Definition and properties

Definition. *Bilinear pairing on* $\hat{e} : G_1 \times G_1 \to G_2$ *must be:*

1. *additive*

$$\forall R, S, T \in G_1 : \; \hat{e}(R + S, T) = \hat{e}(R, T) \cdot \hat{e}(S, T)$$
$$\forall R, S, T \in G_1 : \; \hat{e}(R, S + T) = \hat{e}(R, S) \cdot \hat{e}(R, T)$$

2. *non-constant*

$$\forall R \in G_1^* : \; e(R, R) \neq 1$$

3. *efficiently computable.*

Basic properties:

- $\hat{e}(S, 0) = \hat{e}(0, S) = 1$
- $\hat{e}(-S, T) = \hat{e}(S, -T) = \hat{e}(S, T)^{-1}$
- $\forall a, b \in \mathbb{Z} : \; \hat{e}(aS, bT) = \hat{e}(S, T)^{ab}$
- $\hat{e}(S, T) = \hat{e}(aP, bP) = \hat{e}(P, P)^{ab} = \hat{e}(T, S)$
- $\forall T \in G_1 : \; \hat{e}(S, T) = 1 \quad \Rightarrow \quad S = 0$

General form:

$$\hat{e}(S, T) = g^{\log_P S \log_P T}, \qquad g = \hat{e}(P, P)$$

Number of different pairings: $p - 1$

Various reductions

Discrete logarithm formula:

$$a = \log_P S = \log_g \hat{e}(P, S), \qquad g = \hat{e}(P, P)$$

Corollary (MOV-reduction). *Discrete logarithm problem in G_1 is no harder than in G_2.*

Definition. *The Decision Diffie-Hellman problem(DDH) is to distinguish between*

$$\langle P, aP, bP, abP \rangle, \quad \langle P, aP, bP, cP \rangle, \qquad a, b, c \in \mathbb{Z}_n$$

Corollary. *Decision Diffie-Hellman problem is easy in G_1.*

Proposition. *The functions $f_Q : G_1 \to G_2$ defined by $f_Q(R) = \hat{e}(Q, R)$ form a set of all group homomorphisms $\mathrm{Hom}(G_1, G_2)$. And even more if $Q \neq 0$ then f_Q is an isomorphism.*

Corollary. *If there exists $Q \in G_1^*$ such that equation $\hat{e}(Q, X) = h$ can be efficiently solved for arbitrary group element $h \in G_2$ then DDH is also easy in G_2 and discrete logarithm problems in G_1 and G_2 are polynomially equivalent.*

Diffie-Hellman problem

Definition. *The Computational Diffie-Hellman problem is to calculate* abP *if* P, aP *and* bP *are given and* $P \in G$, $a, b \in \mathbb{Z}_n$ *are picked randomly and* n *is the group order.*

Definition 1. *Let* g *be the generator of group* G *and* $p \in \mathbb{P}$ *a divisor of group order. We say that element* $a = g^{y'}$ *represents implicitly element* $y \in \mathbb{Z}_p$ *if* $y' \equiv y \mod p$ *and write* $y \rightsquigarrow a$.

Implicit calculations with $y \rightsquigarrow a$ and $z \rightsquigarrow b$

$$y = z \Leftrightarrow a^{\frac{|G|}{p}} = b^{\frac{|G|}{p}} \qquad y - z \rightsquigarrow a \cdot b^{|G|-1}$$

$$y + z \rightsquigarrow a \cdot b \qquad z \cdot y \rightsquigarrow DH(a, b)$$

Reduction requires:

- an auxiliary group with simple structure
- effective embedding which uses only algebraic operations
- effective extractor

Reduction sketch

The auxiliary group H structure:

- Elements can be represented as m-tuples over $\mathbb{F}_p$.
- Group operation must be carried out at most α operations.

The parametric embedding $\mathcal{E}mb$ must satisfy:

- Calculation $\mathcal{E}mb(x, e)$ involves only algebraic operations.
- Failure can be detected by algebraic operations.
- Expected running time until embedding succeeds is is at most α algebraic operations.
- There exists efficient inverse map $\mathcal{E}xt$.

$$\mathcal{E}xt(\mathcal{E}mb(x, e), e) = x \quad \text{if} \quad \mathcal{E}mb(x, e) \in H$$

- Extraction takes at most α algebraic operations.

The reduction $\delta : (G; +) \to (\mathbb{Z}_p; +)$

1. Calculate implicit representation $\mathcal{E}mb(x, e) = c$.
2. Calculate discrete logarithm of c using only the implicit representation.
3. Calculate explicit representation of c by exponentiation.
4. Calculate $x = \mathcal{E}xt(\mathcal{E}mb(c, e), e)$.

Bilinear Diffie-Hellman Problem

Definition. *Let* $\hat{e} : G_1 \to G_2$ *be a bilinear pairing then Bilinear Diffie-Hellman problem(BDH) is as follows: Given* $\langle P, aP, bP, cP \rangle$ *for some random* $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{Z}_p^*$*, compute* $W = \hat{e}(P, P)^{abc} \in G_2$.

Corollary. *If computational* DH *is easy in* G_1 *or* G_2 *then BDH is also easy.*

BDH gives a rise to several interesting protocols and primitives:

- one round 3-party Diffie-Hellman key agreement
- key escrow protocol for ElGamal encryption scheme
- short signatures
- identity based encryption
- identity based signatures
- various multi-party signing protocols

Standard three-party key agreement

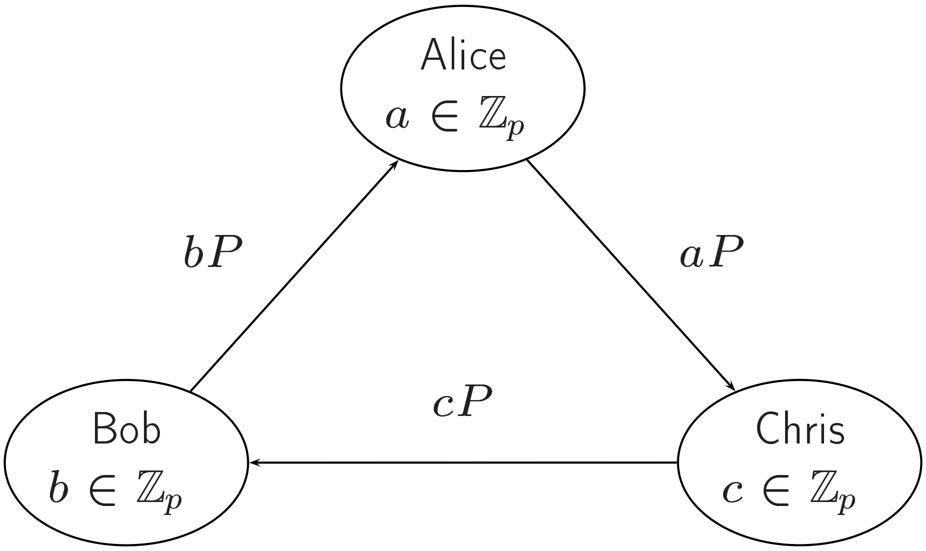

Figure 1: First round of standard 3-party DH

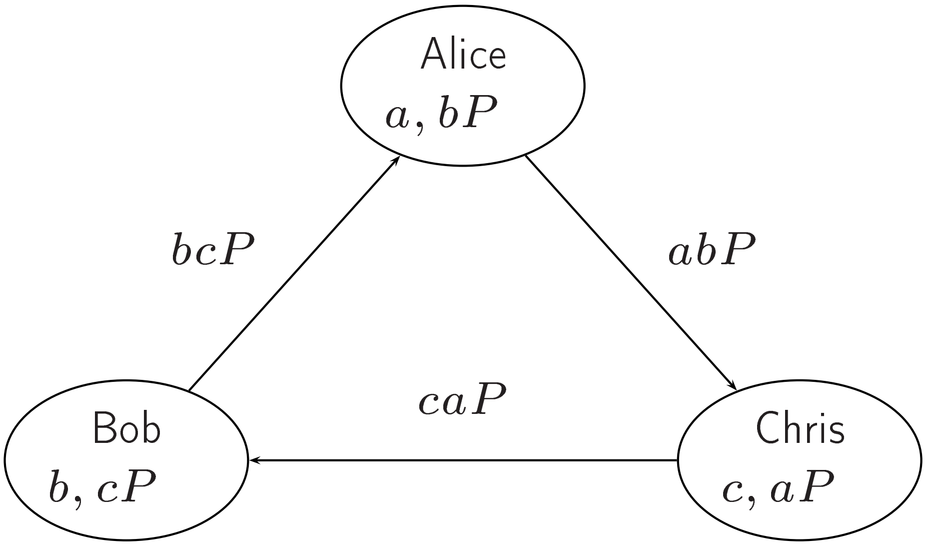

Figure 2: Second round of standard 3-party DH

Three-party one round Diffie-Hellman

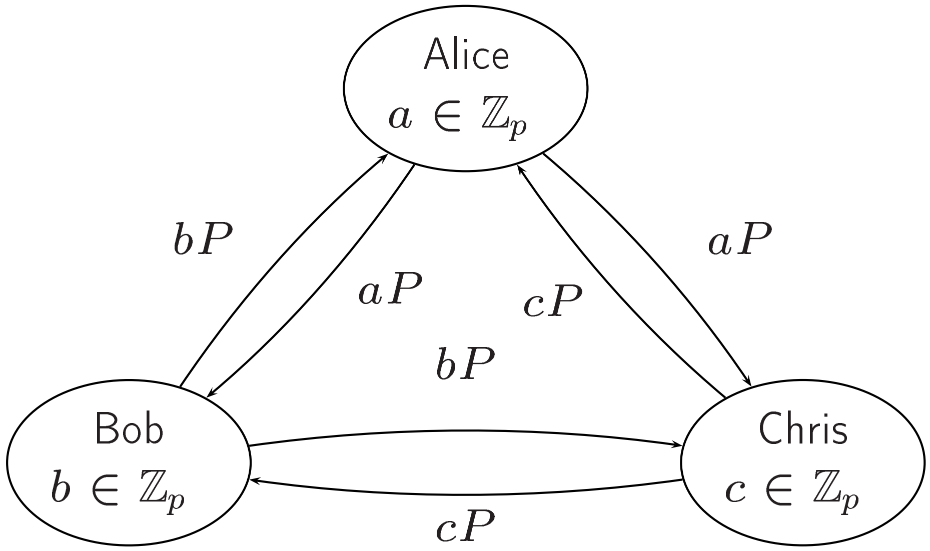

Figure 3: Static 3-party DH

The calculation of the agreed key

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

Corollary. *Three-party Diffie-Hellman key agreement protocol is secure against passive adversary if and only BDH hard in group* G.

Man-in-the-middle attack:

- Dan is impersonating Alice to Bob and Chris;
- Dan is impersonating Chris and Bob to Alice.