# Post-quantum Secure ZRTP

Loïc Ferreira[1] Johan Pascal[2]

[1] Orange Innovation

[2] Belledonne Communications

PQCrypto 2024
June 12-14, 2024


# Introduction

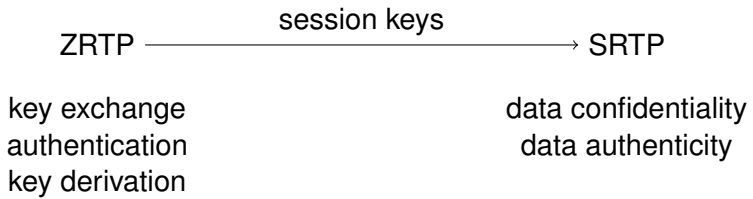
- Context: transition to post-quantum security.
- Goal: providing quantum-safe tools to end-users.
- Target: secure VoIP application.

"*This Commission Recommendation encourages Member States to develop a comprehensive strategy for the adoption of Post-Quantum Cryptography*"

European Commission,
April 11, 2024

# ZRTP

- ZRTP: AKE protocol for VoIP application [ZJC11].
- Akin to   
- Key exchange: (EC)DHE, PSK (not considered).
- Authentication: signature, “Short Authentication String” (SAS).

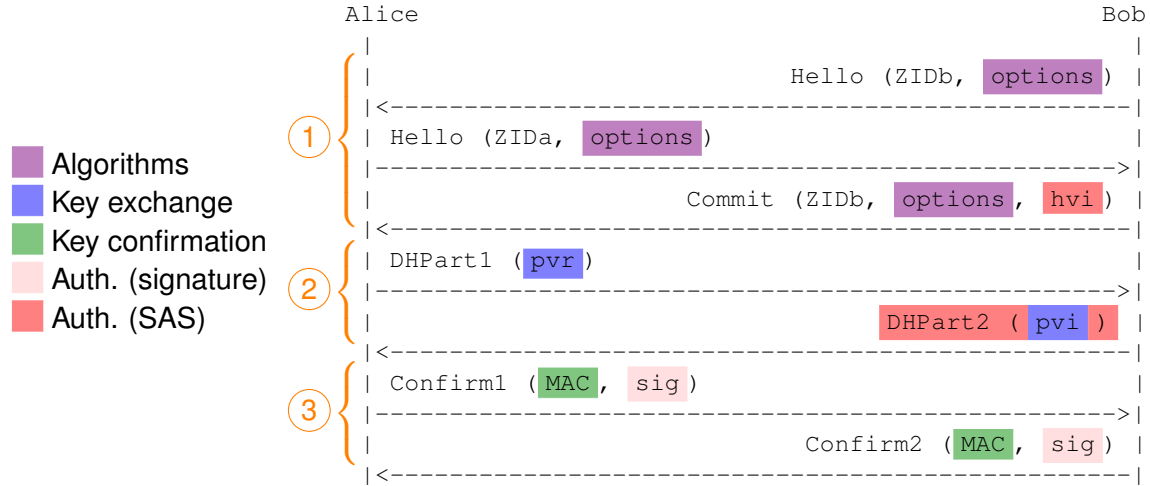



[BMN+04] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman. *The Secure Real-time Transport Protocol (SRTP)*. RFC 3711. 2004.

[ZJC11] P. Zimmermann, A. Johnston, and J. Callas. *ZRTP: Media Path Key Agreement for Unicast Secure RTP*. RFC 6189. 2011.

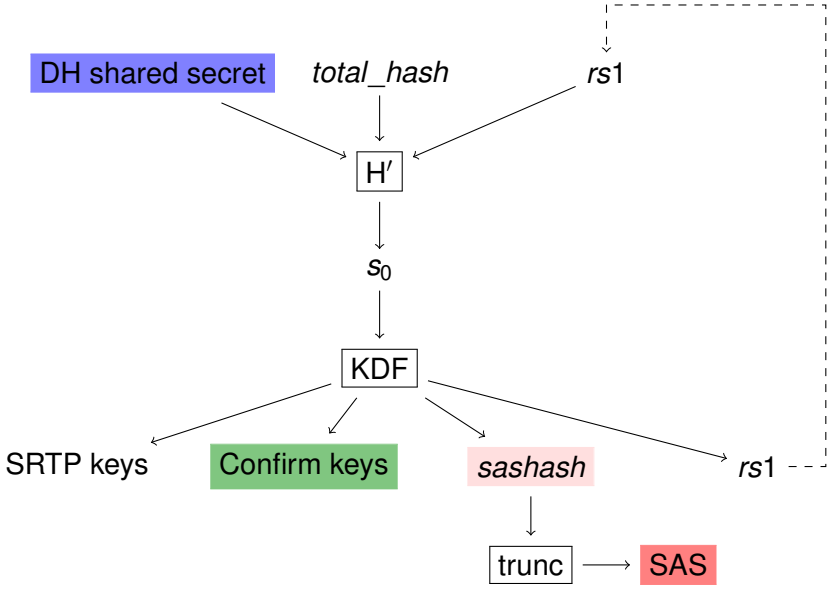
# ZRTP

## Protocol Flow



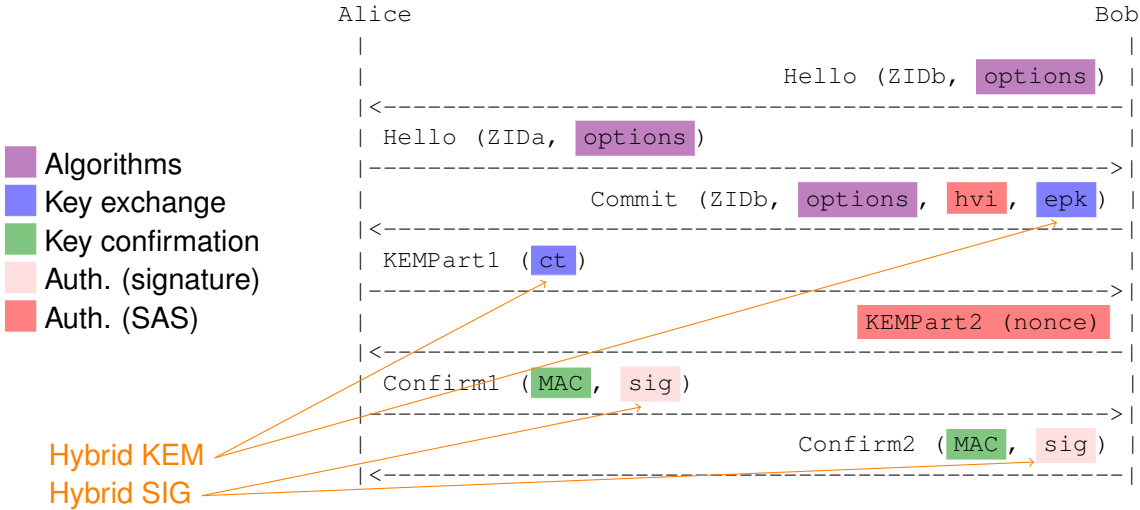
# ZRTP

## Key Derivation



# Post-quantum ZRTP

## Protocol Flow



# Post-quantum ZRTP

## A Few Details

- Hybrid KEM $=$ Combiner$(\mathsf{KEM}_{\mathsf{cl}}, \mathsf{KEM}_{\mathsf{pq}})$
- Hybrid SIG $= \mathsf{SIG}_{\mathsf{cl}} \| \mathsf{SIG}_{\mathsf{pq}}$
- $s_0 = \mathrm{H}'($~~DH~~ KEM shared secret, *total_hash*, *rs*1$)$
- Instantiation

| | |
|---|---|
| $\mathsf{KEM}_{\mathsf{cl}}$ | DHKEM [BBLW22] (with X25519, X448) |
| $\mathsf{KEM}_{\mathsf{pq}}$ | Kyber, HQC |
| Combiner | “nested dual-PRF” [BBF+19] |
| $\mathsf{SIG}_{\mathsf{cl}}$ | EdDSA |
| $\mathsf{SIG}_{\mathsf{pq}}$ | Dilithium |


[BBF+19] N. Bindel, J. Brendel, M. Fischlin, B. Goncalves, and D. Stebila. *Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange.* PQCrypto. 2019.

[BBLW22] R. Barnes, K. Bhargavan, B. Lipp, and C. Wood. *Hybrid Public Key Encryption.* RFC 9180. 2022.

# Post-quantum ZRTP

## Additional Changes

- $total\_hash = \mathrm{H}'(\mathrm{Hello}_I \| \mathrm{Hello}_R \| \mathrm{Commit} \| \mathrm{KEMPart1} \| \mathrm{KEMPart2})$
  $\Rightarrow$ Mitigates Bhargavan et al. attack [BBF+16].

- signed data $= label_{role} \| \text{public key} \| sashash$
  $\Rightarrow$ Mitigates reflection attack (authentication).
  $\Rightarrow$ Avoids misbinding issues (if "*link to the* [public] *key*" is not unique).

- Confirm's IV: computed (session parameters) instead of pseudo-randomly generated [Dra]
  $\Rightarrow$ Saves bandwidth.


[BBF+16] K. Bhargavan, C. Brzuska, C. Fournet, M. Green, M. Kohlweiss, and S. Zanella-Béguelin. *Downgrade Resilience in Key-Exchange Protocols*. S&P. 2016.

[Dra] https://github.com/traviscross/zrtp-drafts/blob/master/rfc6189bis.xml.

# Security Analysis

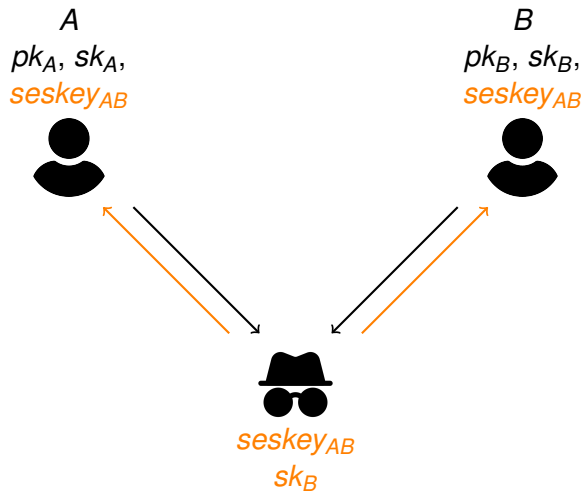
## Security Properties

- Entity authentication: existence of a unique partner instance for an accepting instance.
- Key indistinguishability: indistinguishability of the session key from a random value.
- Forward secrecy: security of past sessions upon disclosure of long-term keys.
- Soundness: two partners share the same session keys.

# Security Analysis

## Adversarial Environment

- The adversary can
  - control the network,
  - corrupt long-term keys,
  - reveal session keys.



# Open-source Code

- liboqs v0.9.1: Kyber512, Kyber1024, HQC-128, HQC-256.
- libdecaf v1.0.2: X25519, X448.
- Mbed TLS v3.4.0: symmetric-key cryptography.

- Authentication: SAS (not signature – yet).

https://gitlab.linphone.org/BC/public/bzrtp

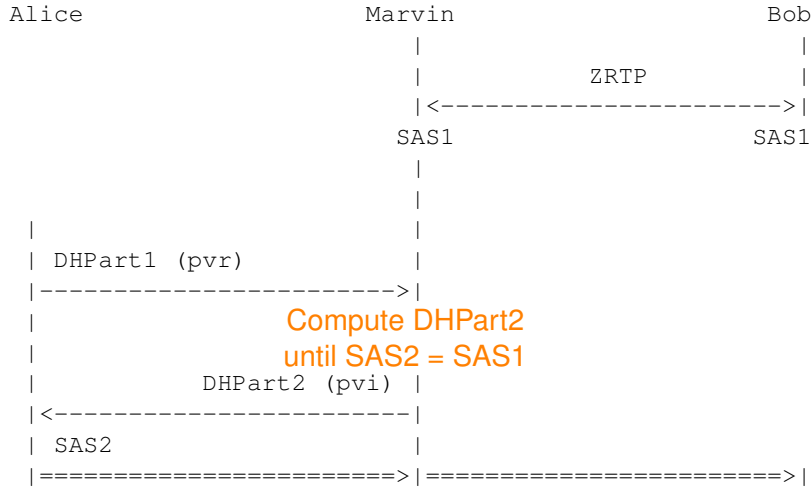
# Summary

- Post-quantum version of ZRTP.
- Mitigation of previous and new flaws.
- Security analysis in a strong security model.
- Open-source code.

# Thank you for your attention!

# ZRTP

## Authentication with SAS



# ZRTP

## Authentication with SAS