Quantum Coin-Flipping

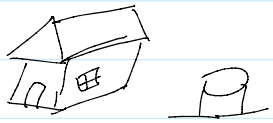
Tuesday, October 31, 2023

Recall: Quantum Cryptography
QKE protocols

1] Application of Quantum Cryptography:

- QKE ✓
- Coin-flipping (today)
- One-time pad
- Quantum money
- Quantum pseudorandom number generator. (QPRNG)

2] Telephone Coin flipping:



① Alice chooses $\alpha \in \{0,1\}$
puts α in an "electronic envelope"
② Bob choose $\beta \in \{0,1\}$ and
tells Alice
③ Alice opens the "envelope" and
reveals α
④ Alice and Bob compute the outcome
of the coin $= \alpha \oplus \beta$

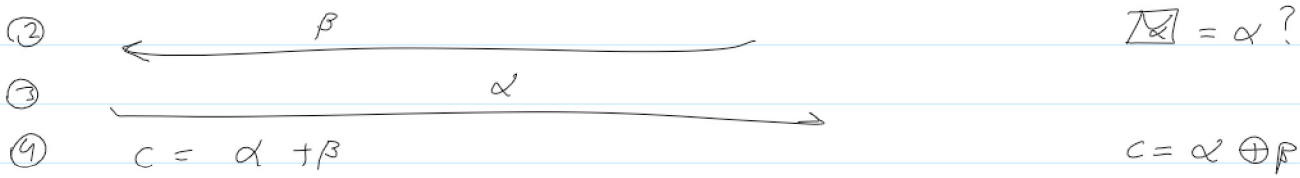
$0 = H$, $1 = T$

Alice	Bob
① α	
	② β
③ Alice opens envelop α	
④ Coin $= \alpha \oplus \beta$	

3] 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)

A: ① $n = \boxed{\alpha}$ → Bob



4] Protocol : Commitment-scheme

1. Choose large primes p, q , s.t. $p < q$
2. To commin on

$\alpha = 0$	$\alpha = 1$
$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 4$
$q \equiv 3 \pmod 4$	$q \equiv 1 \pmod 4$
Send $n = p \cdot q$	send $n = p \cdot q$

3. To open the commitment (the envelope),
   Alice sends p, q and α to Bob
   Bob verifies :
   ① $p < q$ and $n = p \cdot q$
   ② p and q are primes
   ③ check p and q for α

5] e.g. ① A : $n = 35$, $p = 5$, $q = 7 \Rightarrow \alpha = 0$ ✓
↳ $p = 7$, $q = 5 \Rightarrow \alpha = 1$ Reject and claim wi

② A : $n = 77$, $p = 7$, $q = 11 \Rightarrow \alpha = ?$ Reject ; Red

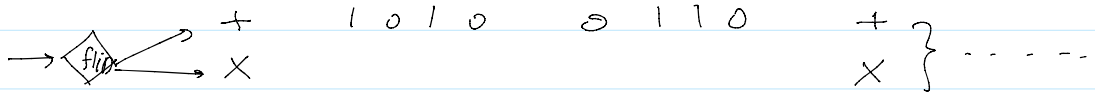
③ A : $n = 55$, $p = 5$, $q = 11 \Rightarrow \alpha = 1$ Reject and claim win

---

6] Quantum Coin flipping :

Idea :

Alice Bob



7] QCF Protocol

① Alice chooses either Rectilinear (+) or Diagonal (X) basis.

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

③ Bob receives the qubits using random bases (+ or X) for each qubit. He stores the bit in two tables [Rectilinear (+)] and [Diagonal (X)]

④ Bob guesses which basis Alice used in Step (1). If he is correct, he wins.

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

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

8] e.g. QCF with $k = 8$

Alice random bits: 1 0 1 0 0 1 1 0

	1	2	3	4	5	6	7	8
① Alice basis	+	X	+	X	+	X	+	X
② Alice sends	↑	→	↑	→	→	↑	↑	→
③ Bob bases	+	X	+	X	+	X	+	X
Rectilinear +	1		1		0		1	
Diagonal X		0		1		0		0
		✓		×		×		✓

④ Bob guess (X)

⑤ Alice announce (Wrong)
and confirm 1 1 0 1

⑥ Bob confirms

Bob guess (+)
Alice announce (correct)
→ (wrong)
but cannot confirm

9] Quantum One-time Pad

Key 101110
P 110110 ⊕
C 011000

For one-qubit

	Classical bit	Qu bit
Encryption	$e = m \oplus k$	$\|e\rangle = X^k \|m\rangle \rightarrow \|m \oplus k\rangle$
Decryption	$m = e \oplus k$ $= (m \oplus k) \oplus k = m$	$\|m\rangle = X^k \|e\rangle$ $= X^k (X^k \|m\rangle)$

The encrypted text (e qubit) is totally independent of the message (m)