CS641

Modern Cryptology

Lecture 16

Properties of Physical Signature

- A physical signature has two key properties:
  1. Forgery is difficult, and
  2. Correctness can be verified by anyone with training.
- Can the same be replicated in digital domain?
- Leads to the notion of digital signatures.

Digital Signatures

- Given a digital document m, Anubha can append string s to m such that:
  - Replacement of m by a different document or signing m with Anubha's signature is hard for anyone except Anubha.
  - Braj, or anyone else, can verify that s is "signature" of Anubha associated with m.
- Public-key encryption algorithms can often be adopted for this.

Digital Signature via RSA

- Anubha announces her public key (e, n) and she has corresponding private key d.
- Assume that document m can be viewed as a number $< n$.
- Signing: Anubha computes $s = m^d \pmod{n}$.
- Verification: Given (m, s), Braj checks if $s = m^e \pmod{n}$.
- Hardness of forgery follows from properties of RSA encryption.

Digital Signature via ECC

- Anubha announces her public key (C, p, P, eP, t) and she has $t - e$ as private key.
  - g is an element of order t in the group and t is a prime number.
- Assume that document m is a number with $1 < m < t$.
- Signing:
  - Anubha picks a random r, $1 < r < t$, and computes $rP = (a, b)$.
  - She computes $s = r^{-1}(m + ae) \pmod{t}$.
  - Signature of document m is the pair (a, s).
- Verification:
  - Given document m and signature (a, s), Braj first computes $s' = s^{-1} \pmod{t}$.
  - Then he computes point $s'mP + s'a(eP) = (a', b')$.
  - He accepts the signature if $a = a'$.

Digital Signature via ECC

- Correctness:

$$(a', b') = s'mP + s'a(eP) = s'(m + ae)P = rP = (a, b).$$

Digital Signature via ECC: Security

- Changing m while keeping signature (a, s) same is not possible:
  - Fixing a fixes r.
  - Therefore, if m changes, so does s.
- Creating signature (a, s) of document m appears as hard as computing private key e:
  - Signature (a, s) of document m satisfies the equation

$$m = rs - ae \pmod{t},$$

    where $rP = (a, b)$.
  - If Ela can compute r and s satisfying above, then she can compute $e = (rs - m)/a \pmod{t}$.
  - It is not clear how can Ela compute a and s without knowing r.

Digital Signature via ECC: Security

- It is essential that for every signature, a random r is chosen.
- If same r is used for signing documents m and m' resulting in signatures (a, s) and (a, s') respectively, then:

$$\begin{aligned} m &= rs - ae \pmod{t} \\ m' &= rs' - ae \pmod{t} \end{aligned}$$

- Therefore,

$$ms' - m's = ae(s - s') \pmod{t},$$

giving

$$e = \frac{ms' - m's}{a(s - s')} \pmod{t}.$$

Digital Signature Post Quantum Computers

- Previous signatures schemes become insecure in the presence of quantum computers.
- The NIST contest has shortlisted three candidates for digital signatures, two of which are based on integer lattices.