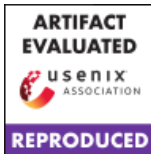
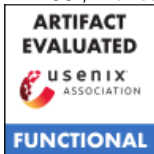
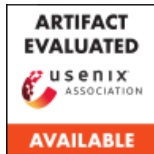


A Tale of Two Worlds, a Formal Story of WireGuard Hybridization

Pascal Lafourcade, Dhekra Mahmoud, Sylvain Ruhault¹, Abdel Taleb¹

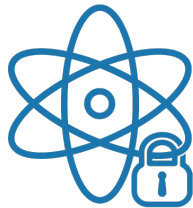


¹ ANSSI, France



August 2025, Seattle

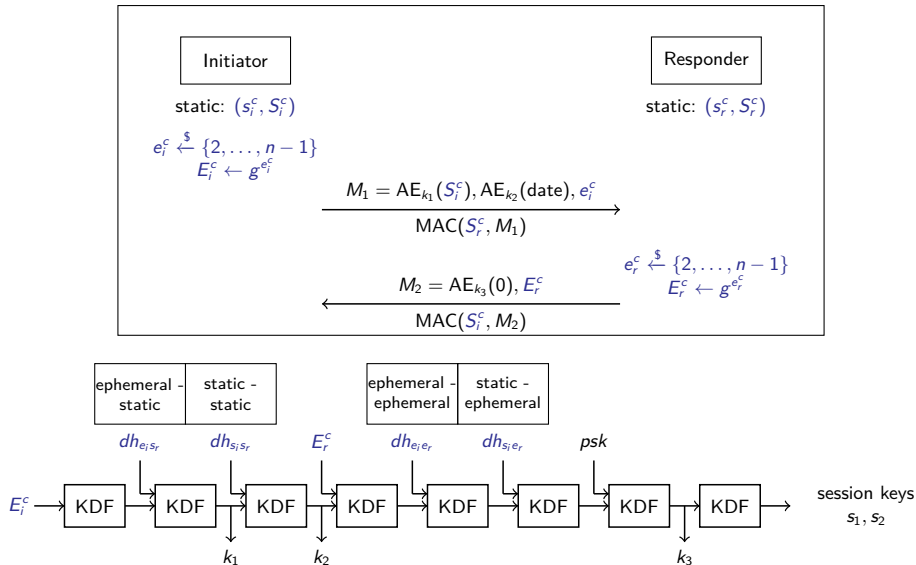
WireGuard [NDSS'17]



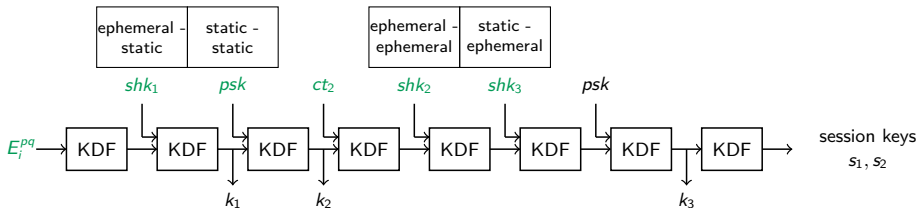
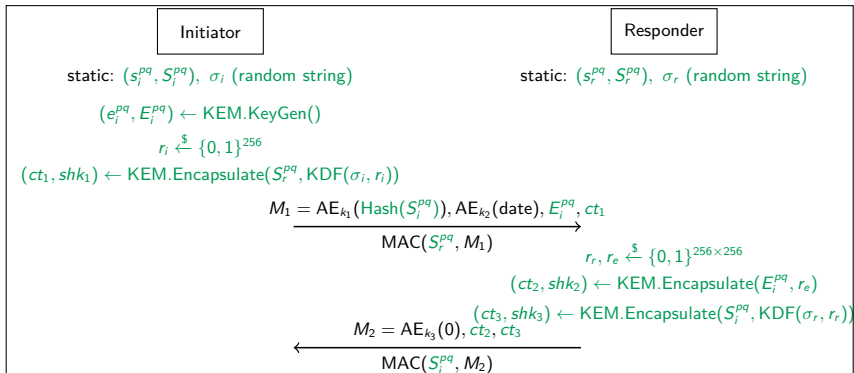
- ▶ Alternative to IPsec/IKEv2 based on Noise
- ▶ Handshake of 2 messages
- ▶ 4 DH shared secrets

WireGuard [NDSS'17]

Simplified Handshake



PQ-WireGuard [IEEE S&P'21]



Contributions



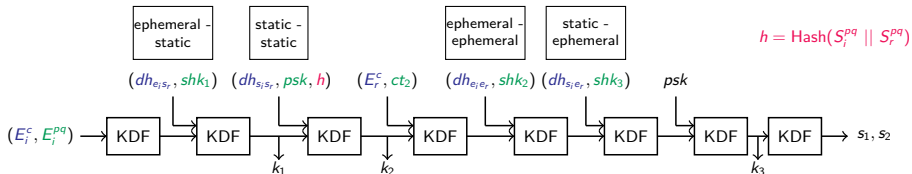
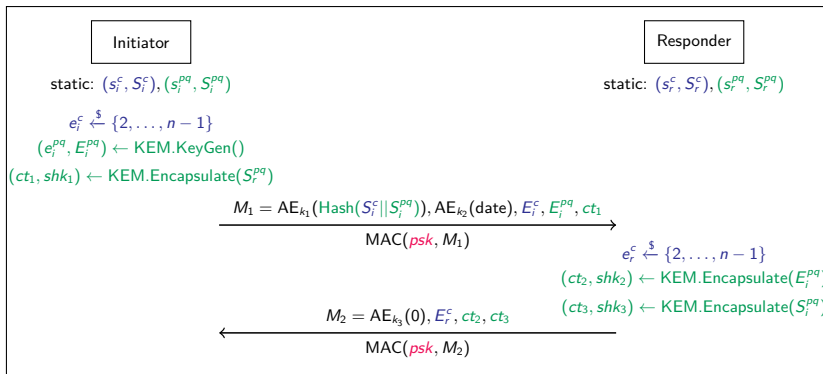
- ▶ Formal analysis of PQ-WireGuard $\Rightarrow$ Flaws
- ▶ Design of PQ-WireGuard* + Formal analysis
- ▶ Design of Hybrid-WireGuard + Formal analysis
- ▶ Implementation in Rust using ML-KEM and Classic McEliece

Contributions

Property	WireGuard [38]	WireGuard [59]	PQ-WireGuard[51]	Rosenpass [75]	Hybrid WireGuard
MEX resistance	✗	✓ ^{t,e}	✓ ^t	✗	✓ ^{t,e}
UKS resistance	✗	✗	✓ ^t	✗	✓ ^t
Session uniqueness	✓ ^t	✗	✓ ^t	✗	✓ ^t
Anonymity	✓ ^t	✓ ^e	✓ ^t	✓ ^e	✓ ^e
Message agreement	✓ ^t	✓ ^t	✓ ^t	✓ ^t	✓ ^t
KCI resistance	✓ ^t	✗	✓ ^t	✗	✓ ^t
Key secrecy	✓ ^t	✓ ^t	✓ ^t	✓ ^t	✓ ^t
Key strong secrecy	✗	✗	✗	✗	✓ ^e
Key mutual secrecy	✗	✗	✓ ^t	✗	✓ ^t
Key FS	✓ ^t	✓ ^t	✓ ^t	✓ ^t	✓ ^t
Key mutual FS	✗	✗	✗	✗	✓ ^t

Hybrid-WireGuard

Combining WireGuard and PQ-WireGuard*



Formal Analysis of Hybrid-WireGuard

Key Secrecy and Anonymity Properties

- ▶ Key secrecy Initiator's view : $\text{psk} \wedge (s_r^c \vee e_i^c) \wedge (\text{dh}_{s_i s_r} \vee s_i^c \vee s_r^c) \wedge (s_r^{\text{pq}} \vee r_i)$
- ▶ Key secrecy Responder's view : $\text{psk} \wedge (s_i^c \vee e_r^c) \wedge (\text{dh}_{s_i s_r} \vee s_i^c \vee s_r^c) \wedge (s_i^{\text{pq}} \vee r_r)$
- ▶ Key mutual secrecy : $\text{psk} \wedge (s_i^c \vee e_r^c) \wedge (s_r^c \vee e_i^c) \wedge (e_i^c \vee e_r^c) \wedge (\text{dh}_{s_i s_r} \vee s_i^c \vee s_r^c) \wedge (s_i^{\text{pq}} \vee r_r) \wedge (s_r^{\text{pq}} \vee r_i) \wedge (\text{esk}_i^{\text{pq}} \vee r_e)$

Performances

Protocol	DH	KEM	Size (bits)
WireGuard [36]	X25519	-	196 + 140
PQ-WireGuard [51]	-	Classic McEliece L3, Dagger L3	1248 + 1160
PQ-WireGuard*	-	Classic McEliece L3,	1124 + 1032
Hybrid-WireGuard	X25519	ML-KEM L1	1156 + 1064

Protocol	Handshake performance (ms)	
	Initiator	Responder
WireGuard [36]	0.49	1.11
PQ-WireGuard*	0.44	0.84
Hybrid-WireGuard	0.87	1.84

Implementation in Rust, Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz

Thanks for your attention



`pascal.lafourcade@uca.fr`