EXPLORING CRYPTOGRAPHY PROTOCOLS

WITH LIMITED EMPHASIS ON MATHEMATICS ☺

Presented By
@7eRoM

ATTENTION

THESE SLIDES HAVE BEEN CRAFTED USING THE FOUNDATION OF MY MSC COURSE IN CRYPTOGRAPHY PROTOCOLS AT THE UNIVERSITY OF ISFAHAN.

I'VE MADE ADJUSTMENTS TO THE CONTENT TO ALIGN WITH THE SPECIFIC OBJECTIVES OF THIS PRESENTATION.

ALSO, MY INTENTION HAS BEEN TO MINIMIZE THE USE OF MATHEMATICAL CONCEPTS, WHICH MAY RESULT IN SOME CONCEPTS BEING SIMPLIFIED OR LESS PRECISE.

Presented By
@7eRoM

Agenda

1. Identification and Entity Authentications Protocols
2. Zero Knowledge Protocols
3. Key Establishment Protocols
4. Threshold Cryptography and Secret Sharing Protocols
5. Special Purpose Protocols (like simultaneous contract signing, mental poker, fair exchange)
6. Identity Based Cryptography
7. Types of Digital Signatures
8. Secure Multiparty Computations

Identity Based Cryptography

Content

Identity Based Cryptography

Identity Based Cryptography

PKI

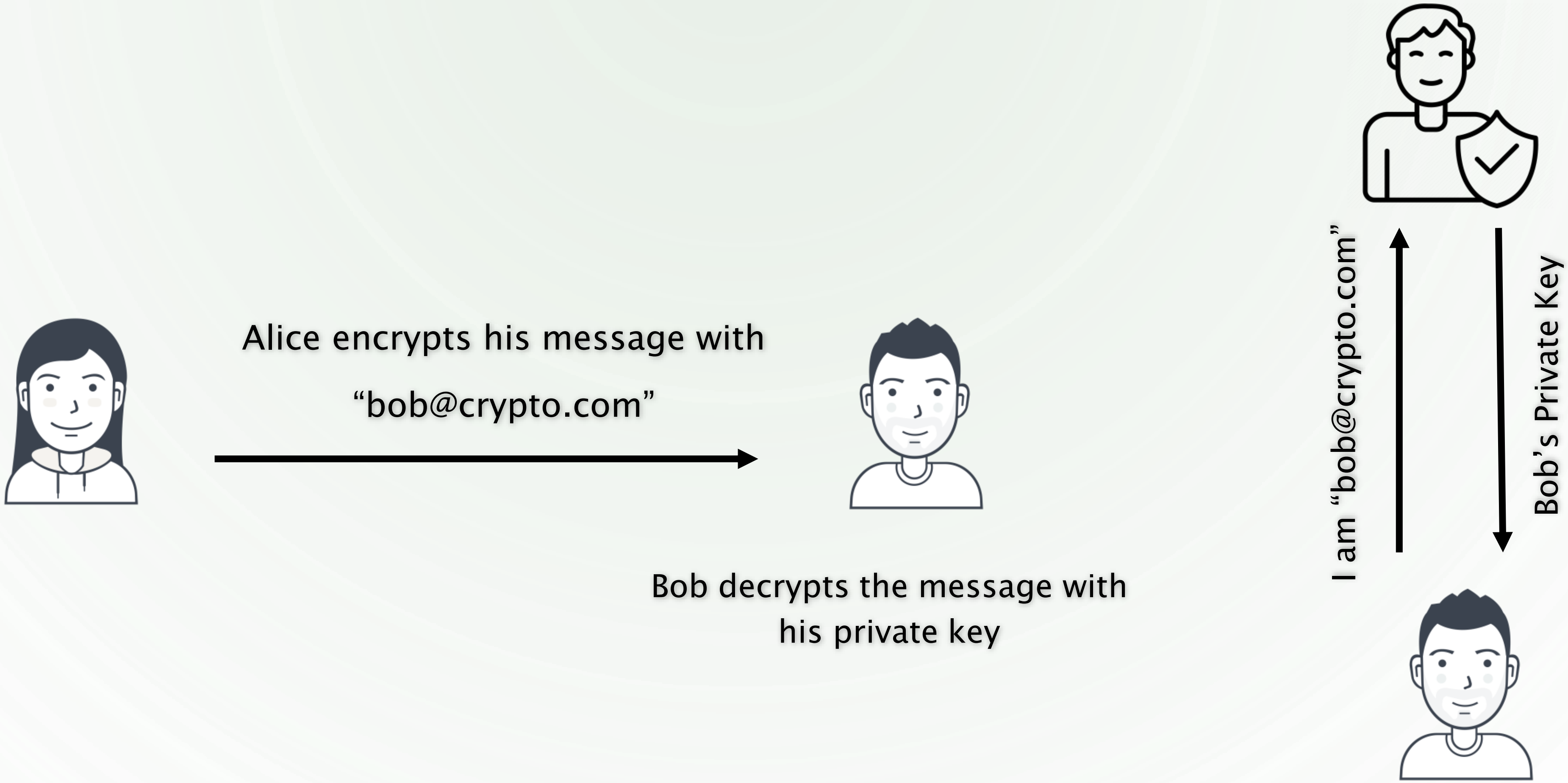
- Using Digital Certifications
- Relation between public key and identity of owner
- The process of key management is cumbersome and time consuming

- What if the public key being generated from identity of the user?
  - No longer need to certification!
  - We need a Key Generation Center (KGC)

- In this method, no need to receive and verify the certificate

Identity Based Cryptography

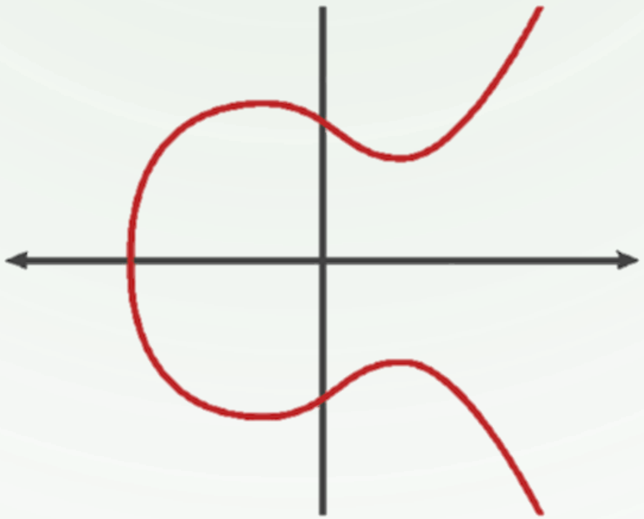
Invented By Shamir (1984)



Identity Based Cryptography

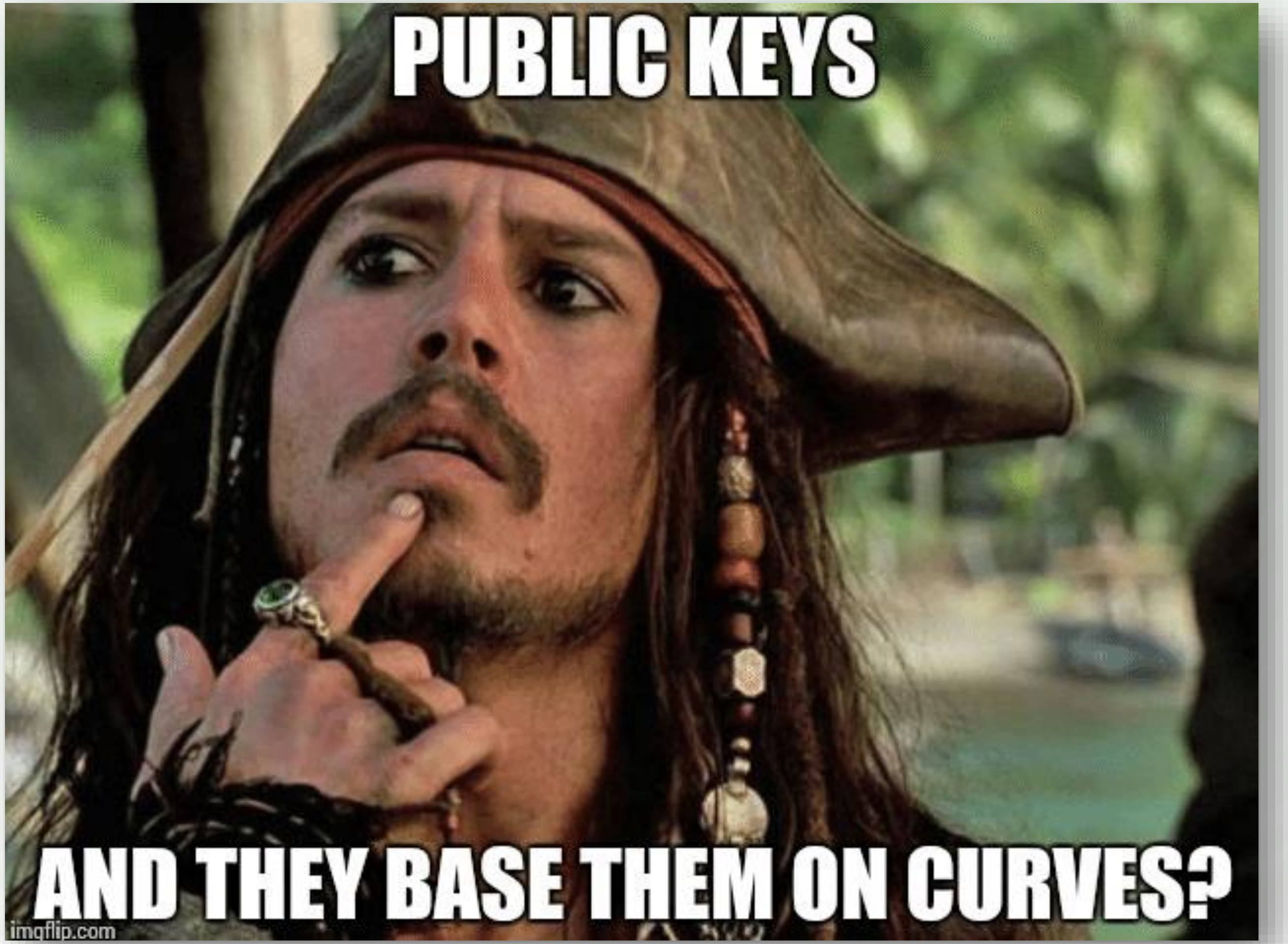
Before continue,

We need some information about **Elliptic Curve Cryptography**



Identity Based Cryptography

Introduction to ECC



7eRoM

Identity Based Cryptography

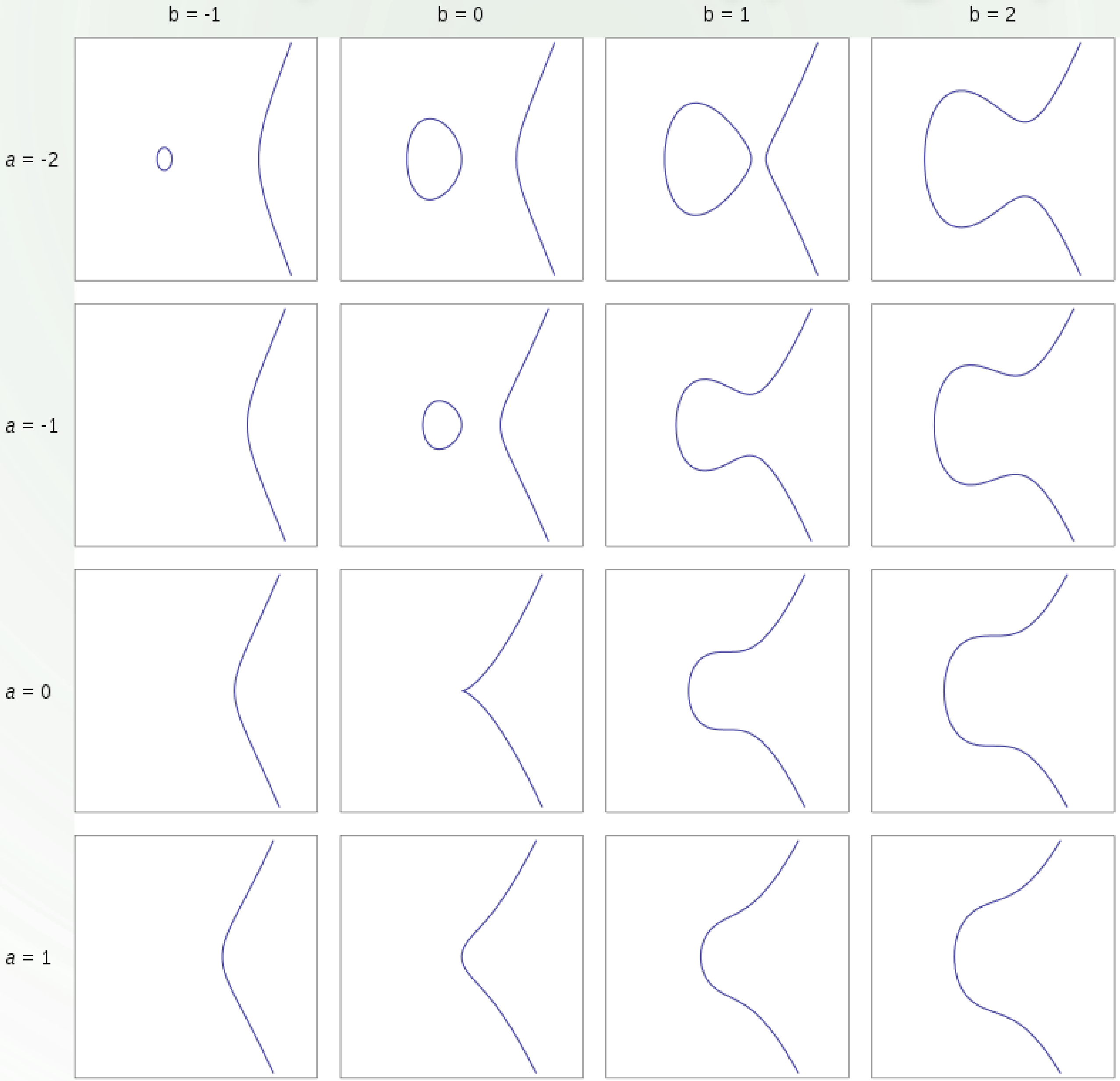
Introduction to ECC

Elliptic curves are generally expressed as Weierstrass equations

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

Discriminant $\Delta = -16(4a^3 + 27b^2)$ must be non zero

Identity Based Cryptography



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

A catalog of elliptic curves. The region shown is $x,\ y \in [-3,3]$

Identity Based Cryptography

Introduction to ECC

- Elliptic curves are generally expressed as Weierstrass equations

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

Let F be a field which is greater than 3

$a, b \in F$

$\Delta = -16(4a^3 + 27b^2)$ must be non zero

- $E(F)$ is the set of all points in F that satisfy the equation together with an additional point I or O at infinity.

$$y^2 = x^3 + 3x + 2 \text{ Over } F_{11}$$

$$\{(2, \pm 4), (3, \pm 4), (4, \pm 1), (6, \pm 4), (7, \pm 5), (10, \pm 3), I\}$$

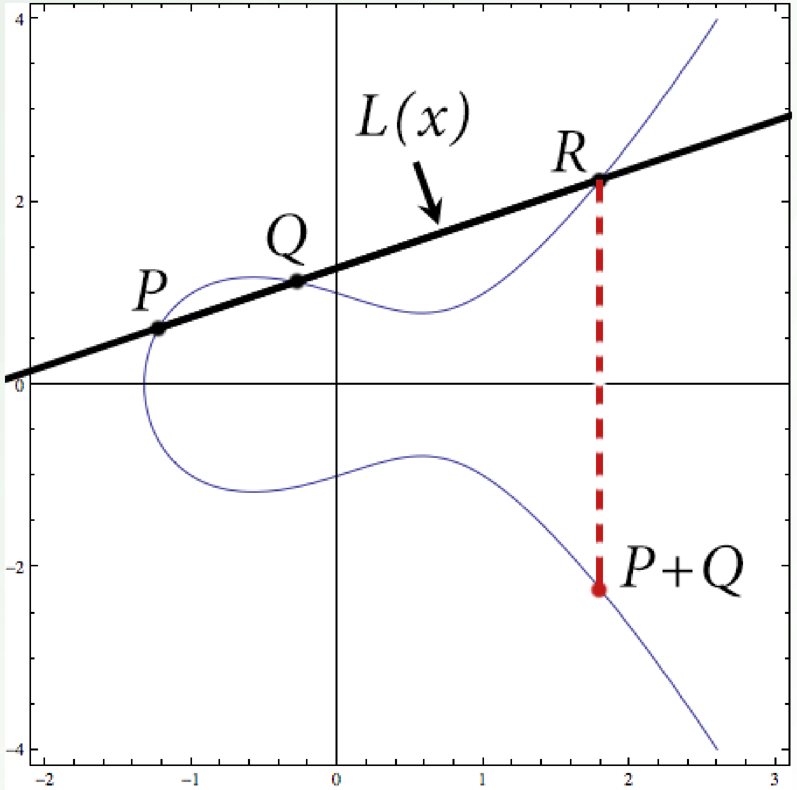
7eRoM

Identity Based Cryptography

Introduction to ECC

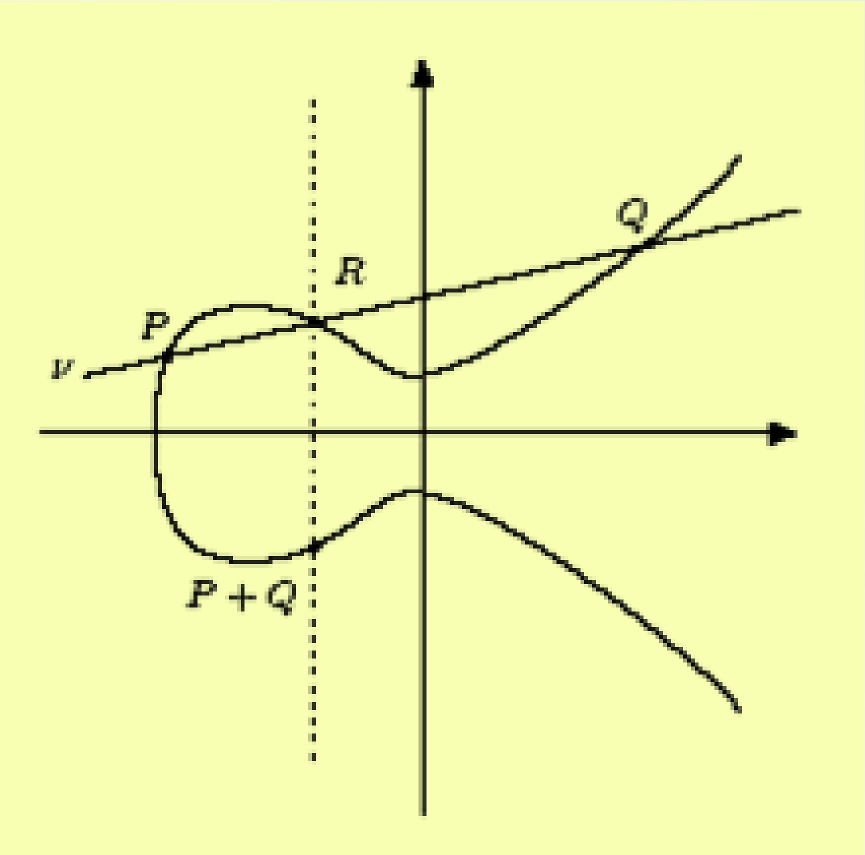
to add $P + Q$, we do the following geometric algorithm:

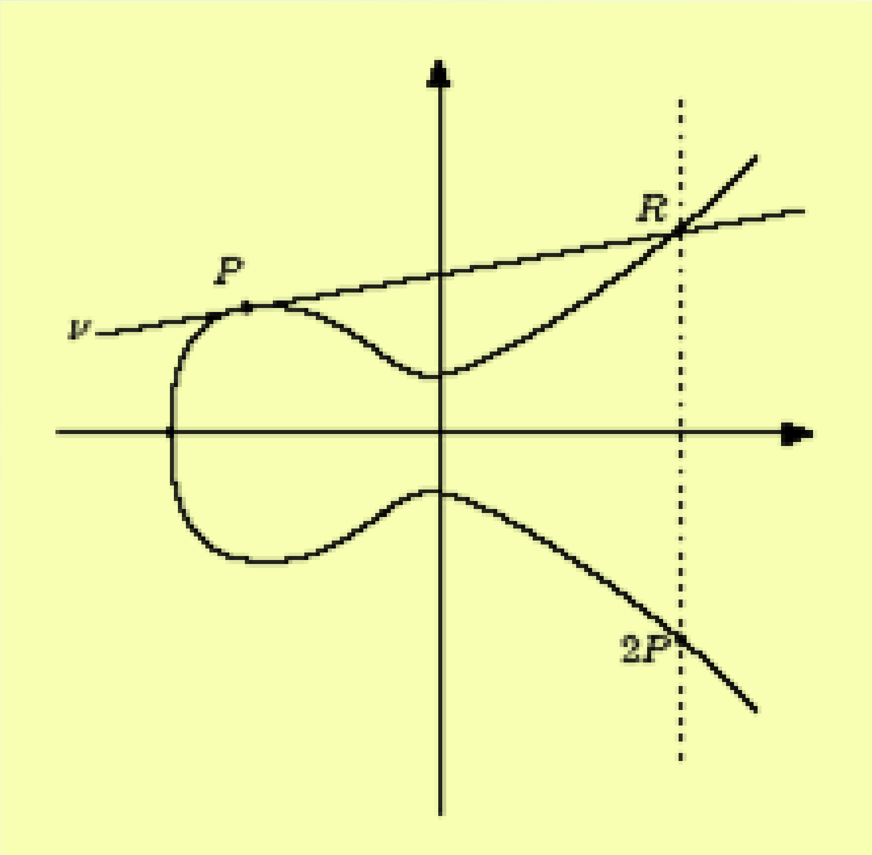
- Form the line $y = L(x)$ connecting P and Q
- Compute the third intersection point of L with E (the one that's not P or Q). Call it R
- Reflect R across the x–axis to get the final point $P + Q$



Identity Based Cryptography

Introduction to ECC



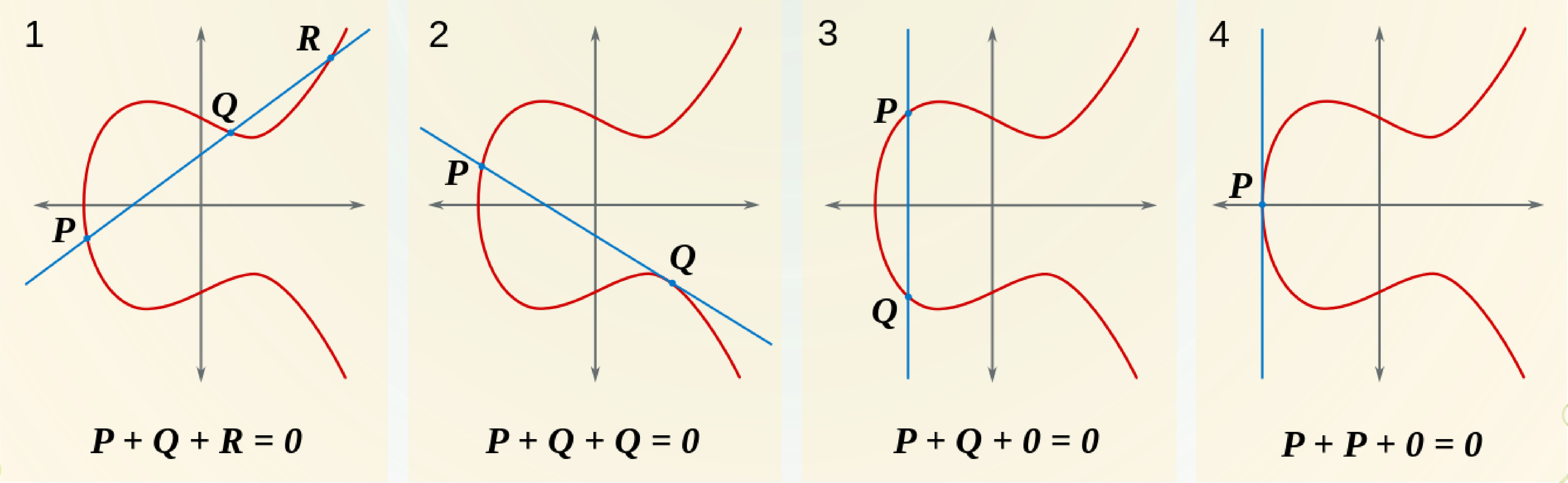


$P + Q = -R$

$2P = p + p = -R$

Identity Based Cryptography

Introduction to ECC



Identity Based Cryptography

Introduction to ECC

- Propertises of point I

  $\mathrm{P} + \mathrm{O} = \mathrm{O} + \mathrm{P} = \mathrm{P}$

  $-\mathrm{O} = \mathrm{O}$

  $\mathrm{P} + (-\mathrm{P}) = (-\mathrm{P}) + \mathrm{P} = \mathrm{O}$

- Multiplication if $m \in Z$ and $P \in E$ and:

  $\mathrm{mP} = \mathrm{P} + \mathrm{P} + \cdots + \mathrm{P} \qquad \mathrm{m} > 0$

  $0\mathrm{P} = \mathrm{O}$

  $\mathrm{mP} = (-\mathrm{m})(-\mathrm{P}) \qquad \mathrm{m} < 0$

Identity Based Cryptography

Introduction to ECC

Theorem: Elliptic Curve Discrete Logarithm Problem (ECDLP)

For a given nP, Finding n is hard-problem

Identity Based Cryptography

Introduction to ECC

Bilinear Pairings

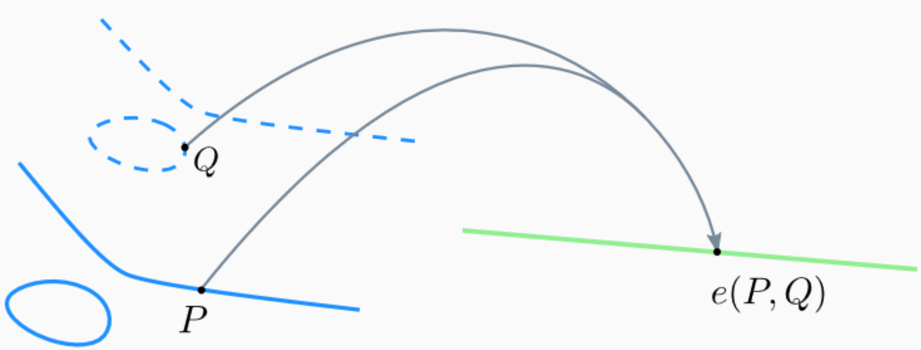
$$e : G_1 \times G_1 \rightarrow G_2$$

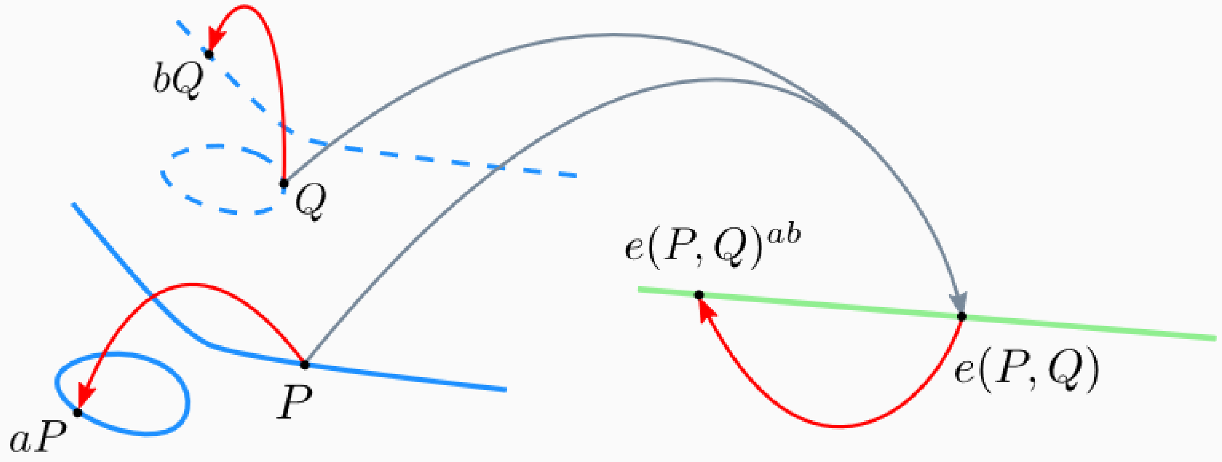
- G_1 is typically a subgroup of an elliptic curve points with prime order q
- G_2 is multiplicative group with prime order q

- Bilinearity: $e(aP, bQ) = e(P, Q)^{ab} = e(bP, aQ)$
- Non-degeneracy: $e(P, Q) \neq 1$

Identity Based Cryptography

Introduction to ECC





Identity Based Cryptography

Boneh-Franklin Scheme

Contains 4 steps:

1. Setup
2. Extraction
3. Encryption
4. Decryption

7eRoM

Identity Based Cryptography

Boneh-Franklin Scheme - 1. Setup

The public key generator (PKG) chooses:

1. the public groups G_1 with generator P and G_2 with the size of q
2. the corresponding pairing e
3. a random private master-key $K_m = s \in Z^*_q$
4. a public key $K_{pub}=sP$
5. a public hash function $H_1 : \{0,1\}^* \to G^*_1$
6. a public hash function $H_2 : G_2 \to \{0,1\}^n$
7. the message space and the cipher space $M = \{0,1\}^n$, $C = G^*_1 \times \{0,1\}^n$

master-key $K_m = s$

$K_{pub}=sP$

$H_1 : \{0,1\}^* \to G^*_1$

$H_2 : G_2 \to \{0,1\}^n$

7eRoM

Identity Based Cryptography

Boneh-Franklin Scheme – 2. Extraction

To create the public key for $ID \in \{0,1\}^*$, the PKG computes:

1. $Q_{ID} = H_1(ID)$
2. the private key $d_{ID} = sQ_{ID}$ which is given to the user

master-key $K_m = s$

$K_{pub} = sP$

$H_1 : \{0,1\}^* \to G^*_1$

$H_2 : G_2 \to \{0,1\}^n$

public key $Q_{ID} = H_1(ID)$

private key $d_{ID} = sQ_{ID}$

Identity Based Cryptography

Boneh-Franklin Scheme – 3. Encryption

Given $m \in M$, the ciphertext c is obtained as follows:

1. $Q_{ID} = H_1(ID) \in G^*_1$
2. Choose random $r \in Z^*_q$
3. Compute $g_{ID} = e(Q_{ID}, K_{pub}) \in G_2$
4. Set $c = (rP, m \oplus H_2(g^r_{ID}))$

Note that K_{pub} is the PKG's public key and thus independent of the recipient's ID

master-key $K_m = s$

$K_{pub} = sP$

$H_1 : \{0,1\}^* \rightarrow G^*_1$

$H_2 : G_2 \rightarrow \{0,1\}^n$

public key $Q_{ID} = H_1(ID)$

private key $d_{ID} = sQ_{ID}$

random r

$g_{ID} = e(Q_{ID}, K_{pub}) \in G_2$

$c = (rP, m \oplus H_2(g^r_{ID}))$

7eRoM

Identity Based Cryptography

Boneh-Franklin Scheme – 4. Decryption

Given $c = (u,v) \in C$, the plaintext can be retrieved using the private key:

$$m = v \oplus H_2(e(d_{ID},u))$$

Proof: $m = v \oplus H_2(e(d_{ID}, u))$

$$= v \oplus H_2(e(sQ_{ID}, rP))$$

$$= v \oplus H_2(e(Q_{ID}, P)^{sr})$$

$$= v \oplus H_2(e(Q_{ID}, sP)^{r})$$

$$= v \oplus H_2(e(Q_{ID}, K_{pub})^{r})$$

$$= v \oplus H_2(g^r{}_{ID})$$

$$= m \oplus H_2(g^r{}_{ID}) \oplus H_2(g^r{}_{ID})$$

master-key $K_m = s$

$K_{pub}=sP$

$H_1 : \{0,1\}^* \rightarrow G^*{}_1$

$H_2 : G_2 \rightarrow \{0,1\}^n$

public key $Q_{ID} = H_1(ID)$

private key $d_{ID} = sQ_{ID}$

random r

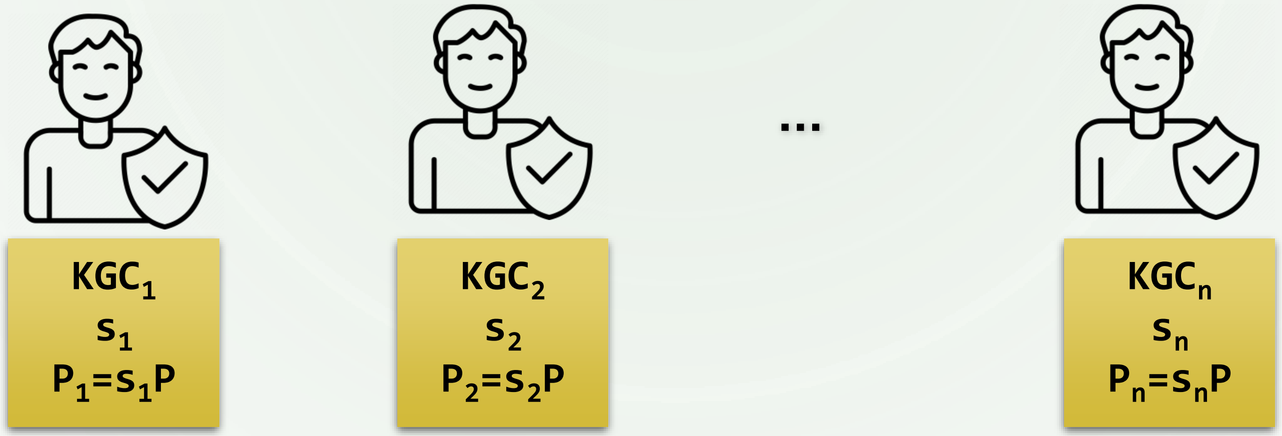
$g_{ID} = e(Q_{ID}, K_{pub}) \in G_2$

$c = (rP, m \oplus H_2(g^r{}_{ID}))$

7eRoM

Identity Based Cryptography

Escrow Remove



$$S_{ID} = s_1Q_{ID} + s_2Q_{ID} + \dots + s_nQ_{ID}$$
$$= (s_1+s_2+\dots+s_n)Q_{ID}$$

$$P_{pub} = \sum_{i=1}^{n} P_i$$

Identity Based Cryptography

Key Agreement – Diffie–Hellman

$a \in Z^*_q$

$T_A = aP$

$T_B = bP$

$b \in Z^*_q$

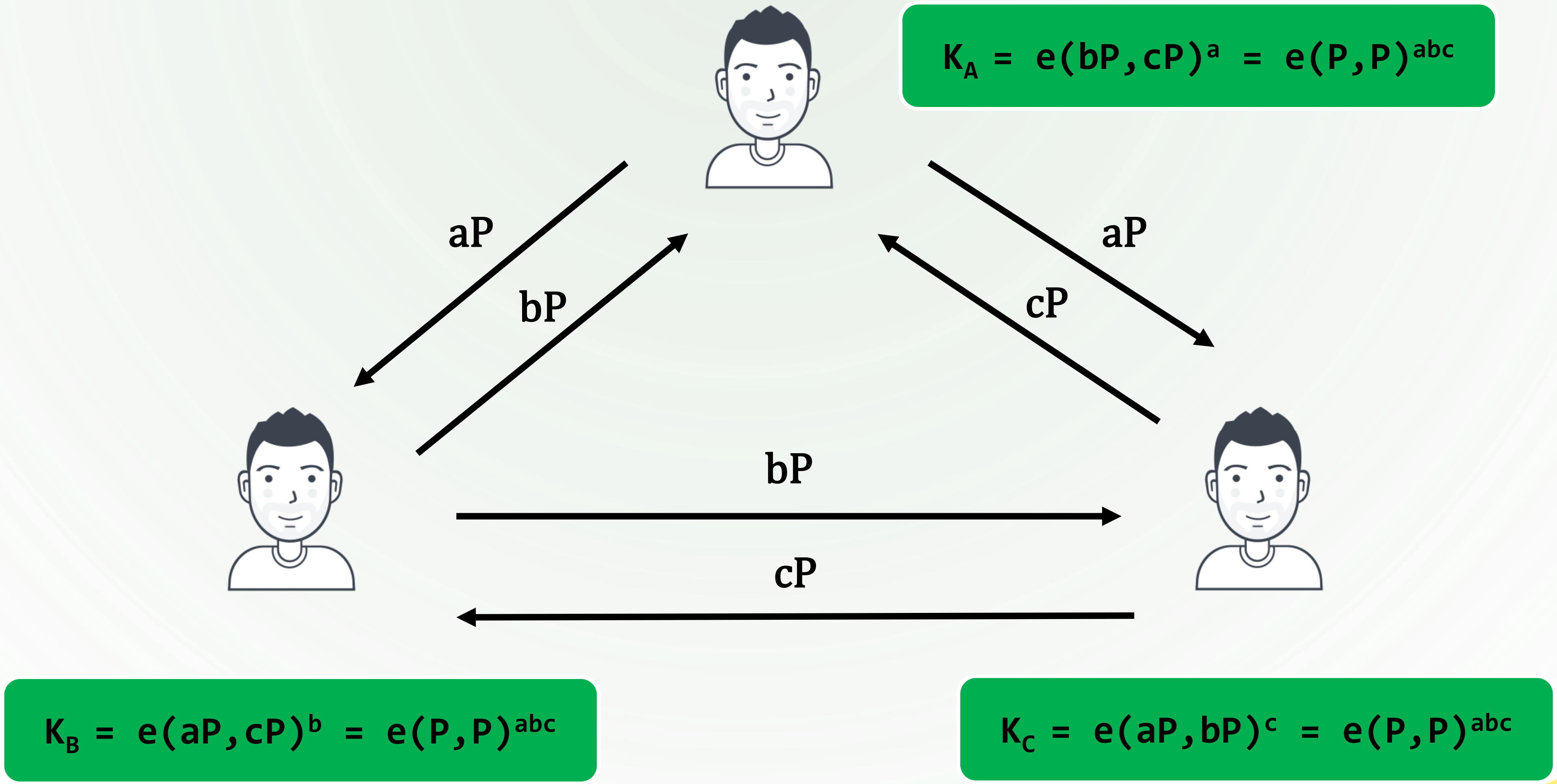
$K_A = abP$

$K_B = baP$

No Authentication

Identity Based Cryptography

Key Agreement – Joux Scheme



Identity Based Cryptography

Key Agreement – The Common Implicit Key Between Pair of Users

$Q_{ID}=H_1(ID)$

$S_{ID}=sQ_{ID}$

$Q_A=H_1(A)$
$S_A=sQ_A$

$T_A = aP$ $\longrightarrow$

$\longleftarrow$ $T_B = bP$

$Q_B=H_1(B)$
$S_B=sQ_B$

$K_A = e(S_A, Q_B) = e(Q_A, Q_B)^s$

$K_B = e(Q_A, S_B) = e(Q_A, Q_B)^s$

Identity Based Cryptography

Key Agreement – Smart Protocol

$a \in Z^*_q$

$T_A = aP$ →

← $T_B = bP$

$b \in Z^*_q$

$K_A = e(aQ_B, P_{pub}).e(S_A, T_B)$

$K_B = e(bQ_A, P_{pub}).e(S_B, T_A)$

$$
\begin{aligned}
K_A &= e(aQ_B, P_{pub}).e(S_A, T_B) \\
&= e(aQ_B, sP).e(sQ_A, bP) \\
&= e(sQ_B, aP).e(bQ_A, sP) \\
&= e(S_B, T_A).e(bQ_A, P_{pub}) \\
&= K_B
\end{aligned}
$$

Ref

1. Cryptography Protocols Course, Dr. Hamid Mala, University of Isfahan
2. https://ecc2017.cs.ru.nl/slides/ecc2017school-aranha.pdf
3. https://people.math.carleton.ca/~cingalls/studentProjects/ecc.pdf
4. https://www.globalsign.com/en/blog/elliptic-curve-cryptography
5. https://en.wikipedia.org/wiki/Elliptic_curve
6. https://jeremykun.com/2014/02/16/elliptic-curves-as-algebraic-structures/
7. https://en.wikipedia.org/wiki/Boneh%E2%80%93Franklin_scheme
8. https://www.iconfinder.com/UsersInsights
9. https://www.iconfinder.com/Chanut-is
10. https://www.iconfinder.com/iconsets/softwaredemo