Protecting communications against forgery

D. J. Bernstein
University of Illinois at Chicago

Secret-key authenticators

Message $m \in 10^{50}\mathbf{Z}$,
at most 1000000 digits.

Sender and receiver know
secret prime p, $10^{39} < p < 10^{40}$,
and secret $k \in \mathbf{Z}$, $0 \le k < 10^{45}$.

Sender transmits (m, a) where
$a = ((m \bmod p) + k) \bmod 10^{45}$.

Forger replaces (m, a)
with (m', a').

Receiver discards (m', a') unless
$a' = ((m' \bmod p) + k) \bmod 10^{45}$.

If (p, k) is uniform:
The forger has chance $< 10^{-33}$
of fooling the receiver.

How many pairs (p, k) satisfy
$a = ((m \bmod p) + k) \bmod 10^{45}$?
At least $9 \cdot 10^{37}$.

How many also satisfy
$a' = ((m' \bmod p) + k) \bmod 10^{45}$?
Fewer than $9 \cdot 10^{4}$ if $m \neq m'$:
for some $\delta \in \{-1, 0, 1\}$ have p
dividing $m - m' + 10^{45}\delta - a + a'$.

Handling multiple messages

Sender and receiver know secrets $p, k_1, k_2, k_3, \ldots$.

Sender transmits nth message m as (n, m, a) where $a = ((m \bmod p) + k_n) \bmod 10^{45}$.

(Gilbert, MacWilliams, Sloane; Wegman, Carter; Karp, Rabin)

Faster system:

Secrets $p_0, k_1, k_2, \ldots \in F$
where $F = \mathbf{Z}/(2^{127} - 1)$.

Transmit nth message $m \in xF[x]$
as $(n, m, m(p_0) + k_n)$.

Generating primes in $F[x]$ is
easier than generating primes in $\mathbf{Z}$.

Unpredictability

Random functions $f, u : S \to T$.
Finite T; uniform u.
Example: $f = \mathrm{RC6}_r$, uniform r.

f is **unpredictable** if,
for all fast oracle algorithms A,
$\Pr[A(f) \text{ says yes}] \approx$
$\Pr[A(u) \text{ says yes}]$.

Sender and receiver know
secret f; use $k_n = f(n)$.
Safe if f is unpredictable.

Want f **short**: specified concisely.

If every short fast f
is efficiently predictable
then factoring is poly-time.
(Blum, Blum, Shub)

Derandomization

BPP = P if there is a family of sufficiently unpredictable sufficiently short fast f's.
(Yao)

Some specific families are conjectured to work.

In my talk I should have started by emphasizing that we can deterministically compute the exact average result of a probabilistic algorithm using a short random function, by running through all the possibilities for the function. This average is approximately the average result of the algorithm using a uniform random function; which, by definition of BPP, is approximately 1 or 0 depending on whether the input string is in the language. The random function has to be unpredictable for all algorithms as fast as the algorithm we started with, but still short enough that we can quickly try all the possibilities. It seems sufficient for the number of possibilities to be roughly the fourth power of the run time of the original algorithm.

The Diffie-Hellman system

$$
\begin{tikzcd}
\text{Secret } g^{bc} & \text{Receiver's public key } g^{c} \arrow[l] \\
\text{Sender's secret } b \arrow[u] \arrow[d] & \text{Receiver's secret } c \arrow[u] \arrow[d] \\
\text{Sender's public key } g^{b} \arrow[r] & \text{Secret } g^{bc}
\end{tikzcd}
$$

Can find 300-digit prime q
such that $\ell = 2q + 1$ is prime.
Take g = image of 4 in $(\mathbf{Z}/\ell)^*$.

Or find 50-digit prime q,
300-digit prime $\ell \equiv 1 \pmod{q}$.
Take g of order q in $(\mathbf{Z}/\ell)^*$.

Or find 150-digit prime q
such that $\ell = 2q - 1$ is prime.
Take g of order q in $(\mathbf{F}_{\ell^2})^*$.

Or find 50-digit primes q, ℓ
and point g of order q
on an elliptic curve over $\mathbf{Z}/\ell$.

Public-key signatures

$$\begin{tikzcd}
 & \text{Message } m \arrow[d] \\
\text{Secret } b \arrow[r] \arrow[d] & \begin{array}{c}\text{Signed}\\ \text{message}\\ m, s\end{array} \arrow[d] \\
\begin{array}{c}\text{Public}\\ \text{key } n\end{array} \arrow[r] & \text{Verification}
\end{tikzcd}$$

ElGamal signatures

Public functions H, I.

Public g of prime order q.

Public key $n = g^b$.

(r, u) is a signature of m

if $r = g^{H(m)u} n^{I(r)u}$, $0 < u < q$.

Signer chooses $r = g^e$

for uniform random e.

Modify signatures to save space:

(t, u) is a signature of m
if $t = I(g^{H(m)u} n^{tu})$, $0 < u < q$.

Two elements of $\mathbf{Z}/q$
instead of one element
and one power of g.

(Schnorr, Kravitz)

I said Krovetz when I gave this talk. My apologies to Krovetz and Kravitz. My only excuse is that I was preparing three talks in one frantic week.

Rabin-Williams signatures

Secret 150-digit primes p, q
with $p \bmod 8 = 3$, $q \bmod 8 = 7$.

Public key $n = pq$.
(r, f, s) is a signature of m
if n divides $s^2 - fH(r, m)$
and $f \in \{-2, -1, 1, 2\}$.

Signer chooses r randomly.

Modify signatures to save time:

(r, h, f, s, t) is a signature of m
if $f \in \{-2, -1, 1, 2\}$,
s, t not too large,
$h = H(r, m)$, and $s^2 = fh + tn$.

Verifier computes $s^2 - fh - tn$
modulo a secret 40-digit prime.

Assume 40-digit r.

If forger has *generic* attack
with forgery chance $\geq 10^{-10}$
using 10^{10} valid signatures
and 10^{10} calls to H
then forger can factor n
at about the same speed
with chance $\geq 10^{-11}$.