Class 5: Becoming More Paranoid

Schedule

Wednesday, 9 September (now): Checkup 1 revisions (if desired).

Tuesday, September 15 (8:29pm): Problem Set 1 due.

Wednesday, September 23: Check 2 (was originally scheduled for Monday, September 21)

Readings for next week (should be completed by Monday, September 21 at the latest, but earlier is better):

- Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. The is the original bitcoin paper, which is quite readable and historically interesting.
- *Chapter 6: The Bitcoin Network* and *Chapter 7: The Blockchain* from Andreas Antonopoulos' book.
- *Chapter 2: How Bitcoin Achieves Decentralization* and *Chapter 5: Bitcoin Mining* from Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies*.

Notes

What does it mean for a problem to be *hard*?

If you know an algorithm with running time in $O(2^n)$ for problem P, what do you know about the hardness of problem P?

What are the most common reasons for cryptosystems to fail in practice?

Bitcoin's Curve

Standards for Efficient Cryptography: *SEC 2: Recommended Elliptic Curve Domain Parameters* (Certicom Research, 27 January 2010)

> *Verifiably random parameters offer some additional conservative features. These parameters are chosen from a seed using SHA-1 as specified in ANSI X9.62 [X9.62]. This process ensures that the parameters cannot be predetermined. The parameters are therefore extremely unlikely to be susceptible to future special-purpose attacks, and no trapdoors can have been placed in the parameters during their generation. When elliptic curve domain parameters are chosen verifiably at random, the seed S used to generate the parameters may optionally be stored along with the parameters so that users can verify the parameters were chosen verifiably at random.*

What does it mean for parameters to be "verifiably random"?

Randomness

Kolmogorov Complexity: $K(s)$ = the length of the shortest description of s.

Kolmogorov's Definition of Random: A sequence s is random, if $K(s) = |s| + C$

What is the Kolmogorov Complexity of the string `000100001000001111111100111...`?

What is the Kolmogorov Complexity of the string: '1MRigEo5423vycLnUdSnA4C6Ts691fUiYu 18UikW89q9VgGDftQW3Gmuhe4sQDCFP5kD 19ZQwQmfAsgy47ErehfkW...' ?

Daniel J. Bernstein, Tung Chou, Chitchanok Chuengsatiansup, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, and Christine van Vredendaal. *How to Manipulate Curve Standards: A White Paper for the Black Hat*, 2014.

How likely is it that the parameters for the secp256k1 curve used by bitcoin have a trapdoor?

How should ECC parameters be generated for an important curve in a standard?

Dual-EC PRNG

P and Q are points on the curve, specified by the standard (but not explained how Q is choosen). P is a generator, so there exists some e such that $Q^e = P$.

$s_0 =$ initalize with seed randomness
$s_{i+1} = \varphi(s_i \times P)$

$r_i = \varphi(s_i \times Q)$ $o_i =$ the low-order 16 bits of the x-coordinate of r_i.

Given o_i, how much work is it to find all the possible $r_i = (x, y)$ values?

Given e, what is $\varphi(e \times A)$ where A is a possible r_i value?

Dan Shumow, Niels Ferguson. *On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng*. CRYPTO 2007 Rump Session.

Michael Wertheimer (NSA), *Encryption and the NSA Role in International Standards*, Notices of the American Mathematical Society, February 2015.

Wertheimer's letter is an attempt to respond to *Mathematicians Discuss the Snowden Revelations*.

> *The recent revelations about the NSA's spying programs are both dismaying and encouraging. What is encouraging is that they might lead not just to a reform of the intelligence agencies but also to a more serious look at what the ongoing and inevitable erosion of privacy is doing to our society. What is dismaying is less the intrusive data collection itself and more what it reveals about the decision-making processes inside the government.* (Andrew Odlyzko)