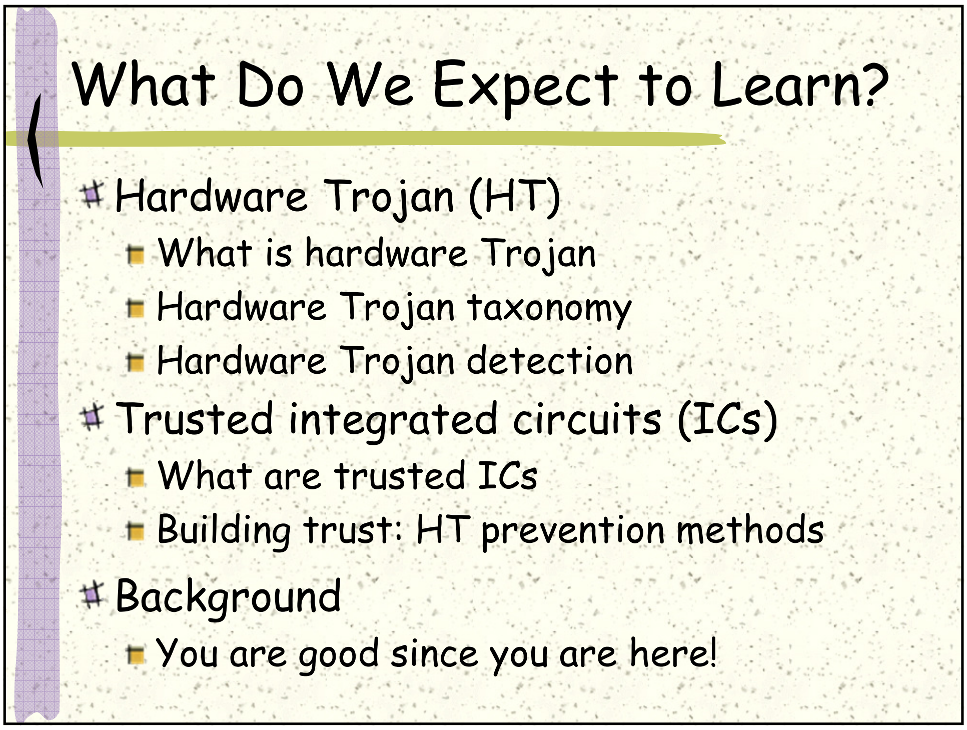
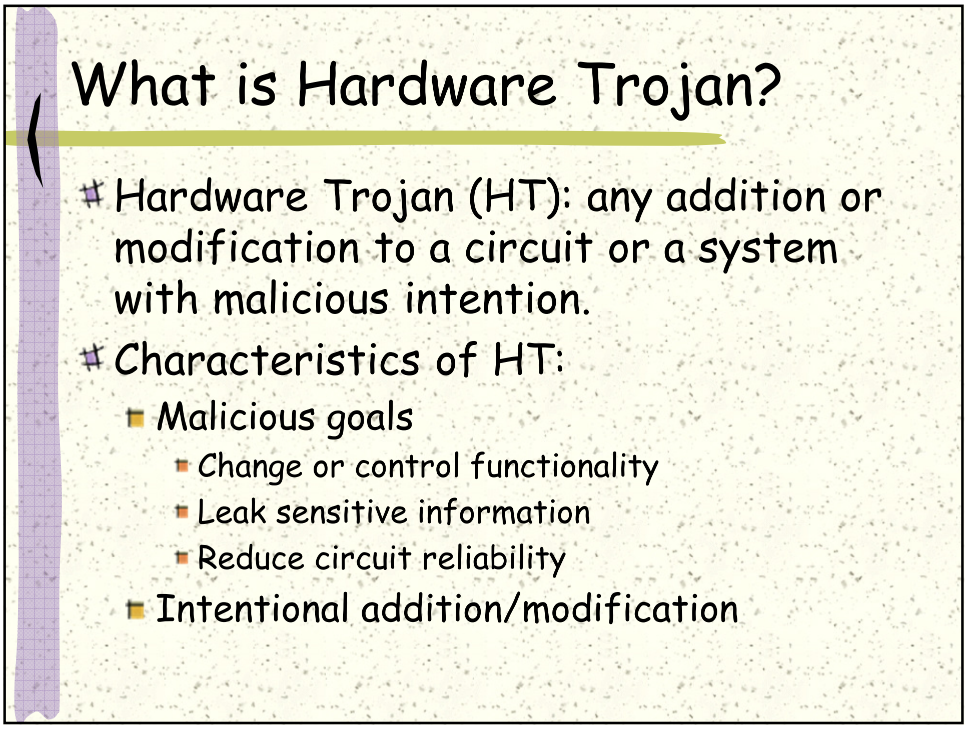
Hardware Security -- Hardware Trojan and Trusted ICs

Cybersecurity Specialization



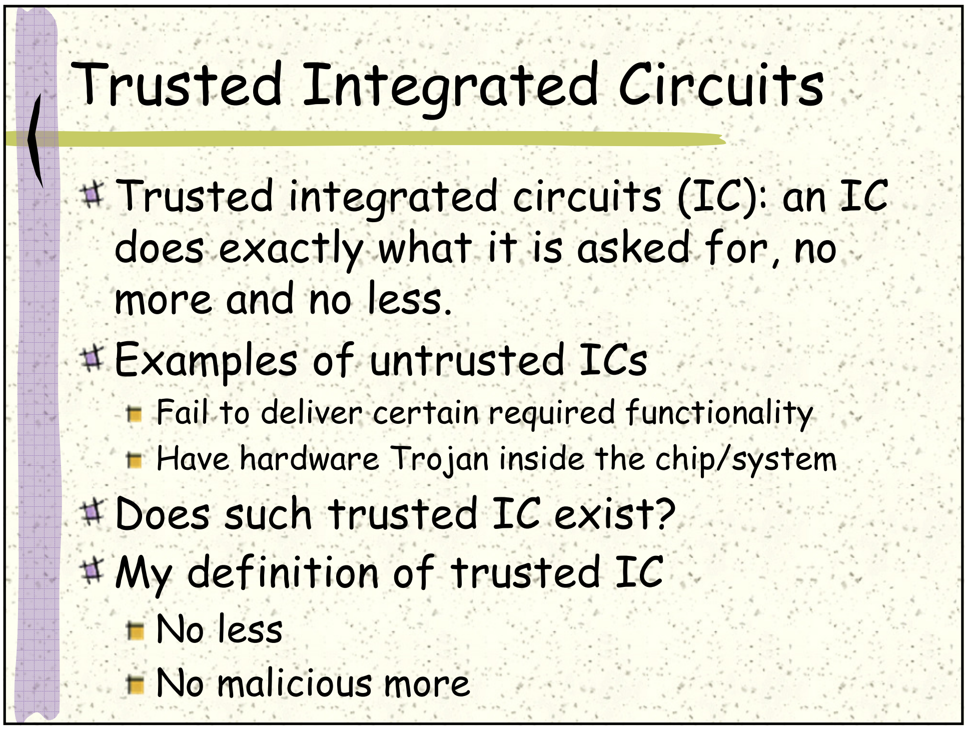
What Do We Expect to Learn?

- Hardware Trojan (HT)
  - What is hardware Trojan
  - Hardware Trojan taxonomy
  - Hardware Trojan detection
- Trusted integrated circuits (ICs)
  - What are trusted ICs
  - Building trust: HT prevention methods
- Background
  - You are good since you are here!



What is Hardware Trojan?

- Hardware Trojan (HT): any addition or modification to a circuit or a system with malicious intention.
- Characteristics of HT:
  - Malicious goals
    - Change or control functionality
    - Leak sensitive information
    - Reduce circuit reliability
  - Intentional addition/modification



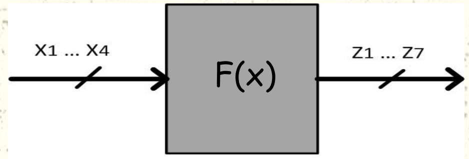
Trusted Integrated Circuits

- Trusted integrated circuits (IC): an IC does exactly what it is asked for, no more and no less.
- Examples of untrusted ICs
  - Fail to deliver certain required functionality
  - Have hardware Trojan inside the chip/system
- Does such trusted IC exist?
- My definition of trusted IC
  - No less
  - No malicious more

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).

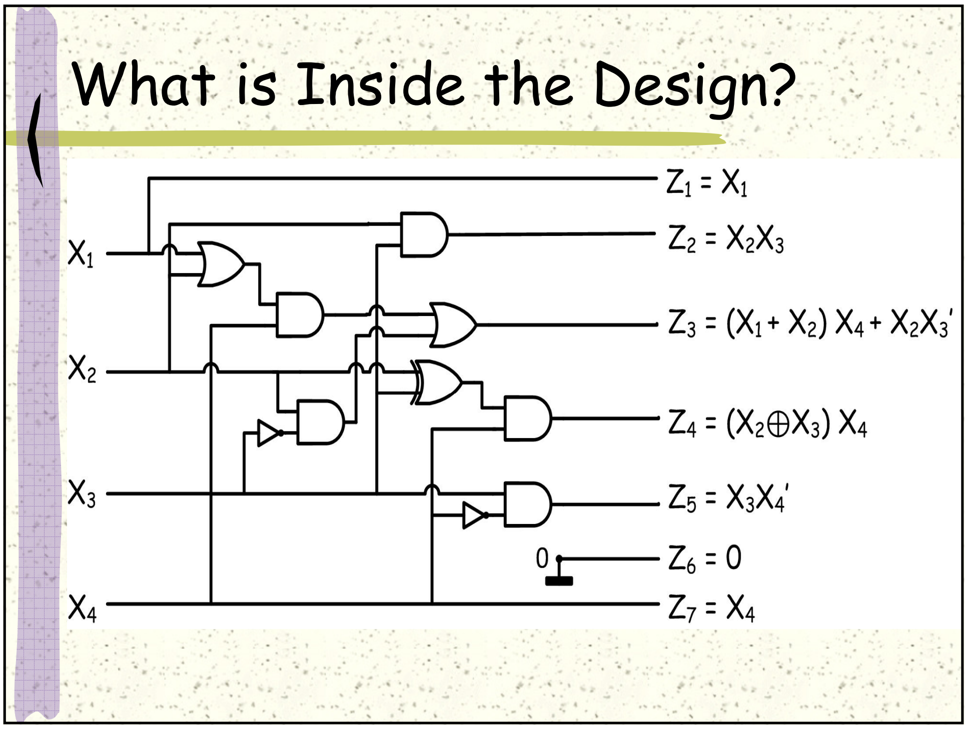
  Assume that $F(x)=x^2$ for x=0,1,2,…,9.
- Bob's design:
  - Input: $\{x_1, x_2, x_3, x_4\}$ (e.g. 0: 0000, 3: 0011)
  - Output: $\{z_1,z_2,z_3,z_4,z_5,z_6,z_7\}$ (e.g. 81:1010001)
  - Functionality: $z = F(x)=x^2$



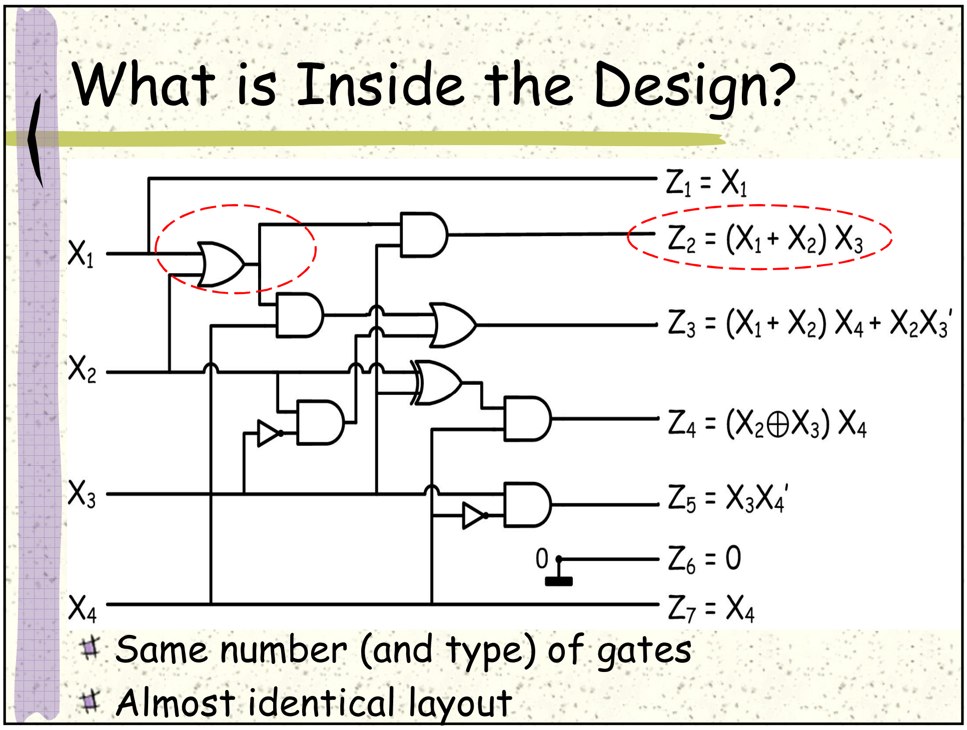
The Exact Design Requirements

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

Hint: some early quiz question ☺

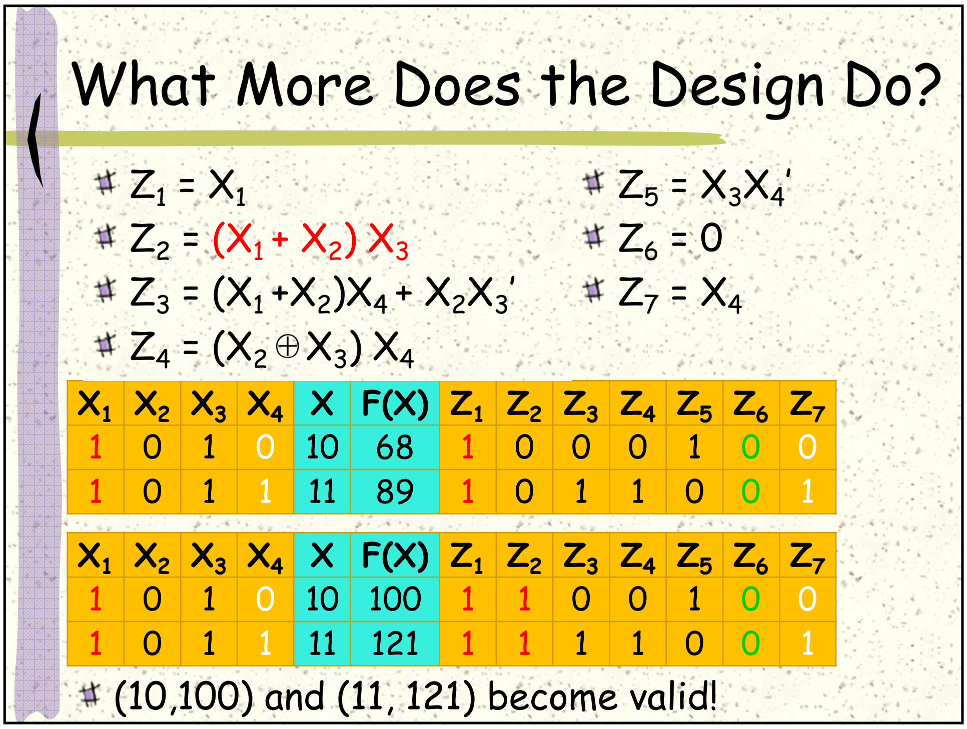


What is Inside the Design?



What is Inside the Design?

- Same number (and type) of gates
- Almost identical layout



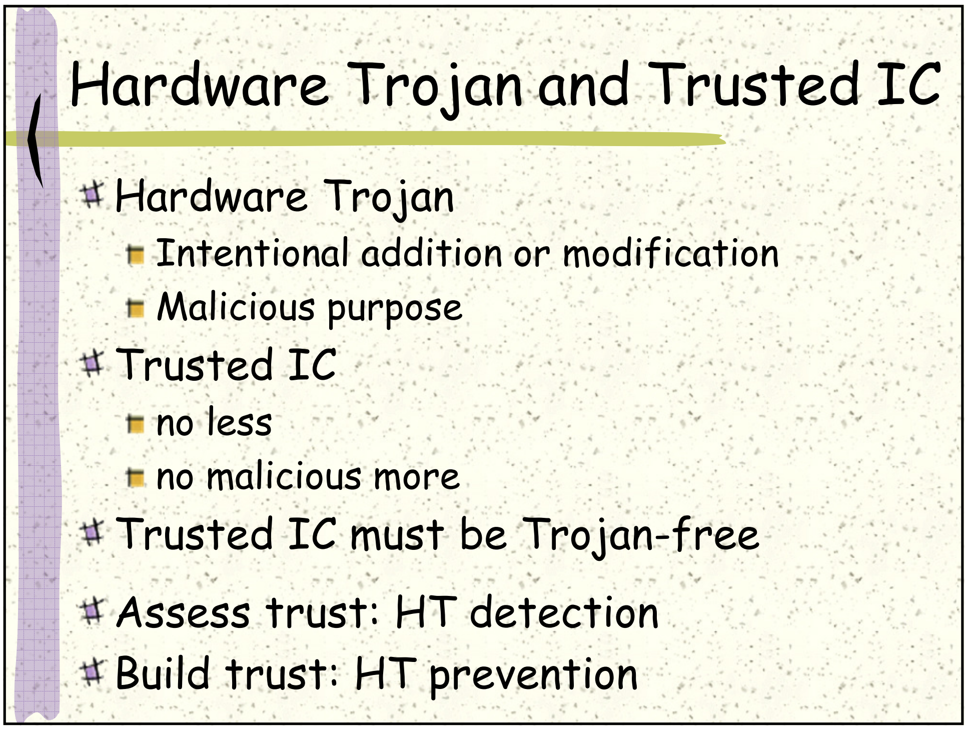
What More Does the Design Do?

- $Z_1 = X_1$
- $Z_2 = (X_1 + X_2) X_3$
- $Z_3 = (X_1 + X_2)X_4 + X_2X_3'$
- $Z_4 = (X_2 \oplus X_3) X_4$
- $Z_5 = X_3X_4'$
- $Z_6 = 0$
- $Z_7 = X_4$

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	68	1	0	0	0	1	0	0
1	0	1	1	11	89	1	0	1	1	0	0	1

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

- (10,100) and (11, 121) become valid!



Hardware Trojan and Trusted IC

- Hardware Trojan
  - Intentional addition or modification
  - Malicious purpose
- Trusted IC
  - no less
  - no malicious more
- Trusted IC must be Trojan-free
- Assess trust: HT detection
- Build trust: HT prevention