Hardware Trojan and Trusted IC

What is Hardware Trojan?

- A **hardware Trojan** is a type of malicious modification made to hardware components—typically to integrated circuits (ICs) or chips—that can allow unauthorized access, data leaks, or other security breaches within a system.
- These modifications are often designed to be subtle and hard to detect, embedded deep within the hardware to perform actions like data exfiltration, function manipulation, or system malfunction under specific conditions.

Characteristics of Hardware Trojans

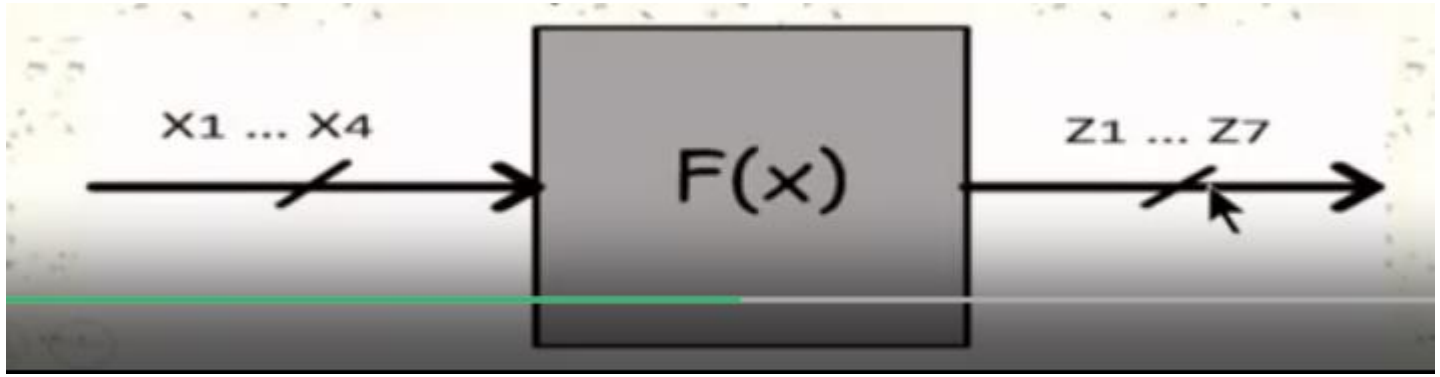
- **Stealth**: They are designed to be hidden and operate without disrupting normal functionality, making them difficult to detect.
- **Trigger Mechanism**: Some Trojans are dormant until triggered by specific events (e.g., certain data patterns, external commands, or power cycles).
- **Payload**: Once activated, the Trojan can perform a range of malicious activities, from leaking sensitive information to causing the device to fail.

Trusted Integrated Circuits

- Trusted Integrated Circuits (TIC): an IC does exactly what it is asked for, no less or no malicious more.
- Examples of untrusted ICs
  - Fail to deliver certain required functionality
  - Have Hardware Trojan inside the chip

Example of Trusted IC and HT

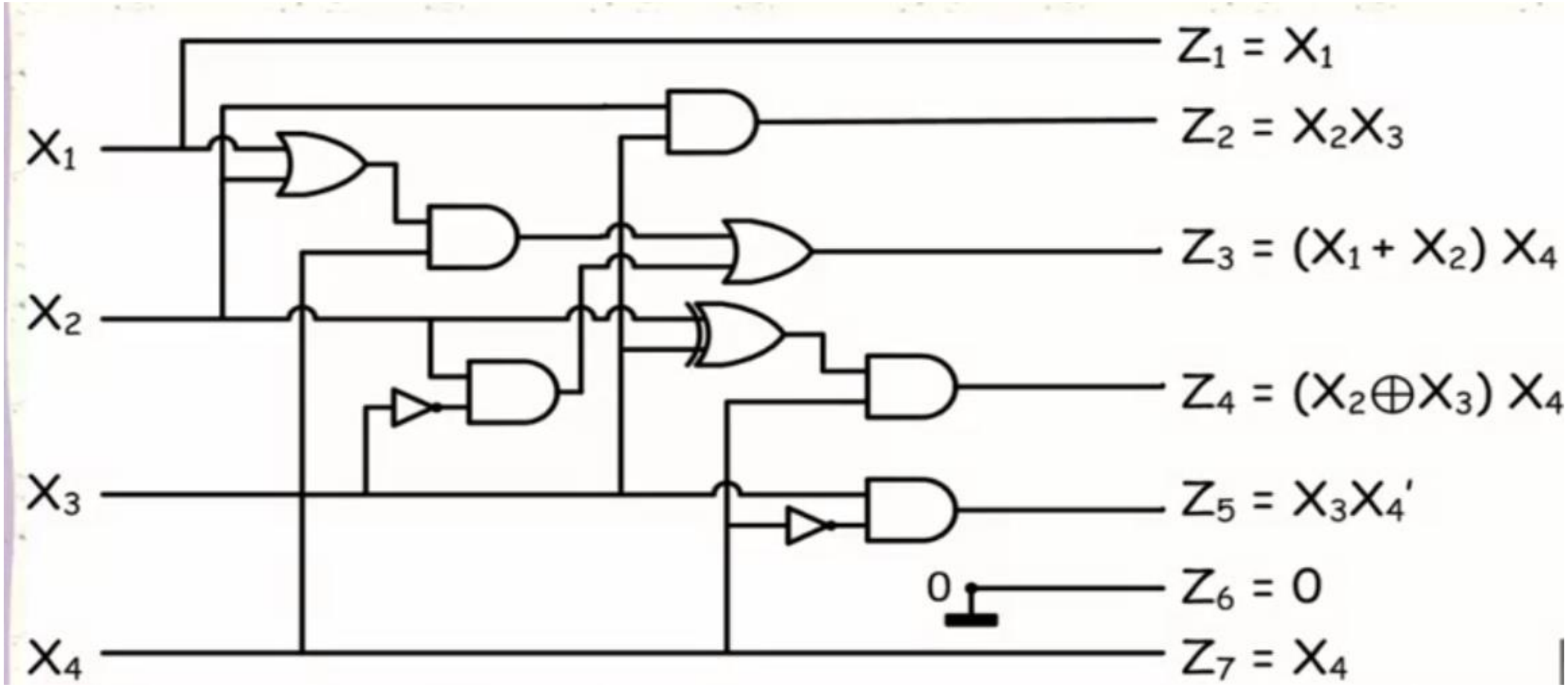
- Alice asks Bob to design a circuit that computes F(x) so she can authenticate the (x, F(x)) pairs as (username, password).
- Assume that $F(x) = x^2$ for x = 0, 1, 2, . . . , 9.
- Bob's Design:
- Input: $\{x_1, x_2, x_3, x_4\}$
- Output: $\{z_1, z_2, z_3\ z_4, z_5, z_6, z_7\}$
- Functionality: z = F(x) = x^2



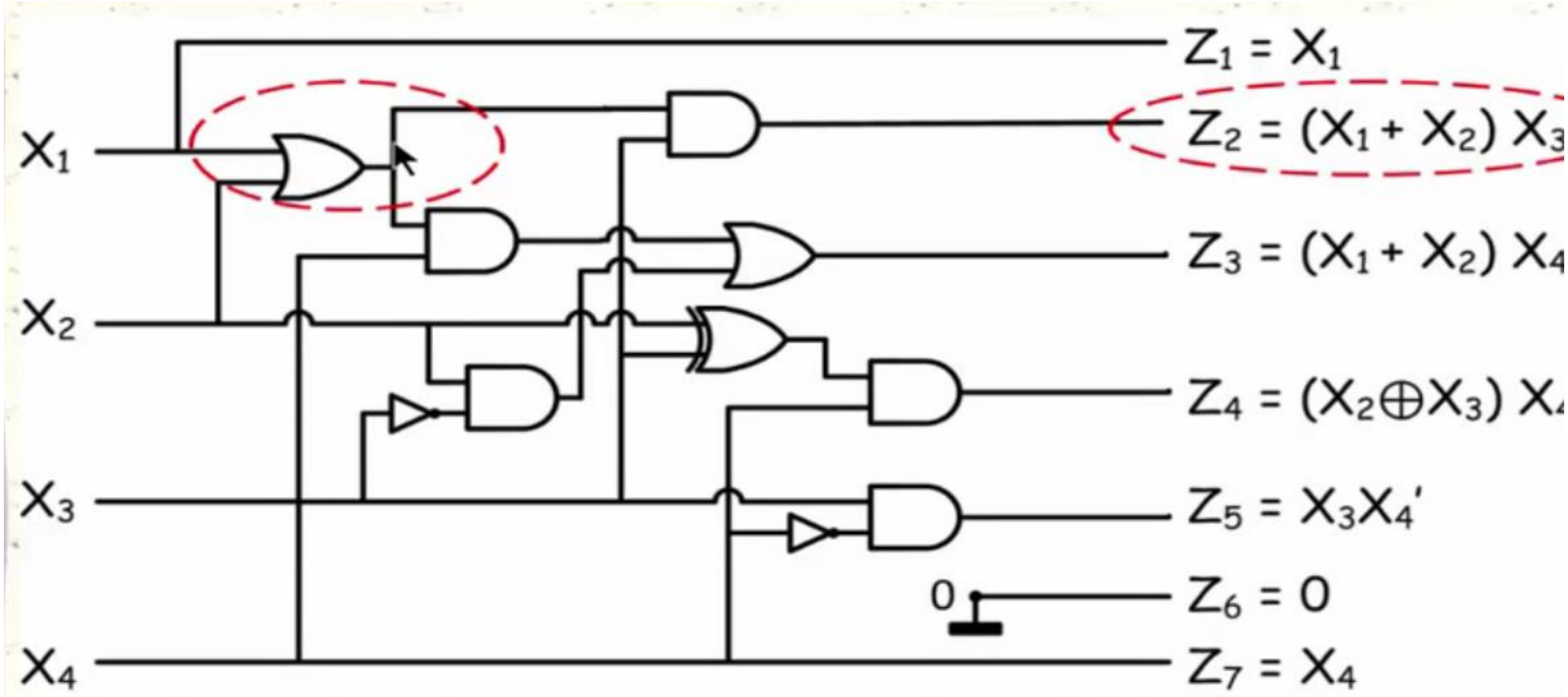
The exact design requirements

X_1	X_2	X_3	X_4	X	X^2	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7
0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	1	1	0	0	0	0	0	0	1
0	0	1	0	2	4	0	0	0	0	1	0	0
0	0	1	1	3	9	0	0	0	1	0	0	1
0	1	0	0	4	16	0	0	1	0	0	0	0
0	1	0	1	5	25	0	0	1	1	0	0	1
0	1	1	0	6	36	0	1	0	0	1	0	0
0	1	1	1	7	49	0	1	1	0	0	0	1
1	0	0	0	8	64	1	0	0	0	0	0	0
1	0	0	1	9	81	1	0	1	0	0	0	1

Circuit Logic Design



Modified Logic Design



- $z_1 = x_1$
- $z_2 = x_1 x_3$
- $z_3 = (x_1 + x_2)x_4 + x_2 x_3'$
- $z_4 = (x_2 + x_3)\, x_4$
- $z_5 = x_3 x_4{}'$
- $z_6 = 0$
- $z_7 = x_4$

X_1	X_2	X_3	X_4	X	F(X)	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7
1	0	1	0	10	68	1	0	0	0	1	0	0
1	0	1	1	11	89	1	0	1	1	0	0	1

- $z_1 = x_1$
- $z_2 = (x_1 + x_2)x_3$
- $z_3 = (x_1 + x_2)x_4 + x_2x_3'$
- $z_4 = (x_2 + x_3)\,x_4$
- $z_5 = x_3x_4'$
- $z_6 = 0$
- $z_7 = x_4$

X_1	X_2	X_3	X_4	X	F(X)	Z_1	Z_2	Z_3	Z_4	Z_5	Z_6	Z_7
1	0	1	0	10	100	1	1	0	0	1	0	0
1	0	1	1	11	121	1	1	1	1	0	0	1

Now (10, 100) and (11, 121) become valid.

Thankyou