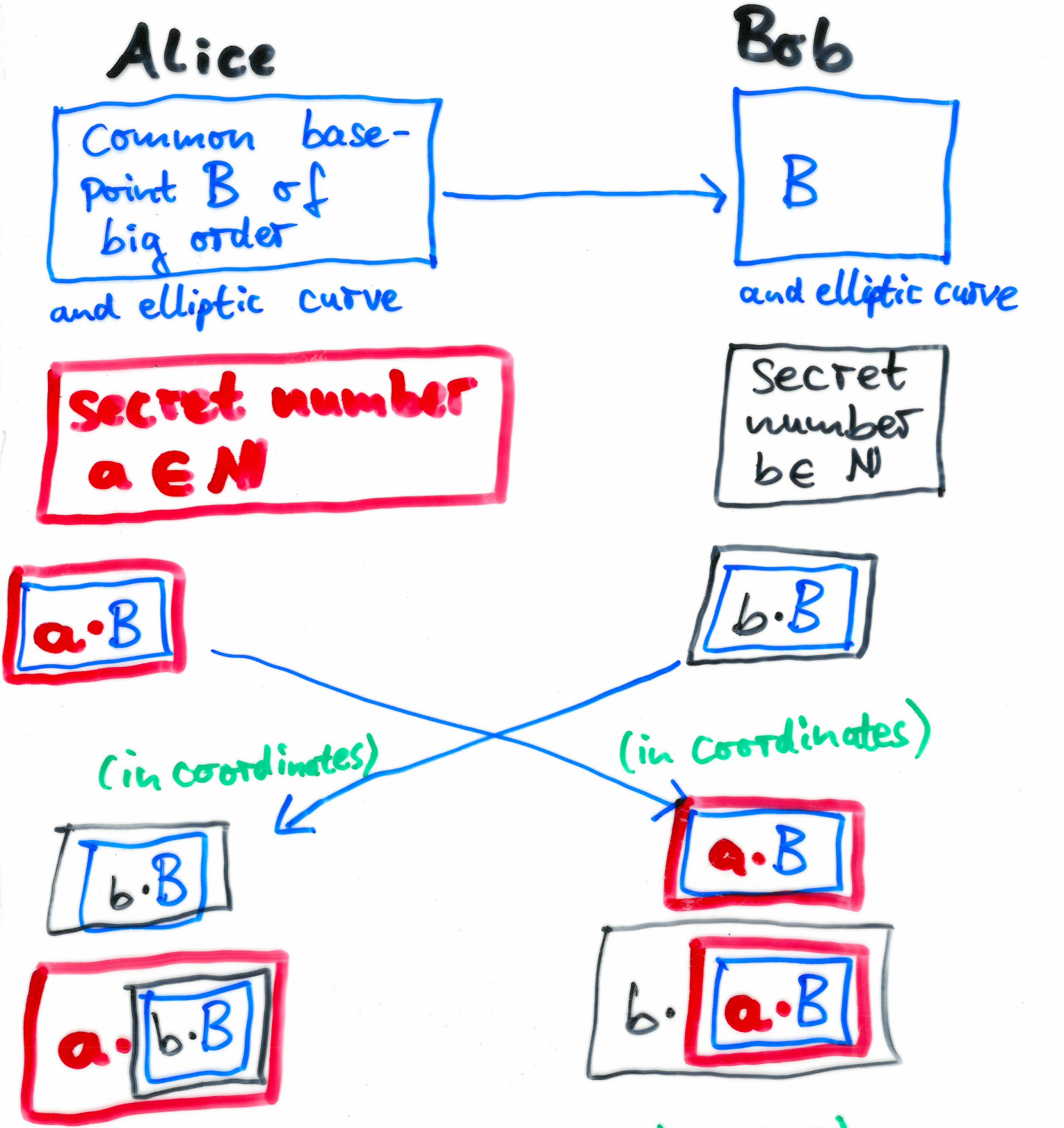
Elliptic curve version of Diffie-Hellmann key exchange



Common secret key: $a(b \cdot B) = b(a \cdot B)$

Private secret numbers: a, b

Public information: $B, a \cdot B, b \cdot B$.

The ElGamal cryptosystem

Alice | **Bob**

g →

$g \in \mathbb{F}_q^*$: generator (or element of high order) in large finite field $\mathbb{F}_q$

Chooses secret element $a \in \mathbb{F}_q^*$

Chooses secret element $b \in \mathbb{F}_q^*$

Sends public key g^a →

g^a

Writes message with blocks $M \in \mathbb{F}_q^*$

g^b and $M \cdot g^{ab}$ ←

Sends g^b and $M \cdot (g^a)^b$

Deciphers using her secret key a:

$(g^b)^a = g^{ba} = g^{ab}$

She computes the multiplicative inverse of $(g^b)^a$ and takes its product with $M \cdot g^{ab}$

Elliptic curve version of the ElGamal cryptosystem

Alice | **Bob**

Alice: B → Bob: Basepoint B on elliptic curve

Chooses secret number $a \in \mathbb{N}$

Chooses secret number $k \in \mathbb{N}$

Sends public key $a \cdot B$ — in coordinates → $a \cdot B$

Writes message with blocks P_m on elliptic curve

Sends $k \cdot B$ and $P_m + k \cdot (a \cdot B)$ — in coordinates → $k \cdot B$ and $P_m + k \cdot (a \cdot B)$

Deciphers using her secret key a:
$a \cdot (k \cdot B) = k \cdot (a \cdot B)$,
which she substracts from $P_m + k \cdot (a \cdot B)$