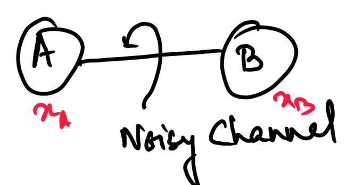
Secure AND Protocol. (using only channel noise)



Input: $x_A, x_B \in \{0,1\}$
Output: $z_A, z_B \in \{0,1\}$

$z_A \oplus z_B = x_A \wedge x_B$

Impossible if channel is noise-free.
↳ possible if computational secrecy; but perfect secrecy is impossible.

Proof

Assume $\exists$ a protocol which generates z_A, z_B

Run ①: A// $x_A \to z_A$; B// $x_B \to z_B$

Run ②: A// $\bar{x}_A \to z_A'$; B// $x_B \to z_B$

z_B → should not have any information about x_A ∴ z_B is generated locally from x_B

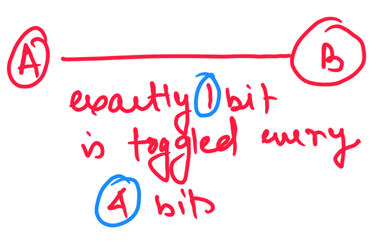
B should not be able to differentiate between Run ① & Run ② (otherwise he will know whether input was x_A or $\bar{x}_A$ violating perfect secrecy)

∴ Recieves same set of messages from z_A
↳ transcript

from Run ②
$$z_A' \oplus z_B = \bar{x}_A \wedge x_B$$
from Run ①
$$z_A \oplus z_B = x_A \wedge x_B$$
Run ① ⊕ Run ②
$$z_A \oplus z_A' = (\bar{x}_A \wedge x_B) \oplus (x_A \wedge x_B)$$
$$= (x_A \oplus \bar{x}_A) \wedge x_B$$
$$= x_B$$

∴ We need noise for perfect secrecy

With Noise.



cannot have ≥ 2 bits toggled for 4 bits (error correcting codes do not exist)

∴ upto 1 bit toggled
⇕
error-correction possible.
⇕
we can simulate noiseless channel which sends parity bits (0 if no bit toggled, 1 if some bit toggled)
⇕
we can allow communication where only 1 bit toggled (exactly)

Protocol.

① A sends 4 bits
$[r_0 \; r_1 \; r_2 \; r_3]$

B recieves
$[s_0 \; s_1 \; s_2 \; s_3]$

② A computes

$$[r_0 \; r_1 \; r_2 \; r_3] \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} = [a_A \; b_A \; c_A]$$

↳ truth table for AND (replace with OR Table to get secureOR)

B computes

$$[s_0 \; s_1 \; s_2 \; s_3] \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} = [a_B \; b_B \; c_B]$$

now we want to show that
$$(a_A \oplus a_B) \wedge (b_A \oplus b_B) = (c_A \oplus c_B)$$

Note that
$$a_A \; b_A \; c_A = [r_0 \; r_1 \; r_2 \; r_3] \times M$$
$$\oplus \quad a_B \; b_B \; c_B = [s_0 \; s_1 \; s_2 \; s_3] \times M$$
$$a_A \oplus a_B \;\; b_A \oplus b_B \;\; c_A \oplus c_B = [r_0 \oplus s_0 \;\; r_1 \oplus s_1 \;\; r_2 \oplus s_2 \;\; r_3 \oplus s_3] \times M$$

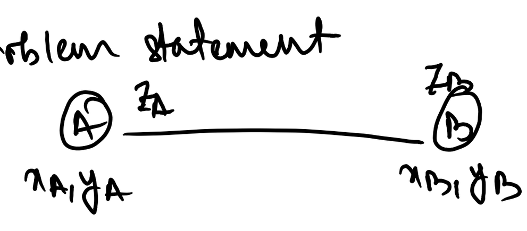
since only 1 bit toggled
∴ Three $r_i = s_i$
One $r_i \neq s_i$ (toggled)
∴ One 1 & Three Zero
Also M is truth table for AND
∴ we are picking 1 row of truth table for $a_A \oplus a_B$, $b_A \oplus b_B$, $c_A \oplus c_B$
∴ $(a_A \oplus a_B) \wedge (b_A \oplus b_B) = (c_A \oplus c_B)$

B does not know anything about a_A, b_A, c_A
A " a_B, b_B, c_B

③ A sends
$(x_A \oplus a_A), (y_A \oplus b_A)$ to B

B sends
$(x_B \oplus a_B), (y_B \oplus b_B)$ to A

Problem statement



$$z_A \oplus z_B = (x_A \oplus x_B) \wedge (y_A \oplus y_B)$$

④ A computes
$$w = x_A \oplus a_A \oplus x_B \oplus a_B$$
$$u = y_A \oplus b_A \oplus y_B \oplus b_B$$
B computes
$$w = x_B \oplus a_B \oplus x_A \oplus a_A$$
$$u = y_B \oplus b_B \oplus y_A \oplus b_A$$

⑤ we use the identity.
$$xy = (x \oplus a)(y \oplus b) \oplus (x \oplus a)b \oplus (y + b)a \oplus ab$$

set
$x = x_A \oplus x_B$
$y = y_A \oplus y_B$
$a = a_A \oplus a_B$
$b = a_B \oplus a_B$

$$\therefore (x_A \oplus x_B)(y_A \oplus y_B) = w \wedge u \oplus w(b_A \oplus b_B) \oplus u(a_A \oplus a_B) \oplus c_A \oplus c_B$$
$$= (w \wedge u) \oplus w \wedge b_A \oplus w \wedge b_B \oplus u \wedge a_A \oplus u \wedge a_B \oplus c_A \oplus c_B$$

$$z_A = (w \wedge u) \oplus (w \wedge b_A) \oplus (u \wedge a_A) \oplus c_A \qquad z_B = (w \wedge b_B) \oplus (u \wedge a_B) \oplus c_B$$

A calculates z_A; B calculates z_B
reveal both; calculate
$$(x_A \oplus x_B) \wedge (y_A \oplus y_B)$$