UNIVERSITY OF HELSINKI
FACULTY OF SCIENCE

HUAWEI

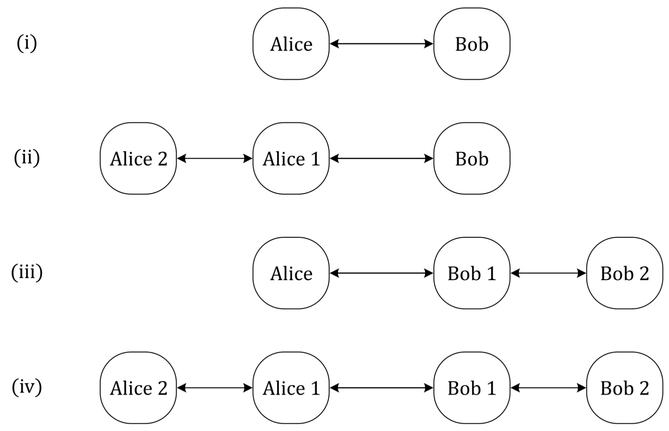
Gizem Akman, Mohamed Taoufiq Damir, Valtteri Niemi
Department of Computer Science, University of Helsinki
Helsinki Institute for Information Technology (HIIT)
Philip Ginzboorg, Sampo Sovio
Huawei Technologies Finland

Split Key for STS-KDF Protocol

Station-to-Station (STS) Protocol

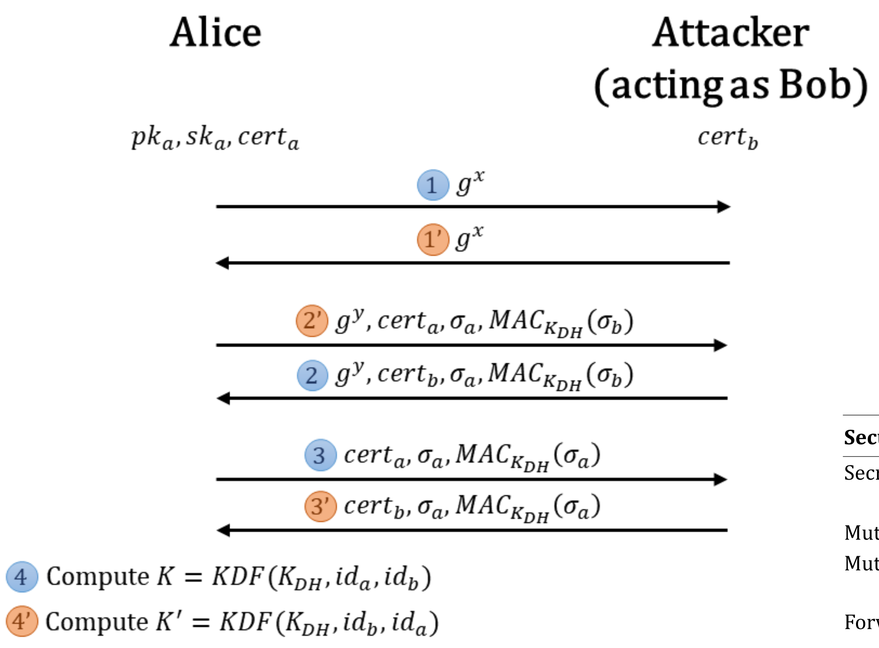
- Authenticated key agreement protocol that combines the Diffie-Hellman (DH) key agreement and signature-based authentication of the two parties and provides mutual authentication.
- STS-KDF is a variant that have *explicit key confirmation* by using a symmetric-key encryption scheme and a message authentication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

Split Key Scenarios



Reflection Attack

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



Split Key

- In situations where a secret cryptographic key may be vulnerable to exposure, splitting the secret key between several devices so that those devices have to cooperate to use the key may reduce the risks of key exposure and provide an additional level of control over key usage.
- The key could be split between: IoT device-smartphone, wireless base-core network, or two different computers in a data center.

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.

Security Properties	Protocol 1	Protocol 2	Protocol 3	Protocol 4	Protocol 5
Secrecy of K	true	true	true	true	true
Mutual Authentication on K_{DH}	true	true	N/A	true	N/A
Mutual Authentication on K	false	false	true	false	true
Forward Secrecy	true	true	true	true	true
Resistance to UKS Attack on K_{DH}	true	true	N/A	true	N/A
Resistance to UKS Attack on K	true	true	true	true	true
Resistance to KCI attack	false	false	false	true*	true*
Anonymity	false	true	true	true	true
Resistance to the Reflection Attack	false	true	true	true	true

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

Protocol 1: STS-KDF
Protocol 2: Privacy-Enhanced STS-KDF-CB
Protocol 3: Privacy-Enhanced STS-KDF-CB with KEM
Protocol 4: Split-Key Privacy-Enhanced STS-KDF-CB
Protocol 5: Split-Key Privacy-Enhanced STS-KDF-CB with KEM

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