

“The End of RSA”



**“The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.”
This is in accordance with DoDI 5230.29, January 8, 2009.**

Approved for Public Release, Distribution Unlimited

The RSA algorithm

- At the core of many widely deployed cryptographic protocols
 - Browser CA PKI is the most prominent use, but not likely the most important
- Recent studies have uncovered severe vulnerabilities in deployed systems using RSA
- **Is RSA likely to fail catastrophically?**
 - What if some country breaks RSA in the future?
 - What if some country already has?

ISAT workshop

- Menlo Park, January 7-8, 2013
- Attendees: mathematicians, cryptographers, real-world implementers, systems analysts
 - Dan Boneh, Martin Hellman, Pete Kind, Butler Lampson, Andrew Odlyzko, Peter Weinberger, ...
- Topics:
 1. What is the state of RSA cryptanalysis?
 2. What systems rely on RSA?
 3. When RSA fails, how will we know that it has failed?
 4. How can we remediate the failure of RSA-based systems?
 5. Assuming that RSA has not yet failed, what should we do now to prepare?

Heninger-Lange-Bernstein Keynote



- With the number field sieve (and optimizations), nation-state resources suffice for factoring a 1024-bit number
 - With COTS GPUs, a 2^{26} watt computer could perform 2^{84} flops in a year, enough to factor one 1024-bit number.
- Further minor improvements to NFS are plausible — especially to linear algebra
- Biggest short-term problems are trust management, key generation and supporting infrastructure (e.g., padding, protocols).
- Quantum computer is biggest identified threat, but not in next five years

Breaking RSA as deployed \neq factoring

- Breaking RSA isn't the same as factoring:
- Breaking PKCS#1 v1.5 isn't the same as breaking RSA
- Finding implementation flaws isn't the same as breaking PKCS#1 v1.5
 - Heninger: no one on the OpenSSL team understands the crypto code they maintain and ship
- CAs and other trusted parties do not always have good opsec

Martin Hellman keynote



- What is the risk of RSA failing? If it hasn't happened yet, how do we estimate the risk?
- We have seen required key sizes doubled circa 1970 (CF), 1980 (LS/QS), and 1990 (NFS); but algorithmic progress has stalled since.
- Modeling these advances as a Poisson process: a 78% chance of at least 1 more advance in the next 20 years.



- Conclusion: “We should not be surprised at another major advance, comparable to the NFS. Such an advance might effectively break RSA as now implemented. Prudence dictates that we have mechanisms *in place* to mitigate such a disaster.”

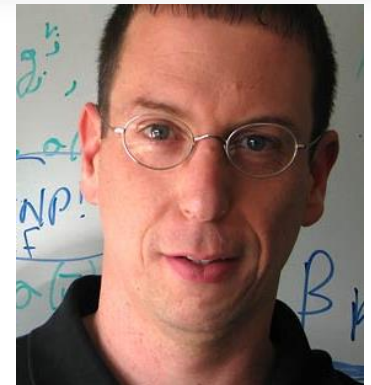
A cryptanalytic breakthrough?

- January 2013: ISAT end-of-RSA workshop
- February 2013, a new discrete log algorithm:

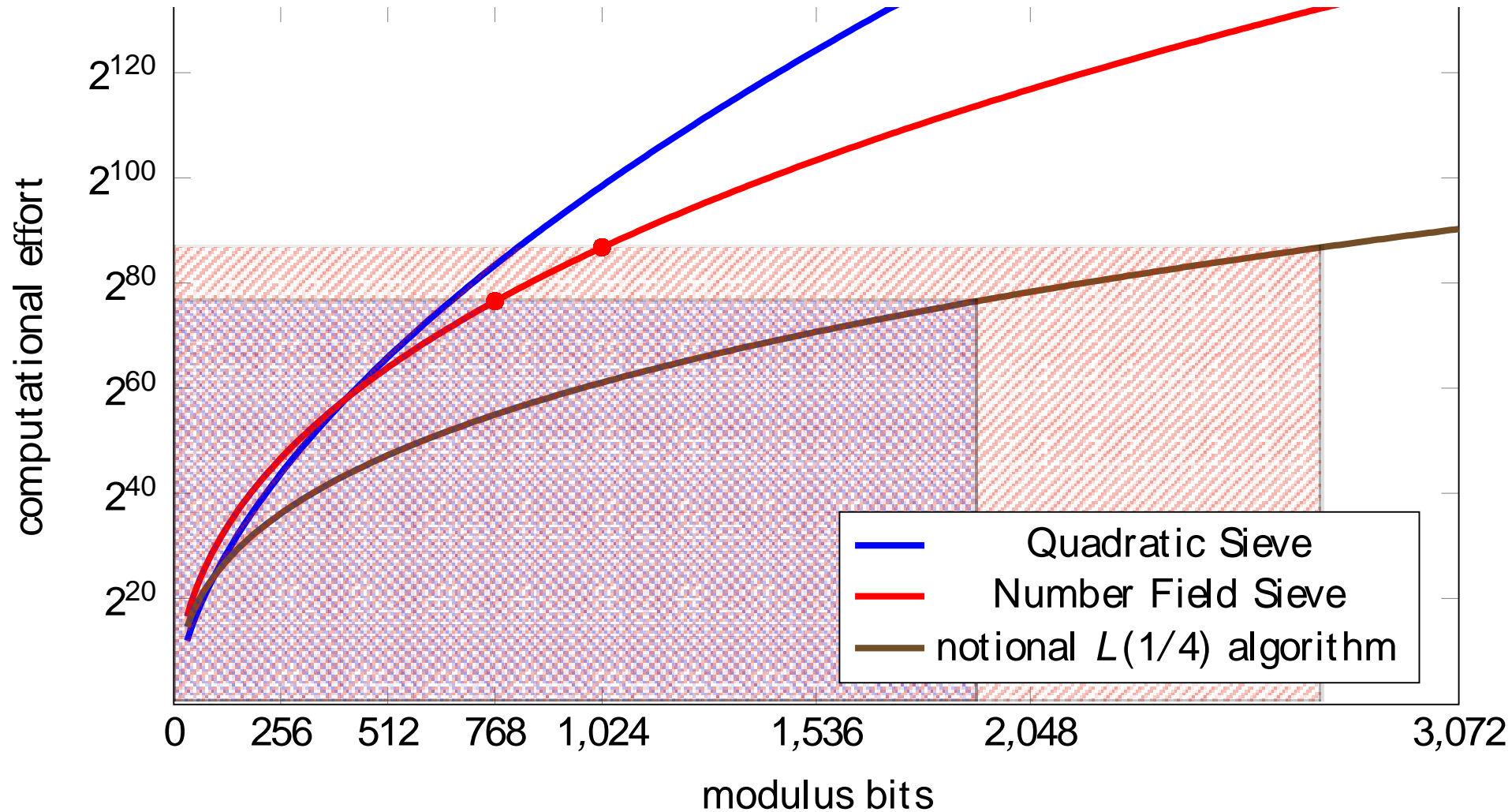
**A new index calculus algorithm
with complexity $L(1/4 + o(1))$ in very small
characteristic
(Draft)**

ePrint 2013/095

- Dan Boneh, March 2013: *“Why does every improvement in attacks on discrete log always lead to similar improvements in attacks on factoring?”*



A world with an $L(1/4)$ factoring algorithm



An RSA break is likely to be used

- Cryptanalytic advantage is a wasting asset
- Tactical benefit of use may be overestimated
- Use is likely to be targeted and specific
 - Likely plausibly deniable (cf. WW2 “spotter planes”)





- Prof. Fingar, Stanford: “In the case of RSA, this leads me to judge: a) that if people could break it, they would assume that others could/already had, and that the defective system would be fixed or replaced as soon as possible; and b) that they should exploit the transitory advantage as soon as possible.”

RSA As a Systems Problem

- Potential impact
- What will survive?
- Emergency response plan
- Preparing and raising awareness

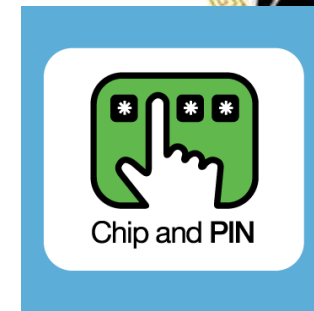
These Will Fail

Probably not the first target

- SSL in Web browsers 
- BIOS and boot keys, authentication of microcode patches  **Be afraid, be very afraid**
- “Invisible” code in SCADA, embedded devices
- Weapons systems?
- The really important uses of RSA are authentication and integrity, not confidentiality

These Will Not ... or will they?

- Kerberos
- Chip-and-PIN architectures
 - Banking networks
- Hash-based OTP systems
 - SecurID
- Most mobile and wireless protocols
 - GSM
- Proprietary gaming protocols
 - Xbox, Playstation, Windows Media Player



GSM



Dealing With Full-System Failures

- *“Engineering failures are tragic, like watching a bridge fall, but we have to worry about all bridges falling at the same time”*
 - Tom Berson
- We do not have full-system risk analysis for RSA-dependent systems



Emergency Response

- Turn off:
 - Code update, TLS, SSH, Tor, hardware crypto, SCADA and industrial networks ...
- Turn on:
 - Ephemeral keys
 - ECC
 - Interactive authentication protocols

**But what if we turn them on
and nothing happens?**

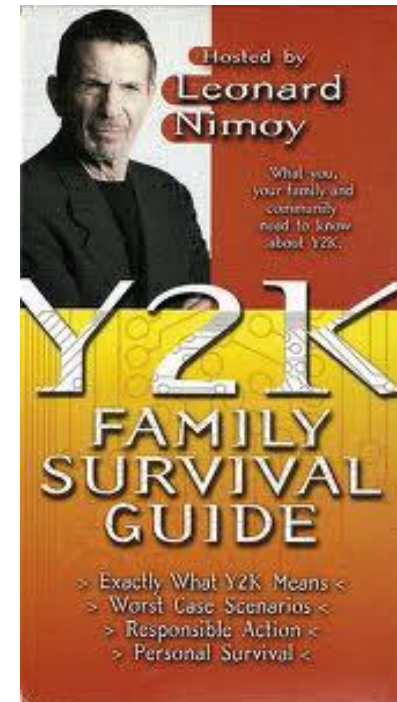


Advice to DoD

- Raising awareness
- Dependency analysis as a discipline
- Designing and testing for crypto agility
- “Belt-and-suspenders” systems

Raising Awareness

- Remember Y2K?
- “A Day Without RSA”
- Grand challenges
 - Factoring
 - Reacting to disaster scenarios



Dependency Analysis

- Do we have an inventory of systems that depend on RSA?
- ... systems that **implicitly** depend on RSA?
- Even simpler: who still uses 1024-bit keys?
- Do we have a **methodology that could help us answer these questions?**
 - Program analysis? Dynamic testing? Fuzzing?
 - This calls for research!

Crypto Agility

- How will existing systems handle ...
 - ... longer keys?
 - ... different crypto suites?
 - ... bad pseudorandom numbers?
- How do we build systems that ...
 - Support rapid key rollover
 - Are “plug-and-play” with multiple crypto schemes
 - Are field-updatable - including microcode!
 - Especially embedded systems



“Belt-and-Suspenders” Systems

- Increased integrity of critical functionality
 - Code update, code update, code update ...
- Built-in fallover mechanisms
 - Existing shared secrets
 - Non-RSA networks (what are they?)
- Learn from finance and ecommerce
 - They don’t use RSA to deal with bad endpoints
 - Instead: behavioral analysis, out-of-band and secondary authentication, “undo” for transactions



“If we are having this conversation again in 10 years, we will have failed”