Countering quantum FUD

Daniel J. Bernstein

Joint work with:

Nadia Heninger

Paul Lou

Luke Valenta

All crypto is broken?

FUD: "Nobody knows exactly when quantum computing will become a reality, but when and if it does, it will signal the end of traditional cryptography."

All crypto is broken?

FUD: “Nobody knows exactly when quantum computing will become a reality, but when and if it does, it will signal the end of traditional cryptography.”

Sales pitch: Buy QKD!
(Never mind QKD security disasters.)

All crypto is broken?

FUD: “Nobody knows exactly when quantum computing will become a reality, but when and if it does, it will signal the end of traditional cryptography.”

Sales pitch: Buy QKD!
(Never mind QKD security disasters.)

Fact check: Actually,
many cryptosystems are unbroken.

Public-key crypto is broken?

FUD: "When the first quantum factoring devices are built the security of public-key cryptosystems will vanish."

Public-key crypto is broken?

FUD: “When the first quantum factoring devices are built the security of public-key cryptosystems will vanish.”

Sales pitch: Buy QKD!
(Never mind lack of functionality.)

Public-key crypto is broken?

FUD: “When the first quantum factoring devices are built the security of public-key cryptosystems will vanish.”

Sales pitch: Buy QKD!
(Never mind lack of functionality.)

Fact check: Actually,
many public-key cryptosystems are unbroken.

RSA and ECC are broken?

FUD: RSA is dead. “There’s not going to be a larger key-size where a classical user of RSA gains a significant advantage over a quantum computing attacker.”

RSA and ECC are broken?

FUD: RSA is dead. “There’s not going to be a larger key-size where a classical user of RSA gains a significant advantage over a quantum computing attacker.”

Sales pitch: Buy codes! Lattices! Multivariates! Hash signatures!

RSA and ECC are broken?

FUD: RSA is dead. “There’s not going to be a larger key-size where a classical user of RSA gains a significant advantage over a quantum computing attacker.”

Sales pitch: Buy codes! Lattices! Multivariates! Hash signatures!

Fact check (new): Actually, RSA survives with big keys.

RSA: Back from the dead

Picture credit: http://fpswin.com/wp-content/uploads/2011/12/cfM0q.jpg

Post-quantum RSA

https://eprint.iacr.org/2017/351

We generated a 1TB RSA key.

Preliminary security analysis:
$>2^{100}$ security against all known attacks.

Post-quantum RSA

https://eprint.iacr.org/2017/351

We generated a 1TB RSA key.

Preliminary security analysis:
$>2^{100}$ security against all known attacks.

Used only about **2 million core-hours**.

Also have preliminary implementation
of RSA-KEM encryption and decryption.