Elliptical Curve Cryto

(now with moar lolz)

Phillip Marcus Wilt

March 12, 2014

Why are we listening to this?

Cryptography has become an essential part of everyday life. It encompasses a large range of fields

- Online Banking
- Secure Communication
- Bitcoin
- Digital Rights Management
- Secure Internet Browsing

Dudes named Diffie-Hellman

Whitfield Diffie and Martin Hellman proposed a symmetric key exchange in 1976.

Mathematical solution to the problem of secure communication over public channels.

Two parties exchange keys and share a secret that allowed them to encrypt and decrypt message to one another (probably about l33t warez).

RSA

Good approach to crypto!

Solves the problems:

- Secure Two Way Communication
- Signing Documents Digitally

Problems:

- Requires Big Big Numbers to be secure
- More Bandwidth, Moar Powah!

Solution!

Elliptic Curves!

Smaller Numbers but still computationally complex to break!

Elliptic Curves

$$y^2 = x^3 + ax + b \tag{1}$$

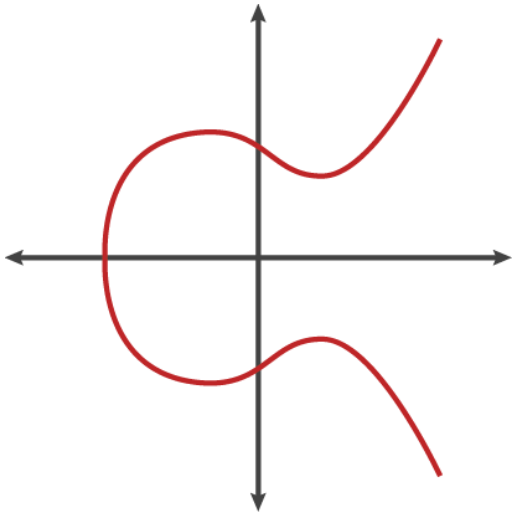

Figure: lululemon logo errr.. Generic Elliptic Curve

Call of Duty: Group Ops

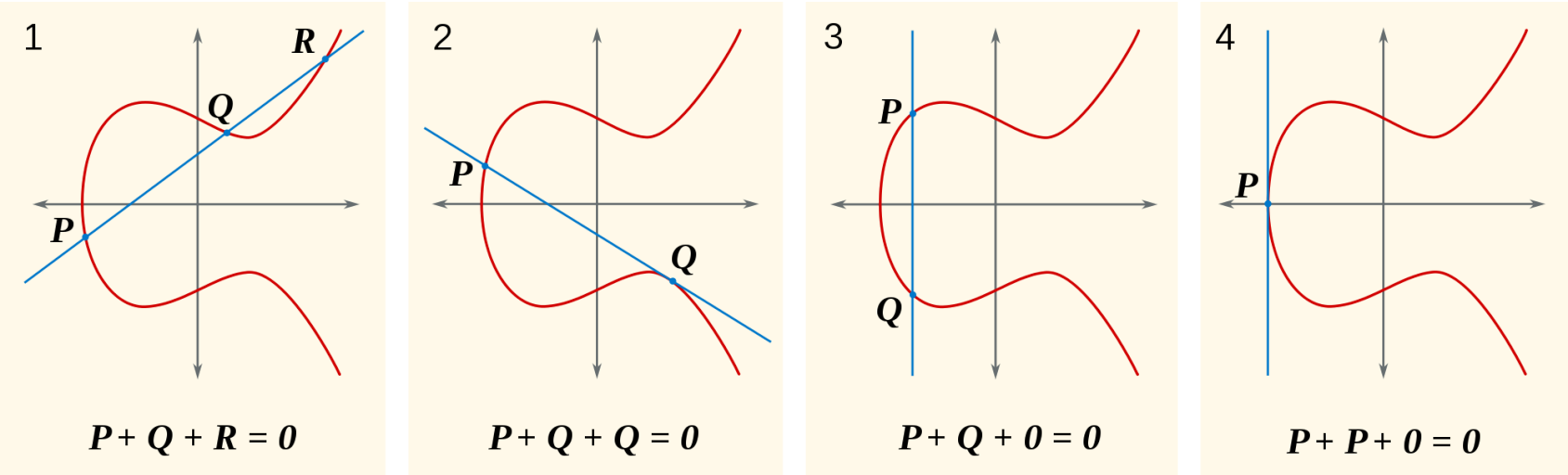

Figure: Operations on Elliptic Curves

Pseudorandom Number Generators

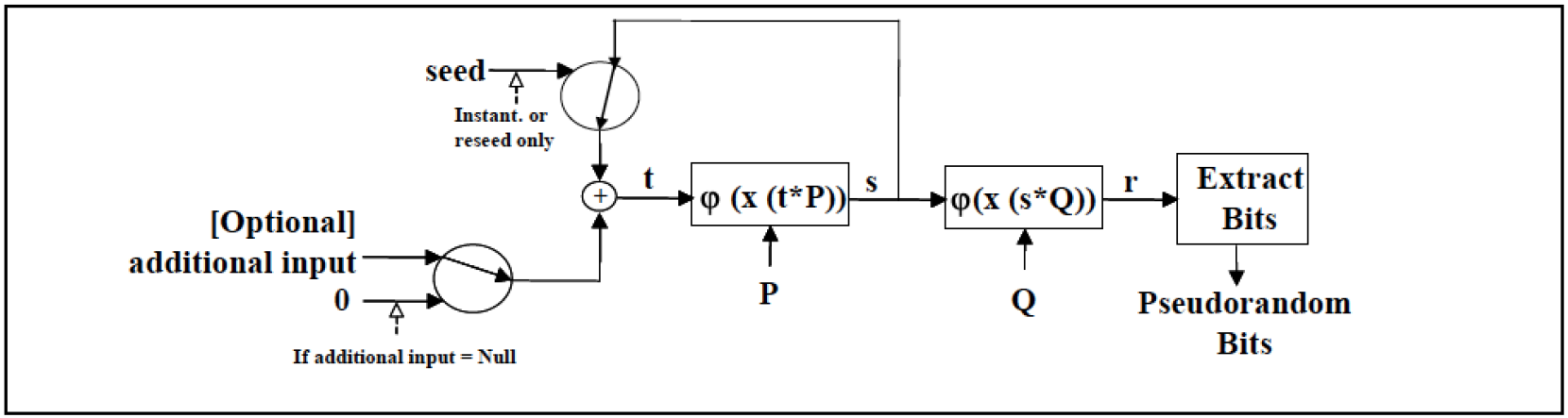

Figure: NIST 800-90A Flowchart

Hey kid, wanna do some math?

1. First we need elliptic curve functions, which are specified in NIST-800-90A (P-256 in proof of concept).
2. Pick points P and Q different and seemingly random on the curve.
3. Add P to itself t times, where $t \in \mathbb{Z}$ and produce a new point with x-coordinate s.
4. Multiply s with Q to output a random x-coordinate r
5. Extract 30-bytes (Least Significant) of r to output a random number.
6. Update next random seed with $t = s$.

If P and Q have no relation then this produces correct random numbers. However, if they have a relation a backdoor exists. Now suppose they have the relation given in Equation 2.

Ghost in the Machine

But what if these points are related...

$$Q = d * P \tag{2}$$

If d is known then let a be the additive order of point P. Then it is easy to compute

$$e = d^{-1} \pmod{a}, e * d = 1 \pmod{a} \tag{3}$$

This will give the relation in equation 4, which will allow predicition of the state of the Dual_EC_DRBG.

Now we can recover our last random multiplier.

$$e * Q = P \tag{4}$$

Given a 30-byte block of output A, it is easy to brute force guess candidates for the missing 2-bytes. Iterating over these candidates and checking

$$e * A = e * (s * Q) = s * (e * Q) = s * (P) = t * P \tag{5}$$

This is the next state in the generator!

Snowden? Pass the shovel.

What we know from the Post-Snowden era:

- RSA was paid $10M by NSA
- The NSA's Bullrun program was designed to exploit technology like this
- A Canadian firm (Certicom) filed a patent for a scheme that had a backdoor for govt agencies
- People like a good story

What we don't know...

Is the government an all-knowing-all-seeing superpower?

Or was it Kyle!?