Using Elliptic Curve for Public Key Cryptography

Public elements: Prime number : q

EC: $E_q(a, b)$

G: Point curve with high order.

Alice pick n_A (privek) $P_A = n_A \times G$

Bob pick n_B (privek) $P_B = n_B \times G$

↳ less than order of G (around size q max)

~~Bob~~ Alice ⟶ Bob

Alice

1. Picks a secret random k, calculate $k \times G$. (C_1)
2. P_m = plaintext msg pt.

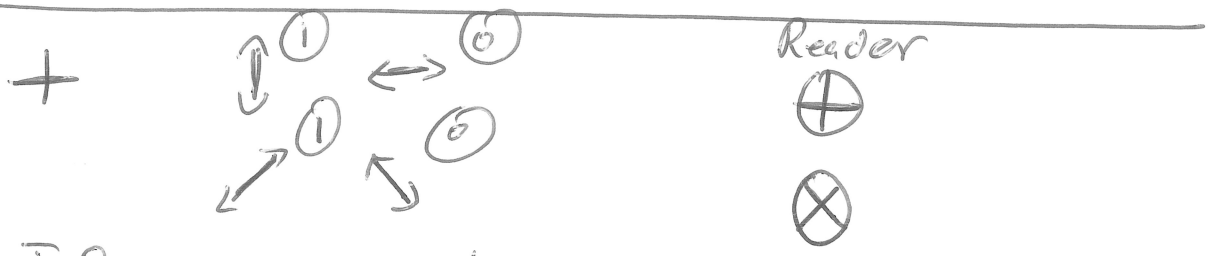
$C_2 = P_m + k \times P_B = \boxed{P_m + (k \times n_B) \times G}$

When Bob receives

1. Calculate $n_B \times C_1 = n_B \times k \times G$
2. Calculates $P_m = C_2 - n_B \times C_1$.

11/18/19 (2)

Quantum Cryptography (Code Book)



If you use the wrong reader, you incorrectly read a bit 50% of the time.

Alice → sends 1000 bits Eve Reader (Reader) Bob

bit orientation	value
+	1
+	−
×	/
×	\

→ Eve ⊕ 1 → ⊗ (Bob will be wrong 50% of the time)

Bob guesses which reader to use.

Alice calls bob tells him the reader orientation. (Anyone can hear)

Bob gets a list of about 500 bits for which he guessed right. (1, 4, 7, 8, ...)

What's the probability that eve listened to all 500 bits and Bob had all 500 correctly read?

eve guesses wrong reader 50% time. Of those times, the bit flips 50% time. 25% of the time Bob gets the wrong bit,

$P(\text{all correct}) = .75^{500} = \text{very small}$

Let's use this idea to exchange a secret key

---

① Alice sends Bob 1000 bits as before

② Talk on phone and determine which bits Bob guessed correctly. (~500 bits)

③ Of those 500 bits, Alice randomly choose 100 of them and tells Bob what she sent.

④ If all 100 are correct, then use the other 400 as a shared secret key.