Pairing-based cryptography I – Pairing basics

Radka Luňáčková

21.11.2015

Outline

1. Motivation
2. Bilinear pairing
3. Application
4. Weil pairing

DLP - definition

Definition (Discrete logarithm problem (DLP), additive notation)

DLP in group $G = \langle P \rangle$ of order n is the problem, given P and Q, of finding the integer $x \in \{0, 1, ..., n-1\}$ such that $Q = xP$.

DLP - example, the easy one

- $\mathbb{Z}_{19} = \langle 3 \rangle = \{0, 1, 2, ..., 18\}$
- Can we find $\log_3 7$?
- Yes, we know that

$$\gcd(3, 19) = 1 = 13 \cdot 3 + 1 \cdot 19$$

and that is why we have

$$7 = 7 \cdot 13 \cdot 3 + 7 \cdot 1 \cdot 19 \bmod 19$$

and we get

$$7 = 15 \cdot 3 \bmod 19.$$

DLP - another examples, the difficult ones

- $\mathbb{Z}_p^*$, where p is prime number
- cyclic subgroups of elliptic curves over finite fields

- We do not know any effective algorithm.
- These cases are interesting for cryptography.

DHP - definition

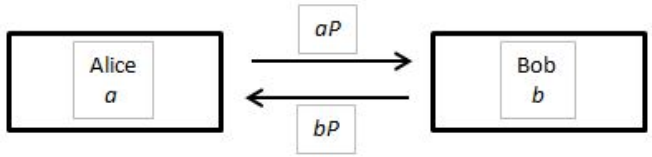
Definition (Diffie-Hellman problem (DHP), additive notation)

DHP in group $G = \langle P \rangle$ of order n is the problem, given P, aP and bP, of finding abP, where $a, b \in \{0, 1, ..., n-1\}$.

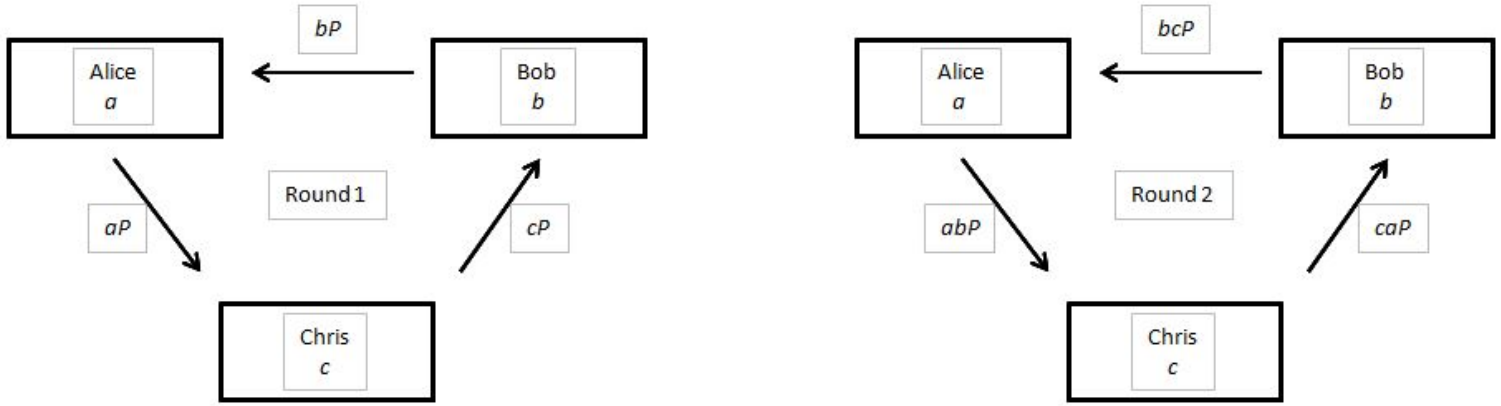
- DHP reduces in polynomial time to the DLP.
- It is generally assumed, for some cases proven, that the DLP reduces in polynomial time to the DHP.

Diffie-Hellman key agreement

- public knowledge: the parameters n and P of group for which the DHP is intractable
- Two-party one-round key agreement protocol: $\mathrm{K} = abP$



- Three-party two-round key agreement protocol: $\mathrm{K} = abcP$



Bilinear pairing - definition

Definition (Bilinear pairing)

Let n be a prime number. Let $G_1 = \langle P \rangle$ be an additively-written group of order n with identity $\mathcal{O}$ and let G_T be a multiplicatively-written group of order n with identity 1. A bilinear pairing on (G_1, G_T) is a mapping $\hat{e} : G_1 \times G_1 \to G_T$ that satisfies the following conditions:

1. bilinearity:
$$\hat{e}(R + S, T) = \hat{e}(R, T)\hat{e}(S, T)$$
$$\hat{e}(R, S + T) = \hat{e}(R, S)\hat{e}(R, T)$$
for all $R, S, T \in G_1$,
2. non-degeneracy: $\hat{e}(P, P) \neq 1$,
3. computability: $\hat{e}$ can be efficiently computed.

Bilinear pairing - properties

For all $S, T \in G_1$ following hold:

1. $\hat{e}(S, \mathcal{O}) = 1$ and $\hat{e}(\mathcal{O}, S) = 1$,
2. $\hat{e}(S, -T) = \hat{e}(-S, T) = \hat{e}(S, T)^{-1}$,
3. $\hat{e}(aS, bT) = \hat{e}(S, T)^{ab}$ for all $a, b \in \mathbb{Z}$,
4. $\hat{e}(S, T) = \hat{e}(T, S)$,
5. If $\hat{e}(S, R) = 1$ for all $R \in G_1$, then $S = \mathcal{O}$.

Bilinear pairing - properties - proofs (1)

For all $S, T \in G_1$ following hold:

1. $\hat{e}(S, \mathcal{O}) = 1$

$$\hat{e}(S, S) = \hat{e}(S, S + \mathcal{O}) = \hat{e}(S, S)\hat{e}(S, \mathcal{O})$$

2. $\hat{e}(S, -T) = \hat{e}(S, T)^{-1}$

$$1 = \hat{e}(S, \mathcal{O}) = \hat{e}(S, T - T) = \hat{e}(S, T)\hat{e}(S, -T)$$

3. $\hat{e}(aS, bT) = \hat{e}(S, T)^{ab}$ for all $a, b \in \mathbb{N}$

$$\hat{e}(aS, bT) = \hat{e}(aS, T + T + ... + T) = \hat{e}(aS, T)^b$$

and also

$$\hat{e}(aS, T)^b = \hat{e}(S + S + ... + S, T)^b = \hat{e}(S, T)^{ab}$$

Bilinear pairing - properties - proofs (2)

For all $S, T \in G_1$ following hold:

1. $\hat{e}(S, T) = \hat{e}(T, S)$

$$\hat{e}(S, T) = \hat{e}(kP, lP) = \hat{e}(P, P)^{kl}$$

and on the other hand

$$\hat{e}(T, S) = \hat{e}(lP, kP) = \hat{e}(P, P)^{kl}$$

2. $\hat{e}(S, R) = 1 \; \forall R \in G_1 \quad \Rightarrow \quad S = \mathcal{O}$

$$1 = \hat{e}(S, S) = \hat{e}(kP, kP) = \hat{e}(P, P)^{2k} \quad \Rightarrow \quad k = 0$$

Bilinear pairing and DLP

DLP in G_1 can be reduced to the DLP in G_T.

Let P and Q be an instance of the DLP in G_1, where $Q = xP$, then we have $g = \hat{e}(P, P)$ and $h = \hat{e}(P, Q) = \hat{e}(P, xP) = \hat{e}(P, P)^x$, elements of G_T.

Now it is clear that $x = \log_P Q = \log_g h$.

BDHP - definition

Definition (Bilinear Diffie-Hellman problem (BDHP))

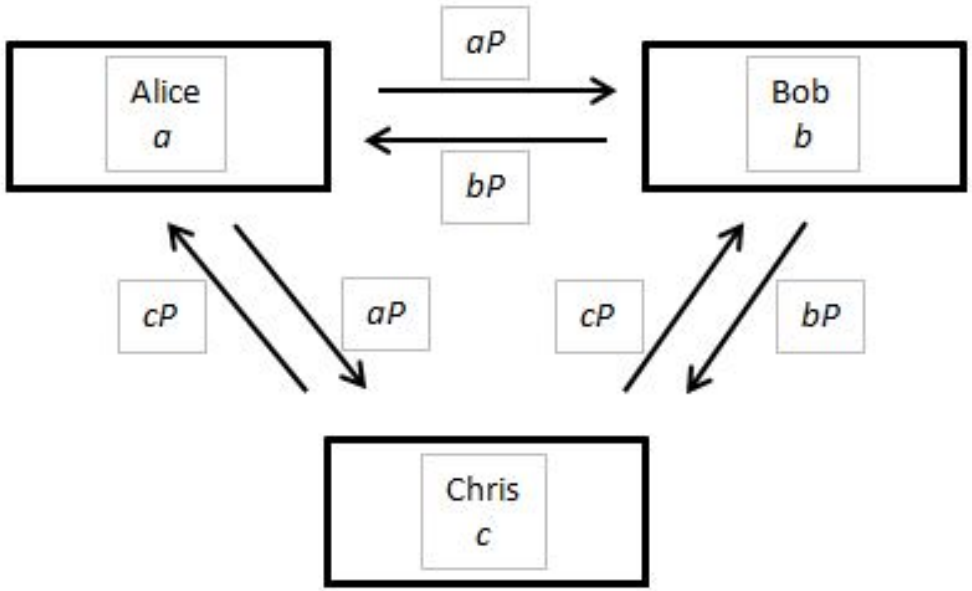
Let $\hat{e}$ be a bilinear pairing on (G_1, G_T). The BDHP is the problem of computing $\hat{e}(P,P)^{abc}$, given P, aP, bP and cP.

- If the DHP in G_1 can be efficiently solved, then one could solve an instance of the BDHP by computing abP and then $\hat{e}(abP, cP) = \hat{e}(P,P)^{abc}$.
- If the DHP in G_T can be efficiently solved, then the BDHP could be solved by computing $g = \hat{e}(P,P), g^{ab} = \hat{e}(aP, bP), g^c = \hat{e}(P, cP)$ and then $g^{abc} = \hat{e}(P,P)^{abc}$.

The BDHP is generally assumed to be just as hard as the DHP in G_1 and G_T.

Three-party one-round key agreement protocol

public knowledge: bilinear pairing $\hat{e}$ on (G_1, G_T) for which the BDHP is intractable



$$K = \hat{e}(P, P)^{abc} = \hat{e}(bP, cP)^{a} = \hat{e}(aP, cP)^{b} = \hat{e}(aP, bP)^{c}$$

Short signatures

- short digital signatures
- RSA schemes (1024-bit modulus) have 1024 bits long signatures
  DSA schemes (1024-bit modulus) have 320 bits long signatures

  Short signatures are 170 bits long with the level of security similar to those above.

BLS short signature scheme

- BLS - Boneh, Lynn and Shacham
- public knowledge:
  bilinear pairing $\hat{e}$ on (G_1, G_T) for which the DHP in G_1 is intractable
  hash function $H : \{0,1\}^* \to G_1 \setminus \{\mathcal{O}\}$
- key generation: Alice's private key is a randomly selected secret integer $a \in \{1, ..., n-1\}$, while her public key is $A = aP$.
- signing: Alice's signature on a message $m \in \{0,1\}^*$ is the element of G_1: $S = aM$, where $M = H(m)$.
- verification: Everyone who has Alice's public key can verify the signature by computing $M = H(m)$ and checking that $\hat{e}(P, S) = \hat{e}(A, M)$.

BLS short signature scheme - how it works (1)

Definition (decisional Diffie-Hellman problem (DDHP))

Let G be a cyclic group, $G = \langle P \rangle$, of order n. The DDHP in G is to decide whether a given quadruple (P, aP, bP, cP) of elements in G is DH-valid, i.e. $cP = abP$.

If G from the definition above is G_1 from bilinear pairing $\hat{e}$ on (G_1, G_T), then DDHP could be efficiently solved by computing

$$\gamma_1 = \hat{e}(P, cP) = \hat{e}(P, P)^c \quad \text{and} \quad \gamma_2 = \hat{e}(aP, bP) = \hat{e}(P, P)^{ab},$$

then

$$cP = abP \Leftrightarrow \gamma_1 = \gamma_2.$$

BLS short signature scheme - how it works (2)

Verification of BLS short signature is actually checking that (P, A, M, S) is DH-valid.

Attacker needs to compute $S = aM$ for given $P, A, M = H(m)$, which is precisely an instance of the DHP in G_1.

Elliptic curve - definition

Definition (Elliptic curve)

Let K be an algebraically closed field and assume that K has characteristic different from 2 and 3. Then we can define elliptic curve E over K by equation

$$y^2 = x^3 + ax + b,$$

where $a, b \in K$ and $4a^3 + 27b^2 \neq 0$. The set of points of E over K is denoted $E(K)$ and defined by

$$E(K) = \left\{(x, y) \in K \times K : y^2 = x^3 + ax + b\right\} \cup \{\mathcal{O}\}.$$

Fact: $E(K)$ forms a group, $(E(K), +, -, \mathcal{O})$.

Divisor - definition

Definition (Divisor)

Let E be an elliptic curve over K. A divisor D is formal sum of points of E:

$$D = \sum_{P \in E(K)} n_P \langle P \rangle,$$

where n_P are integers and $n_P = 0$ except for finitely many $P \in E(K)$.

Note: The angle brackets just indicate that we mean divisor and not the sum of points.

Principal divisor - definition

Note: Let $K(E)$ denote the fraction field of $K[x,y]/f(x,y)$, where $f(x,y) = y^2 - x^3 - ax - b$ and a, b are from the definition of E.

Definition (Principal divisor)

Let E be an elliptic curve over K and $r \in K(E)$. Then we can define divisor of r as

$$div(r) = \sum_{P \in E(K)} m_P \langle P \rangle,$$

where m_P is the multiplicity of P as a root of r. Divisor D is called principal, if there is any $s \in K(E) : D = div(s)$.

Weil pairing - definition

Fact: $D = m\langle P\rangle - m\langle \mathcal{O}\rangle$ is principal divisor. Let f_P denote the element of $K(E) : div(f_P) = D$.

Definition (Weil pairing)

Let E be an elliptic curve over K and let $m > 0$ be an integer prime to characteristic of K. The Weil pairing is a mapping $w : E[m] \times E[m] \to K$ defined by

$$w(P, Q) = (-1)^m \frac{f_P(Q)}{f_Q(P)} \frac{f_Q}{f_P}(\mathcal{O}),$$

where $E[m] = \{P \in E(K) : mP = \mathcal{O}\}$.

Weil pairing - properties

Weil pairing has many properties, following are important for building bilinear pairing.

- bilinearity:

$$w(P+R,Q) = w(P,Q)w(R,Q)$$

$$w(P,Q+R) = w(P,Q)w(P,R)$$

  for all $P, Q, R \in E[m]$,
- non-degeneracy: If $w(P,Q) = 1$ for all $Q \in E[m]$, then $P = \mathcal{O}$.
- computability: Miller's algorithm determines function f_P for given $P \in E(K)$.

Weil pairing - building bilinear pairing - PROBLEM

Let $P \in E(K)$ be point that has order m, m prime and prime to the characteristic of K.
We cloud make bilinear pairing like this:

- $G_1 = \langle P \rangle$
- G_T is the group of m^{th} roots of unity in K
- $\hat{e}(Q, R) = w(Q, R)$ for all $Q, R \in \langle P \rangle$

Note: $\langle P \rangle \subseteq E[m]$ and $Im(w)$ is actually the group of m^{th} roots of unity in K.
However, these is a PROBLEM! $w(P, Q) = 1 \Leftrightarrow P$ and Q are linearly dependent.

Weil pairing - building bilinear pairing - SOLUTION

Bilinear pairing can be define more generally, like a mapping $\hat{e} : G_1 \times G_2 \to G_T$ that satisfies still the same conditions and in addition G_2 is isomorphic to G_1.
There is a way how to find convenient point $Q \in E(K)$ that is linearly independent of P and generates cyclic group of the same order like P.
Then we can use Weil pairing to define bilinear pairing:

- $G_1 = \langle P \rangle$
- $G_2 = \langle Q \rangle$
- G_T is the group of m^{th} roots of unity in K
- $\hat{e}(S, R) = w(S, R)$ for all $S \in \langle P \rangle$ and for all $R \in \langle Q \rangle$

Thank you for your attention.