

# A Symbolic Formal Analysis of EDHOC-PSK

Pascal Lafourcade   Elsa Lopez Perez   **Dhekra Mahmoud**  
Cristina Onete   Vaishnavi Sundararajan   Mališa Vučinić  
Thomas Watteyne

IETF 125 – Shenzhen

16 March 2026

## Context: EDHOC-PSK Protocol

**LAKE-EDHOC** light-weight protocol suitable for IoT

- ▶ Relies on asymmetric static keys

Many IoT rely on **Pre-Shared Keys (PSK)** for authentication

**EDHOC-PSK** is currently under standardization!

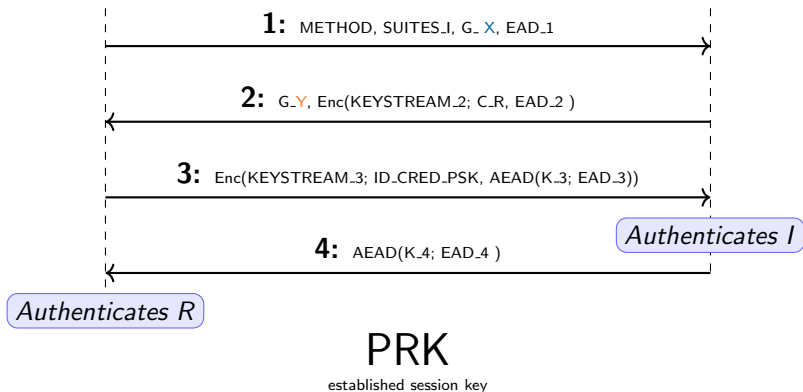
→ LAKE WG call for formal analysis

# EDHOC-PSK High Level Description

Shared Key **PSK** → ID\_CRED\_PSK

**Initiator:** CRED\_I

**Responder R:** CRED\_R



# Formal Verification in the Symbolic Model (Dolev-Yao)

Cryptographic primitives are **perfect**

Protocols encoded in a **formal language**

 is the **Network = Worst Case**

- ▶ Intercept  (Re)play  Delete  Inject 
- ▶ Additional compromise capabilities: PSK, X, Y, PRK, 

**Security properties** formally expressed as **reachability** or **equivalences**

Protocol + Primitives + Attacker + Security Property → **Model**

# Formal Verification in the Symbolic Model: Saptic<sup>+</sup>

SAPIC<sup>+</sup>: protocol verifiers of the world, unite!

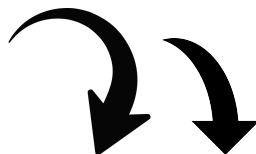
Vincent Cheval<sup>1</sup>, Charlie Jacomme<sup>2</sup>, Steve Kremer<sup>3</sup>, and Robert Künnemann<sup>4</sup>



<sup>1</sup>Inria Paris

<sup>2,4</sup>CISPA Helmholtz Center for Information Security

<sup>3</sup>LORIA & Inria Nancy

June 15, 2022



	Tamarin 	ProVerif 
Soundness	✓	✓
Completeness	✓*	✗
Unbounded Sessions	✓	✓
Trace Properties	✓	✓
Equivalence Properties	✓	✓
DH as AC symbol	✓	✗

✓\* only on trace mode

## As trace properties

### Confidentiality of PRK

- ▷ PRK Secrecy from I's point of view
- ▷ PRK Secrecy from R's point of view
- ▷ PRK Secrecy upon agreement
- ▷ PRK Forward Secrecy

### Mutual authentication & explicit key confirmation

- ▷ Authentication of I to R and injective agreement on exchanged data
- ▷ Authentication of R to I and injective agreement on PRK

## As equivalence properties

### Identity protection<sup>1</sup>

- ▷ Anonymity of I
- ▷ Anonymity of R
- ▷ Unlinkability of I
- ▷ Unlinkability of R

---

<sup>1</sup>Only against passive attackers

## Minimal Compromise Scenarios

Trace Property	Active	Active + $\mathcal{O}_{\infty}^{DL}$
PRK secrecy from I's view	$PSK \vee PRK$	PSK
PRK secrecy from R's view	$PSK \vee PRK$	PSK
PRK secrecy upon agreement	$(PSK \wedge X) \vee (PSK \wedge Y) \vee PRK$	PSK
PRK forward secrecy	$X \vee Y$	$\times$
Authentication* of I to R	PSK	-
Authentication* of R to I	PSK	-

Authentication\*: authentication and full agreement on the protocol's exchanged data G\_X, G\_Y etc, thus on PRK.

## Minimal Compromise Scenarios

Equivalence Property	Passive	Passive + $\mathcal{O}_{\infty}^{DL}$	Active	Active + $\mathcal{O}_{\infty}^{DL}$
Anonymity of I	$(PSK \wedge X) \vee (PSK \wedge Y)$	PSK	PSK	PSK
Anonymity of R	$(PSK \wedge X) \vee (PSK \wedge Y)$	PSK	PSK	PSK
Unlinkability* of I	$X \vee Y$	X	X	X
Unlinkability* of R	X	X	X	X

Unlinkability\* of  $X$  is formulated as follows: all protocol sessions  $S_i$  in which identity  $X$  interacts with  $Y_i$  should be indistinguishable from sessions executed by distinct identities  $X_j$ .

This means that  $S_1(X, Y_1) \mid S_2(X, Y_2) \mid \dots \mid S_n(X, Y_n) \equiv S_1(X, Y_1) \mid S_2(X_2, Y_2) \mid \dots \mid S_n(X_n, Y_n)$ .

In particular,  $S_1(X, Y) \mid S_2(X, Y) \equiv S_1(X, Y) \mid S_2(X_2, Y)$ .

## Next Steps!

Can be integrated immediately within our models



### Cryptographic Primitives

More precise  $\oplus$  model in Tamarin (using xor builtin)

Additional algebraic properties for DH exponentiation in ProVerif

More precise aead model (separate tag and ciphertext)

Replacing DH with a standard KEM model

### Security Properties

Session key secrecy as an equivalence property

Resistance to Unknown Key Share Attacks (BUKS & UUKS)

Equivalence properties with DeepSec (with KEM)

# Next Steps!



Not immediate

Protocol Model

Stateful protocol with keys update and resumption: desynchronization?

Cipher-suites negotiation

Cryptographic Primitives

Minimal properties needed for the KEM to replace DH (Tamarin library)

Full DH model with `dh-with-addition` (new Tamarin builtin)

Weak DH

Weak aead

Weak hash functions

Attacker Model

Full control on randomness generation