Distributed Symmetric-Key Establishment (DSKE)

Daniel R. L. Brown

Quantum Bridge Technologies

ETSI/IQC Quantum Safe Cryptography Conference 2026

Aim: AES-based (quantum-resistant) key establishment (with distributed trust in third parties)

Establish a secret key (such as an AES key) between Alice and Bob

Quantum-resistant security

Only rely upon computational security of AES-256-GCM (or better)

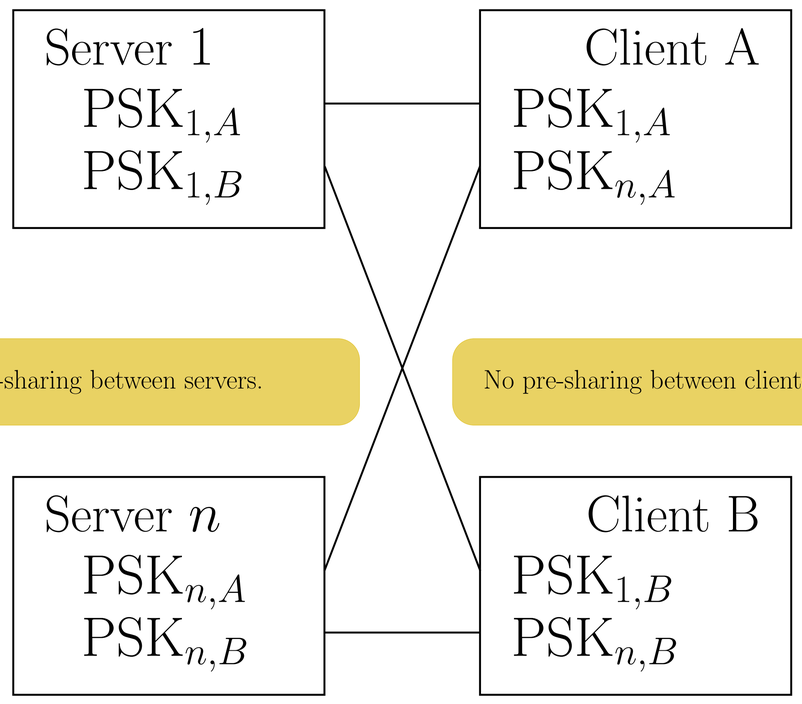
Do not rely upon operational security of any single trusted third party

AES-based
$\Longrightarrow$ No public keys
$\Longrightarrow$ No PQC
$\Longrightarrow$ No (computational) conjectures beyond AES security
$\Longrightarrow$ Exceeds quantum-resistance (less risky than PQC)

No single TTP
$\Longrightarrow$ No single point of system weakness

Initial One-Time Setup: Pre-shared Keys

Per each pair of a server and a client: pre-share a secret key (onboarding)

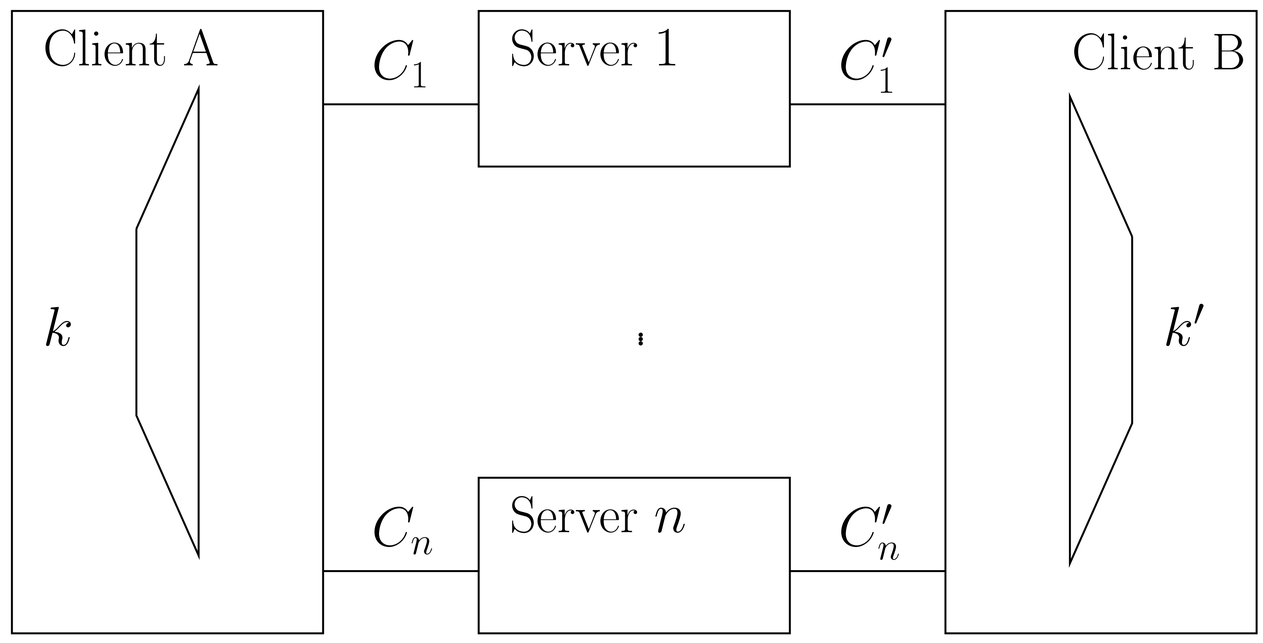


No pre-sharing between servers.

No pre-sharing between clients.

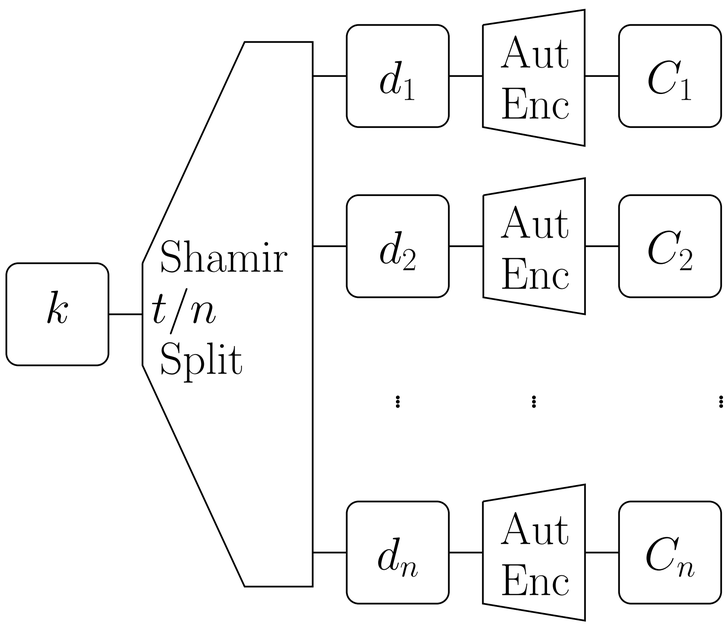
Physically secret channel, such as USB drive, QR code, Keyboard

DSKE Run-time Data Flow Overview



Client A Actions

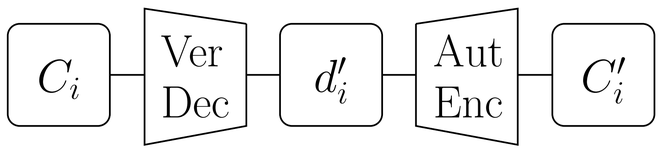
Threshold secret sharing (or threshold encryption)



Not shown: metadata, key redundancy

Server i Actions

Decrypt with PSK$_{i,A}$, then encrypt with PSK$_{i,B}$.

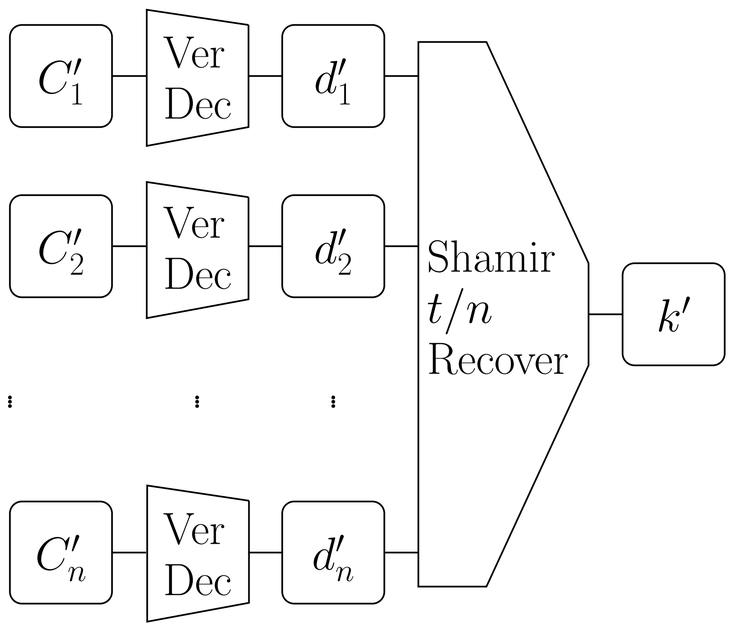


Not shown: metadata

Combinable with:
QKD
PQC
ECC

Client B Actions

Threshold secret sharing (or threshold encryption)



Not shown: metadata, key redundancy

References

[1] Hoi-Kwong Lo, Mattia Montagna, Manfred von Willich. *Distributed symmetric key establishment: A scalable, quantum-proof key distribution system*, `https://arxiv.org/abs/2205.00615`, 2024.

[2] Jie Lin, Manfred von Willich, Hoi-Kwong Lo. *Composable security of distributed symmetric key establishment protocol*, `https://arxiv.org/abs/2304.13789`, 2024.

[3] Paolo D'Arco and Douglas Stinson. *On Unconditionally Secure Robust Distributed Key Distribution Centers*, **Asiacrypt**, 2002.