Split Key for STS-KDF Protocol

Station-to-Station (STS) Protocol

- Authenticated key agreement protocol that combines the Diffie-Hellman (DH) key agreement and signature-based authentication of the two parties and provides mutual authentication.
- STS-KDF is a variant that have explicit key confirmation by using a symmetric-key encryption scheme and a message authentication code and prevents Unknown Key Share (UKS) attacks.

Reflection Attack

We assume that Alice and Bob have the same signing and verifying key, but different identities.

Key Encapsulation Mechanism (KEM)

- Public encryption scheme that produces a shared key that can be used for symmetric encryption.
- The shared key is generated by one party and sent to the other. This key is encrypted with the public key of the receiver.

(Split-Key) Privacy-Enhanced STS-KDF-CB with KEM

Formal Verification of the protocols are done by using ProVerif tool. The table presents ProVerif results for the security properties.