Hybrid Post-Quantum Password Authenticated Key Exchange

draft-vos-cfrg-pqpake

https://eprint.iacr.org/2025/1343.pdf

IETF 123 - CFRG

PAKE Landscape

Classical PAKE specifications and deployments exist en masse

SRP, Dragonfly, and SPAKE2+ exist and are all used in production today

CPace and OPAQUE are on their way to being specified

Post-quantum PAKEs exist primarily in the literature, with differing properties and assumptions

NoIC, OCAKE, CHIC, …

Motivation

We want a post-quantum PAKE with the following properties:

Post-quantum: table stakes

Augmented: drop-in replacement for existing augmented PAKEs (SRP and SPAKE2+)

Hybrid: Hedge against cryptographic or protocol design or implementation vulnerabilities

And built on standard assumptions (ROM) and primitives (ML-KEM)

OQUAKE

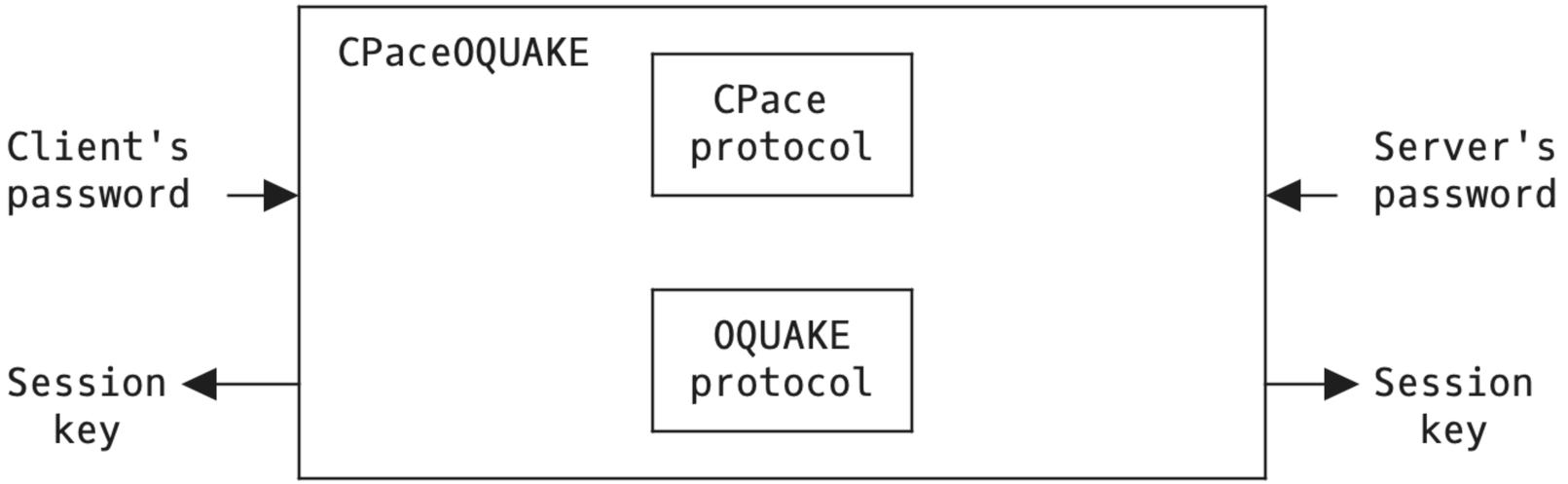
UC PAKE from KEM in the ROM

κ is a security parameter, λ_{pk} is an integer s.t. $\lambda_{pk} \geq \kappa$
KEM is a KEM and $\mathcal{P}$ is a set s.t. $\mathsf{KEM}.\mathrm{KeyGen}(1^\kappa)$ generates (pk, sk) s.t. $pk \in \mathcal{P}$
$\phi : \mathcal{P} \mapsto \{0,1\}^{\lambda_{pk}}$ is a uniform encoding of random $\mathcal{P}$ elements as random λ_{pk}-bit strings
$\mathtt{H}, \mathtt{H}', \mathtt{H}_{\mathsf{kc}}$ are hash functions onto resp. $\{0,1\}^{\lambda_{pk}}$, $\{0,1\}^{3\kappa}$, and $\{0,1\}^{2\kappa} \times \{0,1\}^{\kappa}$

User U on input $(\mathsf{ssid}, S, \mathsf{pw}_U)$		**Server** S on input $(\mathsf{ssid}, U, \mathsf{pw}_S)$
	$\mathsf{fsid} = (\mathsf{ssid}, U, S)$	
$(pk, sk) \leftarrow \mathsf{KEM}.\mathrm{KeyGen}(1^\kappa)$		
$bpk \leftarrow \phi(pk)$		
$r \leftarrow_R \{0,1\}^{3\kappa}$		
$T \leftarrow bpk \oplus \mathtt{H}(\mathsf{fsid}, \mathsf{pw}_U, r)$		
$s \leftarrow r \oplus \mathtt{H}'(\mathsf{fsid}, \mathsf{pw}_U, T)$		
$\mathbf{Epk} \leftarrow (s, T)$	$\xrightarrow{\mathbf{Epk}}$	
		$(s, T) \leftarrow \mathbf{Epk}$
		$r \leftarrow s \oplus \mathtt{H}'(\mathsf{fsid}, \mathsf{pw}_S, T)$
		$bpk \leftarrow T \oplus \mathtt{H}(\mathsf{fsid}, \mathsf{pw}_S, r)$
		$pk \leftarrow \phi^{-1}(bpk)$
		$(c, k) \leftarrow \mathsf{KEM}.\mathrm{Encaps}(pk)$
	$\xleftarrow{c, h}$	$(h, \mathsf{K}) \leftarrow \mathtt{H}_{\mathsf{kc}}(\mathsf{fsid}, \mathbf{Epk}, c, pk, \mathsf{pw}_S, k)$
$k \leftarrow \mathsf{KEM}.\mathrm{Decaps}(sk, c)$		
$(h', \mathsf{K}') \leftarrow \mathtt{H}_{\mathsf{kc}}(\mathsf{fsid}, \mathbf{Epk}, c, pk, \mathsf{pw}_U, k)$		
If $h' \neq h$ then re-set $\mathsf{K}' \leftarrow_R \mathbb{K}$		
$\mathsf{ftr} \leftarrow (\mathsf{fsid}, \mathbf{Epk}, c, h)$		$\mathsf{ftr} \leftarrow (\mathsf{fsid}, \mathbf{Epk}, c, h)$
Output $(\mathsf{K}', \mathsf{ftr})$		Output $(\mathsf{K}, \mathsf{ftr})$

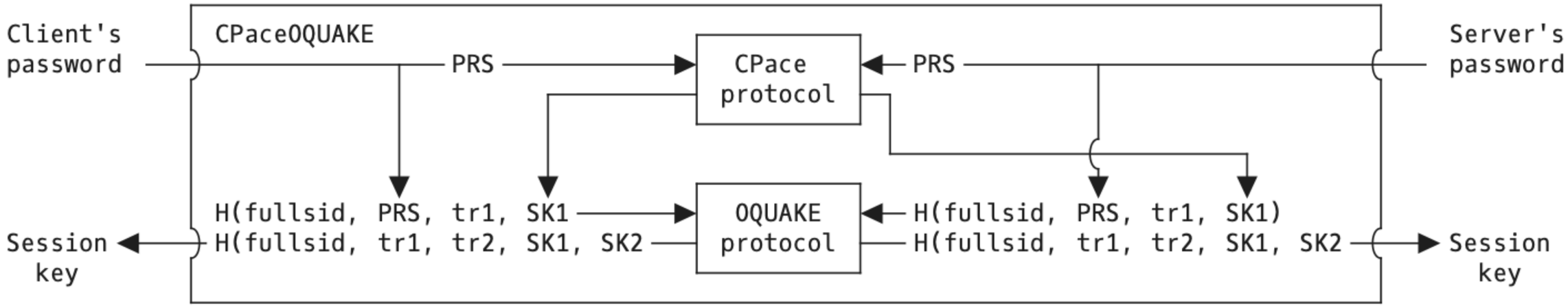
CPaceOQUAKE

Hybrid CPace and OQUAKE



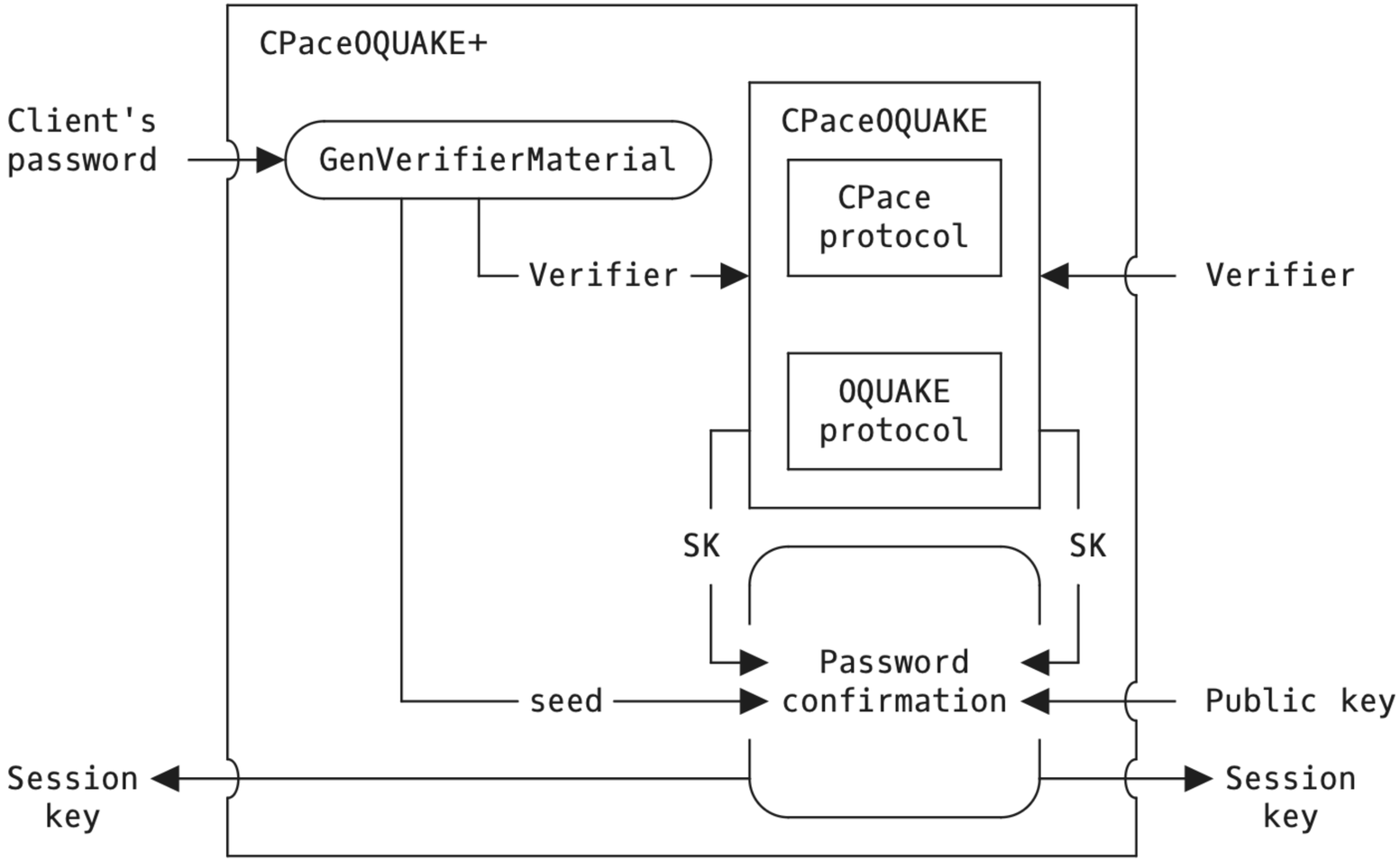
CPaceOQUAKE

Hybrid CPace and OQUAKE



CPaceOQUAKE+

Augmented variant



Limitations

Multiple rounds due to sequential hybrid combiner

Integration into TLS more difficult (but not impossible)

Small dependencies beyond ML-KEM

Requires some new cryptographic primitives (Kemeleon)

Questions for CFRG / SEC

Is this interest in this work (or the non-hybrid protocol OQUAKE)?

Should specification of a PQ (a)PAKE happen inside or outside of the CFRG?

If inside CFRG, we propose work on the general problem of PQ-PAKEs, with OQUAKE, CPaceQUAKE, and CPaceOQUAKE+ being part of the solution space

If outside CFRG, BoF?

Hybrid Post-Quantum Password Authenticated Key Exchange

draft-vos-cfrg-pqpake

IETF 123 - CFRG