Pairings in protocols

2nd meeting of ECLIPSES

V. Vitse

Université Versailles Saint-Quentin - Laboratoire PRiSM

March 25, 2010

General settings

Parameters

- κ security level
- r prime number, q a prime power
- E elliptic curve defined over $\mathbf{F}_q$ s.t. $r | \#E(\mathbf{F}_q)$
- k embedding degree (smallest integer s.t. $r | q^k - 1$)
- $G_1 = E(\mathbf{F}_q)[r]$, $G_3 = \mu_r(\mathbf{F}^*_{q^k})$
- $\rho = \log q / \log r$

pairing = bilinear and non degenerate map

$$E(\mathbf{F}_q)[r] \times E(\mathbf{F}_{q^k})[r] \to \mu_r(\mathbf{F}^*_{q^k})$$

In practice, replace $E(\mathbf{F}_{q^k})[r]$ by a cyclic subgroup G_2

General settings

Needs in cryptography

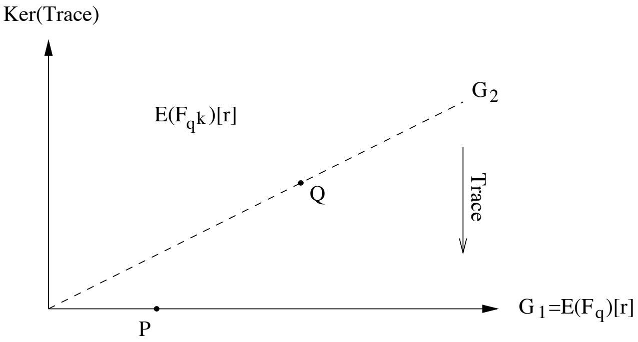
1. DLP hard in $G_1 \rightsquigarrow r > 2^{2\kappa}$
2. DLP hard in $G_3 \rightsquigarrow$ lower bounds on q^k
3. boundwidth and efficiency

κ	$\lvert r \rvert_2$	$\lvert q^k \rvert_2$	k $(\rho \simeq 1)$	k $(\rho \simeq 2)$
80	160	960 – 1280	6 – 8	3 – 4
112	224	2200 – 3600	10 – 16	5 – 8
128	256	3000 – 5000	12 – 20	6 – 10
192	384	8000 – 10000	20 – 26	10 – 13
256	512	140000 – 18000	28 – 36	14 – 18

Choice of G_2

1. $G_2 = G_1$: degeneracy except for modified pairings on supersingular curves
   - advantage: oracle DDH on G_1 ($e(aP, bP) = e(P, cP)$)
     $\rightsquigarrow$ useful in IBE scheme security proof
   - drawbacks: $k \leq 6 \rightsquigarrow$ no short representation of elements on G_1

2. $G_2 \neq G_1$



Choice of $G_2 \neq G_1$

Trace map: $E(\mathbf{F}_{q^k})[r] \to E(\mathbf{F}_q)[r]$

1. $G_2 = \ker Tr_{\mathbf{F}_{q^k}/\mathbf{F}_q}$
   - can hash onto G_2
   - k even $\rightsquigarrow$ point compression by a factor 2: $G_2 \simeq \tilde{E}(\mathbf{F}_{q^{k/2}})[r]$
   - drawbacks: no known computable isomorphism from G_2 to G_1
     $\rightsquigarrow$ stronger security assumptions needed to compensate

2. $G_2 = \langle Q \rangle \neq \ker Tr_{\mathbf{F}_{q^k}/\mathbf{F}_q}$
   - advantage: trace map gives an isomorphism $G_2 \to G_1$
   - drawbacks: cannot hash onto G_2 and no point compression

Construction of pairing-friendly curves

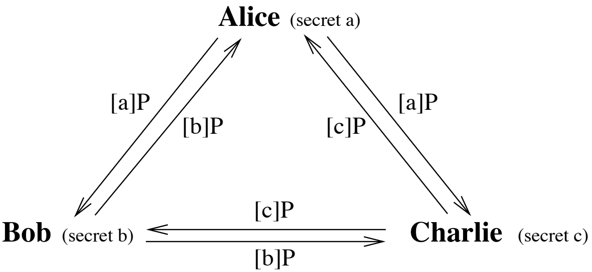
1. supersingular case: well classified, but $k = 4$ resp. $k = 6$ only available in char 2 resp. 3 (index calculus methods more efficient in those cases)

2. ordinary curves: several families currently available, all relying on the complex multiplication method
   - construction requires floating point arithmetic (or table look-up)
   - curves defined over prime fields

Key distribution scheme

Tripartite Diffie-Hellman in one round (Joux)

$P \in E(\mathbf{F}_q)[r]$ and $G_1 = \langle P \rangle$



- $K = e([b]P, [c]P)^a = e([a]P, [c]P)^b = e([a]P, [b]P)^c = e(P, P)^{abc}$
- also in the asymmetric case, but twice more broadcasts needed

Identity based encryption

Basic scheme of Boneh-Franklin

- `setup`
  - Public parameters: $\langle G_1, G_2, G_3, e, P, P_{pub} = [s]P, H_1, H_2 \rangle$
    $G_1, G_2 = \langle P \rangle, G_3$ cyclic of prime order r
    $e : G_1 \times G_2 \to G_3$
    $H_1 : \{0;1\}^* \to G_1$ and $H_2 : G_3 \to \{0;1\}^n$ ($n =$block size)
  - Master Key: $s \in \mathbf{Z}_r^*$

- `encrypt` : to send the message M to Id
  - compute $Q_{Id} = H_1(Id) \in G_1$ and choose $t \in_R \mathbf{Z}_r^*$
  - send

$$C = \langle C_1, C_2 \rangle = \langle [t]P, M \oplus H_2(e(Q_{Id}, P_{pub})^t) \rangle$$

- `extract` : compute $S_{Id} = [s]Q_{Id} \in G_1$

- `decrypt` :

$$M' = C_2 \oplus H_2(e(S_{Id}, C_1))$$

Short signature

Boneh-Lynn-Shacham's scheme

- `setup`
  - Public parameters: $\langle G_1, G_2, G_3, e, Q, Q_{pub} = [s]Q, H_1 \rangle$
    $G_1 = \langle P \rangle$, $G_2 = \langle Q \rangle$, G_3 cyclic of prime order r
    $e : G_1 \times G_2 \rightarrow G_3$
    $H_1 : \{0; 1\}^* \rightarrow G_1$
  - Private signature key: $s \in \mathbf{Z}_r^*$

- `sign` : to sign the message M, compute $S = [s]H_1(M) \in G_1$

- `verify` : check that

$$e(S, Q) = e(H_1(M), Q_{pub})$$

Security consideration

- secret values appear as multiplier of points in G_1 and G_2 and as exponent over G_3

- pairing arguments are public values, except in the IBE scheme

Pairings in protocols

2nd meeting of ECLIPSES

V. Vitse

Université Versailles Saint-Quentin - Laboratoire PRiSM

March 25, 2010