More news from the Rabin-Williams front

D. J. Bernstein

Thanks to:
University of Illinois at Chicago
NSF CCR–9983950
Alfred P. Sloan Foundation
Math Sciences Research Institute
University of California at Berkeley
American Institute of Mathematics

Signature length

30-digit public key pq.

Rabin-Williams signature
of message m under public key pq
is vector (e, f, r, s) such that
$s^2 \equiv \text{blah} \pmod{pq}$.

Three bits to store e, f, r;
but 30 digits to store s.

Compressing signatures to 1/2 size

(Bleichenbacher 2003)

Compute s/pq continued fraction:

$$\frac{s}{pq} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}.$$

Define v_i as denominator of

$$a_0 + \frac{1}{a_1 + \frac{1}{\cdots + \frac{1}{a_i}}}.$$

Find maximum i with $v_i \le 10^{15}$.
Print (e, f, r, v_i).

Only 15 digits plus 3 bits.

Using pq, can convert e, f, r, v back to e, f, r, s.

To verify e, f, r, v directly, check that $1 \leq v \leq 10^{15}$ and that v^2(blah) mod pq is a square in $\mathbf{Z}$.

Larger pq for security

For 1536-bit pq:
Compress keys to 512 bits.
Compress signatures to 771 bits.
Total key+signature size: 1283 bits.
Without compression: 3072 bits.

Still not as small as
elliptic-curve key+signature with
comparable conjectured security.
But much faster verification.

Expanded signatures

Signature: (e, f, r, s) such that $s^2 \equiv \text{blah} \pmod{pq}$.

Expanded: (e, f, r, s, t) such that $s^2 - \text{blah} - pqt = 0$.

Fast randomized verification: Check $((s \bmod n)^2 - (\text{blah} \bmod n) - (pq \bmod n)(t \bmod n)) \bmod n = 0$ for secret random 100-bit prime n.

Primality proofs

(Selfridge Weinberger, improved by Lukes Patterson Williams 1996)

An integer $n \in [2^{20}, 2^{100}]$ is prime iff

- $r^{(n-1)/2} \equiv \pm 1 \pmod{n}$ for all primes $r \leq 367$;
- $r^{(n-1)/2} \equiv -1 \pmod{n}$ for some odd prime $r \leq 367$ if $n \bmod 8 = 1$;
- $2^{(n-1)/2} \equiv -1$ if $n \bmod 8 = 5$;
- n is not a perfect power; and
- n has no prime divisors below 2^{20}.

Use Pollard's rho method: define $x_0 = 0$, $x_i = (x_{i-1}^2 + 11) \bmod n$; if n coprime to $(x_1 - x_2)(x_2 - x_4) \cdots (x_{3575} - x_{7150})$ then no prime divisors below 2^{20}. (Somewhat messier with converse.)

Also 73 exponentiations. < 20000 mults total. Various speedups available. Fastest known proving method.

Proof relies on big computation:
every nonsquare $x < 2^{80}$, $x \in 1 + 8\mathbf{Z}$,
is nonsquare mod some prime ≤ 367.
(Williams, Wooding 2003)

2^{80} is scary but save
$\approx 2^{10}$ from focused enumeration;
$\approx 2^{10}$ more, doubly focused;
and lots of streamlining.

This is doable even though
100-bit primes are unguessable.