Class 4: Verifiably Random?

Schedule

Project 1 is due **Friday, 30 January** (11:59pm).

Scheduled office hours:
Dave — after class Mondays, Thursdays 4-5pm (both in Rice 507)
Nick — Mondays 5-7pm (in Rice 442), Fridays (noon-2pm in Hackcville, #9 Elliewood Ave)

Signing with Elliptic Curves

Elliptic curve discrete logarithm problem: given points P and Q on an elliptic curve, it is hard to find an integer k such that $Q = kP$.

Parameters: curve, G (a point on curve), (large) n such that $nG = 0$.

Key pair:
Private key: d = pick a random integer in [1, n-1]
Public key: point on the curve, $Q = dG$

Signing:
pick random integer k in [1, n-1]
compute curve point: $(x, y) = kG$
signature = (x mod n, k-1($z + rd$) mod n)

What are the reasons for prefering ECC for signatures in bitcoin over RSA-based signature algorithms?

For an interesting history of improvements in factoring, see Carl Pomerance, *A Tale of Two Sieves*, Notices of the AMS, December 1996:

> *John Pollard in 1988 circulated a letter to several people outlining an idea of his for factoring certain big numbers via algebraic number fields. His original idea was not for any large composite, but for certain "pretty" composites that had the property that they were close to powers and had certain other nice properties as well. He illustrated the idea with a factorization of the number $2^{2^7} + 1$, the seventh Fermat number. I must admit that at first I was not too keen on Pollard's method, since it seemed to be applicable to only a few numbers. . . . But what of general numbers? In the summer of 1989 I was to give a talk at the meeting of the Canadian Number Theory Association in Vancouver. It was to be a survey talk on factoring, and I figured it would be a good idea to mention Pollard's new method. On the plane on the way to the*

> *meeting I did a complexity analysis of the method as to how it would work for general numbers, assuming myriad technical difficulties did not exist and that it was possible to run it for general numbers. I was astounded. The complexity for this algorithm-that-did-not-yet exist was of the shape* $\exp(c(\log n)^{1/3} (\log \log n)^{2/3})$.

Erich Wenger and Paul Wolfger, *Solving the Discrete Logarithm of a 113-bit Koblitz Curve with an FPGA Cluster*.

> *It is possible to repeatedly fold a standard letter-sized sheet of paper at the midway point about six to seven times. In 2012, some MIT students were able to fold an 1.2 kilometer long toilet paper 13 times. And every time the paper was folded, the number of layers on top of each other doubled. Therefore, the MIT students ended up with 213 = 8192 layers of paper on top of each other. And poor Eve's job was to manually count all layers one by one. Similar principles apply in cryptography, although bigger numbers are involved. In Elliptic Curve Cryptography (ECC), where* log2 n*-bit private keys are used, Eve does not have to iterate through all possible n keys. Instead, Eve would use the more efficient parallelizable Pollard's rho algorithm that finishes in approximately* sqrt(n) _steps. The omnipresent question is how big n_ *has to be such that even the most powerful adversaries are not able to reconstruct a private key. Especially in embedded, cost-sensitive applications, it is important to use keys that are only as large as necessary.*

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 `0001000010000011111111100111...`?

What is the Kolmogorov Complexity of the string: 1MRigEo5423vycLnUdSnA4C6Ts691fUiYu 18UikW89q9VgGDftQW3Gmuhe4sQDCFP5kD 19ZQwQmfAsgy47ErehfkW3SeSzNGFfH9iN 1AZCH1insc6JrT2Z9SiNvgtTugXg8sF8yd 15qYggRJvmyZfpchxvNqr6h3pNjw6bGBV9 1C943NwPPffUFY7VDzi3kt7KikXwc2vdkN 1JBhLLCgNYhR8f6AZcRS3mjfEAmMzPvwyf 1JvDrBSYm6o4ZTQUhwUE4FhPFxd2wuXWUR 1KcBM1RNhcp1oENycoD4AezA5Se4SrsZnA 16JZWC433XRxjWwR7X65uxRVFdLTmoPr4t 149LB8VYaT1BdMLyQUL92Kj6KrJfNwcp64 16zDGuzbwkHjW8dNYMw9stDjRbTzVSLZU1 1HfMaZn53ZDWKgmhWxk1UPZMjQ6QmpW6m...?

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?

Root Zone DNSSEC KSK Ceremonies Guide. If you have a few hours to spare, you can watch a key signing for the DNSSEC (Domain Name System): DNSSEC KSK Ceremony 20

Dual-EC PRNG

NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators

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)

How satisfying is the NSA's response? Are you more dismayed or encouraged?