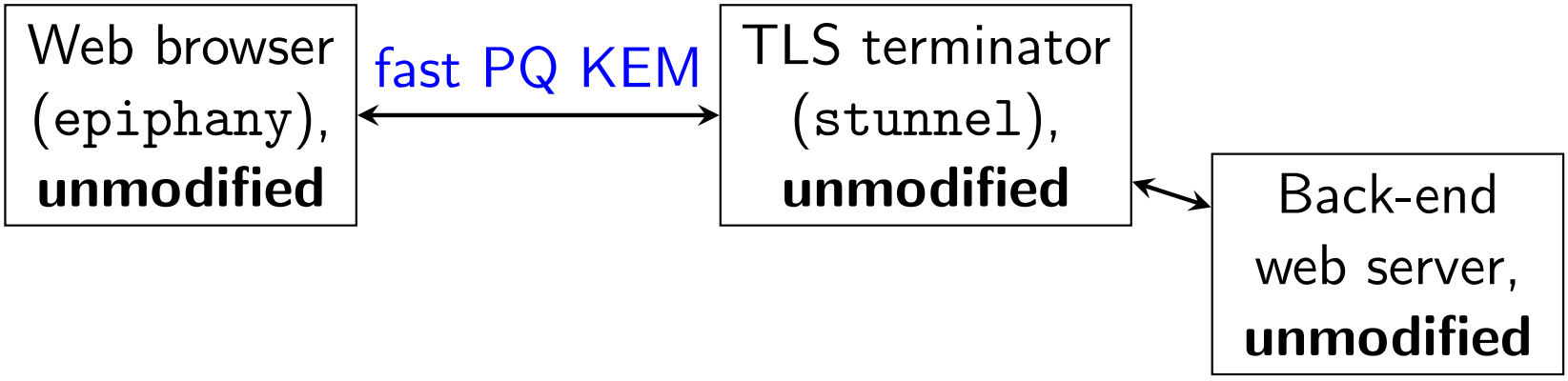
OpenSSLNTRU: experiences integrating a post-quantum KEM into TLS 1.3 via an OpenSSL ENGINE

Speaker: Daniel J. Bernstein

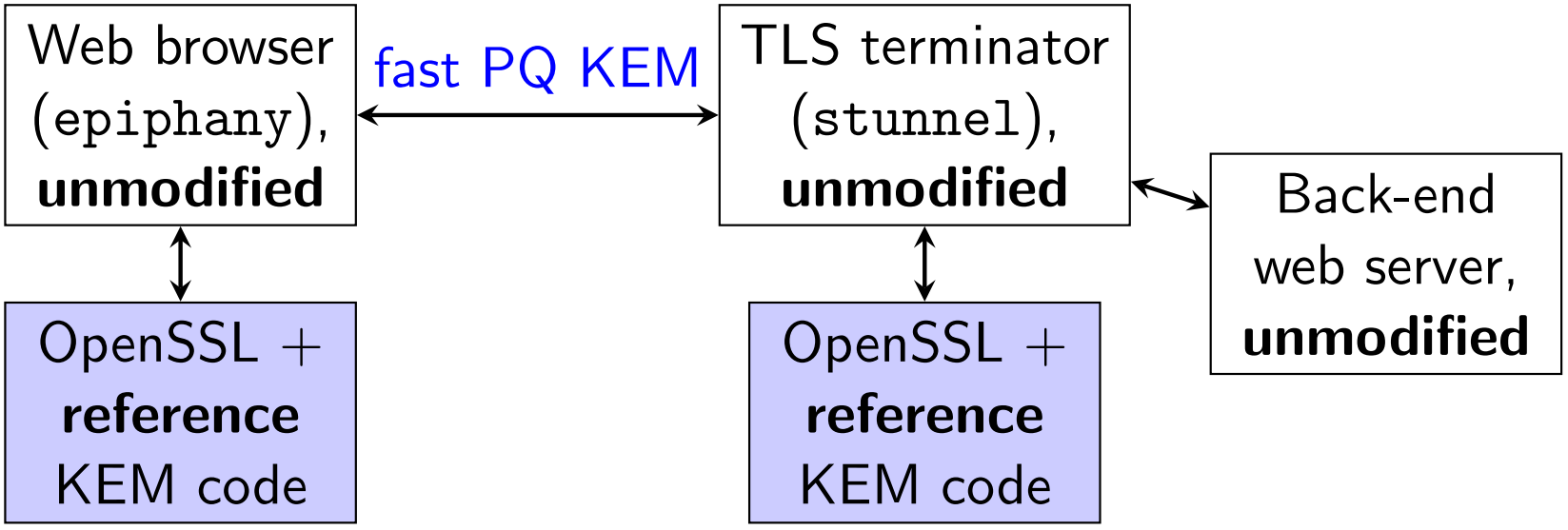
Joint work with: Billy Bob Brumley, Ming-Shing Chen (`libsntrup761` leader), Nicola Tuveri (`engntru` leader)

https://openssllntru.cr.yp.to

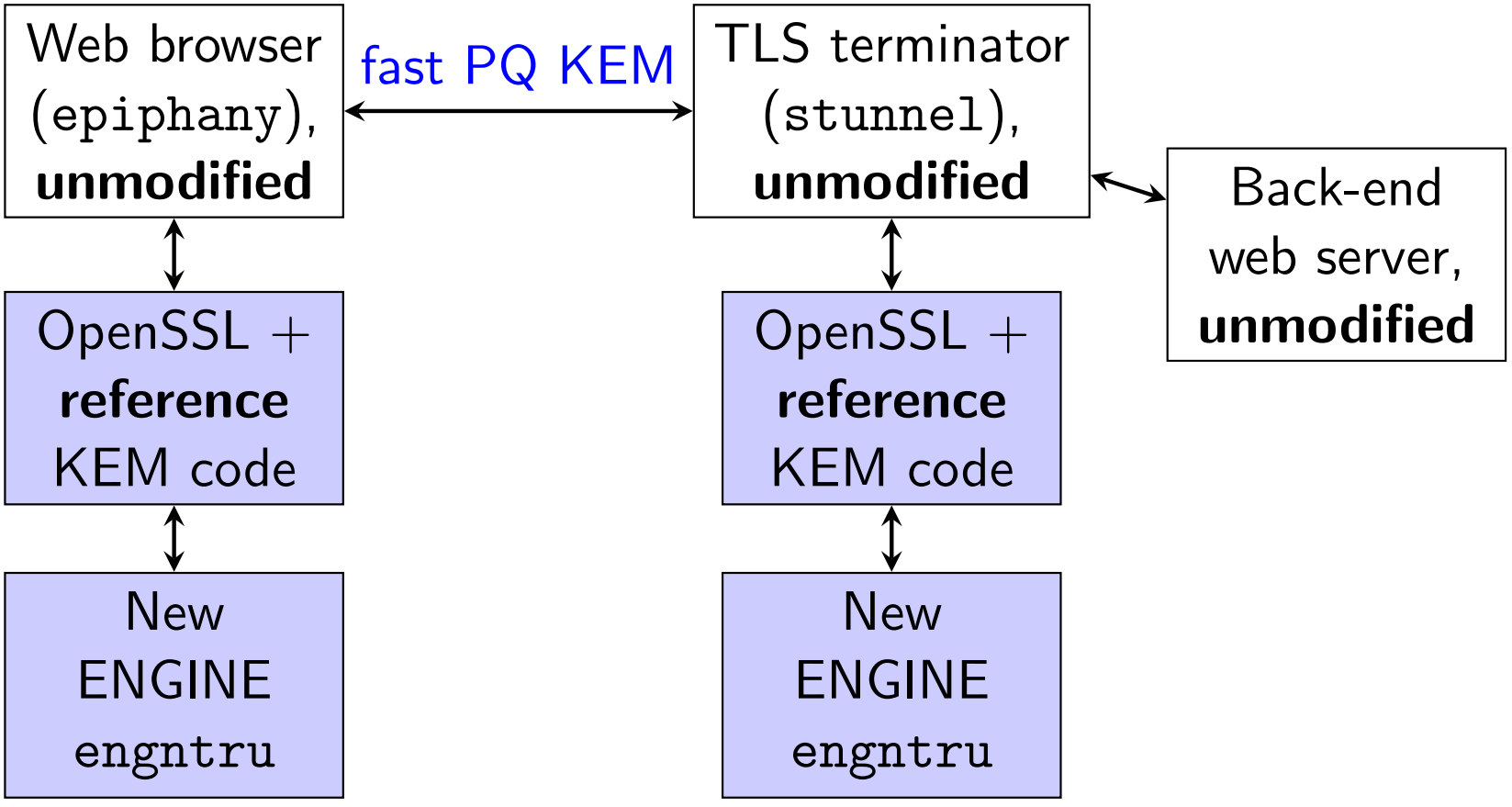
OpenSSLNTRU software architecture



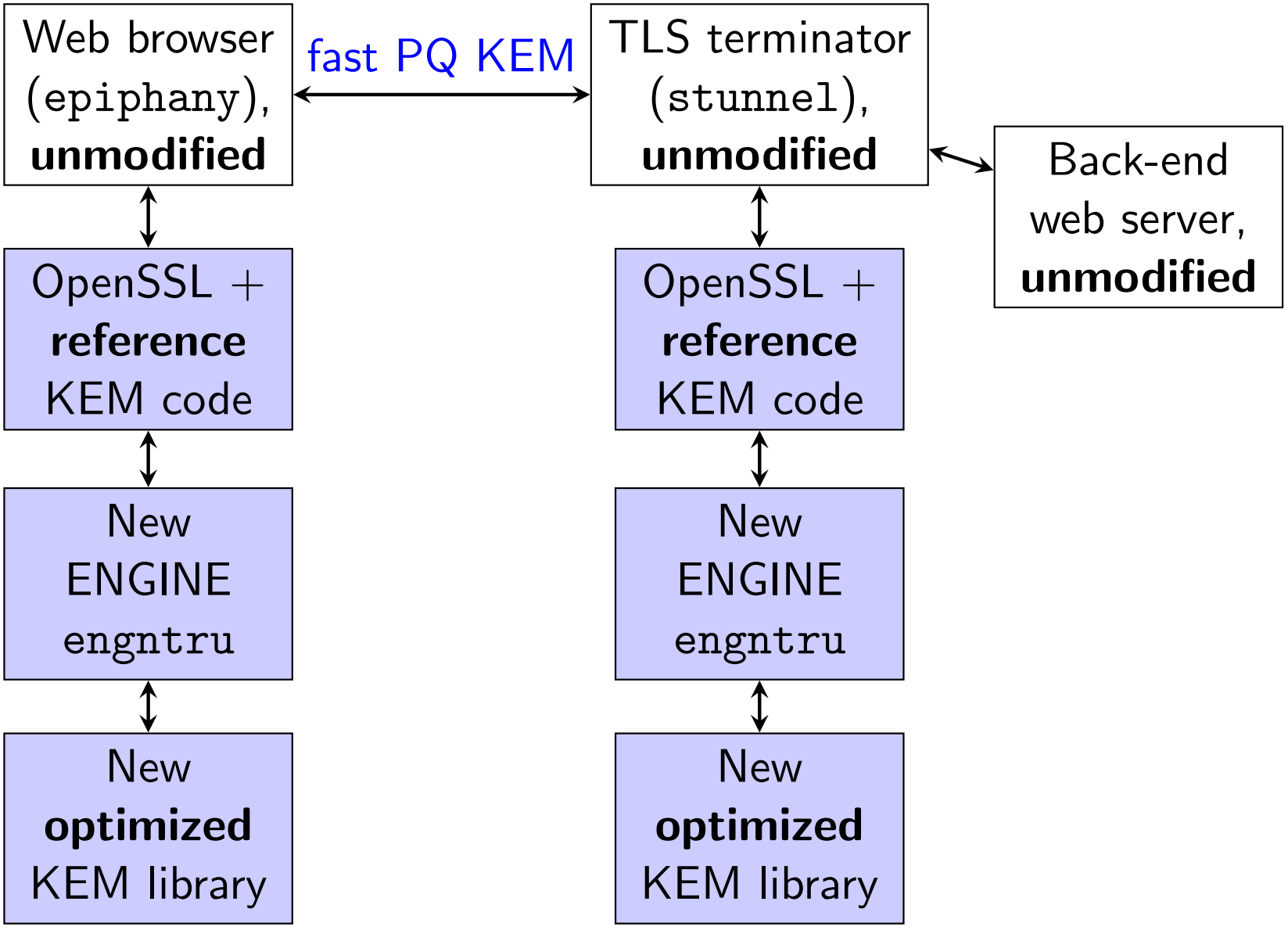
OpenSSLNTRU software architecture



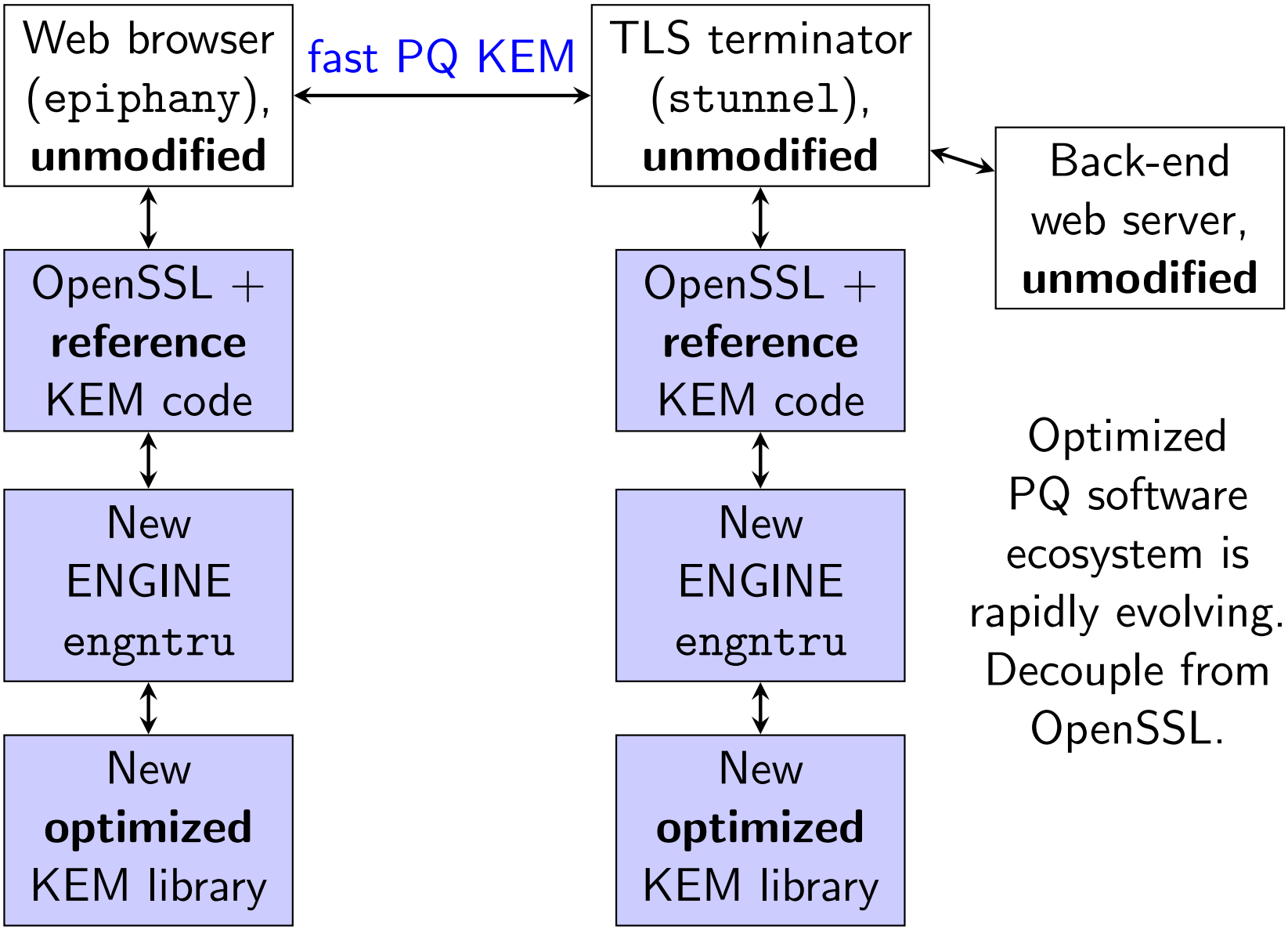
OpenSSLNTRU software architecture



OpenSSLNTRU software architecture



OpenSSLNTRU software architecture



Optimized PQ software ecosystem is rapidly evolving. Decouple from OpenSSL.

OpenSSLNTRU cryptography

OpenSSLNTRU adds the new PQ KEM to TLS 1.3.
Protocol flow: similar to Google-Cloudflare CECPQ2 experiment.

Higher performance than post-quantum component of CECPQ2.
New software for **faster key generation**. Also **higher security.**

OpenSSLNTRU cryptography

OpenSSLNTRU adds the new PQ KEM to TLS 1.3.
Protocol flow: similar to Google-Cloudflare CECPQ2 experiment.

Higher performance than post-quantum component of CECPQ2.
New software for **faster key generation**. Also **higher security.**

NIST submission	`ntruhrss701`	`sntrup761`
key+ciphertext traffic	2276 bytes	2197 bytes
keygen time	272028 cycles	166000 cycles (new)
enc time	26116 cycles	48780 cycles
dec time	63632 cycles	59120 cycles
PQ Core-SVP security	2^{125}	2^{139}
cyclotomic concerns	yes	no
used in	CECPQ2	OpenSSLNTRU

OpenSSLNTRU cryptography

OpenSSLNTRU adds the new PQ KEM to TLS 1.3.
Protocol flow: similar to Google-Cloudflare CECPQ2 experiment.

Higher performance than post-quantum component of CECPQ2.
New software for **faster key generation**. Also **higher security.**

NIST submission	`ntruhrss701`	`sntrup761`
key+ciphertext traffic	2276 bytes	2197 bytes
keygen time	272028 cycles	166000 cycles (new)
enc time	26116 cycles	48780 cycles
dec time	63632 cycles	59120 cycles
PQ Core-SVP security	2^{125}	2^{139}
cyclotomic concerns	yes	no
used in	CECPQ2	OpenSSLNTRU

`kyber768`: faster keygen but has cyclotomic concerns, consumes 2272 bytes, and is threatened by US patents 9094189 and 9246675.