CS 359C – Classics of Cryptography April 26, 2017

Lecture 4: Elliptic Curve Cryptography

Instructor: Henry Corrigan-Gibbs, David Wu *Scribe: Will Kovacs*

1 Big Picture

To understand the relationships between primitives, we used the following analogy. For constructing cryptographic methods:

- Nail = symmetric key crypto
- Hammer = public key crypto (RSA, DDH)
- Pantheon = zero knowledge
- Skyscraper = MPC/OT
- Rocketship = lattice based crypto

For breaking crypto:

- Wrecking ball = classical cryptanalysis
- Laser = quantum cryptanalysis

2 Review from last time

We reviewed the following concepts from last lecture:

- Factoring: Given N = pq, produce (p,q)
  RSAe: Given $(N, e, a \xleftarrow{r} Z_N)$, produce $a^{\frac{1}{e}} \text{mod} N$
  Strong RSA: $(N, a \xleftarrow{r} Z_N)$, produce ($a^{\frac{1}{e}} \text{mod} N$, e $\neq \pm 1$)
- Factoring $\geq$ RSAe $\geq$ Strong RSA
- Random self-reduction: If RSAe is hard for any $a \to Z_N$, then it is hard for almost all $a \in Z_N$
- Hash-and-sign sigs: (*Must hash)
  Sign(sk, m) = H(m)^{d}modN
  Verify(vk, m,σ) = (H(m) == σ^emodN)
- Threshold RSA Sign $\to$ split sk into p parts, need all p to sign
- Blind Signatures

3 Elliptic Curves

The reason why we want to use elliptic curves is the modulus size. To achieve 128 bits of security on RSA, we need 3072 bit modulus. This is because there are factoring algorithms that factors n-bit numbers in time $\approx 2^{\tilde{O}(n^{1/3})}$, while forces n to grow λ^3. Meanwhile, for elliptic curves, the best attack is $\approx 2^{\tilde{O}(n^{1/2})}$, so n just has to grow 2λ.

3.1 Groups

Groups are defined with respect to a pair $(G, *)$ where G is a set and $*$ is a binary operation on the elements of the set. An example of a group is $\mathbb{Z}_p^*$ where $G = \{1, ..., p-1\}$ and $*$ is defined as multiplication mod p.
A group must satisfy four properties:

1. Closure
2. Associativity
3. Identity: $g * I = g$ where I is the identity element
4. Inverses $g * h = I$ where I is the identity element

3.2 ECDH

In an elliptic curve group, G is the set of points $(x, y) \in \mathbb{F}_q^2$ that satisfy the relation $y^2 = x^3 + Ax + B$ for some fixed $A, B \in \mathbb{F}_q$ and an additional "point at infinity". We can then define a special group operation on these elements, which makes G a group.

It turns out that these elliptic curve groups are cyclic, meaning that there exists a generator $g \in G$ such that all elements in $h \in G$ can be represented as a power of g ($h = g^x$ for some $x \in \mathbb{Z}_q$). Therefore, to reason about elliptic curve groups, we don't have to think in terms of pairs $(x, y) \in \mathbb{F}_q^2$, we can fix a generator $g \in G$ and just think in terms of cyclic groups.

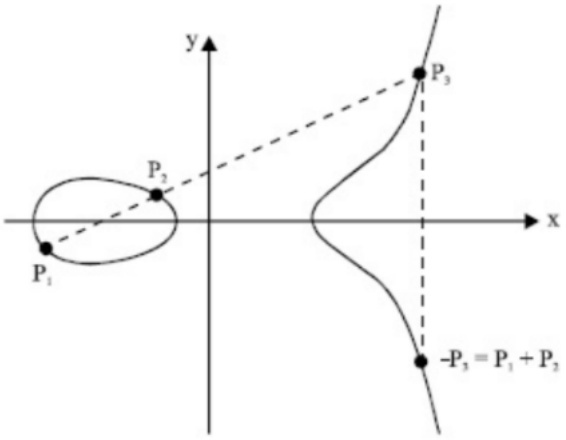

Figure 1: Example of EC from http://scialert.net/fulltext/?doi=jas.2005.604.633

3.3 Computational Problems

We can define the following computational problems on elliptic curves. Fix an elliptic curve group G of order q and a generator g.

- **Discrete Log** (DLog): Let $a \xleftarrow{R} \mathbb{Z}_q$. Then, given (g, g^a, g^b), produce g^{ab}.
- **Computational Diffie-Hellman** (CDH): Let $a, b \xleftarrow{R} \mathbb{Z}_q$. Then, given (g, g^a, g^b), produce g^{ab}.
- **Decisional Diffie-Hellman** (DDH): Let $a, b, c \xleftarrow{R} \mathbb{Z}_q$. Then, given either (g, g^a, g^b, g^{ab}) or (g, g^a, g^b, g^c), decide which one.

A simple reduction shows that DLog $\geq$ CDH $\geq$ DDH.

3.4 PRG from DDH

Recall PRG $f : K \to \{0,1\}^n$(s.t. $n > \log|K|$)
then $\{k \xleftarrow{R} K : f(k)\} \overset{c}{\approx} \{Z \leftarrow \{0,1\}^n\}$

A simple PRG then can be constructed as follows:
Fix (g, g^a), where $a \xleftarrow{R} \mathbb{Z}_q$
$f : \mathbb{Z}_q \to G^2$
$f_{g,g^a}(k) = \langle g^k, g^{ak} \rangle$
$\{(g^k, g^{ak})\} \approx \{(g^k, g^r)\}$ by DDH, where $r \xleftarrow{R} \mathbb{Z}_q$

3.5 PRF From DDH (Naor, Reingold)

Recall PRF $f : K \times X \to Y$
$\{k \xleftarrow{R} K : f(k, \cdot)\} \overset{c}{\approx} \{f \xleftarrow{R} funs[X, Y] : F(\cdot)\}$
$K = \mathbb{Z}_q^{n+1} \leftarrow$ (n+1) EC points
$X = \{0,1\}^n$
$Y = G$
$\vec{k} = (k_0, k_1, ..., k_n) \in \mathbb{Z}_q^{n+1}$
$\vec{x} = x_1, x_2, ..., x_n \in \{0,1\}^n$
$f_{\vec{k}}(\vec{x}) = g^{k \cdot \prod_{i=1}^n k_i^{x_i}} \in G$

Example: $f(110110....) = g^{k_0 k_1 \_ k_3 k_4 \_} \in G$
By DDH, f is a secure PRF