Cryptographic aspects in WireGuard, a modern VPN protocol

Veronica Cristiano

September 20, 2022

Telsy

www.telsy.com

- Founded in 1971
- Today 100% part of TIM group
- Focused on cryptography and cybersecurity
- Both governmental (B2G) and business (B2B) markets
- Under Golden Power
- Strong research activity

What is WireGuard?

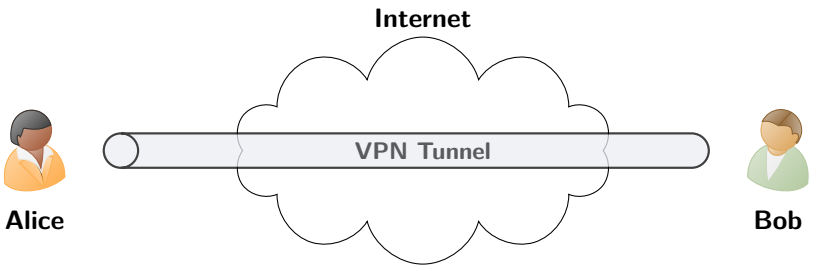
- modern VPN protocol presented in 2016 by Jason A. Donenfeld [Don17]
- merged into Linux kernel in 2020
- better performance than the other VPNs such as IPsec, OpenVPN
- designed with ease-of-implementation and simplicity in mind

Outline

1- Network aspects

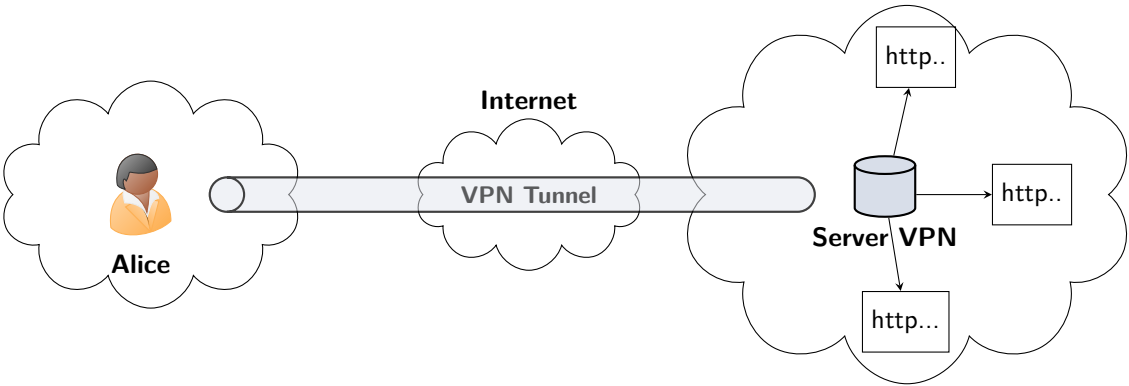
VPN (Virtual Private Network)

- to establish a virtual secure connection
- tunneling protocol



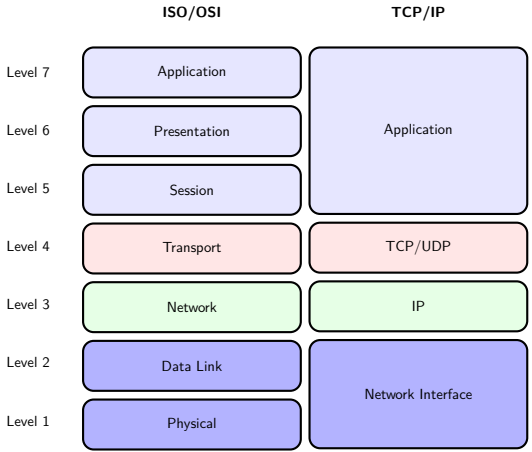
VPN (Virtual Private Network)

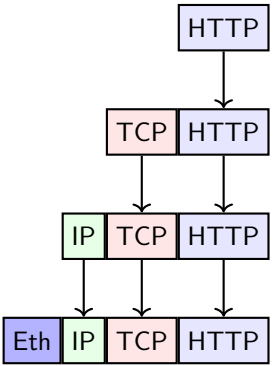
- to establish a virtual secure connection
- tunneling protocol



Telsy

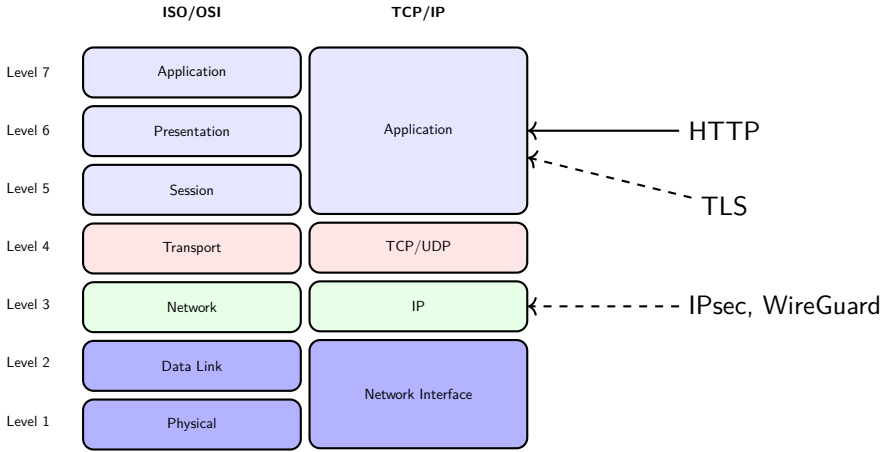
Communication Models





Where is encryption used?

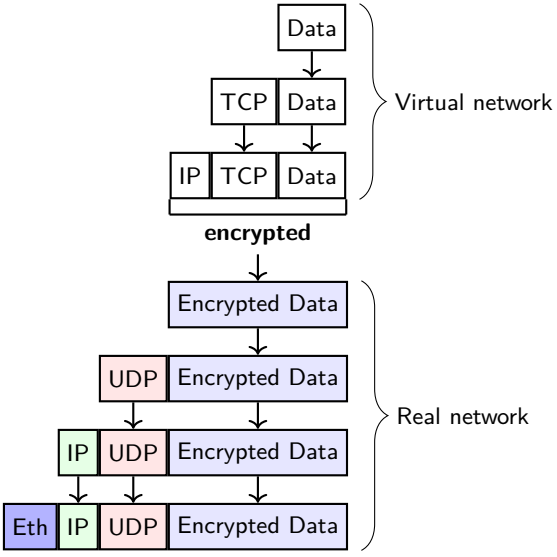
Communication Models



Where is encryption used?

Telsy

WireGuard Packet



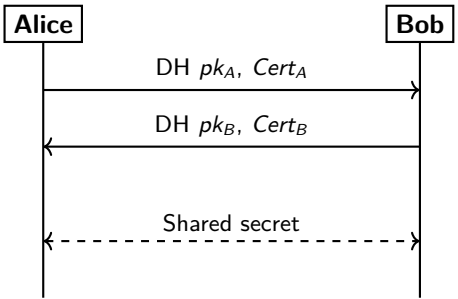
2- Authenticated Key Exchange

Authenticated Key Exchange

- Interactive method for establishing one or more shared secrets which provides (mutual) authentication
- Security against active adversaries
- Cryptographic properties:
  - Forward secrecy (FS or PFS)
  - Key-Compromise Impersonation (KCI) attacks resistance
  - Replay attacks resistance
- Other desirable properties:
  - Denial of Service (DoS) attacks mitigation
  - Identity hiding of static public keys

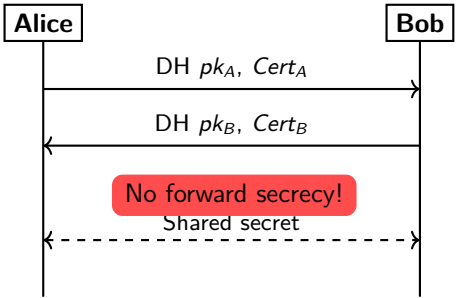
Authenticated Key Exchange - Design

- Starting point: authenticated (certified) static keys
- Typically, AKEs use Diffie-Hellman for key exchange



Authenticated Key Exchange - Design

- Starting point: authenticated (certified) static keys
- Typically, AKEs use Diffie-Hellman for key exchange

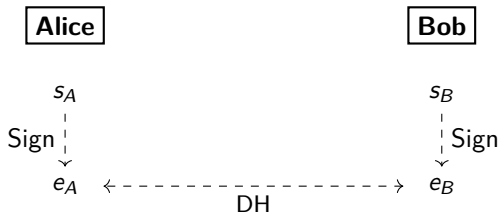


$\Longrightarrow$ Use ephemeral keys

Combine ephemeral keys with static authenticated keys

Authenticated Key Exchange - Design

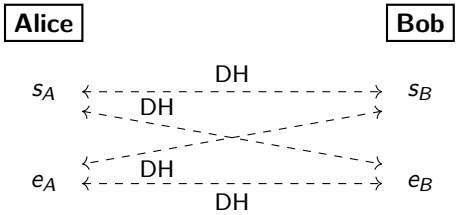
With signature
(explicit authentication)



adopted in

- TLS
- OpenVPN
- IPsec

Without signature
(implicit authentication)

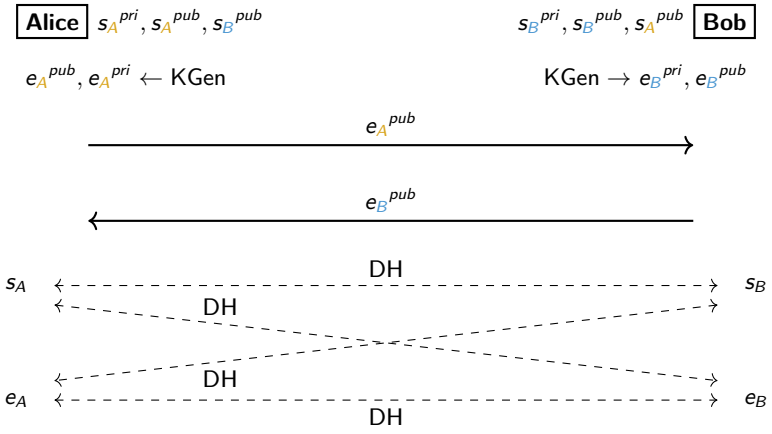


adopted in

- WhatsApp (client-server)
- Signal (X3DH)
- Noise protocol framework [Per18]
- WireGuard

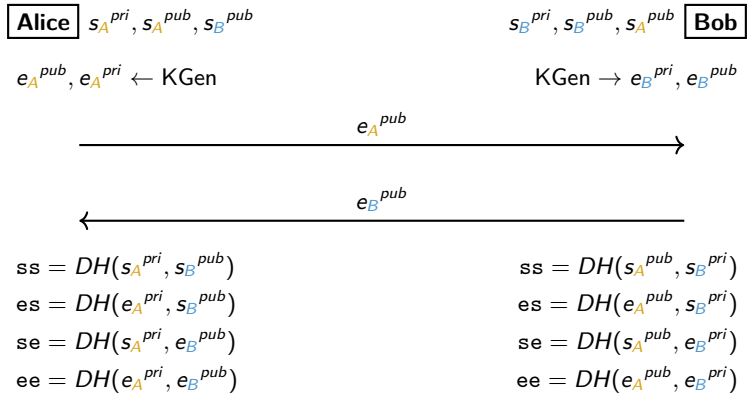
3- WireGuard Protocol

Towards WireGuard Protocol

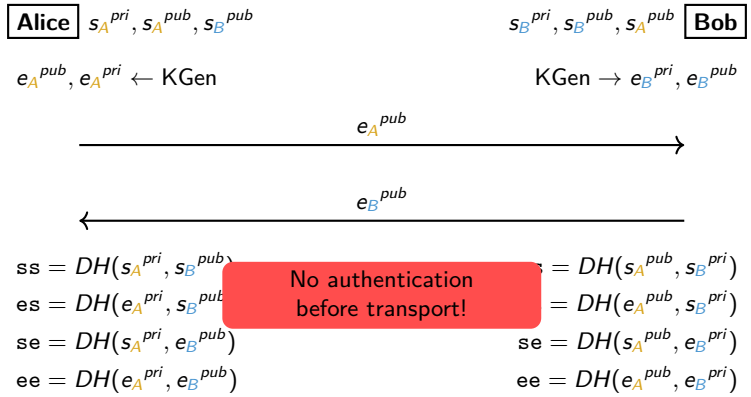


Telsy

Towards WireGuard Protocol

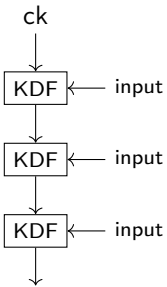


Towards WireGuard Protocol



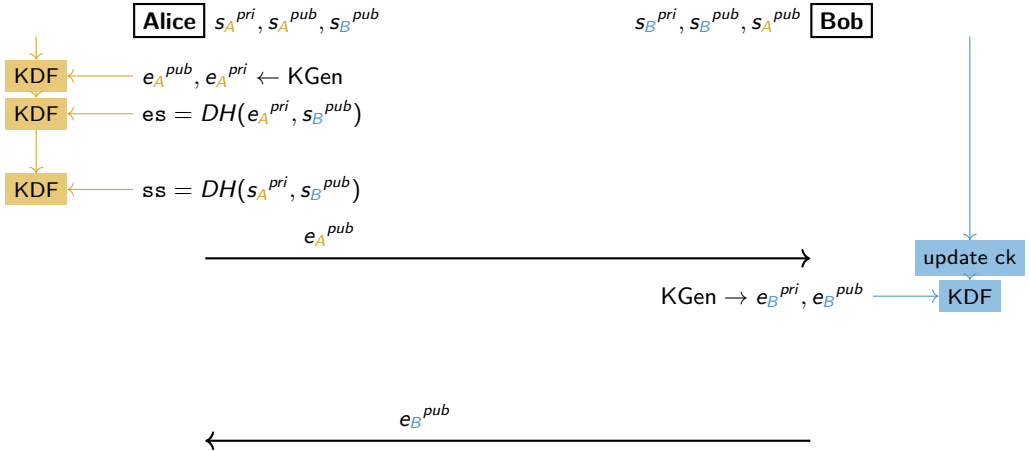
Valuable Ingredients

- KDF (Key Derivation Function)
- Chaining Key

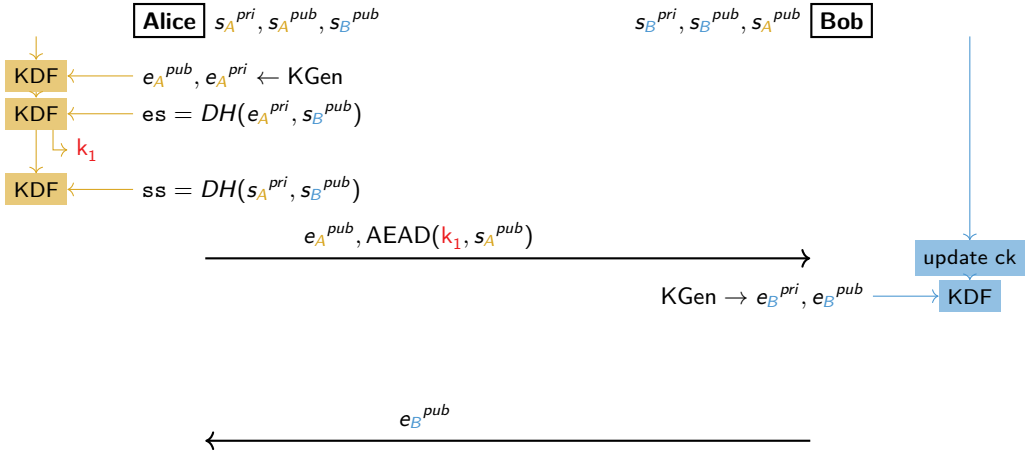


- AEAD (Authenticated Encryption with Associated Data)

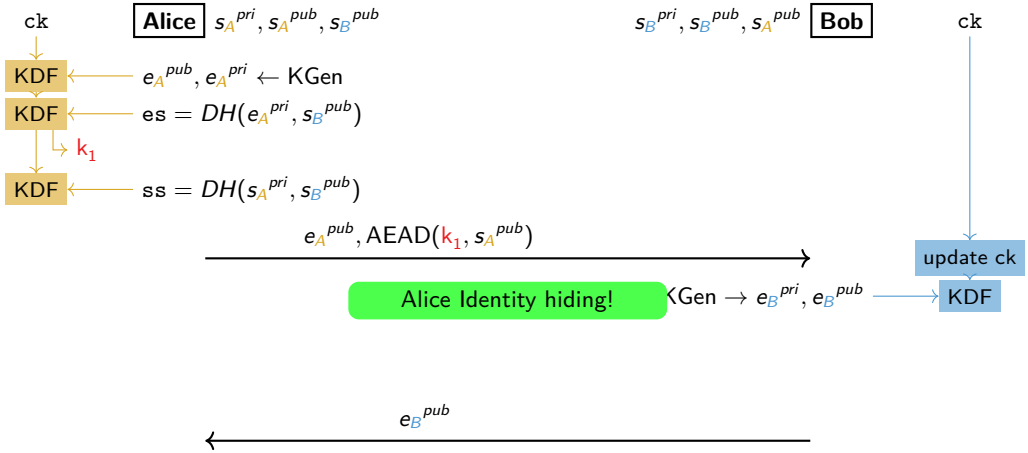
Towards WireGuard Protocol



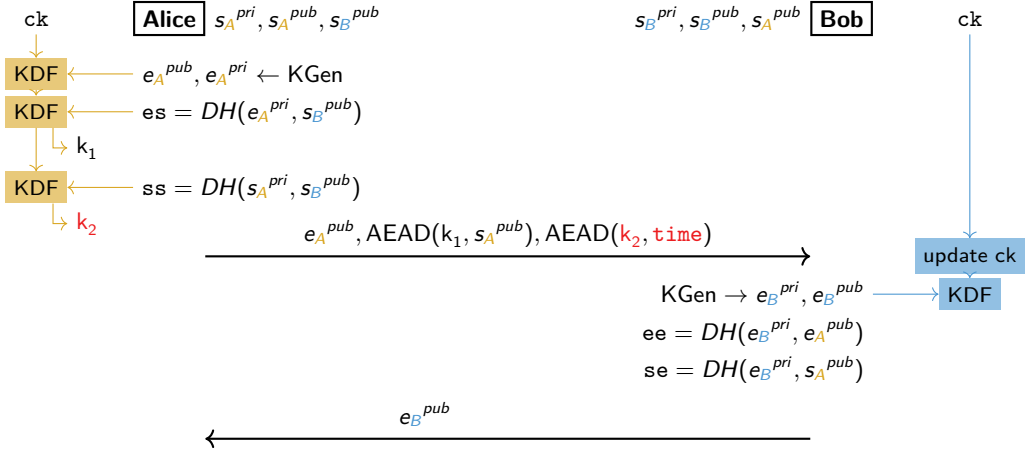
Towards WireGuard Protocol



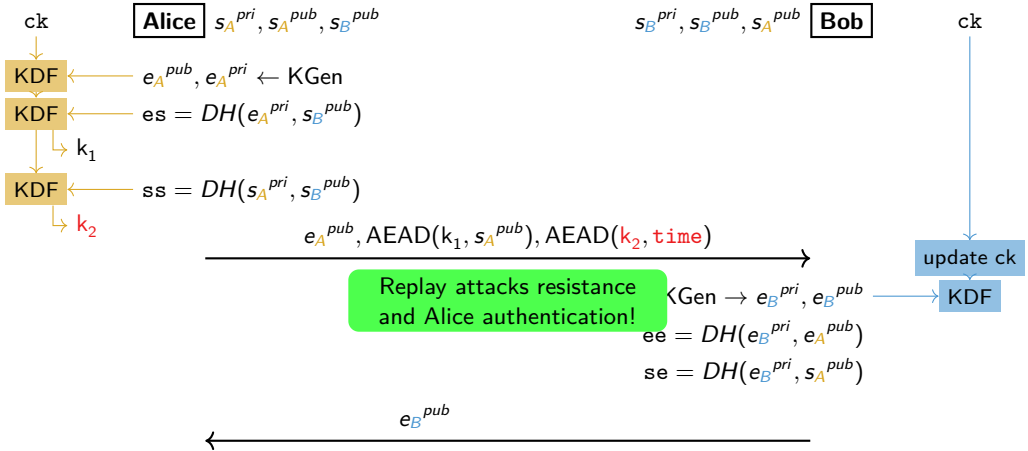
Towards WireGuard Protocol



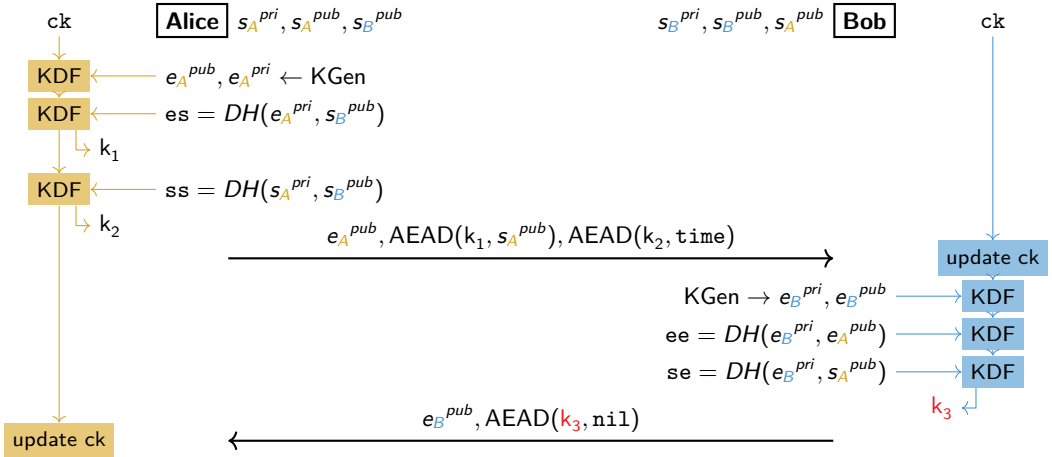
Towards WireGuard Protocol



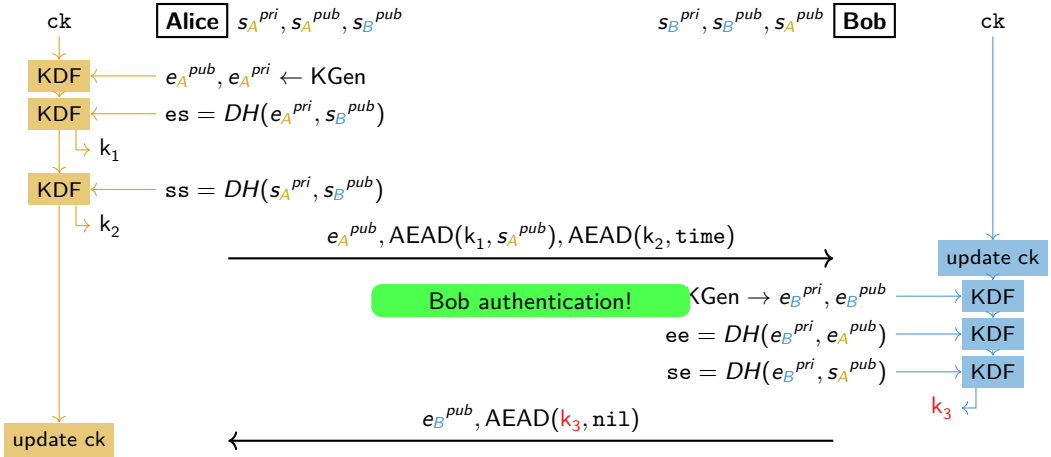
Towards WireGuard Protocol



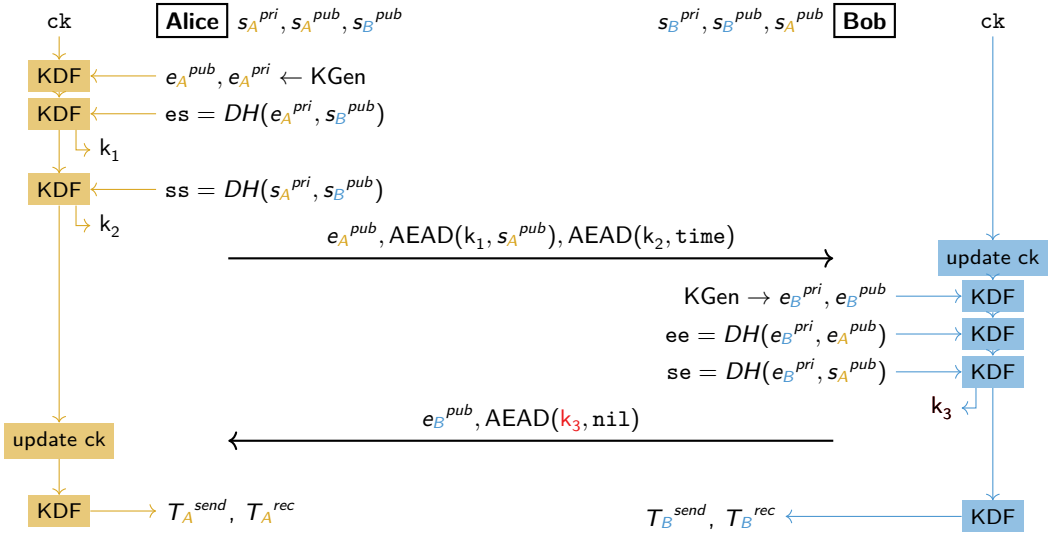
Towards WireGuard Protocol



Towards WireGuard Protocol



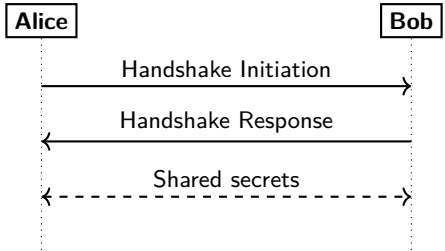
Towards WireGuard Protocol



Telsy

4- Other Security Considerations

Primitives and no negotiation phase



- No negotiation phase. Reduces the number of handshake packets and eliminate any potential negotiation attacks.
- Opinionated choice of cryptography. Supported Crypto Suite:
  - **DH**: X25519
  - **AEAD**: ChaCha20-Poly1305
  - **Hash**: Blake2s
  - **KDF**: HKDF with HMAC-BLAKE2s

Post-Quantum Cryptography in WireGuard

WireGuard proposes an optional pre-shared symmetric key to achieve post-quantum confidentiality

Totally PQ solution

Post-quantum WireGuard, Hülsing et al. [Hül+21]

- maintain all security properties
- McEliece for static keys
- a Saber variant for ephemeral keys

Hybrid solution

Combine classic cryptography with post-quantum cryptography.

- DH are replaced with KEMs that are interactive
- Post-quantum keys and ciphertexts are bigger than the classic ones.

Security properties

Formal verifications

- Computational proof in eCK-PFS-PSK model, Benjamin Dowling and Kenneth G. Paterson [DP18]
- Symbolic verification using Tamarin, Jason A. Donenfeld and Kevin Milner [DM17]

- Key confidentiality
- Key uniqueness
- Authentication
- Forward-secrecy
- KCI attack resistance
- Replay attack resistance
- DDos mitigation
- Identity hiding

Conclusions

WireGuard strengths:

- Easily implemented
- No negotiation phase
- Opinionated choice of primitives

security efficiency auditability

References

[DM17] Jason A Donenfeld and Kevin Milner. "Formal verification of the WireGuard protocol". In: *Technical Report, Tech. Rep* (2017).

[Don17] Jason A Donenfeld. "Wireguard: next generation kernel network tunnel.". In: *NDSS*. 2017, pp. 1–12.

[DP18] Benjamin Dowling and Kenneth G Paterson. "A cryptographic analysis of the WireGuard protocol". In: *International Conference on Applied Cryptography and Network Security*. Springer. 2018, pp. 3–21.

[Hül+21] Andreas Hülsing, Kai-Chun Ning, Peter Schwabe, Florian Weber, and Philip R Zimmermann. "Post-quantum wireguard". In: *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2021, pp. 304–321.

[Per18] Trevor Perrin. "The Noise protocol framework". In: *PowerPoint Presentation* (2018).

Thanks for your attention

Q&A

veronica.cristiano@telsy.it