of TLS 1.3[1]
Future outlook	Insights into the MAc-then-SIGn protocol to inform further developments.

[1] Davis et al.: On the Concrete Security of TLS 1.3 PSK Mode | springerprofessional.de

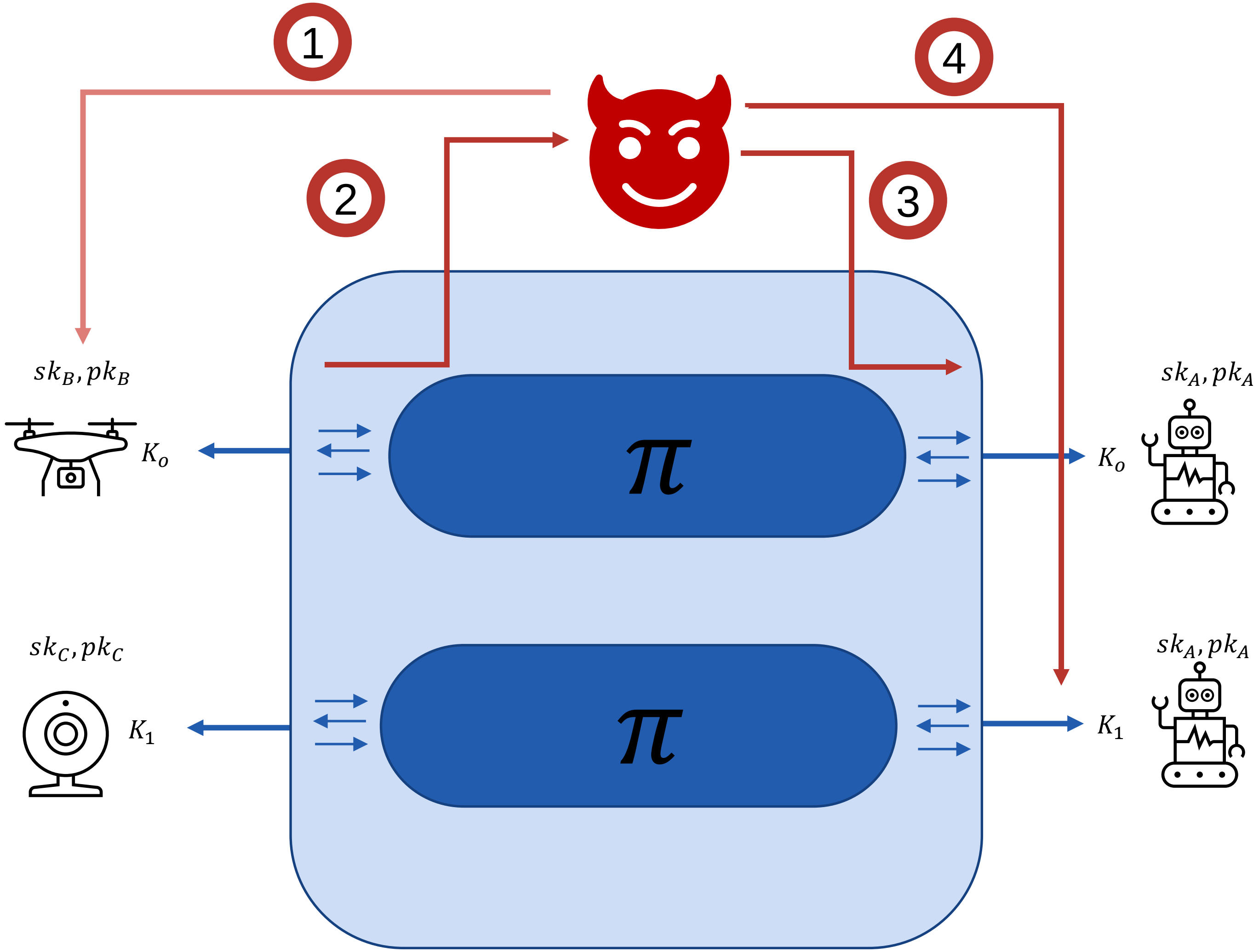
The Multi-Stage Key Exchange Model[1]





[1] 1:Dowling et al. A Cryptographic Analysis of the TLS 1.3 Handshake Protocol | SpringerLink

The Multi-Stage Key Exchange Model[1]



1) Reveal long-term secrets

2) Eavesdrop all communications

3) Modify messages arbitrarily

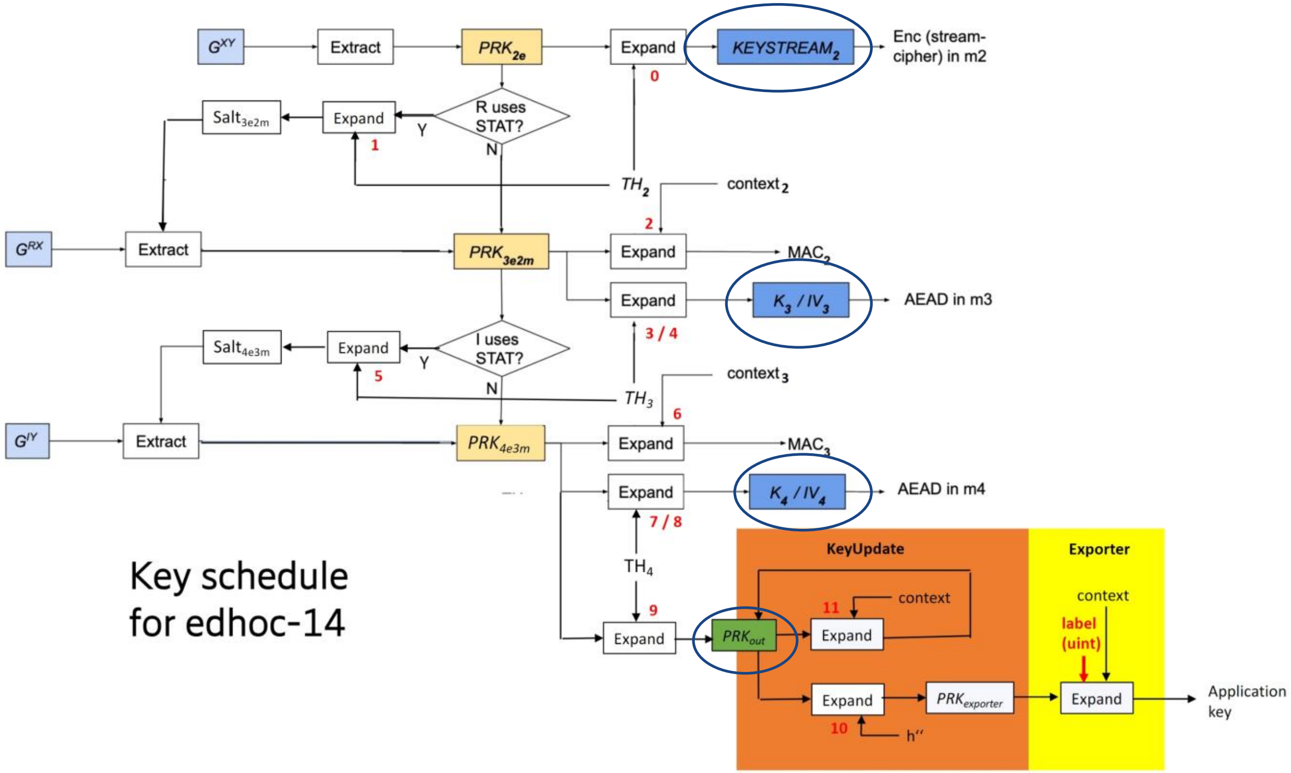
Key indistinguishability:

4) Test session keys

😈 Cannot distinguish K_1 from 🎲

[1]: Dowling et al. A Cryptographic Analysis of the TLS 1.3 Handshake Protocol | SpringerLink

EDHOC is a multi-stage key exchange protocol



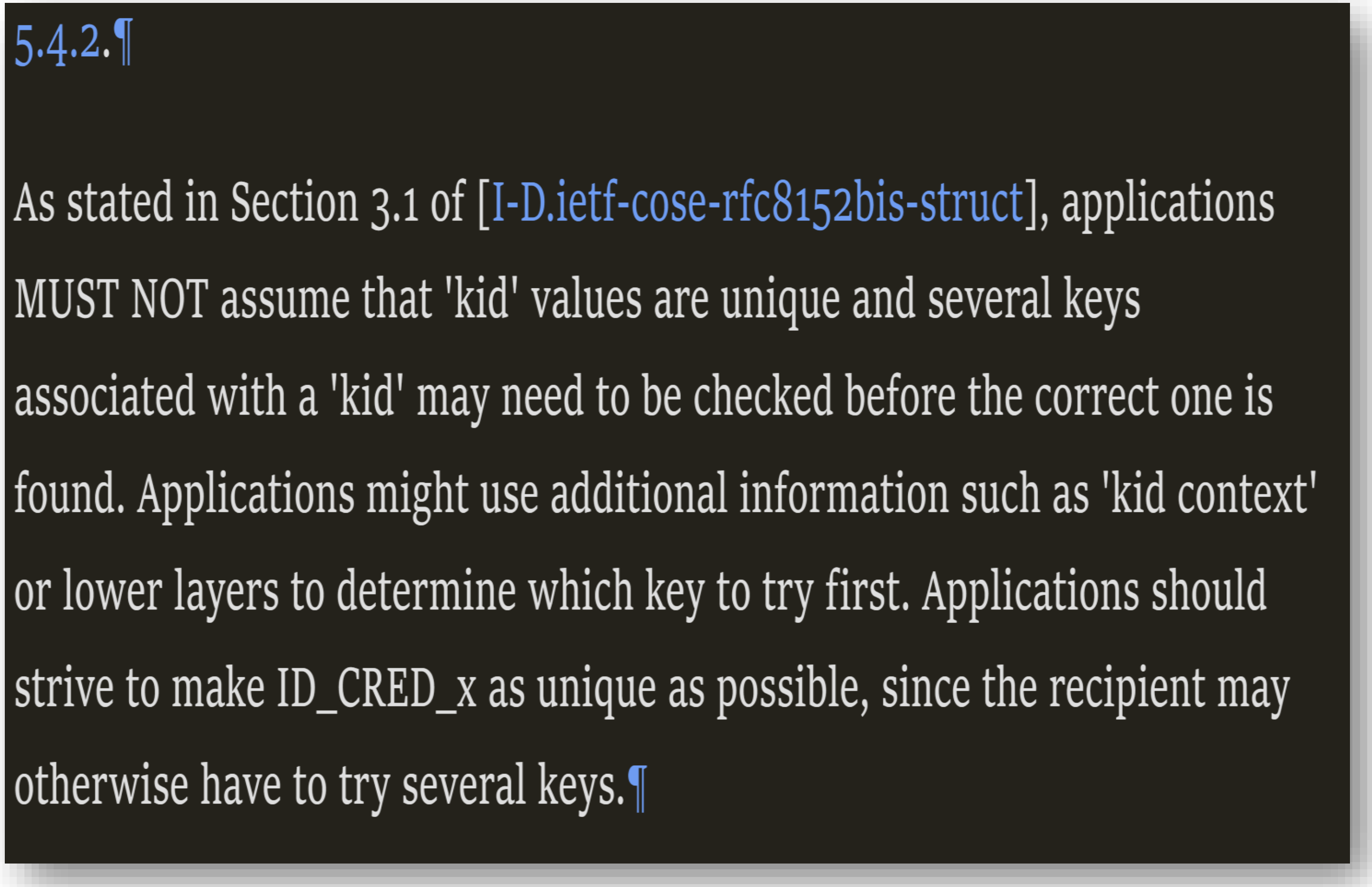
Key schedule for edhoc-14

1. Source: https://openwsn.atlassian.net/wiki/spaces/LAKE/pages/1932427302/Key+Schedule

EDHOC is a multi-stage key exchange protocol

Multi Stage protocols	Multiple stage keys Mixed key usage(internal vs. external) Potentially unwanted dependencies
The MSKE model	Stage-specific security properties Captures dependencies Security proof covers all stages

Explicit Authentication with non-unique credential identifiers



5.4.2.¶

As stated in Section 3.1 of [I-D.ietf-cose-rfc8152bis-struct], applications MUST NOT assume that 'kid' values are unique and several keys associated with a 'kid' may need to be checked before the correct one is found. Applications might use additional information such as 'kid context' or lower layers to determine which key to try first. Applications should strive to make ID_CRED_x as unique as possible, since the recipient may otherwise have to try several keys.¶

Explicit authentication Informally:

> “Only the intended peer knows about the shared session key **and** they actively demonstrated knowledge of the session key”.

In our model:

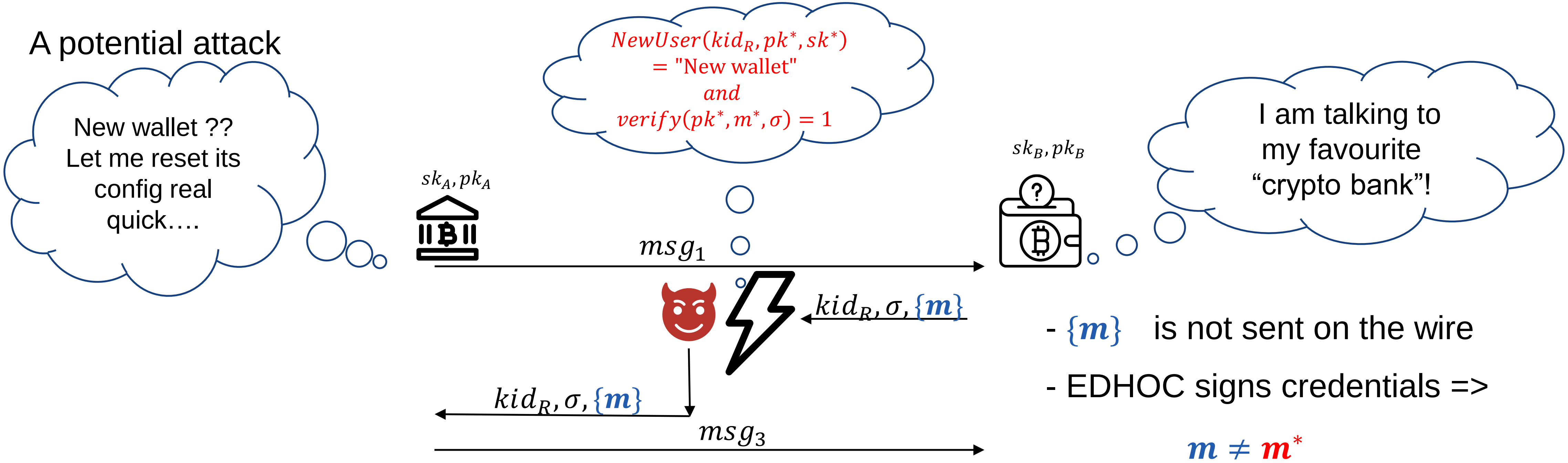
- Conservative approach
- All ID_CRED are non-unique
- The adversary is allowed to choose ID_CRED of all users even honest ones

Source: https://www.ietf.org/archive/id/draft-ietf-lake-edhoc-14.html#name-identification-of-credentia

Explicit authentication in EDHOC requires more than unforgeability

- Authentication at first glance in SIG-SIG: $\exists pk_U \in kid_X : verify(pk_U, m, \sigma) = 1$

- A potential attack


New wallet ?? Let me reset its config real quick….
sk_A, pk_A
$NewUser(kid_R, pk^*, sk^*) = \text{"New wallet"}$ and $verify(pk^*, m^*, \sigma) = 1$
sk_B, pk_B
I am talking to my favourite “crypto bank”!
msg_1
$kid_R, \sigma, \{\boldsymbol{m}\}$
$kid_R, \sigma, \{\boldsymbol{m}\}$
msg_3

- $\{\boldsymbol{m}\}$ is not sent on the wire

- EDHOC signs credentials =>

$$\boldsymbol{m} \neq \boldsymbol{m}^*$$

Explicit authentication in EDHOC requires unforgeability and exclusive ownership

- Transcript hash nor PRK_2em are modified => protocol finishes execution without errors(applicable to SIG-STAT and STAT-SIG as well).
- Signature schemes must provide “exclusive ownership” guarantees.
- With $\boldsymbol{m} \neq \boldsymbol{m}^*$ we only need “destructive exclusive ownership”.
- The original Mac-then-SIGn is vulnerable to a similar attack if the signature scheme contains weak keys.
- Other potential problem avoided in EDHOC because CBOR is unambiguous.
- Example: Potential encoding collisions on concatenation

external_aad = << TH_2, CRED_R, ? EAD_2 >> => Could forge CRED_R’ = <<CRED_R, ?EAD_2>>

Explicit authentication in EDHOC Sig-Sig:
Exclusive ownership of Ed25519 and ECDSA*(the way it is used in EDHOC)

- Our analysis of EDHOC Sig-Sig in the MSKE model show that the signatures in SIG-SIG provide universal exclusive ownership.
- Ed25519 is known to provides universal exclusive ownership[2]..
- ECDSA is not necessarily UEO secure:
  - However, scheme attaching the public key to a message before signing provides exclusive ownership assuming no weak keys[1].
  - Insecure implementations of ECDSA may weaken UEO security. e.g.: psychic Signatures CVE-2022-21449
- Besides exclusive ownership, our proof required strong unforgeability under chose message attacks.
  - MAc-then-SIGn: the signature is over the MAC instead of the other way around(e.g.: TLS 1.3).
  - Without SUF-CMA, a modified signature is accepted.
  - ECDSA and original Ed25519 are not SUF-CMA secure. Ed25519-IETF is SUF-CMA.
  - Practical impact is probably un-interesting: the transcript hashes will diverge.

[1] Digital Signatures Do Not Guarantee Exclusive Ownership | SpringerLink
[2] The Provable Security of Ed25519: Theory and Practice (iacr.org)

Strengthening explicit authentication by adding the credentials in the transcript hash

Suggestions to strengthen explicit authentication

Augment transcript hashes with credentials[2]:

- TH_3 = H(TH_2, PTXT_2, CRED_R)
- TH_4 = H(TH_3, PTXT_3, CRED_I)

Benefits

Makes explicit which users authenticated themselves in the transcript hash.

Strengthens explicit auth against identity mis-binding attack. Such an attack would lead to diverging hashes assuming collision resistance.

EDHOC SIG-SIG security bound

Theorem 5.1 Let $EDHOC\text{-}Sig\text{-}Sig$ be the EDHOC protocol in SIG-SIG mode for authentication. Moreover, let $\mathbb{G} = \langle G \rangle$ be a cyclic group of order q, and H be a hash function, Sig be a digital signature scheme, $Extract$ be a PRF, $Expand$ be a variable-length PRF, n_U be the total number of users and n_S be the total number of sessions. Finally, let $\mathcal{A}$ be an MSKE adversary against $EDHOC\text{-}Sig\text{-}Sig$. Then there exist adversaries $\mathcal{B}_4, \mathcal{B}_{I.2}, \mathcal{B}_{I.4}, \mathcal{B}_{II.A2}$,$\mathcal{B}_{II.B2}, \mathcal{B}_{II.B3}$ such that:

$$\mathrm{Adv}_{\mathcal{A}}^{MSKE}(EDHOC\text{-}Sig\text{-}Sig) \leq \frac{n_S^2}{q} + Adv_{\mathcal{B}_4}^{CR}(H)$$

$$+ 4n_S \left(n_U \cdot Adv_{\mathcal{B}_{I.2}}^{SUF-CMA}(Sig) + Adv_{\mathcal{B}_{I.4}}^{S-UEO}(Sig) \right)$$

$$+ 4n_S \left(n_U \cdot Adv_{\mathcal{B}_{II.A2}}^{SUF-CMA}(Sig) + Adv_{\mathcal{B}_{II.B2}}^{snPRF-ODH}(Extract) + Adv_{\mathcal{B}_{II.B3}}^{PRF}(Expand) \right)$$

The snPRF-ODH assumption states that Extract keyed with the share DH secret $xy * G$ is PRF Given:

- $x * G, y * G$
- Single oracle access $\mathcal{O}_x(S, u) = Extract(u, x * S)$
- No oracle access to $\mathcal{O}_y(S, v) = Extract(v, y * S)$

Evaluation of past recommendations

Specify a final session key	Clean indistinguishability proof for final key PRK_{OUT}.
Transcript hash over plaintexts	Simplified proof and no reliance on potentially non-standard properties of the encryption scheme.