NSS Cryptanalysis II

The Return of The Keys

Michael Szydlo
RSA Laboratories
Joint work with
Jakob Jonsson(RSA)
Jacques Stern (ENS)
Craig Gentry(DoCoMo)

RSA LABORATORIES

NSS Scheme (HPS 2000)

- Ring: $R = Z_q[x]/(x^N - 1)$
  - (Use N=251, q=128).
  - |f|=140, |g|=80, |m|=64.
- **Study Scheme in EUROCRYPT 2001.**
- Private f, g. Public: $h = f^{-1}g$
- For message m, choose masks: $w_1 + 3w_2$
- Sign with: $s = f(m + w_1 + 3w_2), t = hs$
- Verify: s-m and t-m’ small (mod 3).

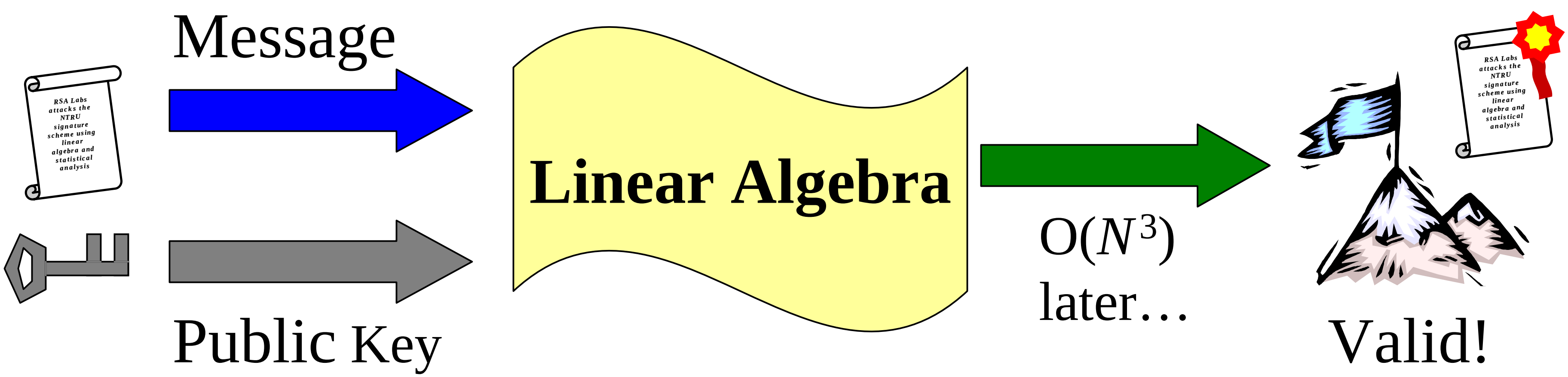
RSA LABORATORIES

Efficient Forgery for *m*

- Fix ~$N/2$ coefficients s_k and ~$N/2$ coefficients t_r so that

$$\begin{cases} s_k \bmod 3 = m_k \\ t_r \bmod 3 = m'_r \end{cases}$$

- Solve the N x N matrix equation $t = hs \bmod q$.
- s-m and t-m' mod 3 = 0 often ⇒ **Valid Sign!**



Transcript Exposes Keys

- Look at the distribution of s_k
- To get info about f_{k-i}
- By Affecting Term $m_i + w_i$ How? Set: $m_i = 1$
- Recall the convolution formula:

$$s_k = (m_i + w_i) f_{k-i} + (m_{i+1} + w_{i+1}) f_{k-i-1} + \ldots$$

- **Unique m+w Distrib.**
- **Multiplied by** f_{k-i} **!**

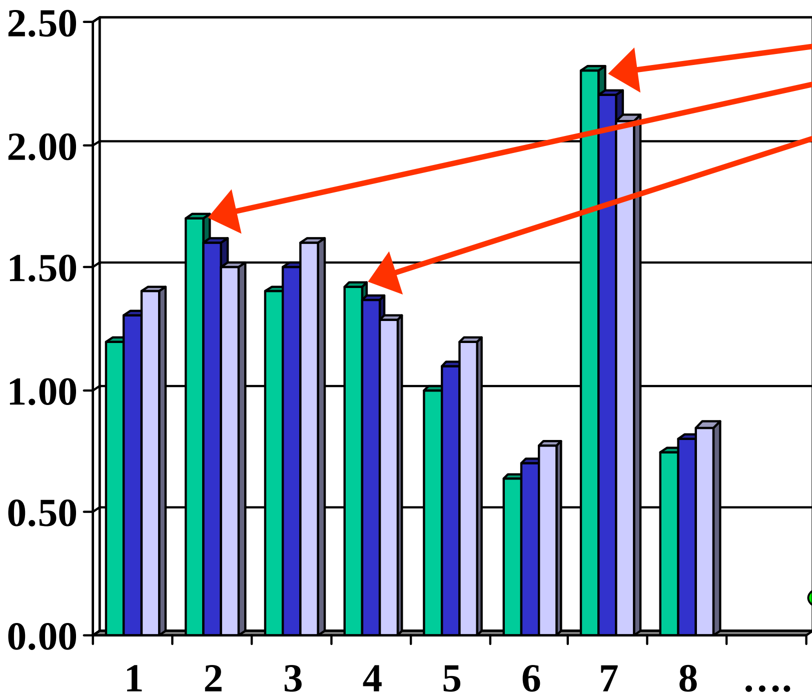
Measure **s** given **m** *reveals* **f**.

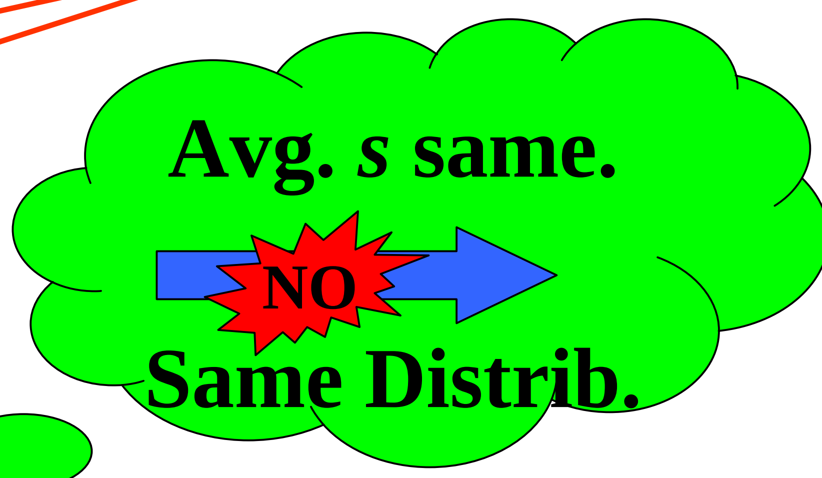
RSA LABORATORIES

Comparing Distributions

- Pre-computed S Frequency Distribution, for f=-3,0,3.
  (Not to scale)
- Which does our sample distribution resemble?

A high *s* freq (2,4,7) in our sample suggests *f* = -3.

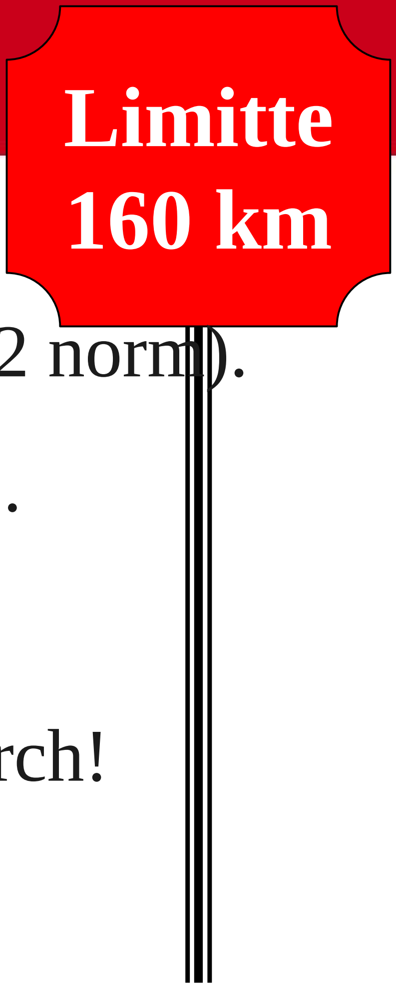




(Without Fix#1

~200 signs give key)

Convergence Rates



- Compare sample to 3 background (e.g. L2 norm).
- For a key bit, use all 32 s coefs with m=1.
- 100,000 Signatures to recover key.
- Number of mistakes in [1-4]. Direct Search!
- Conjecture: 50,000 with Hybrid Attack.
  - **Same Technique for g.**
  - **Take The Confident Half Indices, g=fh.**

RSA LABORATORIES

'Fast Keys' Used in Practice.

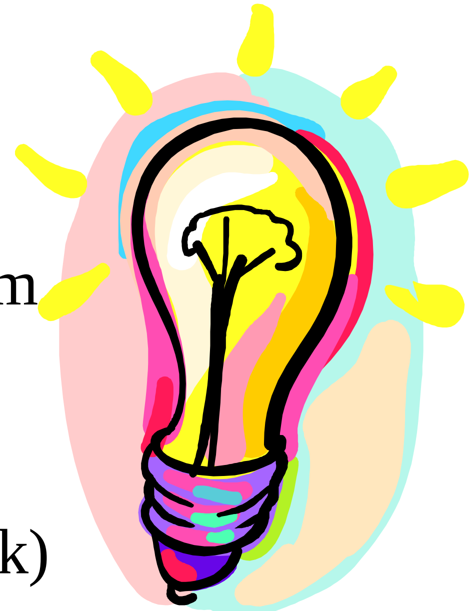
$$f = f_1 f_2, g = g_1 g_2.$$

- Product of Very Small Polynomials (8-14 1's)
- Some 6 and –6 Coefficients in Appear in f & g.
- Convergence Faster!
- **Need Only 30,000 Signatures.**
- **Conjecture:** Maybe 20,000 with f,g hybrid!

RSA LABORATORIES

The State of NSS

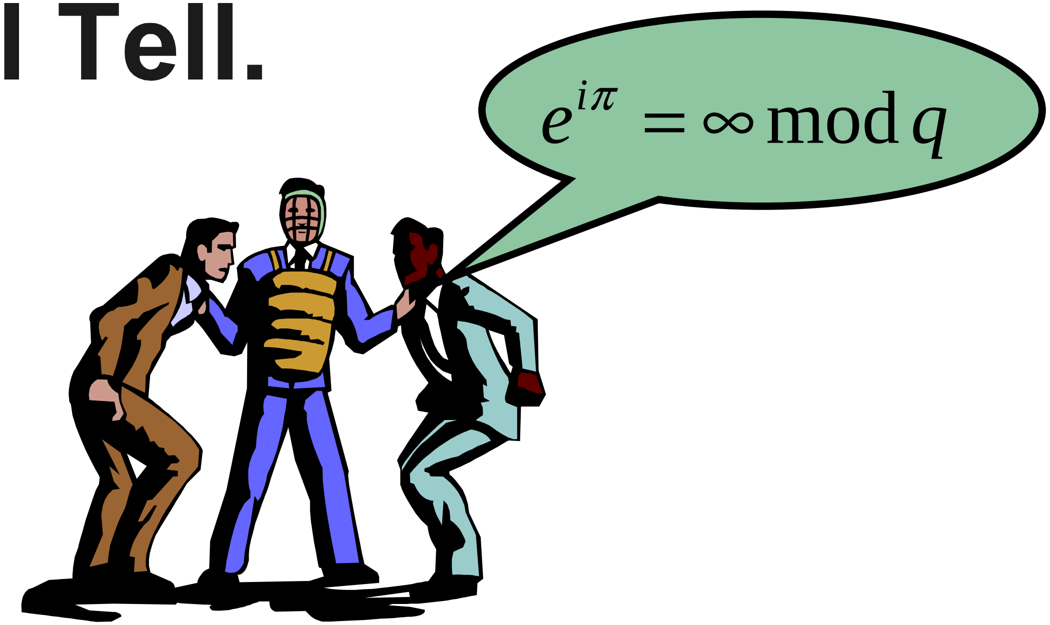
- **NSS00** Published + prelim. Standard Is Broken
  - Forging Easy &Private Key Pops Out.
  - Fundamental Problem:
  - NSS *Related to*, not <u>Based on</u>, Lattice Problem



- *New Version:* **'NSS3',** May 9, 2001
  - New Private Key u. (Thwart Transcript Attack)
  - Different Sign Proc: Uses u^-1 mod 3,s=f(new mes)
  - New Verify Procedure: (|43(s-m)|,|43(t-m)| must be small)
  - Thwarts fast Matrix Attack. **(NSS# is open Research)**

Do More Research

- **Are New Statistical/Forgery Attempts Possible?**
- **Time will Tell.**



New Scheme Summary

- New Secret small key: u. f=u+pf1,g=u+pf2.
- As before w1 and w2 are small masking polys.
- Let v= u^-1 mod 3, so uv=1+3d, for a small d.
- Sign m, define w_0=v(m+w1).
- Let s=f(w0+pw2) mod q, t=hs mod q.
- Verify: Check 43(s-m), 43 (t-m) have small norm.
  - Some secondary checks on mod 3 distribution

RSA LABORATORIES

New Statistical Attacks

- We are given many S=F(w0+pw2) mod q,   t=hs
- S-m=(u+pf1)(v(m+w1)+pw2)-m
- =uvm-m+uvw1+upw2+pf1vm+pf1vw1+p^2f1w2 (q)
- 43(s-m)=43(uv-1)m+43w1+dw1+f1v(m+w1) +w2(u+pf1)
- =(d+f1v)(m+w1)+43w1+w2(u+pf1) = useful+random
- Notice Distrib of 43(s-m) heavily depends on f (when m=1)
- Get d+f1v! Quickly (500 sigs?) Gives=>Fv /Similar get Gv
- Same Idea in previous scheme might crack faster??(5,000 sigs)
- What to do with Fv and Gv?

RSA LABORATORIES

Using the Extracted Info

- Potential Lattice Attack: <u>Dim N</u> lattice.
- Lattice :A(f v)=B(gv) for all polys A,B (No wraps!).
- Has short Vector (g,f). So Try LLL variant.
- Is N=251 to big?: Open Question for this Special Lattice.
- Direct Forgery for m, given extracted vf.
  - Try s=fv(m+w1)+43w1+3fv x^a, for some w1 & a in Z.
  - Set t=hs. (we try to replace the 3fw2 term by fvx^a).
  - We Likely pass the main norm & Deviation Tests. (Other tests?).

Disclaimer: ALL of the Above Attacks

On May 8 NSS are Preliminary.

RSA LABORATORIES