Analysing the HPKE Standard

Joël Alwen[1], Bruno Blanchet[3], Eduard Hauck[2], Eike Kiltz[2], Benjamin Lipp[3], Doreen Riepel[2]

October 18, 2021

Wickr[1], Ruhr-University Bochum[2], Inria Paris[3]

Hybrid Public Key Encryption (HPKE)

- *Hybrid* in the spirit of the KEM/DEM paradigm:
  asymmetric building block as Key Encapsulation Mechanism (KEM),
  symmetric building block as Data Encapsulation Mechanism (DEM)
- Standard in development by the Crypto Forum Research Group
  `https://github.com/cfrg/draft-irtf-cfrg-hpke`

  Usage in TLS 1.3's Encrypted Client Hello (ECH) extension, and
  the Messaging Layer Security (MLS) group messaging protocol

Overview of the Construction

HPKE defines multiple interfaces and modes; we analyse the **Single-Shot Encryption** interface in **Auth** mode.

Authenticated KEM to generate a shared secret

+

key schedule function to derive a symmetric key and a nonce

+

DEM to encrypt message using this key and nonce

The HPKE standard's construction of **Authenticated Public Key Encryption**

Security Notions for AKEM and APKE

Chosen-Ciphertext Indistinguishability (CCA)
confidentiality of AKEM and APKE ciphertexts

Authenticity (Auth)
unforgeability of AKEM and APKE ciphertexts

Both of them in two variants:

Outsider adversary can choose from the honest key pairs when calling oracles, no honest key pair is compromised

Insider adversary can choose sender or receiver secret key, this is stronger than compromise of honestly generated key pairs

We prove **Outsider-CCA**, **Insider-CCA**, **Outsider-Auth** for the standard's instantiation of AKEM and for the generic APKE construction.

There are **attacks against Insider-Auth** of the standard's instantiation of AKEM and the generic APKE construction.

Elliptic Curves and Nominal Groups

The HPKE standard allows for different elliptic curves, in particular the NIST curves P-256, P-384, P-521, as well as Curve25519 and Curve448.

- The NIST curves are prime-order groups.
- Curve25519 and Curve448 are not prime-order groups.
  For each honestly generated public key, there is a small number of equivalent public keys.

We define a framework of **(rerandomisable) nominal groups** to cover both prime-order and non-prime-order groups in one model.

In short: We do not assume a group structure, but only an exponentiation function with certain properties.

Conclusion, Contributions of This Work

- HPKE Auth mode satisfies its desired security properties with a maximum security level of 128 bit.
  - CryptoVerif proofs for Outsider-CCA, Insider-CCA, Outsider-Auth of the standard's Diffie-Hellman-based instantiation of AKEM
  - CryptoVerif proof of PRF-security of HPKE's KeySchedule
  - CryptoVerif proofs of composition theorems for Outsider-CCA, Insider-CCA, and Outsider-Auth of the AKEM/DEM construction
  - Hand-written non-tight proof of single-user/two-user ⇒ multi-user security notions for AKEM, to close gap to proofs of, e.g., PQ KEMs
  - open question: multi-key security of current AEAD schemes
- Introduction of (Rerandomisable) Nominal Groups to cover prime-order and non-prime-order groups in one model

Paper: `ia.cr/2020/1499`

CryptoVerif models: `doi.org/10.5281/zenodo.4297811`

CryptoVerif learning material: `cryptoverif.inria.fr/tutorial`