Post-quantum RSA (pqRSA)

Daniel J. Bernstein

Joint work with:

Josh Fried

Nadia Heninger

Paul Lou

Luke Valenta

Parameters

Scaled-down targets for cryptanalysis:

- `pqrsa15`: 2^{15}-byte keys using 512-bit primes.
- `pqrsa20`: 2^{20}-byte keys using 512-bit primes.
- `pqrsa25`: 2^{25}-byte keys using 1024-bit primes.

Primary parameter set included in submission:

- `pqrsa30`: 2^{30}-byte keys using 1024-bit primes.

Feasible option not included in submission:

- `pqrsa40`: 2^{40}-byte keys using 4096-bit primes.
  Yes, we generated one of these keys.

Speeds

Approximate cycles/byte on 1 core of 3GHz Intel Skylake:

	keygen	dec	enc
`pqrsa15`	110000	3700	530
`pqrsa20`	110000	5800	1000
`pqrsa25`	540000	15000	1400
`pqrsa30`	550000	21000	1700

(Expect future speedups, especially for keygen.)

`pqrsa30` keygen: 2.3 days; dec: 2.1 hours; enc: 10.1 minutes.

Speeds

Approximate cycles/byte on 1 core of 3GHz Intel Skylake:

	keygen	dec	enc
pqrsa15	110000	3700	530
pqrsa20	110000	5800	1000
pqrsa25	540000	15000	1400
pqrsa30	550000	21000	1700

(Expect future speedups, especially for keygen.)

pqrsa30 keygen: 2.3 days; dec: 2.1 hours; enc: 10.1 minutes.

Submission also says "... quadrillion cycles".
Should say "trillion". NIST didn't notice?

Network traffic

For `pqrsa30`:

- Key: ..... 2^{30} bytes.
- Signature: ..... $\approx 2^{30}$ bytes.
- Ciphertext for `kem`: ..... 2^{30} bytes.
- Ciphertext for `encrypt`: ..... 2^{30} bytes, *including* $\approx 2^{30}$ bytes of encrypted message.

Submission does not cover options for compressing signed messages.

Security against known attacks

`pqrsa30` security analysis in submission:

- 2017 Häner–Roetteler–Svore $\Rightarrow$
  $\approx 2^{110}$ Toffoli gates using $\approx 2^{34}$ qubits.
  Beyond NIST Category 2 under reasonable assumptions.

Security against known attacks

`pqrsa30` security analysis in submission:

- 2017 Häner–Roetteler–Svore $\Rightarrow$
  $\approx 2^{110}$ Toffoli gates using $\approx 2^{34}$ qubits.
  Beyond NIST Category 2 under reasonable assumptions.
- Actually higher security: consider communication costs.

Security against known attacks

`pqrsa30` security analysis in submission:

- 2017 Häner–Roetteler–Svore $\Rightarrow$
  $\approx 2^{110}$ Toffoli gates using $\approx 2^{34}$ qubits.
  Beyond NIST Category 2 under reasonable assumptions.
- Actually higher security: consider communication costs.
- Actually higher security: consider latency limits.
  NIST Categories 3–5 are not clearly defined!

Security against known attacks

`pqrsa30` security analysis in submission:

- 2017 Häner–Roetteler–Svore $\Rightarrow$
  $\approx 2^{110}$ Toffoli gates using $\approx 2^{34}$ qubits.
  Beyond NIST Category 2 under reasonable assumptions.
- Actually higher security: consider communication costs.
- Actually higher security: consider latency limits.
  NIST Categories 3–5 are not clearly defined!
- Maybe lower security: e.g., lower-cost multiplications?

Security against known attacks

`pqrsa30` security analysis in submission:

- 2017 Häner–Roetteler–Svore $\Rightarrow$
  $\approx 2^{110}$ Toffoli gates using $\approx 2^{34}$ qubits.
  Beyond NIST Category 2 under reasonable assumptions.
- Actually higher security: consider communication costs.
- Actually higher security: consider latency limits.
  NIST Categories 3–5 are not clearly defined!
- Maybe lower security: e.g., lower-cost multiplications?
- Prime size: 512 bits probably ok; 1024 ample.

Security against known attacks

`pqrsa30` security analysis in submission:

- 2017 Häner–Roetteler–Svore $\Rightarrow$
  $\approx 2^{110}$ Toffoli gates using $\approx 2^{34}$ qubits.
  Beyond NIST Category 2 under reasonable assumptions.
- Actually higher security: consider communication costs.
- Actually higher security: consider latency limits.
  NIST Categories 3–5 are not clearly defined!
- Maybe lower security: e.g., lower-cost multiplications?
- Prime size: 512 bits probably ok; 1024 ample.

Submitted to NIST as Category 2.

Security stability

RSA has tons of mathematical structure.
Long history of many scary RSA security losses.

Security stability

RSA has tons of mathematical structure.
Long history of many scary RSA security losses.

pqRSA already has close to the worst performance-security tradeoffs in this competition. Further security losses would not be surprising. e.g. Shor vs. small primes has barely been studied.

Security stability

RSA has tons of mathematical structure.
Long history of many scary RSA security losses.

pqRSA already has close to the worst performance-security tradeoffs in this competition. Further security losses would not be surprising. e.g. Shor vs. small primes has barely been studied.

But users keep using RSA.

Security stability

RSA has tons of mathematical structure.
Long history of many scary RSA security losses.

pqRSA already has close to the worst performance-security tradeoffs in this competition. Further security losses would not be surprising.
e.g. Shor vs. small primes has barely been studied.

But users keep using RSA.
RSA-512 publicly broken: "Let's use RSA-768."

Security stability

RSA has tons of mathematical structure.
Long history of many scary RSA security losses.

pqRSA already has close to the worst performance-security tradeoffs in this competition. Further security losses would not be surprising. e.g. Shor vs. small primes has barely been studied.

But users keep using RSA.
RSA-512 publicly broken: "Let's use RSA-768."
RSA-768 publicly broken: "Let's use RSA-1024."

Security stability

RSA has tons of mathematical structure.
Long history of many scary RSA security losses.

pqRSA already has close to the worst performance-security tradeoffs in this competition. Further security losses would not be surprising. e.g. Shor vs. small primes has barely been studied.

But users keep using RSA.
RSA-512 publicly broken: "Let's use RSA-768."
RSA-768 publicly broken: "Let's use RSA-1024."
RSA-2048 publicly broken by quantum computers:

Security stability

RSA has tons of mathematical structure.
Long history of many scary RSA security losses.

pqRSA already has close to the worst performance-security tradeoffs in this competition. Further security losses would not be surprising. e.g. Shor vs. small primes has barely been studied.

But users keep using RSA.
RSA-512 publicly broken: "Let's use RSA-768."
RSA-768 publicly broken: "Let's use RSA-1024."
RSA-2048 publicly broken by quantum computers:
"Yeah, NSA already told us to use RSA-3072."

Familiarity

Users care about more than security+performance.

"I learned RSA in school."

Familiarity

Users care about more than security+performance.

"I learned RSA in school."

"Factorization has been deeply studied by some of the great mathematicians going back to the ancient Greeks."

Familiarity

Users care about more than security+performance.

"I learned RSA in school."

"Factorization has been deeply studied by some of the great mathematicians going back to the ancient Greeks."

No mention of how much security has been lost.

Familiarity

Users care about more than security+performance.

"I learned RSA in school."

"Factorization has been deeply studied by some of the great mathematicians going back to the ancient Greeks."

No mention of how much security has been lost.
Is the quoted argument competent cryptography? No.

Familiarity

Users care about more than security+performance.

"I learned RSA in school."

"Factorization has been deeply studied by some of the great mathematicians going back to the ancient Greeks."

No mention of how much security has been lost.
Is the quoted argument competent cryptography? No.
Do users continue using RSA? Yes.

Familiarity

Users care about more than security+performance.

"I learned RSA in school."

"Factorization has been deeply studied by some of the great mathematicians going back to the ancient Greeks."

No mention of how much security has been lost.
Is the quoted argument competent cryptography? No.
Do users continue using RSA? Yes.

Analogy: "Lattice problems have been deeply studied by some of the great mathematicians going back to Gauss."

Familiarity, continued: quotes from 1997

Lenstra: "The elliptic curve discrete logarithm problem has been around for a relatively short amount of time."

Adleman: "I suspect that the lack of a sub-exponential algorithm is merely a matter of neglect."

Schnorr: "It is unreasonable to assume that it has straight exponential complexity."

Silverman: "Nor is it backed up by as many years of active cryptanalytic research as the RSA results are."

Risk management

Very plausible nightmare scenario:

- Quantum computers are built.
- Many users continue using RSA.

Important to analyze the security of pqRSA.

Risk management

Very plausible nightmare scenario:

- Quantum computers are built.
- Many users continue using RSA.

Important to analyze the security of pqRSA.

If we say "Don't use RSA; system X is better": Will users obey?

Risk management

Very plausible nightmare scenario:

- Quantum computers are built.
- Many users continue using RSA.

Important to analyze the security of pqRSA.

If we say "Don't use RSA; system X is better": Will users obey?

Analogy: If we say "Use 256-bit cipher keys": Will users obey?

Risk management

Very plausible nightmare scenario:

- Quantum computers are built.
- Many users continue using RSA.

Important to analyze the security of pqRSA.

If we say "Don't use RSA; system X is better": Will users obey?

Analogy: If we say "Use 256-bit cipher keys": Will users obey?

And is it clear that system X *is* better?
Maybe `pqrsa30` is the strongest system in the NIST competition!