draft-schwabe-kyber-cfrg-kyber

https://github.com/bwesterb/draft-schwabe-cfrg-kyber

R. Avanzi
J. Bos
L. Ducas
E. Kiltz
T. Lepoint
V. Lyubashevsky
J. Schanck
P. Schwabe
G. Seiler
D. Stehle
B. Westerbaan

CRYSTALS-Kyber

- Post-quantum KEM (≠ DH)
- Computationally fast. Much faster than X25519.
- Larger ciphertext (ct) and public key (pk).
- Will likely perform great for TLS in the Web.

Kyber-512					
Sizes (in bytes)		Haswell cycles (ref)		Haswell cycles (avx2)	
sk:	1632	gen:	122684	gen:	33856
pk:	800	enc:	154524	enc:	45200
ct:	768	dec:	187960	dec:	34572
Kyber-768					
Sizes (in bytes)		Haswell cycles (ref)		Haswell cycles (avx2)	
sk:	2400	gen:	199408	gen:	52732
pk:	1184	enc:	235260	enc:	67624
ct:	1088	dec:	274900	dec:	53156
Kyber-1024					
Sizes (in bytes)		Haswell cycles (ref)		Haswell cycles (avx2)	
sk:	3168	gen:	307148	gen:	73544
pk:	1568	enc:	346648	enc:	97324
ct:	1568	dec:	396584	dec:	79128

Context

- July 5th, NIST announced they will standardize Kyber as *the* **post-quantum key agreement**. Standard is expected *2024*.
- Small but backwards incompatible **changes** are likely.
- We expect many early adopters before 2024.

Goal

- 🐘 We want to **match** NIST's final standard.
- What's the point then?
  - Drafts can be used as reference for early adopters.
  - We will include a machine-readable specification (for now in Python) which NIST probably will not.
  - Feedback from IETF into NIST's choices as Kyber team will help out on this draft.
  - Unlock usage for IETF protocols (TLS, where codepoints are cheap).

Questions?
Concerns?
Interest in adoption?

Kyber on a napkin

$R := GF(q)[x] / \langle x^{256} + 1 \rangle$ has very fast NTT-based mult.

$q := 13 \cdot 2^8 + 1$

	k	η_1	η_2	d_u	d_v	level
Kyber 512	2	3	2	10	4	I
Kyber 768	3	2	2	10	4	III
Kyber 1024	4	2	2	11	5	IV

$$GF(q) \underset{\text{decompr}_d}{\overset{\text{compr}_d}{\rightleftarrows}} \{0, \dots, 2^{d-1}\}$$

$\text{compr}_d(x) = \lceil 2^d x / q \rfloor \mod 2^d$

$\text{decompr}_d(x) = \lceil q x / 2^d \rfloor$

$\text{CBD}(\eta)$: centered binom dist. with $n = 2\eta$.

KYBER.CPAPKE, IND-CPA secure PKE

Keygen A $k \times k$ matrix over R sampled uniformly from seed ρ

s, e from R^k sampled with $\text{CBD}(\eta_1)$

Public key: A, $t := As + e$ Private key: s

Encryption of message m. Sample r, e_1, e_2 from R^k, R^k, R (resp.) with CBD $\eta = \eta_1, \eta_1, \eta_2$.

$u := A^T r + e_1$ $v := t^T r + e_2 + \text{decompr}_1(m)$

Ciphertext: $c_1 := \text{compr}_{d_u}(u)$, $c_2 := \text{compr}_{d_v}(v)$

Decryption $u := \text{decompr}_{d_u}(c_1)$ $v := \text{decompr}_{d_v}(c_2)$

$m := \text{compr}_1(v - s^T u)$

Kyber is the F.O.-transform of the scheme on the left to get IND-CCA2 secure KEM.