# Pairing Based Cryptography

Presentation Project 2

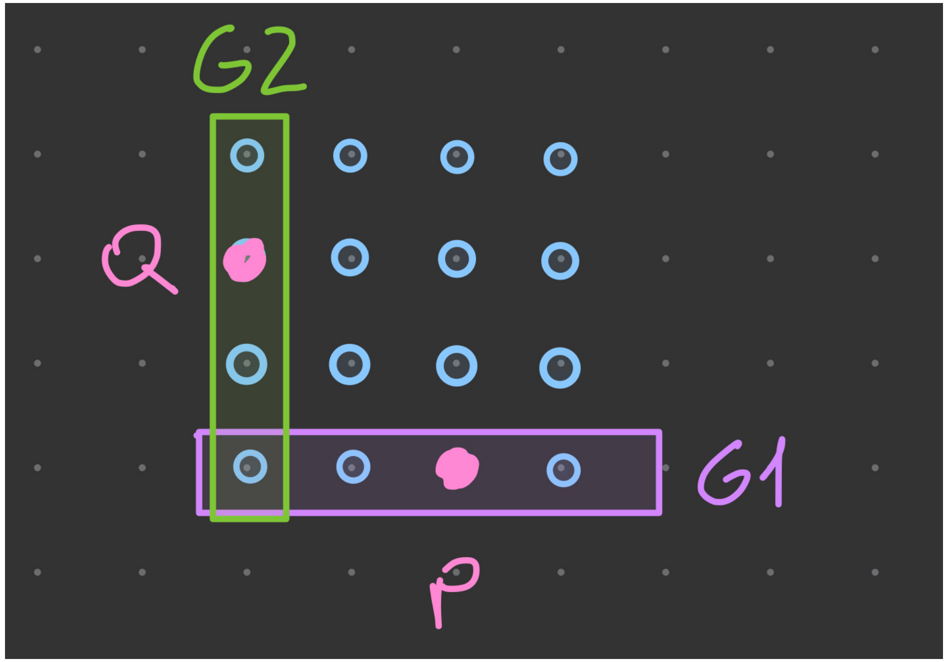
by

Joel Robles

Berner
Fachhochschule

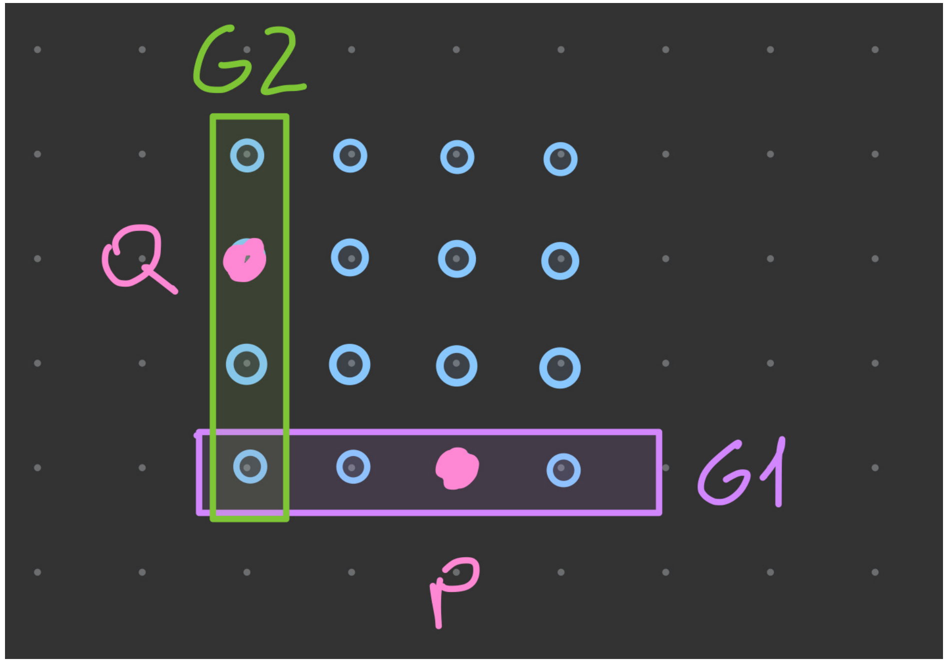
# What is a pairing?

$$G_1 \ x \ G_2 \rightarrow G_T$$



# What is a pairing?

$$G_1 \ x \ G_2 \rightarrow G_T$$
$$e(G_1, G_2)$$



# Characteristics: Bilinearity

$$e(G_1, G_2\ )$$
$$Def:\ (a, b) \rightarrow Scalars\ , (P_x, Q_x) \rightarrow Group\ elements$$

$$1.\, e(P_1 + P_2, Q_1) = e(P_1, Q_1)e(P_2, Q_1)$$
$$2.\, (aP_1, bQ_1) = e(P_1, Q_1)^{ab}$$
$$3.\, e(aP_1, bQ_1) = e(abP_1, Q_1)$$
$$4.\, e(aP_1, bQ_1) = e(bP_1, aQ_1)$$
$$5.\, e(P_1, Q_1)^k \neq 1, k \neq 0$$

Berner
Fachhochschule

# Different Pairings

- Weil Pairing: $e(P,Q) \;\coloneqq\; f_{r,P}(Q)/f_{r,Q}(P)$

- Tate Pairing: $e(P,Q) \;\coloneqq\; f_{r,P}(Q)^{(p^{\alpha}-1)/r}$

- Ate Pairing: $e(Q,P) \;\coloneqq\; f_{T,Q}(P)^{(p^{\alpha}-1)/r}$ where $T = t\; - 1$

$$t\ is\ the\ trace\ of\ Frobenius, size\ of\ a\ Reduced\ curve$$

Berner Fachhochschule

# Applications: BLS Signatures

- **Alice generates:**
- $sk = random\ scalar$
- $G_1 \ \rightarrow Generator\ (Base\ Point)\ on\ E(F_p)$
- $pk = sk * G_1$
- $S = sk * H(msg) \mid H() = \ Hash - to - curve$

Berner
Fachhochschule

# Applications: BLS Signatures (Prove)

- Alice sends $G_1, S, msg$ to Bob
- $e(G_1, S) = e\big(pk, H(msg)\big)$
- $e(G_1, S) = e(G_1, sk * H(msg)) = e(sk * \ G_1, H(msg))$
- $e(sk * \ G_1, H(msg)) = e\big(pk, H(msg)\big) = e\big(pk, H(msg)\big)$

# Applications: Zero-Knowledge-Proof

- Alice wants to prove she knows the answer to $x^2 - x - 42 = 0$
- $e(P_1, Q_1)^k \neq 1, k \neq 0 \; \rightarrow \; e(P_1, Q_1)^k = 1, k = 0$
- $e(P_1, Q_1)^{x^2 - x - 42} = 1$
- $e(P_1, Q_1)^{x^2} e(P_1, Q_1)^{-x} e(P_1, Q_1)^{-42} = 1$
- $e(xP_1, xQ_1) \;\; e(P_1, -xQ_1) \;\; e(P_1, -42Q_1) \quad = 1$

- Alice only needs to prove the knowledge of $xP_1 \; and \; xQ_1$

Berner
Fachhochschule