Coin Flipping

Monday, April 26, 2021 4:51 PM

Recall : QKE

BB84 , B92

1] Applications of Quantum Cryptography

- Quantum Money
- Coin flipping
- Quantum One-time pad.

2] Quantum Money (by Peter Shor)

Quantum money is a quantum cryptographic protocol where a mint can create quantum states which

1. Can be verified publicly.

   Each quantum money state ψ has a S/N which tells how to verify it (verification Test)

2. Cannot be duplicated.

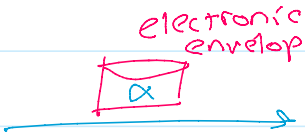
   Holding the money state ψ and knowing the verification Test, Eve cannot make two states ϕ_1 and ϕ_2 that both pass the verification test as ψ.

3] Telephone Coin Flipping:

$0 \to H$, $1 \to T$

Protocol:

① Alice chooses $\alpha \in \{0,1\}$ puts α in an "electronic envelope"



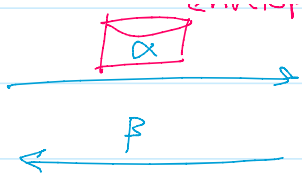
puts α in an "electronic envelope"

② Bob chooses $\beta \in \{0,1\}$ and sends to Alice

③ Alice opens the "envelope" and reveals α

④ Alice and Bob compute

$$\text{Coin} = \alpha \oplus \beta$$



③ Alice opens the envelope

④ Coin = $\alpha \oplus \beta$

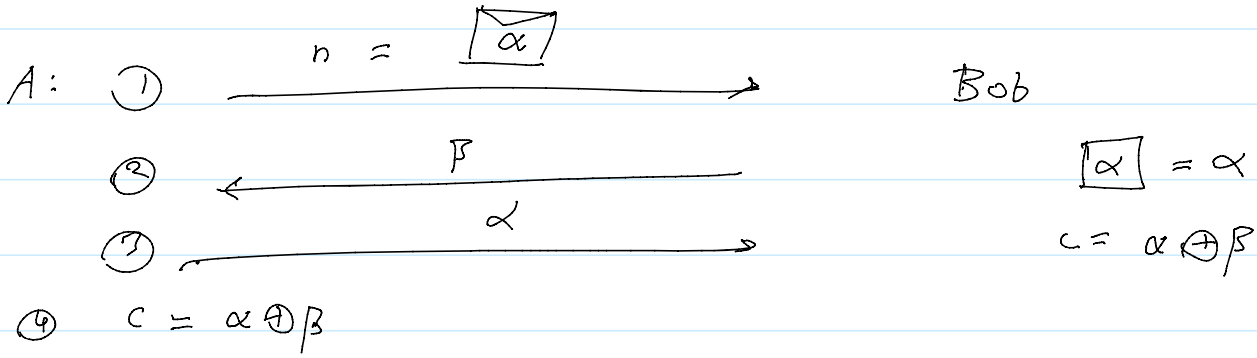
4] Commitment - Scheme §1.2.3 Bellare & Rogaway

① Allows Alice to put α inside the "envelope"

② Bob cannot see α until Alice opens it.

③ Alice cannot change the value of α after commitment.

"It can only be opened one way"



5] Protocol: Commitment Scheme

1. Choose 2 large primes p, q : s.t. $p < q$

2. To commit on α

for $\alpha = 1$	for $\alpha = 0$
$p \equiv 3 \pmod 4$	$p \equiv 1 \pmod 4$

$p \equiv 3 \pmod 4$	$p \equiv 1 \pmod 4$
$q \equiv 1 \pmod 4$	$q \equiv 3 \pmod 4$
Send $n = p \cdot q$	Send $n = p \cdot q$

3. To open the commitment (the envelope)

Alice sends : p, q and α

Bob verifies : ① $p < q$; $n = p \cdot q$

② p and q are primes.

③ check p, q for α

6] e.g. Alice

① $n = 35$, $(p = 5, q = 7, \alpha = 0) \Rightarrow \alpha = 0$ ✓ ok

② $n = 77$, $(p = 7, q = 11, \alpha = 1) \Rightarrow \alpha = ?$ Redo? ok

③ $n = 55$, $(p = 11, q = 5, \alpha = 1) \Rightarrow \alpha = 0$? Redo? No

$\Rightarrow$ Reject / claim winning.

7] Quantum coin flipping:

Protocol:

① Alice chooses either + or × basis

② Alice generates k random qubits, and sends them to Bob

③ Bob receives the qubits using random bases + and ×, and stores the bits in 2 tables (Rectilinear^{+} / Diagonal$^{\times}$)

④ He guesses which basis Alice used

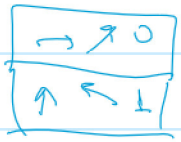
④ He guesses which basis Alice used in step 1. If he is correct, he wins.

⑤ Alice announces if Bob guess is correct. She must confirm all the qubits sent to Bob at step ②

⑥ Bob compares Alice list with his tables and confirms no cheating.

e.g. $k = 8$

	1	2	3	4	5	6	7	8
① Alice basis +	1	0	1	0	0	1	1	0
② She sends	↑	→	↑	→	→	↑	↑	→
③ Bob bases	+	×	+	×	+	×	+	×



Rectilinear +	1	1	0	1
Diagonal ×	0	1	1	1

④ Bob guess	×
⑤ Alice says	+
	1 win
⑥ Bob confirms	

	1	1	0	1

8] Quantum one-Time Pad (Q-OTP)

For one qubit:

	Classic bit	Quantum bit

	Classic	Quantum
encryption	$e = m \oplus k$	$\|e\rangle = X^k \|m\rangle \rightarrow \|m \oplus k\rangle$ k is classical
Decrypt	$m = e \oplus k$ $= (m \oplus k) \oplus k = m$	$\|m\rangle = X^k \|e\rangle$ $= X^k (X^k \|m\rangle)$

Note:

The encrypte text (qubit) is totally independent of the message

End of ICS 439

تم بحمد الله