

Updates on KEM-based Authentication for EDHOC

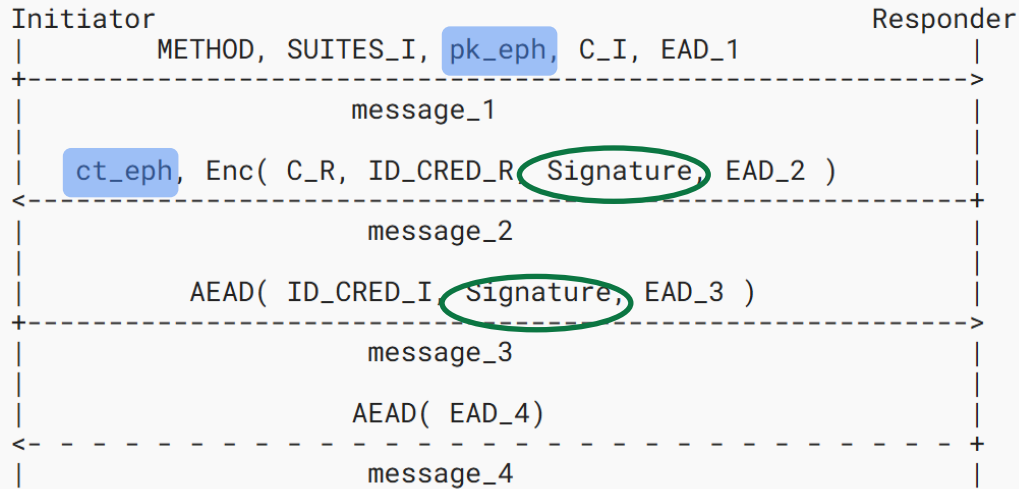
(draft-pocero-authkem-edhoc-02)

Authors: L. Pocero Fraile, C. Koulamas, A. P. Fournaris, E. Haleplidis

Affiliations: ISI, R.C. ATHENA

Presenter: Lidia Pocero Fraile



PQ Signature-based authentication of EDHOC *



* Also recently extended for PQ with PSK-based authentication → Just need QR Ephemeral KEM

- PQ EDHOC described in EDHOC **RFC9528 using method 0**
- Completed with new cipher suites with quantum-resistant algorithms [**draft-spm-lake-pqsuites-01**]*
 - **QR Ephemeral KEM** →
ex: ML-KEM-512
 - **QR Digital Signatures** →
ex: ML-DSA-44

KEM-based Authentication methods for EDHOC - Motivation

- The PQ with PSK-based EDHOC  Limited to scenarios where nodes share a PSK provided out of band
- The PQ with signature-based EDHOC, using NIST standardized signature schemes  Introduces significant overhead
 - Long key sizes and signatures
 - High processing times
 - High memory overhead

KEM-based Authentication methods for EDHOC - Motivation

- **KEM-based authentication methods** in EDHOC:
 - Enable **signature-free** authentication for one or both parties
 - **V01**: support mixed modes where one party uses KEM-based authentication and the other uses signatures.

EDHOC

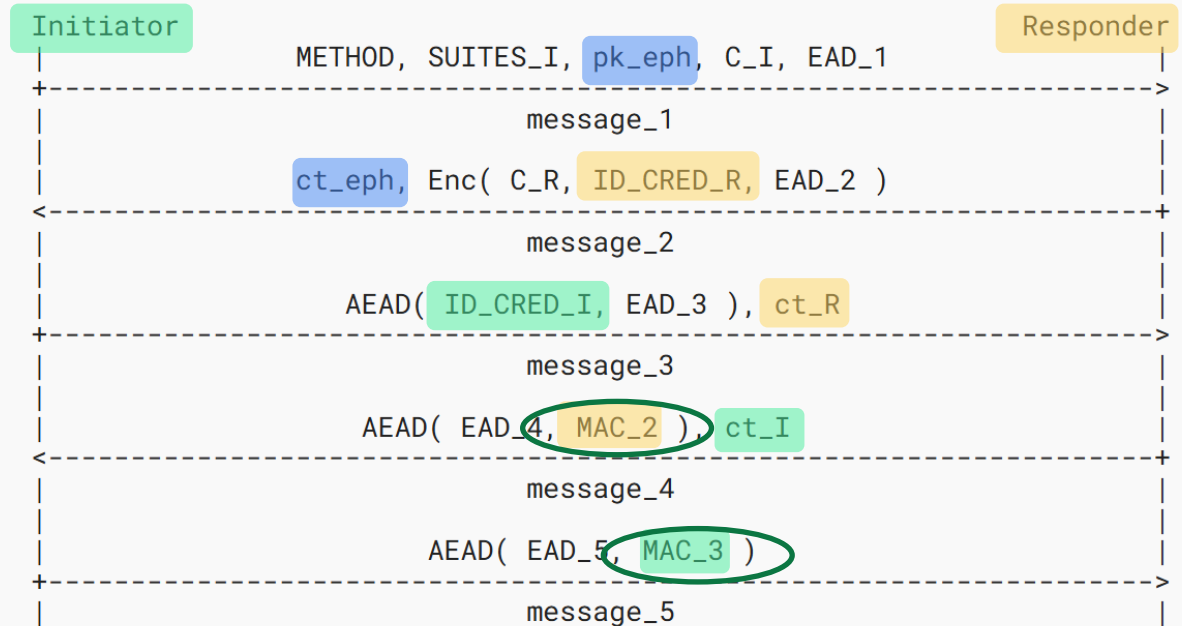
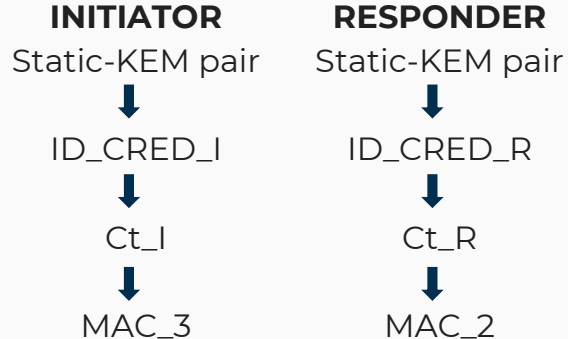
Method	Method Type Value	Initiator Authentication Key	Responder Authentication Key
Method 3	4	Static KEM Key	Static KEM Key
Method 2	5	Static KEM Key	PQC Signature
Method 1	6	PQC Signature	Static KEM Key

PQ

Method 4: KEM-based Initiator/KEM-based Responder

EDHOC Method 3 Logic:

- Both parties authenticate without digital signatures



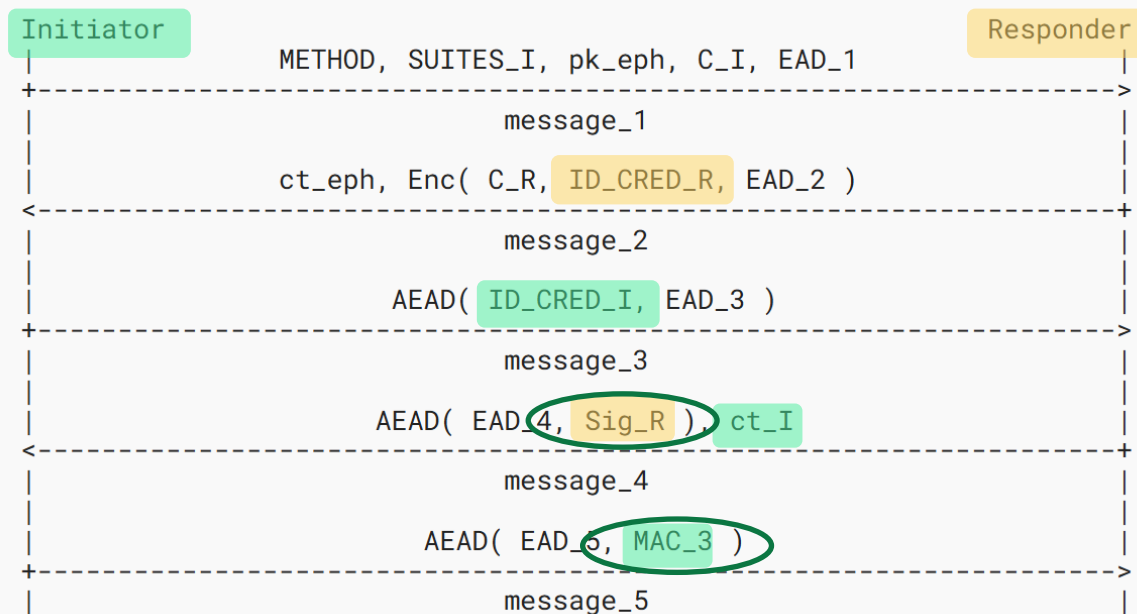
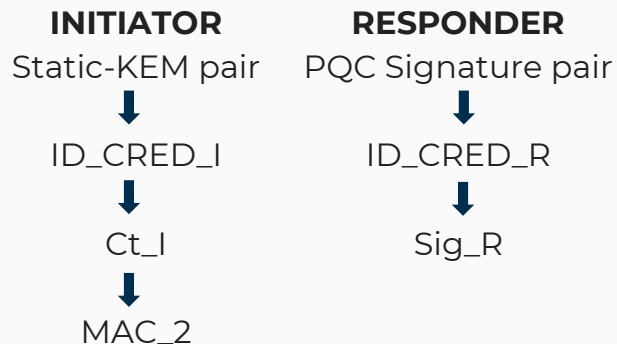
EDHOC KEM-based Authentication methods

Message-flow-preserving approach

Method 5: KEM-based Initiator/Signature-based Responder

EDHOC Method 2 Logic:

- Initiator authenticates without digital signatures



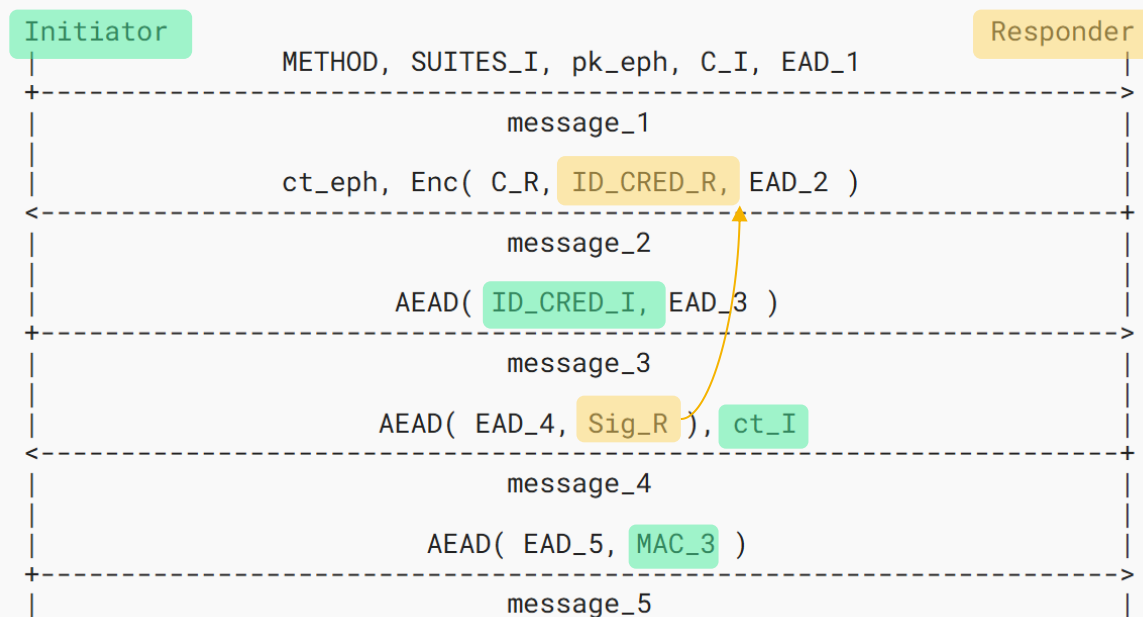
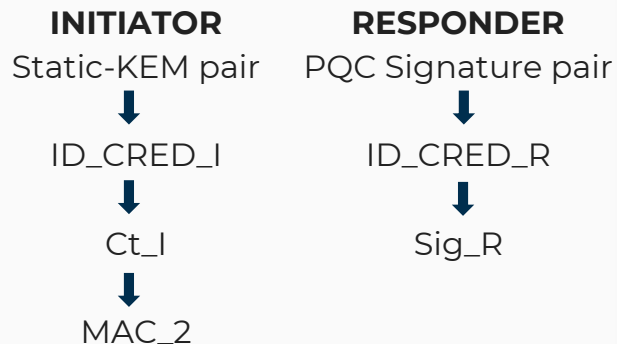
EDHOC KEM-based Authentication methods

Early Authentication Approach

Method 5: KEM-based Initiator/Signature-based Responder

EDHOC Method 2 Logic:

- Initiator authenticates without digital signatures



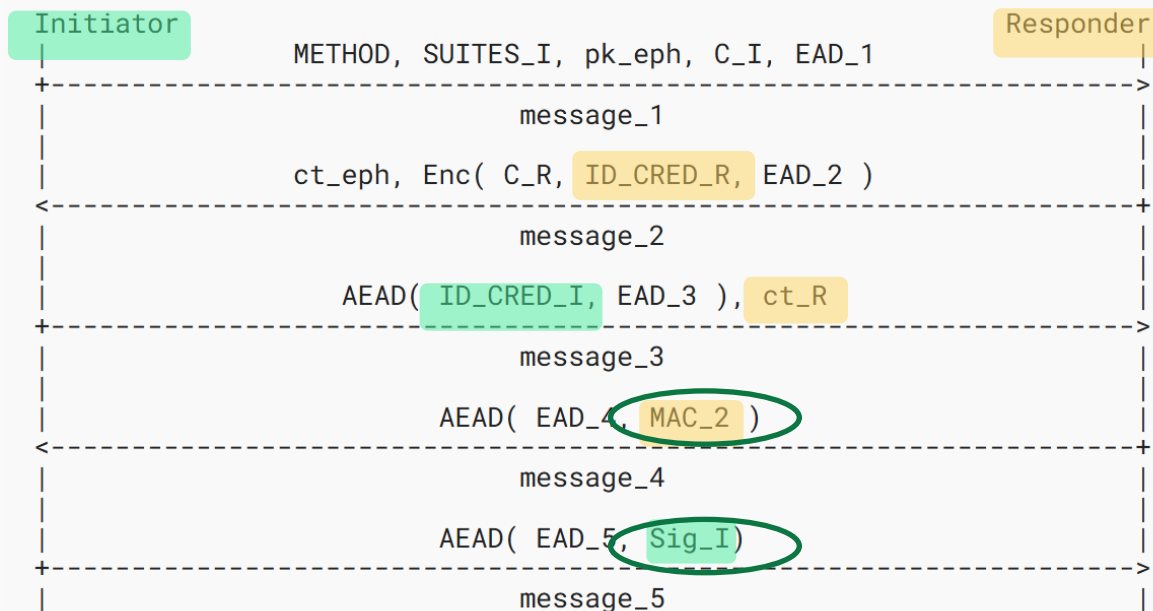
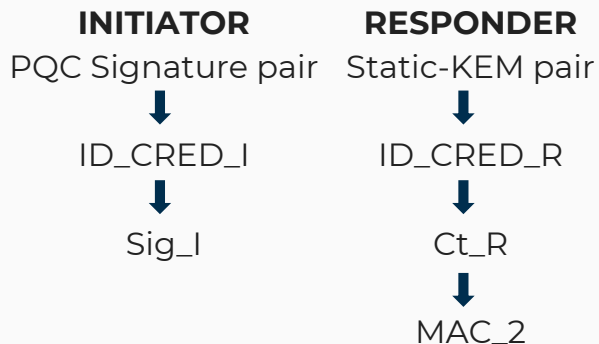
EDHOC KEM-based Authentication methods

Message-flow-preserving approach

Method 6: Signature-based Initiator/KEM-based Responder

EDHOC Method 1 Logic:

- Responder authenticates without digital signatures



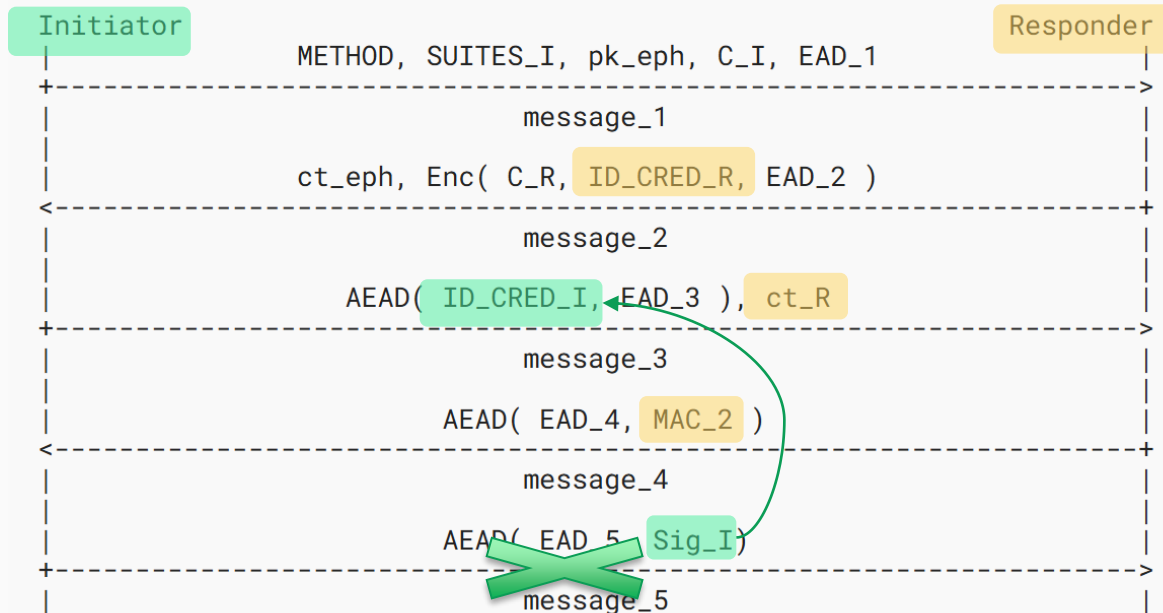
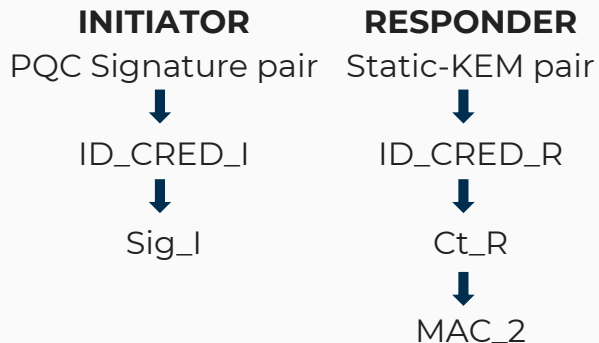
EDHOC KEM-based Authentication methods

Early Authentication Approach

Method 6: KEM-based Initiator/KEM-based Responder

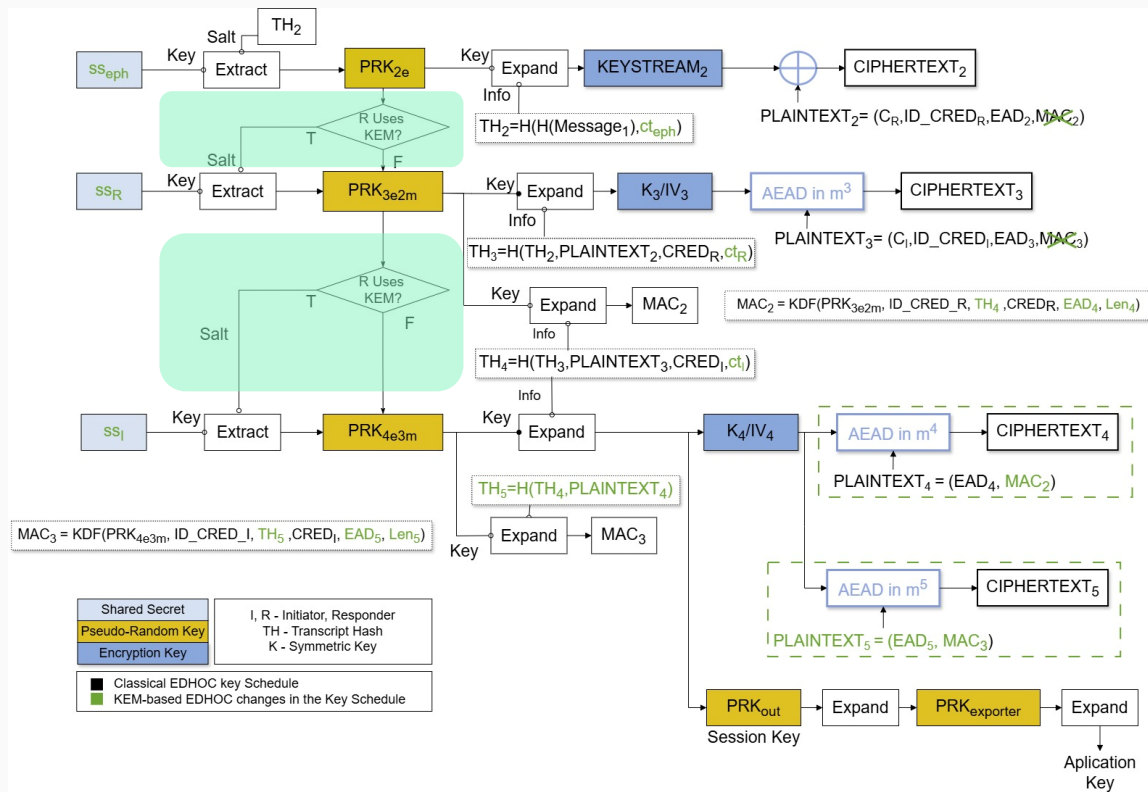
EDHOC Method 1 Logic:

- Responder authenticates without digital signatures



EDHOC KEM/based Authentication methods

Key Schedule



Updates in the New Draft Version (-02)

Update	Section	Update (in draft -02)
#1	Changed in Section 4.2.2 and 4.2.3	Processing order corrected: compute TH_2 before deriving PRK_2e
#2	Add New Section 2.1.5	PQ methods increase message sizes → MAY need a fragmentation mechanism in a constrained network
#3	Changes in Section 4.2.3	Introduces the requirement for the responder's credential validation
#4	Add New Section 6.2	Add KEM Security Consideration Section

Updates in the New Draft Version (-02)

2. Add new Transport Consideration Section

- Responder Identity Protection (Active Attacks)

- The Initiator's credentials (ID_CRED_I) are encrypted using AEAD, providing confidentiality and integrity (but not Initiator's Authentication).
- The encryption key is derived from two shared secrets:

- Ephemeral KEM secret (**ss_eph**)
- Responder static KEM secret (**ss_R**)



Only the legitimate Responder, who owns (**sk_R**), can derive the session key and **decrypt message_3**

- Change for Improved Identity Protection

- The application MUST authenticate and validate the Responder's credentials (ID_CRED_R) before the Initiator sends its own credentials.
- This prevents the Initiator from revealing its identity to a responder with valid but untrusted credentials
- Aligning with the security model of EDHOC [RFC9528]

Updates in the New Draft Version (-02)

3. Introduces requirement for credential validation

- The KEM-based EDHOC authentication methods are **transport-independent**, similar to classical EDHOC.
- Post-quantum KEMs and Signatures(NIST) use larger public keys and ciphertexts → **increase EDHOC message sizes.**
- In constrained networks, larger messages may require **fragmentation** → split and reassemble EDHOC messages.
 - Example Mechanism: **CoAP Block-Wise Transfer**
 - Block1/Block2 [RFC7959]
 - Q-Block1/Q-Block2 [RFC9177])

Updates in the New Draft Version (-02)

4. Add new KEM Security Considerations section

- **IND-CCA2** security alone is not sufficient to prevent attacks in KEM-based key exchange protocols.
- **Re-encapsulation attacks** may occur, leading to Unknown Key Share (UKS) situations where two parties derive the same secret but associate it with different identities.
- To prevent this, a KEM must:
 - Provide **IND-CCA2 security**
 - Ensure the **shared secret is cryptographically bound to the recipient's public key.**
- This binding prevents re-encapsulation and key-substitution attacks.



ML-KEM ✓

Formal Verification of the KEM-based method 4 (KEM-based/KEM-based)

- We **formally verify** some properties of method 4 (KEM-based/KEM-based) authentication in Tamarin (with Vaishnavi Sundararajan, IIT Delhi)
 - Required modelling the KEM encapsulation/decapsulation operations as well as AEAD operations
 - KEM Encapsulation produces a pair (ct, ss), so two function symbols kemEncCt and kemEncSs are used to produce each part
 - The function kemPk returns the public key corresponding to a secret KEM key
 - Needs extra equations to be specified to Tamarin

Formal Verification of the KEM-based method 4 (KEM-based/KEM-based)

- Verified in Tamarin the following trace properties:
 - **Secrecy of prk_out** (key finally established) : At the end of a session between an initiator I and a responder R establishing prk_out, nobody but I and R knows prk_out
 - **Injective agreement for I** : If I finishes a run as an initiator believing that they have communicated with a responder R using communication identifiers C_I and C_R, with ephemeral KEM keys pkeph, sseph, then R must have been running exactly one session involving communication identifiers C_I and C_R with ephemeral KEM keys pkeph, sseph. (Cannot get guarantees about R knowing I's identity; common across EDHOC)
 - **Injective agreement for R** : Similar, but we can also include R's identity

Formal Verification of the KEM-based method 4 (KEM-based/KEM-based)

- Managed to verify the following trace properties (contd):
 - **Secrecy of intermediate key material** : At the end of a session between an initiator I and a responder R involving IKM prk_{2e} , prk_{3e2m} , prk_{4e3m} , nobody but I and R knows prk_{2e} , prk_{3e2m} , prk_{4e3m}
 - **Perfect forward secrecy (PFS)** of prk_{out}
 - PFS also yields weak **post-compromise security** of prk_{out}
- Next steps: Protection of ID_CREDs
 - Somewhat implied by injective agreement and secrecy of IKM, but needs a separate formal proof of an equivalence flavour (to be done in ProVerif)

Updates on KEM-based Authentication for EDHOC in Initiator-Known Responder (IKR) Scenarios (draft-pocero-authkem-ikr-edhoc-02)

Authors: L. Pocero Fraile, C. Koulamas, A. P. Fournaris, E. Haleplidis

Affiliations: ISI, R.C. ATHENA

Presenter: Lidia Pocero Fraile

KEM-based Authentication for EDHOC in IKR Scenarios - Motivation

- Target:

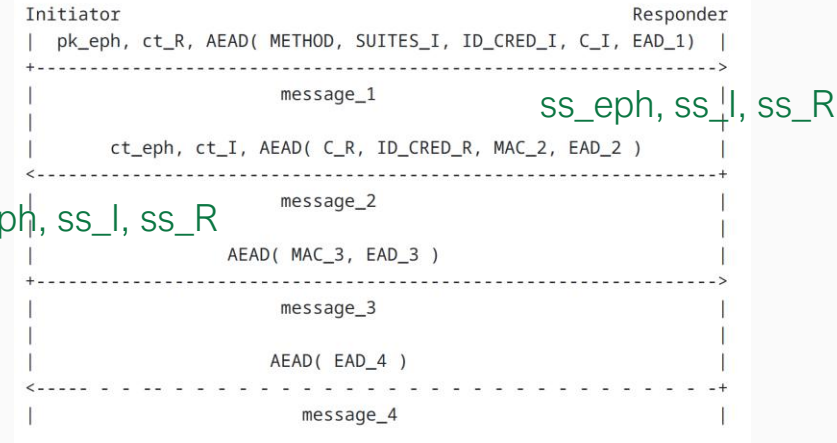
- Reduce the handshake to 3 messages
- In constrained environments where the Initiator already knows the Responder's credentials.

- Key Schedule

- Follows the Noise design principle (which inspired EDHOC).
 - Each new shared secret is immediately incorporated into the key schedule, strengthening protection of subsequent messages.

- The EDHOC key schedule incorporates all shared secrets after message_1 (Responder) and message_2 (Initiator).

- KEM-based/Signature-based combination methods can be added



KEM-based Authentication for EDHOC in IKR Scenarios – Updates 02

Update	Section	Update (in draft -01 and -02)
#1	Changes in Section 5.1	Update the IANA Consideration Section
#2	Changes in Section 6	Reworded the paragraph in the Security Considerations section regarding repudiation
#3	Changes in Section 4.1 and Section 3	<ul style="list-style-type: none">• Replaced XOR encryption with AEAD encryption for Message1 and updated the corresponding text• Updated key derivations• Modify Key derivation schemes
#4	Add in Section 1.1 and Section 4.4	Strengthen the explanation of the key schedule choice.

Looking for feedback/adoption from the WG !



Funded by
the European Union

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the European Commission can be held responsible for them.

