Curvas Elípticas e Discrete Lattice Cryptography

Teórica #10s de Criptografia Aplicada

O que são Curvas Elípticas?

Curvas elípticas são um conjunto de soluções à equação:

```
Y^2 = X^3 + A*X + B
```

Estas equações são identificadas como equações **Weierstrass**.

As curvas elípticas são aplicadas na criptografia através de campos finitos (Finite Fields).

O problema ECDLP

O problema DLP diz que é difícil encontrar um número *y*, dada uma base *g*, onde `x = g^y (mod(p))` para um número primo grande *p*.

O problema ECDLP é similar ao DLP, no sentido em que este diz que é difícil encontrar um valor *k*, dado um ponto base *P*, onde o ponto `Q = k*P`.

Um diferença importante a notar entre o ECDLP e o DLP, é que o ECDLP permite trabalhar com números baixos e manter o mesmo nível de segurança.

Como resolver o problema ECDLP?

Ao encontrar a colisão entre dois outputs (`c1*P + d1*Q = c2*P + d2*q`), é possível determinar que `Q = k*P`, para um valor *k* desconhecido e *c1*, *d1*, *c2* e *d2* valores conhecidos que permitem encontrar *k*, produzindo o mesmo output.

Assinaturas com Curvas Elípticas

Algoritmo standard para assinar com ECC é o **ECDSA** (Eliptic Curve Digital Signature Algorithm), que substituiu assinaturas RSA e assinaturas clássicas DSA, em diversas aplicações. É o algoritmo de assinaturas usado em Bitcoin e também em algumas implementações TLS e SSH.

O algoritmo decorre da seguinte maneira:

1. Assinar mensagem com uma função criptográfica tal como *SHA-256* ou *BLAKE2*, que resulta no valor *h*, interpretado entre 0 e n-1;
2. Usar um valor aleatório *k*, entre 1 e n-1;
3. Calcular o ponto `k*G`, de coordenadas (x,y);
4. Calcular `r = x (mod (n))` e calcular `s = (h + rd)/k (mod(n)), sendo a assinatura dado pelos valores (r, s)`.