Efficient Signcryption Schemes on Elliptic Curves

Yuliang Zheng, Monash University, Australia
Hideki Imai, University of Tokyo, Japan

http://www.pscit.monash.edu.au/~yuliang/
Points on an Elliptic Curve

- The points on an EC, together with the point at infinity, form an abelian group under “addition” defined by the “tangent and chord” method.
- The number of points on an elliptic curve $C$ over $GF(p^m)$ is
  \[ \#C = p^m + 1 - t, \quad \text{where} \quad |t| \leq 2\sqrt{p^m} \]
- $t$ is called the trace of the curve

Curves to be Avoided

- super-singular curves whose traces satisfy
  \[ t = \pm \sqrt{i \cdot p^m}, \]
  where $i = 0, 1, 2, 3$ or $4$
  (Menezes, Okamoto & Vanstone, 93)
- curves over $GF(p)$ with trace 1, namely
  \[ \#C = p \]
  (Satoh & Araki, & Smart, 97)
### Signcryption on EC--
**Public & Secret Parameters**

- **Public to all**
  - C: an EC over GF(p^m),
  - q: a large prime
  - G: a point on C with order q
  - hash, KH, (E,D)

- **Alice’s keys**
  - v_a: secret key
  - P_a: public key
  - (note: P_a = v_a G)

- **Bob’s keys**
  - v_b: secret key
  - P_b: public key
  - (note: P_b = v_b G)

### Signcryption on EC-- 1st example

- **Signcrypt by Alice**
  - k = hash(v P_b)
    - where \( v \in \{1, \ldots, q - 1\} \)
  - k \( \rightarrow \) k_1, k_2
  - r = KH_{k_2}(m)
  - s = \frac{v}{r + v_a} \mod q
  - c = E_{k_1}(m)
  - **output** (c, r, s)

- **Unsigncrypt by Bob**
  - u = s v_b \mod q
  - k = hash(u P_a + ur G)
  - k \( \rightarrow \) k_1, k_2
  - m = D_{k_1}(c)
  - **output**
    - \( m \) if \( r = KH_{k_2}(m) \)
    - "invalid" if \( r \neq KH_{k_2}(m) \)
Signcryption on EC—2nd example

- **Signcrypt by Alice**
  - $k = \text{hash}(v P_b)$
  - *where* $v \in \mathbb{F}_q \{1, \ldots, q-1\}$
  - $k \leftarrow k_1, k_2$
  - $r = KH_{k_2}(m)$
  - $s = \frac{v}{1 + v a r} \mod q$
  - $c = E_{k_1}(m)$
  - output $(c, r, s)$

- **Unsigncrypt by Bob**
  - $u = s v_b \mod q$
  - $k = \text{hash}(u G + u r P_a)$
  - $k \leftarrow k_1, k_2$
  - $m = D_{k_1}(c)$
  - output
    - $m$ if $r = KH_{k_2}(m)$
    - "invalid" if $r \neq KH_{k_2}(m)$

EC Signcryption v.s. EC Signature-then-Encryption

- **Reduction in comp. cost**
  \[
  \frac{5.17 - 2.17}{5.17} = 58\%
  \]

- **Reduction in comm. overhead**
  \[
  \frac{|\text{hash}(\cdot)| + 2|q| - (|KH(\cdot) + |q|)}{|\text{hash}(\cdot)| + 2|q|} = \frac{|q|}{\frac{1}{2}|q| + 2|q|} = 40\%
  \]