Pairings I

Impact on security

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

Pairings

Let $(G_1, +), (G_2, +)$ and $(G_T, \cdot)$ be groups of prime order ℓ and let $e : G_1 \times G_2 \to G_T$ be a map satisfying

$$e(P+Q, R') = e(P, R')e(Q, R'), \quad e(P, R'+S') = e(P, R')e(P, S')$$

and that e is non-degenerate in the first argument,
i.e., $e(P, R') = 1$ for all $R' \in G_2$, implies P is the identity in G_1.

Such an e is called a bilinear map or pairing.

Pairings

Let $(G_1,+),(G_2,+)$ and $(G_T,\cdot)$ be groups of prime order ℓ and let $e: G_1 \times G_2 \to G_T$ be a map satisfying

$$e(P+Q,R') = e(P,R')e(Q,R'), \quad e(P,R'+S') = e(P,R')e(P,S')$$

and that e is non-degenerate in the first argument, i.e., $e(P,R') = 1$ for all $R' \in G_2$, implies P is the identity in G_1.

Such an e is called a bilinear map or pairing.

Weil and Tate pairing have $G_1 \subseteq E(\mathbf{F}_p)$ and map to $\mathbf{F}^*_{p^k}$.
More precisely, $G_T \subset \mathbf{F}_{p^k}$, with order ℓ.

By Legendre, ℓ must divide $p^k - 1 = \#\mathbf{F}^*_{p^k}$, for subgroup to exist.
Less obvious: $G_2 \subset E(\mathbf{F}_{p^k})$.

Pairings

Let $(G_1, +), (G_2, +)$ and $(G_T, \cdot)$ be groups of prime order ℓ and let $e : G_1 \times G_2 \to G_T$ be a map satisfying

$$e(P+Q, R') = e(P, R')e(Q, R'), \quad e(P, R'+S') = e(P, R')e(P, S')$$

and that e is non-degenerate in the first argument,
i.e., $e(P, R') = 1$ for all $R' \in G_2$, implies P is the identity in G_1.

Such an e is called a bilinear map or pairing.

Weil and Tate pairing have $G_1 \subseteq E(\mathbf{F}_p)$ and map to $\mathbf{F}^*_{p^k}$.
More precisely, $G_T \subset \mathbf{F}_{p^k}$, with order ℓ.

By Legendre, ℓ must divide $p^k - 1 = \#\mathbf{F}^*_{p^k}$, for subgroup to exist.
Less obvious: $G_2 \subset E(\mathbf{F}_{p^k})$.

The embedding degree k satisfies k is minimal with $\ell \mid (p^k - 1)$.
Cost of pairing computation: polynomial in $\log_2(\ell)$ and $\log_2(p^k)$.

Consequences of pairings – DDHP

Assume that $G_1 = G_2$ and $e(P, P) \neq 1$.

For all triples $(aP, bP, cP) \in \langle P \rangle^3$ can decide whether

$$\log_P(cP) = \log_P(aP) \log_P(bP)$$

Consequences of pairings – DDHP

Assume that $G_1 = G_2$ and $e(P, P) \neq 1$.

For all triples $(aP, bP, cP) \in \langle P \rangle^3$ can decide whether

$$\log_P(cP) = \log_P(aP) \log_P(bP)$$

by comparing $e(aP, bP)$ and $e(P, cP)$.

Consequences of pairings – DDHP

Assume that $G_1 = G_2$ and $e(P, P) \neq 1$.

For all triples $(aP, bP, cP) \in \langle P \rangle^3$ can decide whether

$$\log_P(cP) = \log_P(aP)\log_P(bP)$$

by comparing $e(aP, bP)$ and $e(P, cP)$.

This means that the decisional Diffie-Hellman problem is easy if such a pairing is available.

Consequences of pairings – DDHP

Assume that $G_1 = G_2$ and $e(P, P) \neq 1$.

For all triples $(aP, bP, cP) \in \langle P \rangle^3$ can decide whether

$$\log_P(cP) = \log_P(aP) \log_P(bP)$$

by comparing $e(aP, bP)$ and $e(P, cP)$.

This means that the decisional Diffie-Hellman problem is easy if such a pairing is available.

Only very special pairings have $G_1 = G_2$ and $e(P, P) \neq 1$.

Consequences of pairings – DLP

Even if $G_1 \neq G_2$ one can transfer the DLP in G_1 to a DLP in G_T, if one can find an element $P' \in G_2$ with $P \to e(P, P') \neq 1$.

Consequences of pairings – DLP

Even if $G_1 \neq G_2$ one can transfer the DLP in G_1 to a DLP in G_T, if one can find an element $P' \in G_2$ with $P \to e(P, P') \neq 1$.

DL with base P, target $Q = aP$ in G_1 maps to
DL with base $g = e(P, P')$, target
$h = e(Q, P')$

Consequences of pairings – DLP

Even if $G_1 \neq G_2$ one can transfer the DLP in G_1 to a DLP in G_T, if one can find an element $P' \in G_2$ with $P \to e(P, P') \neq 1$.

DL with base P, target $Q = aP$ in G_1 maps to
DL with base $g = e(P, P')$, target
$h = e(Q, P') = e(aP, P') = (e(P, P'))^a = g^a$.
The DL system G_1 is at most as secure as the system G_T.

Pairings are interesting attack tool if DLP in G_T is easier to solve.
Note $G_T \subset \mathbf{F}_{p^k}^*$ which has index calculus attacks.

Pairings exist for all elliptic curves but typically k is large, making $\mathbf{F}_{p^k}^*$ a worse target.