Signature sizes: a call to action

D. J. Bernstein
 University of Illinois at Chicago &
 Technische Universiteit Eindhoven

RSA signatures are big.

RSA signatures are big.

1990 Schnorr signatures
are much smaller:
3n bits for security 2ⁿ.

Often misquoted as 4*n* bits; e.g., 2009 Neven–Smart– Warinschi claims to improve Schnorr from 4*n* to 3*n* ("saving twenty-five percent in signature size"). RSA signatures are big.

1990 Schnorr signatures
are much smaller:
3n bits for security 2ⁿ.

Often misquoted as 4*n* bits; e.g., 2009 Neven–Smart– Warinschi claims to improve Schnorr from 4*n* to 3*n* ("saving twenty-five percent in signature size").

2001 Boneh–Lynn–Shacham pairing-based "short signatures": 2*n* bits. 1996 Patarin "HFEv-", 2001 Patarin–Courtois–Goubin "Quartz": *n* bits.

"Very short asymmetric signatures".

Also achieved by many other MQ signature schemes, often with smaller keys; but HFEv- has a long history and inspires confidence.

Further save, e.g., 10 bits at expense of multiplying verification cost by $\leq 2^{10}$. "Message recovery":

signature conveys message. Measure "signature overhead": signature size – message size. Often 4*n* or 3*n*, sometimes 2*n*.

Many papers/standards: message recovery for RSA.

1993 Nyberg–Rueppel,
2000 Pintsov–Vanstone,
2001 Naccache–Stern:
message recovery for ECDSA.
Deployment stopped by patents.

Latest message-recovery paper: 2012 Kiltz–Pietrzak–Szegedy "Digital signatures with minimal overhead". Rumor: will appear at Crypto 2013.

"Our main contribution is to revisit the question if there exists a digital signature scheme with message recovery that has minimal ($\approx n$ bits) overhead.... The best previous constructions required an overhead of 2n."

Conclusions:

1. Many people care about signature size.

Conclusions:

Many people care about signature size.

2. Many people are shockingly ignorant of short MQ signatures.

Conclusions:

Many people care about signature size.

2. Many people are shockingly ignorant of short MQ signatures.

3. Need to raise awareness
of MQ capabilities.
e.g. add Quartz to eBATS.
http://bench.cr.yp.to