EC El Gamal Digital Signature

A signature is appended to a document.

Properties: ① Signing (Alice) w/ public/private key pair — Input: Document m

Output: Signed document, ie. pair (m, sig)

(sig depends on m, public/private key pair)

② Verifying (Bob) — Input: Alice's public key, Signed message

Output: YES/VALID or NO/INVALID.

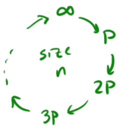
③ Key Properties: It hard to produce pairs (m, sig) that validate YES without access to Alice's private key.

"forging"

E.C. Digital Signature

Setup: $E/\mathbb{F}_p$, $P \in E(\mathbb{F}_p)$

p prime, $n = \text{order}(P)$



Message: $0 < m < n$.

Alice: Private Key: $0 < a < n$.

Public Key: $A = aP$

Signing: Choose secret $0 < k < n$, $\gcd(k,n) = 1$.
(Alice)

$R = kP$

$s = k^{-1}(m - ax) \pmod{n}$

where $x = x(R)$
(x-coord)

Signed Message: $(m, \underbrace{R, s}_{\text{sig}})$

Verification: $V_1 = xA + sR$
(Bob)

$V_2 = mP$

If $V_1 = V_2$: VALID

If $V_1 \neq V_2$: INVALID

Correctness:

$$
\begin{aligned}
V_1 &= xA + sR \\
&= xaP + skP \\
&= (xa + sk)P \\
&= (xa + m - ax)P \\
&= mP \\
&= V_2
\end{aligned}
$$

Security:

1. If you can do $\overset{EC}{DLP}$ then get a, sign anything. ✓
2. Don't re-use k (Exercise).
3. Can you alter m and alter sig (R, s) to remain valid? $V_1 = V_2$

Keep R, change s:

$$xA + sR = mP$$

$$sR = mP - xA \leftarrow \text{public}$$

keep; changed known; public; from R ✓

ECDLP problem.

Choose R, s together?

?? seems hard ??

Keep s, change R:

$$sR = (mP - xA)$$

depen R ✓

even worse, similar

Formal Security

$n = \text{order}(P) = \text{size of task}$

A = adversary

m = message

Can:

- has Alice's public key
- ask for Alice's signature on any document besides m.
- compute polynomial time algorithm.

"success" means: can output (m, sig) that verifies as VALID with non-negligible probability

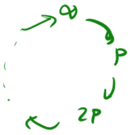
negligible:

$$\left(\text{prob}(\text{success}) < \frac{1}{\text{poly}(\log n)} \right)$$

Discrete Logarithm Problem on Elliptic Curves

Given P, $Q = aP \in E(\mathbb{F}_p)$, find a.

Note: a lives modulo $\underbrace{\text{order}(P)}_{\text{size of the problem}}$.



Attacks:

Birthday/Collision	✓		expon.
Baby-Step-Giant-Step	✓		expon.
Index Calculus	✗	(no analog)	sub-exp.

Because of ↑, this is <u>stronger</u> than DLP mod p or in $\mathbb{F}_{p^n}$.

$\Longrightarrow$ in practice, smaller keys.

Isogeny-Based Cryptography

elliptic curves

What is an isogeny? A map $\varphi : E_1 \longrightarrow E_2$ given by rational functions such that $\varphi(P+Q) = \varphi(P) + \varphi(Q)$

(looks like polynomial numerator/denominator)

(implies $\varphi(\infty) = \infty$)

"homomorphism of groups"

Example. $E_1 : y^2 = x^3 + 1 \mod 11$

$\downarrow \varphi$

$E_2 : y^2 = x^3 + 6 \mod 11$

$(x, y) \in E_1$

$\downarrow$

$\left(\dfrac{x^3+4}{x^2}, \dfrac{x^3 y + 3y}{x^3} \right) \in E_2$

Eg. $(0,1) \longmapsto \left(\frac{4}{0}, \frac{3}{0} \right) = \infty \in E_2$

$(1,1) \longmapsto \left(\frac{5}{1}, \frac{4}{1} \right) = (5,4) \in E_2$

on E_1

kernel $= \{ P \in E_1 : \varphi(P) = \infty \}$

The degree of an isogeny is the # of pts in the kernel

For this ex, $\{\infty, (0,1), (0,10)\} \Rightarrow \deg(\varphi) = 3.$ "3-isogeny"

$$\to 1 \to g \to g^2 \to g^3 \to$$

$$\to \infty \to P \to 2P \to 3P \to$$

$$E_0 \xrightarrow{\varphi} E_1 \xrightarrow{\varphi'} E_2 \to \cdots$$