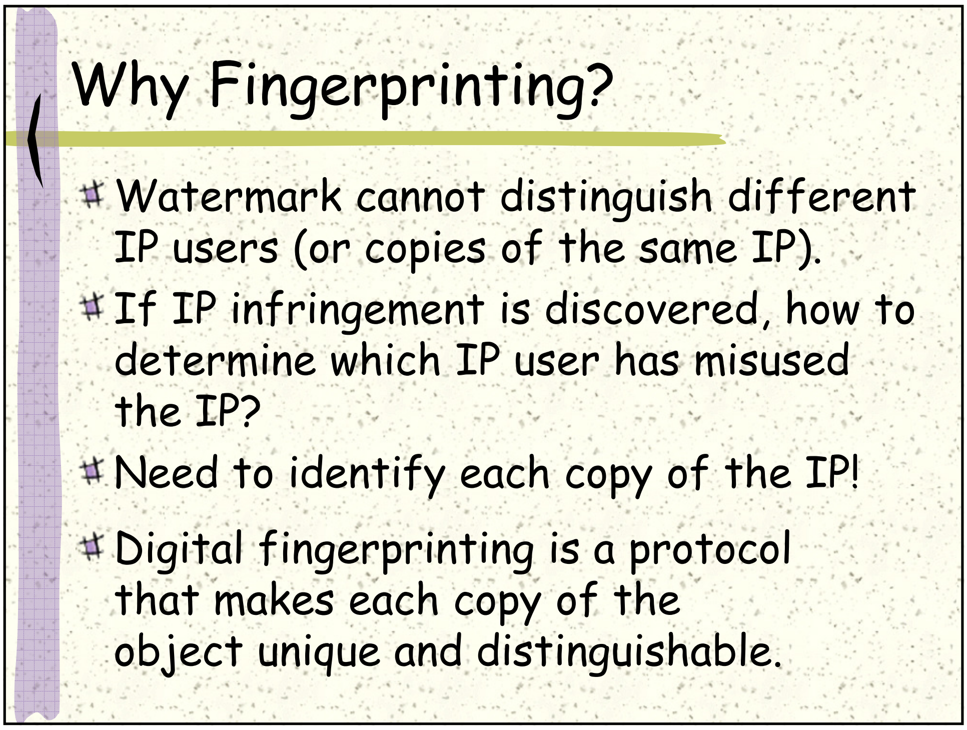
Intellectual Property Protection -- Fingerprinting

Cybersecurity Specialization
-- Hardware Security



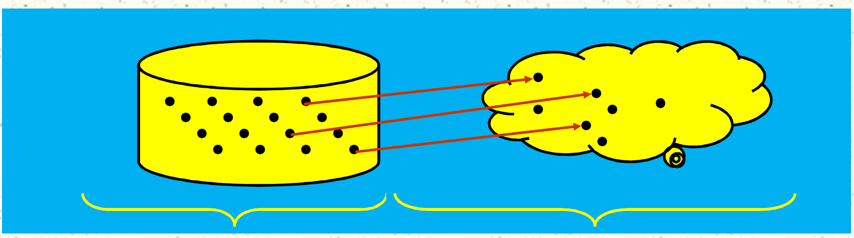
Why Fingerprinting?

- Watermark cannot distinguish different IP users (or copies of the same IP).
- If IP infringement is discovered, how to determine which IP user has misused the IP?
- Need to identify each copy of the IP!
- Digital fingerprinting is a protocol that makes each copy of the object unique and distinguishable.

Fingerprinting vs. Watermarking

- Both are (invisible) identification codes permanently embedded as an integral part within a design for IPP.
  - Watermark: same for all copies
  - Fingerprint: unique for each copy
- Fingerprint = multiple distinct watermarks
- Basic needs for fingerprinting methods:
  - Effective method to create fingerprints
  - Collusion-free distribution of fingerprints

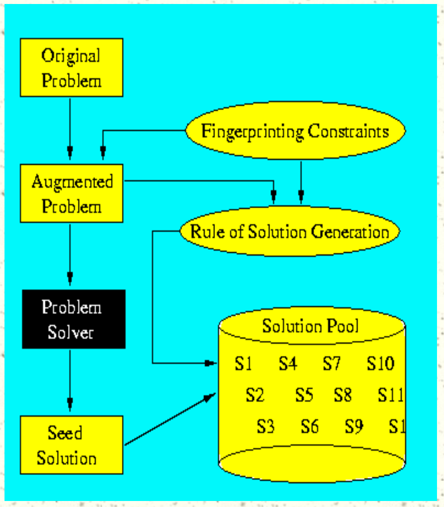
Approach and Challenges



Generation protocol
- Quantity
- Quality
- Run-time

Distribution protocol
- Uniqueness
- Robustness
- Collusion-free

Two Fingerprinting Techniques



Original Problem

Fingerprinting Constraints

Augmented Problem

Rule of Solution Generation

Problem Solver

Solution Pool

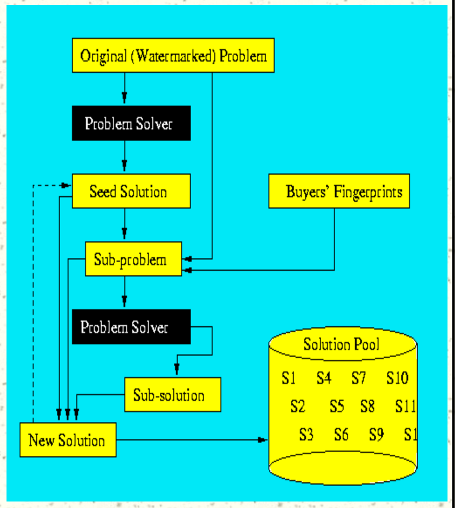
S1 S4 S7 S10

S2 S5 S8 S11

S3 S6 S9 S1

Seed Solution

Constraint addition



Original (Watermarked) Problem

Problem Solver

Seed Solution

Buyers' Fingerprints

Sub-problem

Problem Solver

Solution Pool

S1 S4 S7 S10

S2 S5 S8 S11

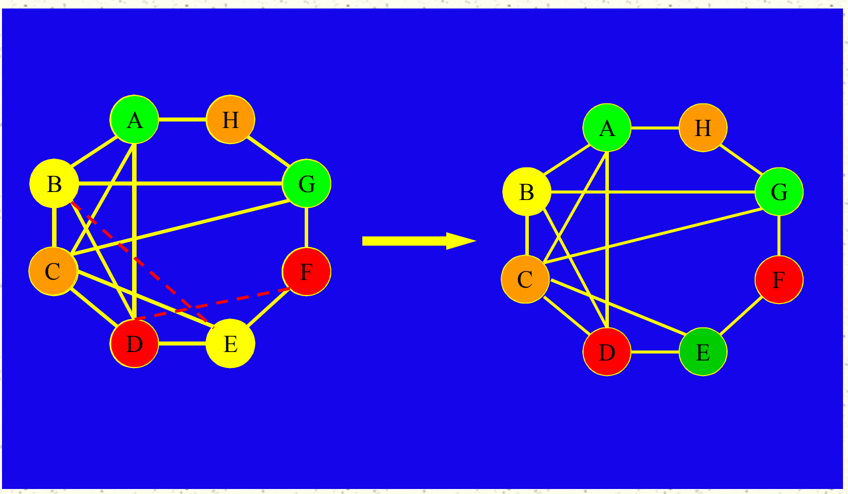
S3 S6 S9 S1

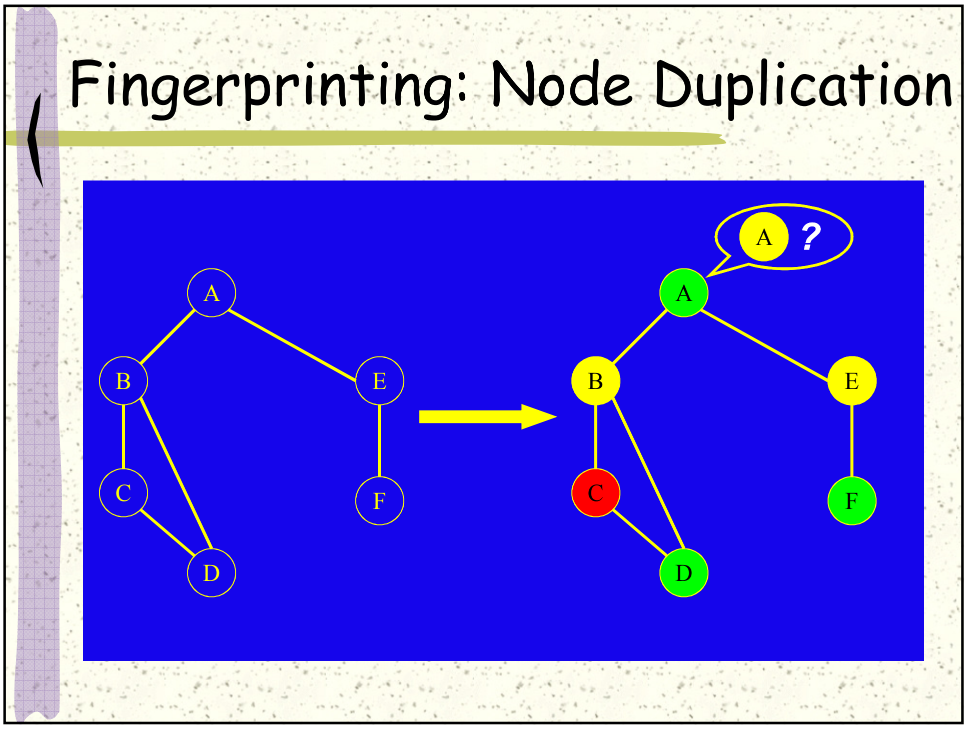
Sub-solution

New Solution

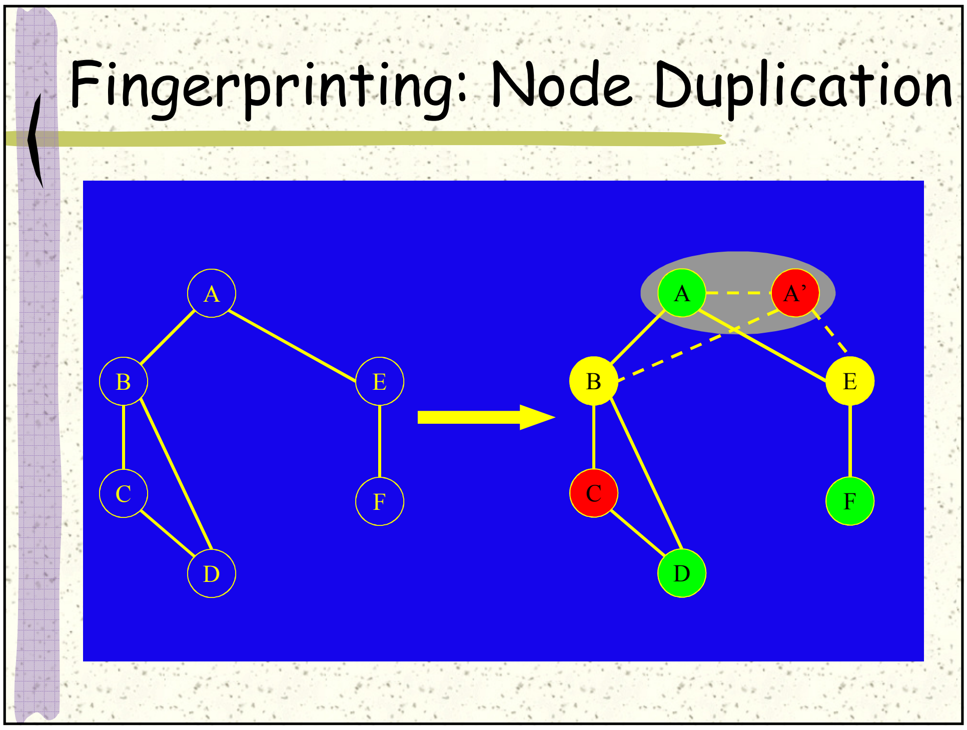
Iterative technique

Fingerprinting: Iterative Approach



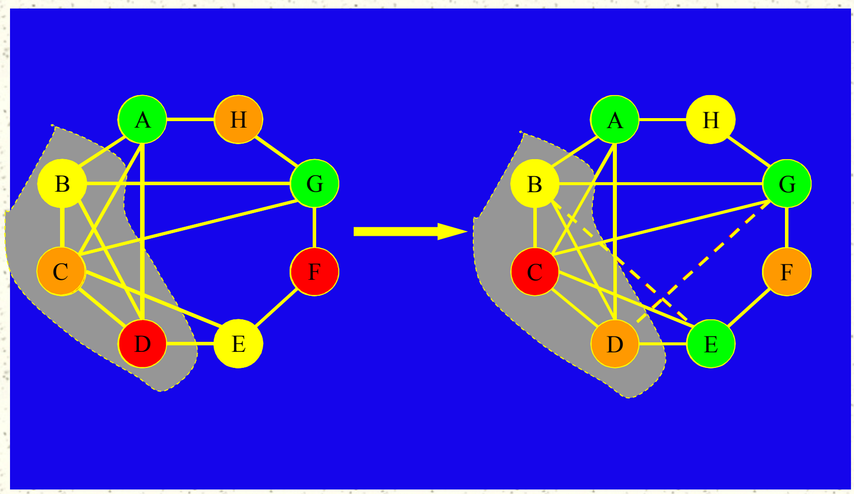


Fingerprinting: Node Duplication

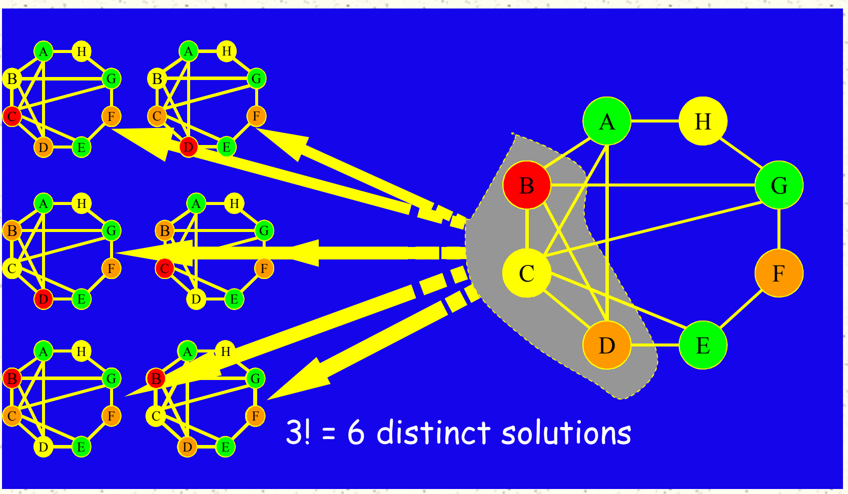


Fingerprinting: Node Duplication

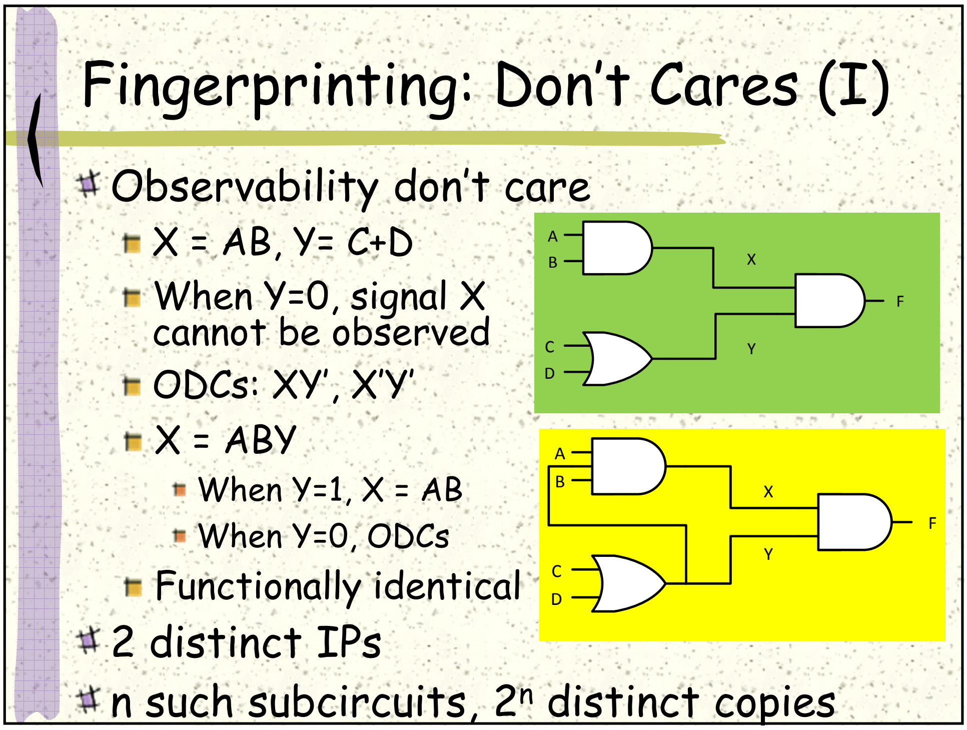
Fingerprinting: Clique Manipulation



Fingerprinting: Clique Manipulation

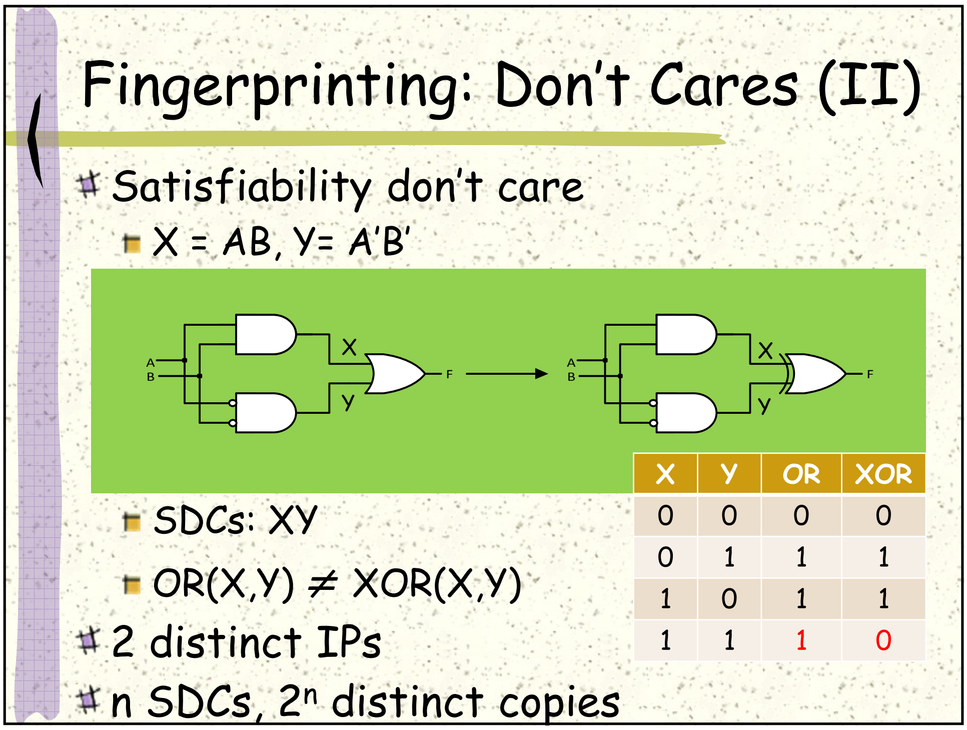


3! = 6 distinct solutions



Fingerprinting: Don't Cares (I)

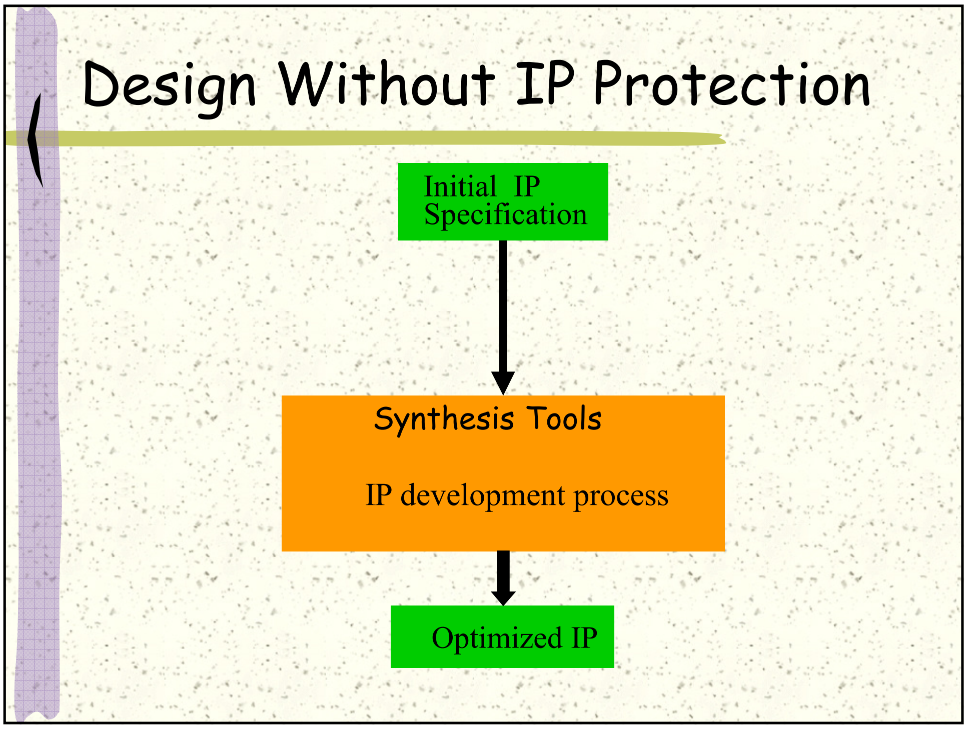
- Observability don't care
  - X = AB, Y= C+D
  - When Y=0, signal X cannot be observed
  - ODCs: XY', X'Y'
  - X = ABY
    - When Y=1, X = AB
    - When Y=0, ODCs
  - Functionally identical
- 2 distinct IPs
- n such subcircuits, 2^n distinct copies



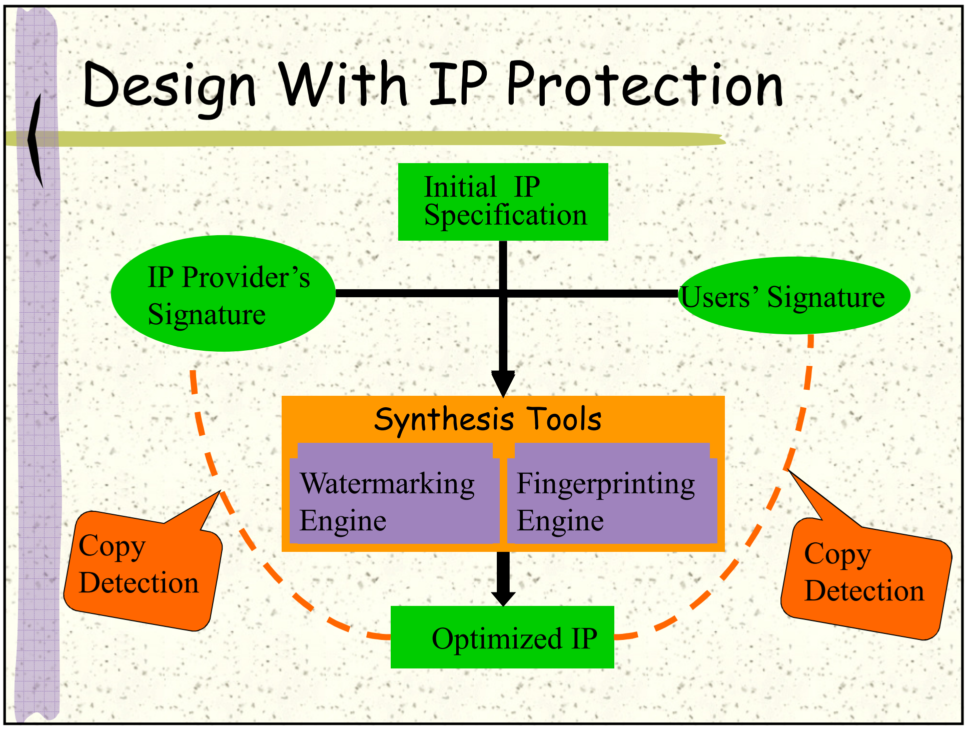
Fingerprinting: Don't Cares (II)

- Satisfiability don't care
  - X = AB, Y= A'B'
  - SDCs: XY
  - OR(X,Y) ≠ XOR(X,Y)
- 2 distinct IPs
- n SDCs, 2^n distinct copies

X	Y	OR	XOR
0	0	0	0
0	1	1	1
1	0	1	1
1	1	1	0



Design Without IP Protection



Design With IP Protection