Bilinear Pairings

Diego F. Aranha & Ricardo Dahab

Institute of Computing
UNICAMP

Introduction

Pairing-Based Cryptography (PBC):

- Initially destructive
- Allows innovative protocols
- Flexibilizes curve-based cryptography

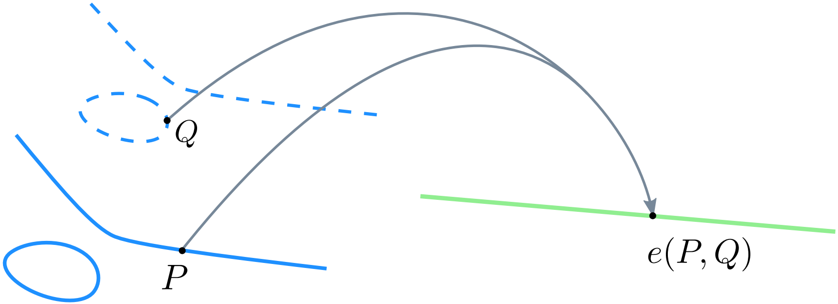
Bilinear pairings

Let $\mathbb{G}_1 = \langle P \rangle$ and $\mathbb{G}_2 = \langle Q \rangle$ be additive groups and $\mathbb{G}_T$ be a multiplicative group such that $|\mathbb{G}_1| = |\mathbb{G}_2| = |\mathbb{G}_T| =$ prime n.

An efficiently-computable map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is an **admissible bilinear map** if the following properties are satisfied:

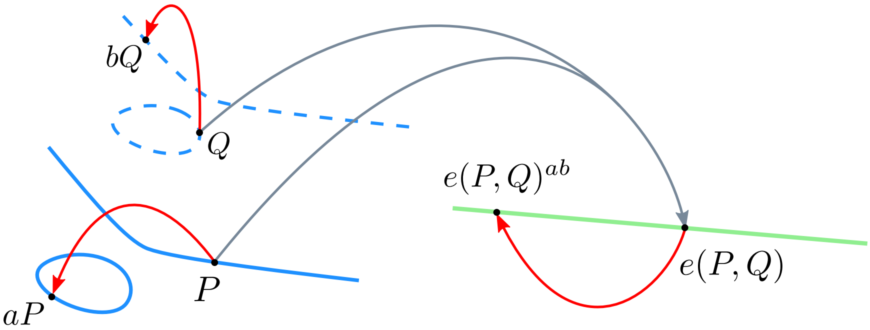
1. *Bilinearity:* given $(V,\ W) \in \mathbb{G}_1 \times \mathbb{G}_2$ and $(a,\ b) \in \mathbb{Z}_q^*$:
   $e(aV, bW) = e(V, W)^{ab} = e(abV, W) = e(V, abW)$.
2. *Non-degeneracy:* $e(P, Q) \neq 1_{\mathbb{G}_T}$, where $1_{\mathbb{G}_T}$ is the identity of the group $\mathbb{G}_T$.

Bilinear pairings



[Picture: Avanzi, Cesena 2009]

Bilinear pairings



If $\mathbb{G}_1 = \mathbb{G}_2$, the pairing is **symmetric**.

Example of protocol

Joux's tripartite Diffie-Hellman:

1. Define an elliptic curve E with generator G and order n
2. Parties A, B, C generate short-lived secrets a, b, c from $\mathbb{Z}_n^*$ respectively
3. Parties A, B, C broadcast aG, bG, cG to the other parties, respectively
4. A computes $K_A = e(bG, cG)^a$
5. B computes $K_B = e(aG, cG)^b$
6. C computes $K_C = e(bG, cG)^c$
7. Shared key is $K = K_A = K_B = K_C = e(G, G)^{abc}$.

Example of protocol

Joux's tripartite Diffie-Hellman:

1. Define an elliptic curve E with generator G and order n
2. Parties A, B, C generate short-lived secrets a, b, c from $\mathbb{Z}_n^*$ respectively
3. Parties A, B, C broadcast aG, bG, cG to the other parties, respectively
4. A computes $K_A = e(bG, cG)^a$
5. B computes $K_B = e(aG, cG)^b$
6. C computes $K_C = e(bG, cG)^c$
7. Shared key is $K = K_A = K_B = K_C = e(G, G)^{abc}$.

Bilinear Diffie Hellman Problem (BDHP)

Compute $e(P, Q)^{abc}$ from $\langle P, aP, bP, cP, Q, aQ, bQ, cQ \rangle$.