Emmy Noether-Programm
DFG Deutsche Forschungsgemeinschaft
Funded by
DFG Deutsche Forschungsgemeinschaft
German Research Foundation
CASA Cyber Security in the Age of Large-Scale Adversaries
Ruhr Universität Bochum
RUB

AUTOMATED VERIFICATION OF PHYSICAL SECURITY PROPERTIES

PASCAL SASDRICH

ACKNOWLEDGEMENT

JAN RICHTER-BROCKMANN

JAKOB FELDTKELLER

THE BOCHUM CYBERSECURITY ECOSYSTEM

A UNIQUE SECURITY ECOSYSTEM

- Leading research institutions: 300 researchers, 1000 students
- Numerous successful start-ups, supported through incubator
- Home of various established companies (G-Data, escrypt)

COMPUTER-AIDED VERIFICATION (CAVE) GROUP

ACTIVE AND PASSIVE PHYSICAL IMPLEMENTATION ATTACKS

- Side-Channel Analysis (SCA)
- Fault-Injection Analysis (FIA)
- Combined Attacks (CA)

FORMAL SECURITY DEFINITIONS AND MODELS

- Adversary models for SCA, FIA, and CA
- Security models and definitions for SCA, FIA, and CA
- Compositional properties of security definitions

COMPUTER-AIDED SECURITY ENGINEERING

- Automated formal verification of physical security properties (today)
- Computer-aided design and generation of secure design
- Automated optimization and automated repair of secure designs

DR.-ING. PASCAL SASDRICH

GROUP LEADER

ARMAND SCHINKEL, M. SC.

PHD CANDIDATE

MOTIVATION | STANDARD ADVERSARY

ADVERSARY CAN SEND AND RECEIVE

INPUTS AND OUTPUTS OF CRYPTOGRAPHIC OPERATIONS

(BLACK-BOX MODEL)

MOTIVATION | PHYSICAL ADVERSARY

ADVERSARY CAN OBSERVE AND MANIPULATE

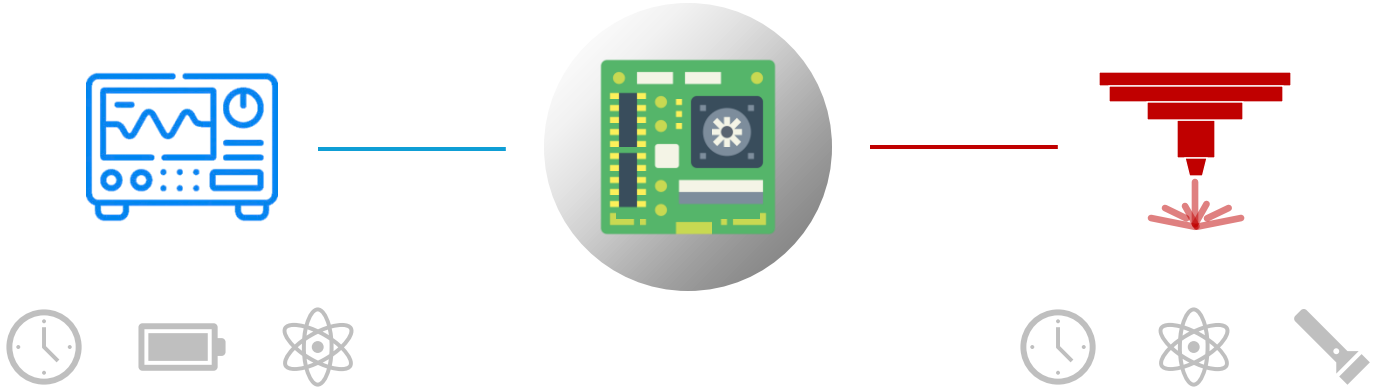
THE PHYSICAL EXECUTION ENVIRONMENT OF THE DEVICE

(GRAY-BOX MODEL)

MOTIVATION | SECURITY TESTING

SIDE-CHANNEL ANALYIS

FAULT INJECTION ANALYIS

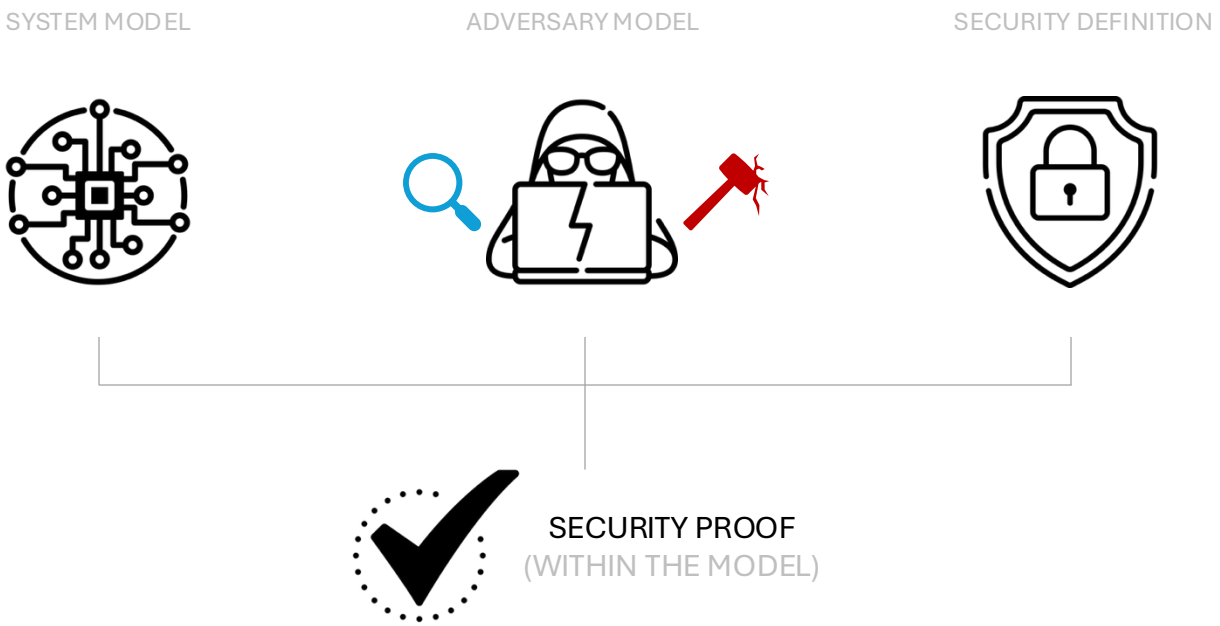


TEST QUALITY IS HIGHLY DEPENDENT ON

EVALUTOR'S RIGOR, EXPERTISE, AND CREATIVITY.

TESTING CANNOT OFFER GUARANTEES.

MOTIVATION | SECURITY VERIFICATION



FORMAL VERIFICATION USES MATHEMATICAL MODELS THAT

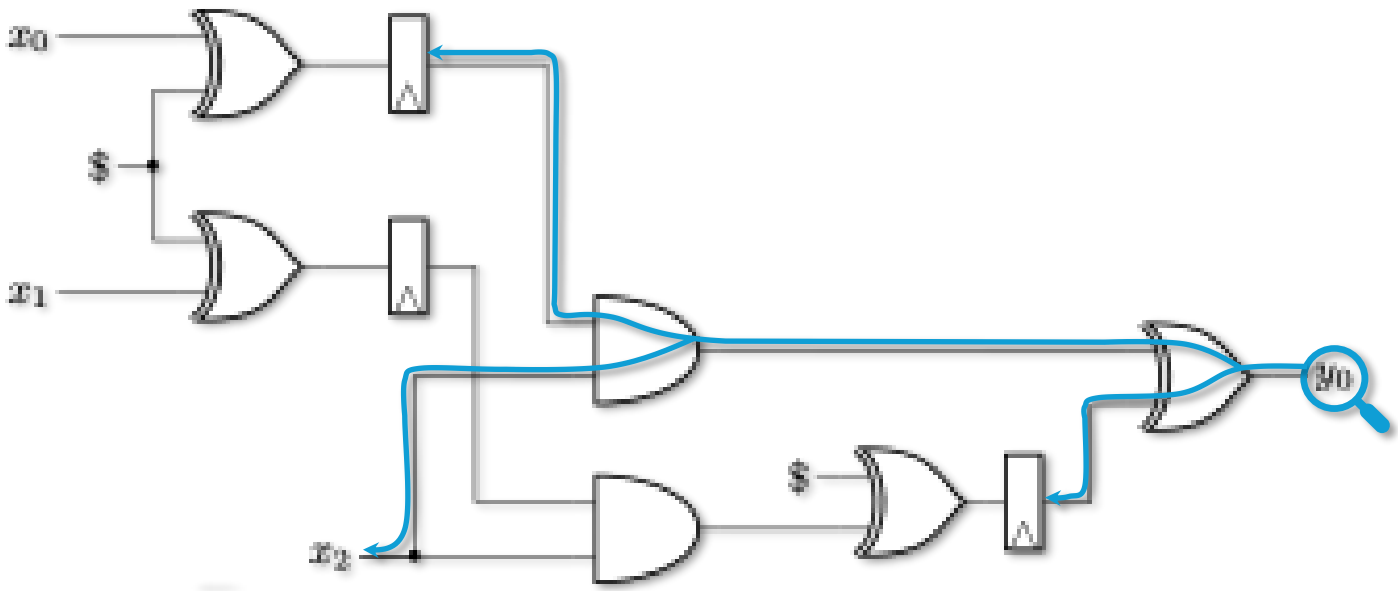
REPRESENT SYSTEMS AND ATTACKERS TO PROOF SECURITY

(WITHIN THE CONSIDERED MODELS)

AGENDA

1. **WHO WE ARE**
2. **MOTIVATION** | WHY SECURITY VERIFICATION?
3. **BACKGROUND** | SECURITY MODELS
4. **VERIFICATION** | TECHNIQUES AND TOOLS
5. **RESULTS** | CASE STUDIES
6. **CONCLUSION**

BACKGROUND | (ROBUST) THRESHOLD PROBING MODEL

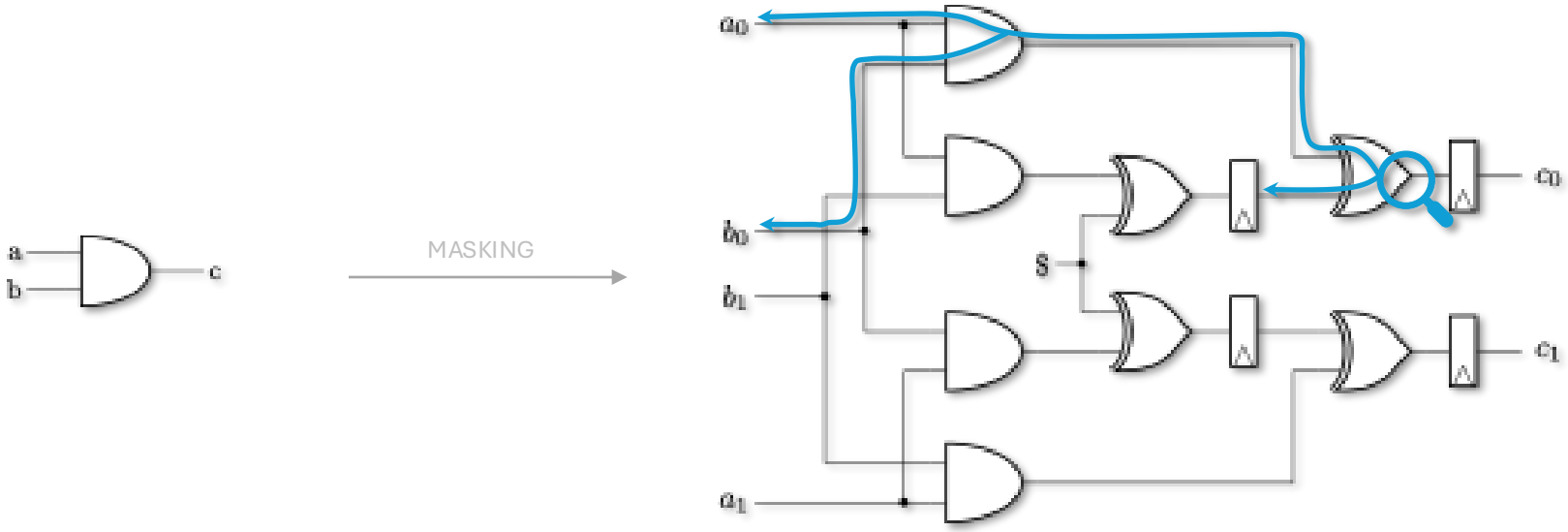


SYSTEM MODEL: DIGITAL LOGIC CIRCUIT
We model digital logic circuits as a directed graph with nodes as digital logic gates and edges as signal wires.

ADVERSARY MODEL: GLITCH-EXTENDED d-THRESHOLD PROBING [ISW03,FGM+18]
Free placement of up to d probes on wires that leak the value of the last stable signals (synchronization points).

SECURITY DEFINITION: d-PROBING SECURITY
Distribution of adversarial any observation (probes) can be simulated without knowledge of any secret.

BACKGROUND | BOOLEAN MASKING



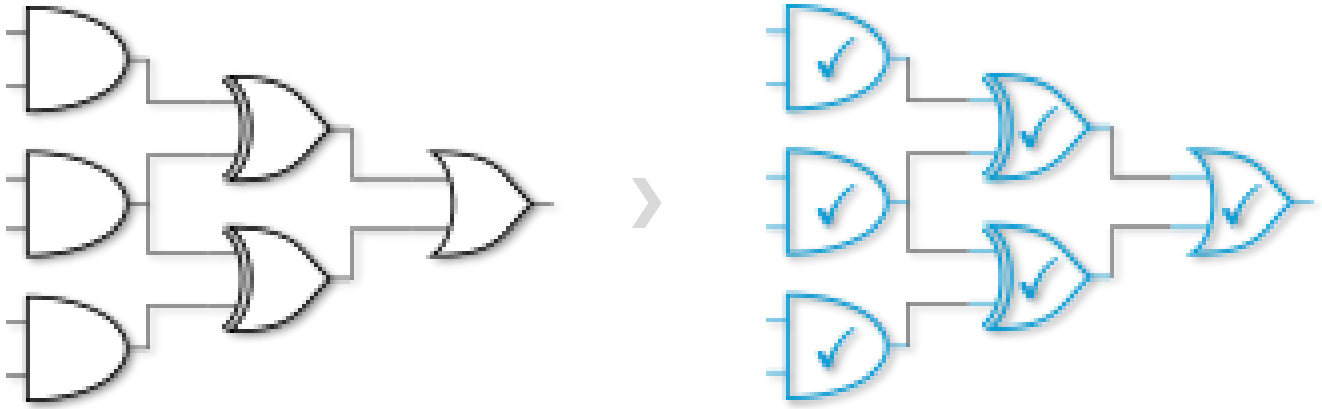
PROTECTION MECHANISM: BOOLEAN MASKING

Each secret bit x is replaced by a vector of bits $\langle x_0, x_1, \ldots, x_{d-1}, x_d \rangle$ such that each true subset is independent of x but $x = x_0 \oplus x_1 \oplus \cdots \oplus x_{d-1} \oplus x_d$.

BACKGROUND | PROTECTION VIA COMPOSITION

GATE-LEVEL

CIRCUIT-LEVEL

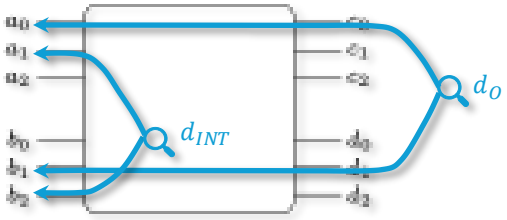


INSECURE GATES ARE REPLACED BY

SECURELY MASKED GADGETS WITH SPECIAL COMPOSABILITY PROPERTIES

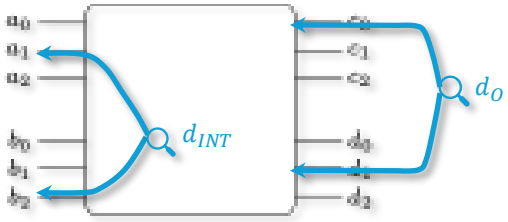
(ALL INPUTS/OUTPUTS ARE SHARED)

BACKGROUND | PROBING COMPOSABILITY



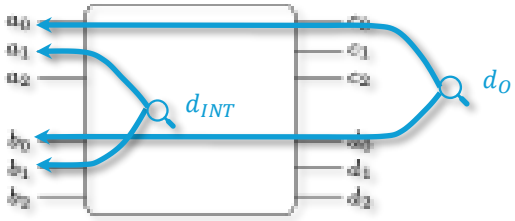
PNI [BBD+15]
PROBE NON-INTERFERENCE

$d_{INT} + d_O \leq d$



PSNI [BBD+16]
PROBE STRONG NON-INTERFERENCE

$d_{INT} + d_O \leq d$



PINI [CS20]
PROBE-ISOLATING NON-INTERFERENCE

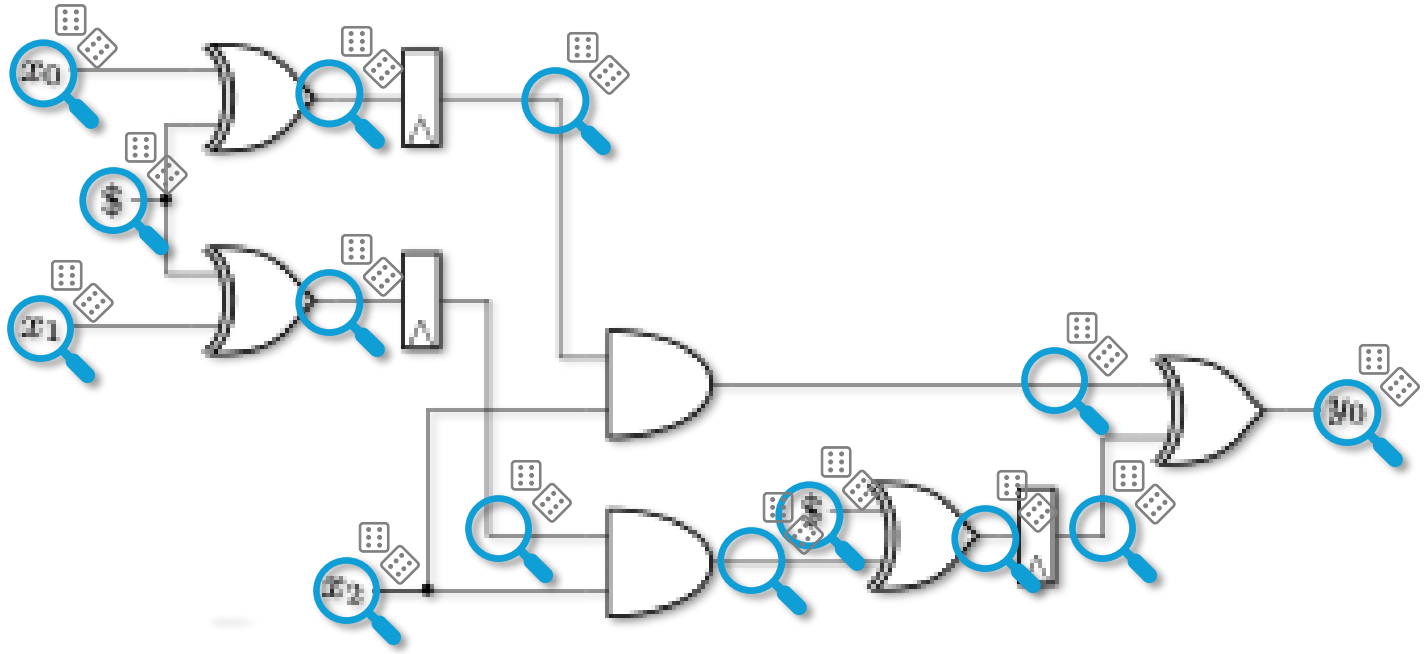
$d_{INT} + d_O \leq d$

PROBING COMPOSABILITY NOTIONS DEFINE

RULES FOR THE CORRECT AND SECURE COMPOSITION OF GADGETS

UNDER PROBE PROPAGATION (INFORMATION FLOW).

BACKGROUND | RANDOM PROBING MODEL

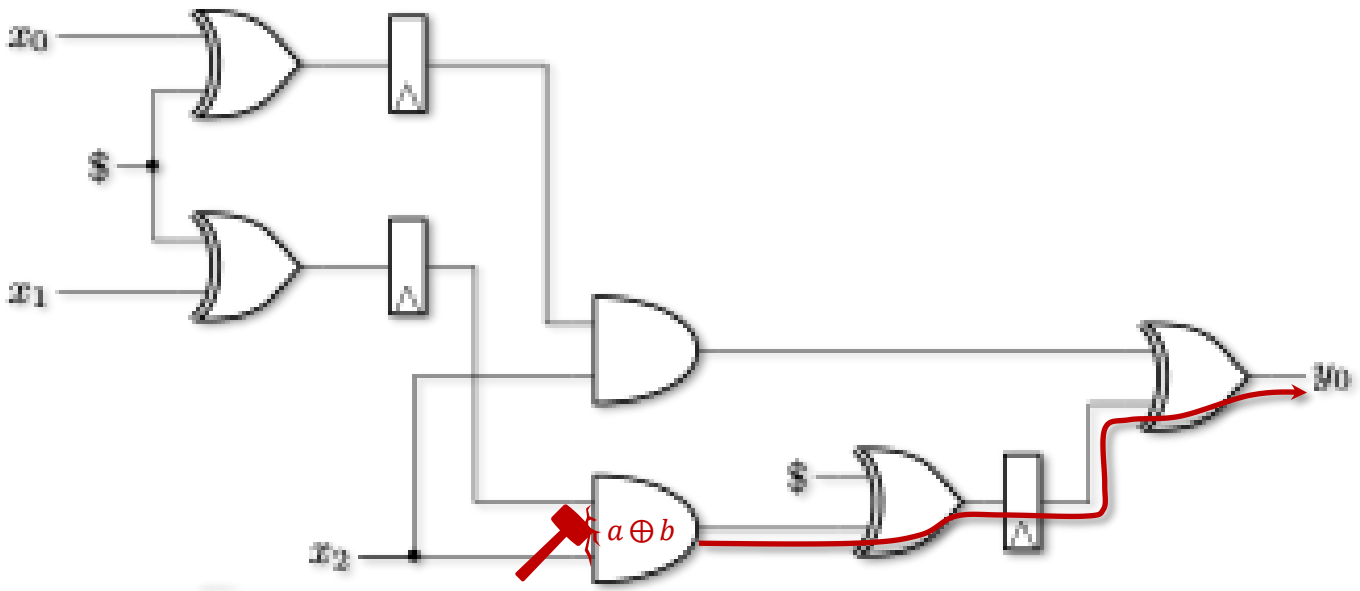


SYSTEM MODEL: DIGITAL LOGIC CIRCUIT
We model digital logic circuits as a directed graph with nodes as digital logic gates and edges as signal wires.

ADVERSARY MODEL: p-RANDOM PROBING [DDF14]
All wires leak information, but each individual wire only leaks with probability p.

SECURITY DEFINITION: (p, ϵ)-RANDOM PROBING SECURITY [DDF14]
A circuit is (p, ϵ)-random probing secure if the probability of leaking secret information is bounded by ϵ.

BACKGROUND | THRESHOLD FAULTING MODEL

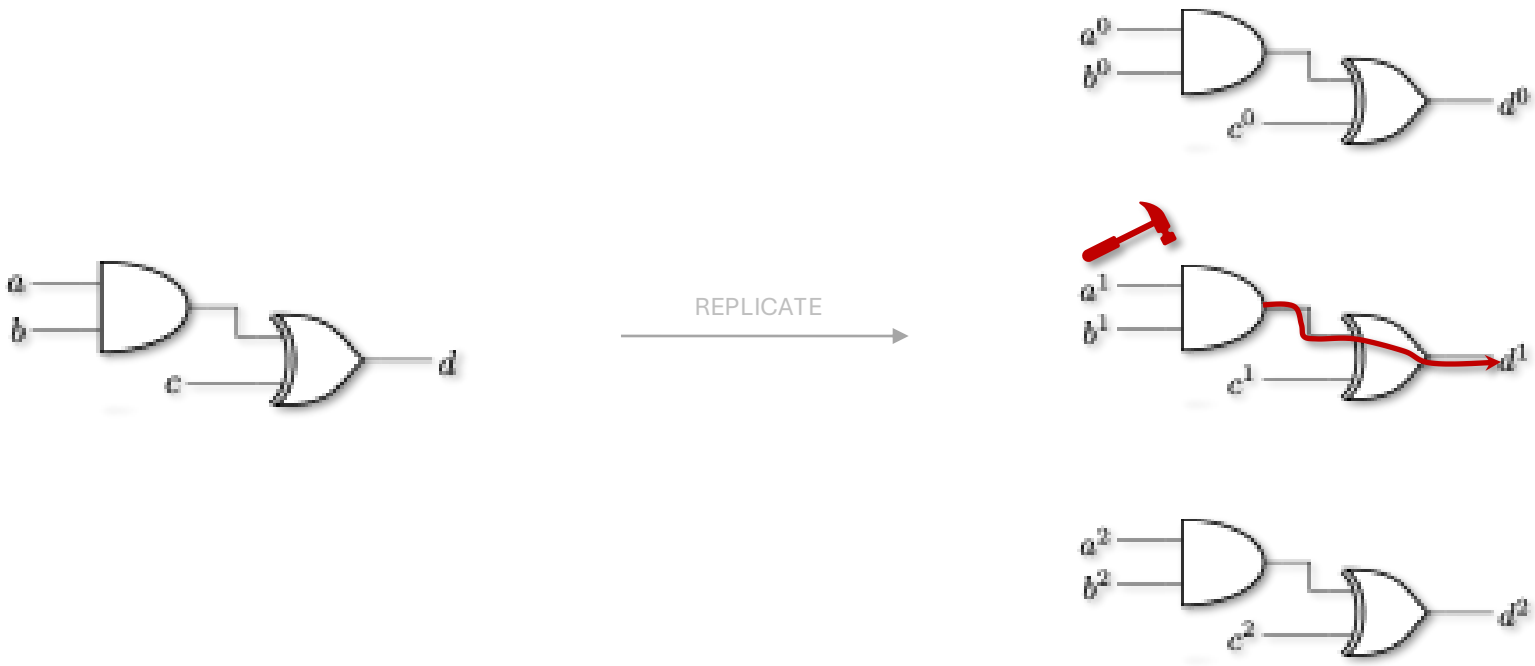


SYSTEM MODEL: DIGITAL LOGIC CIRCUIT
We model digital logic circuits as a directed graph with nodes as digital logic gates and edges as signal wires.

ADVERSARY MODEL: k-THRESHOLD FAULTING [IPS+06,RSG23]
Free selection of up to k gates which are manipulated according to a chosen fault transformation (fault model).

SECURITY DEFINITION: k-FAULT SECURITY
Faulty behavior can be detected or corrected at the circuit output.

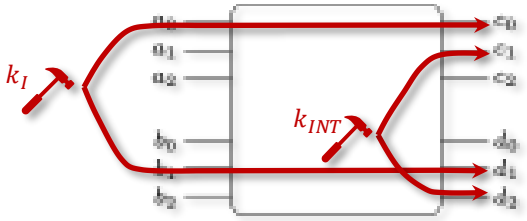
BACKGROUND | REPLICATION



PROTECTION MECHANISM: REPLICATION

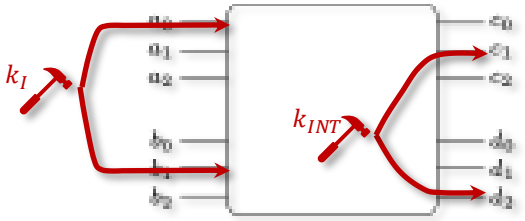
Each bit $\boldsymbol{x}$ is replaced by a vector of bits $\langle \boldsymbol{x^0}, \boldsymbol{x^1}, \ldots, \boldsymbol{x^{n-1}}, \boldsymbol{x^n} \rangle$ such that $x^i = x^j$.

BACKGROUND | FAULTING COMPOSABILITY



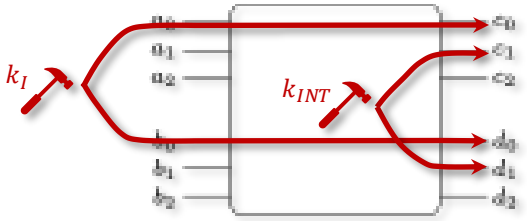
FNI [DN20]
FAULT NON-INTERFERENCE

$\underline{k_I + k_{INT}} \leq k$



FSNI [DN20]
FAULT STRONG NON-INTERFERENCE

$k_I + \underline{k_{INT}} \leq k$



FINI [FRS+22]
FAULT-ISOLATING NON-INTERFERENCE

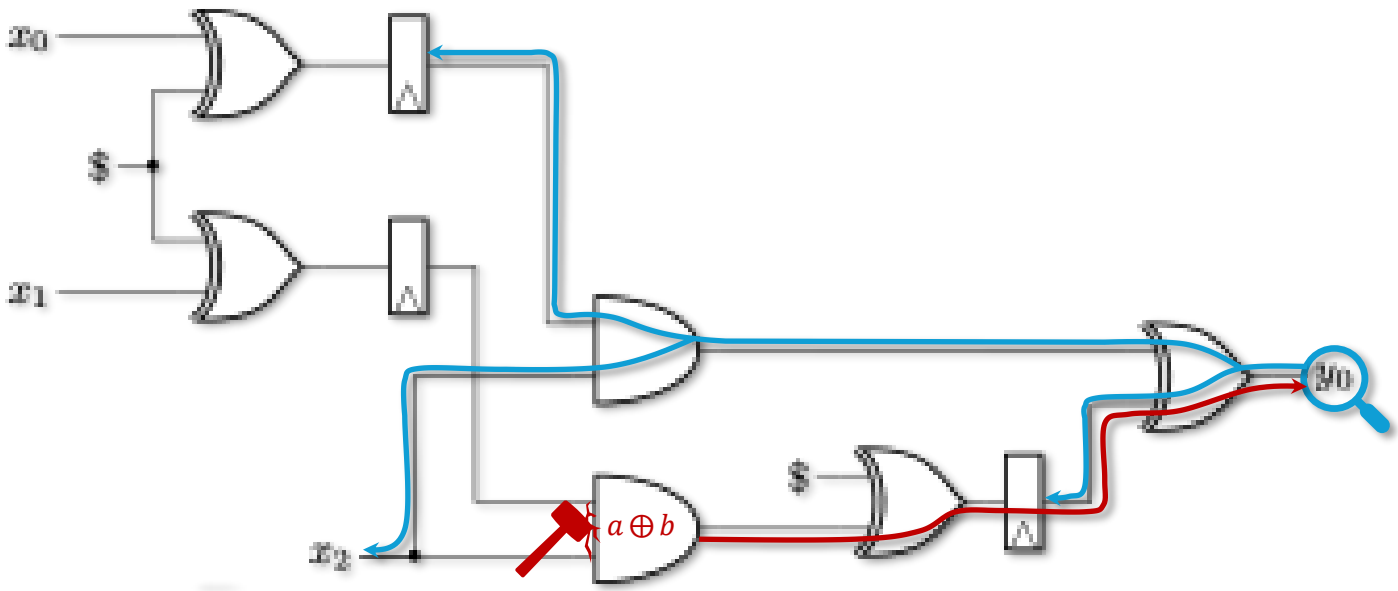
$\underline{k_I + k_{INT}} \leq k$

FAULTING COMPOSABILITY NOTIONS DEFINE

RULES FOR THE CORRECT AND SECURE COMPOSITION OF GADGETS

UNDER FAULT PROPAGATION (INFORMATION FLOW).

BACKGROUND | THRESHOLD COMBINED MODEL

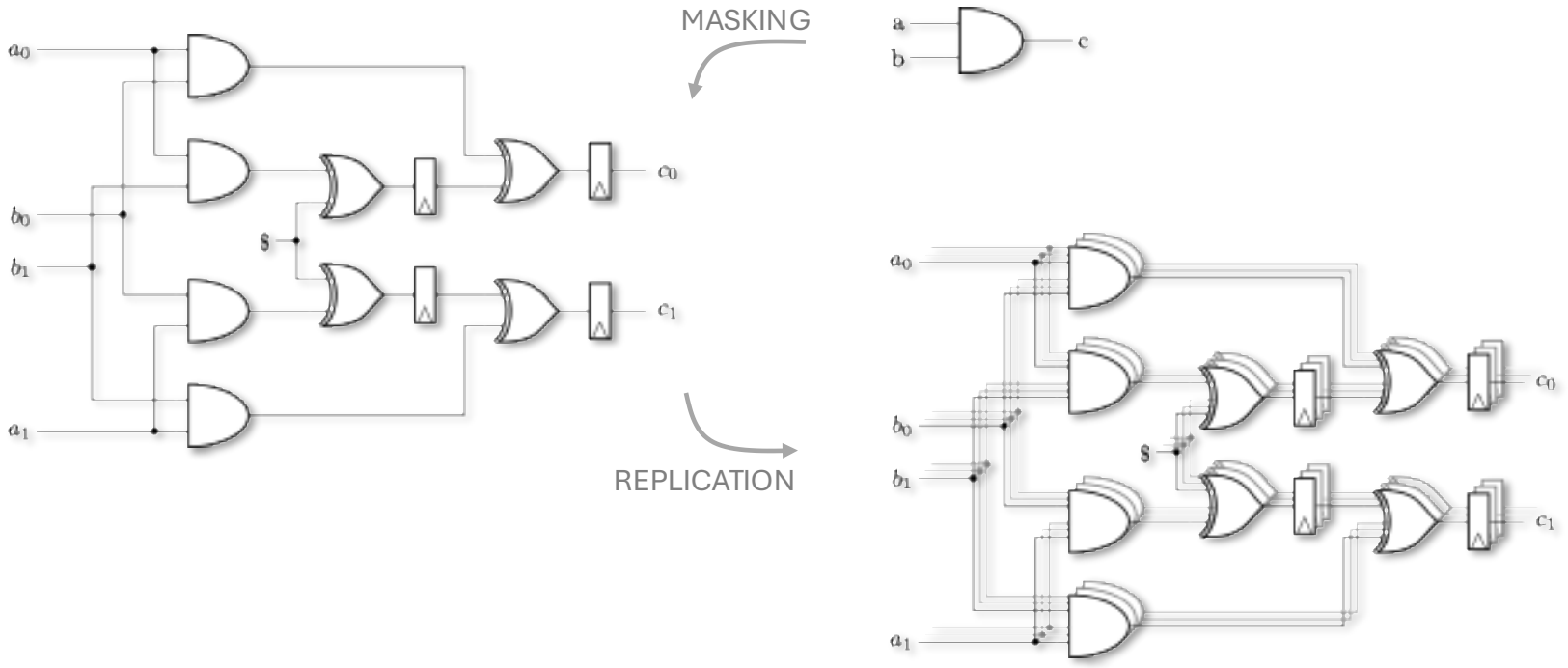


SYSTEM MODEL: DIGITAL LOGIC CIRCUIT
We model digital logic circuits as a directed graph with nodes as digital logic gates and edges as signal wires.

ADVERSARY MODEL: (d,k)-THRESHOLD COMBINED PROBING AND FAULTING [DN20,RFS+22]
Free placement of up to ***k* faults** on gates or randomness and up to ***d* probes** on wires.

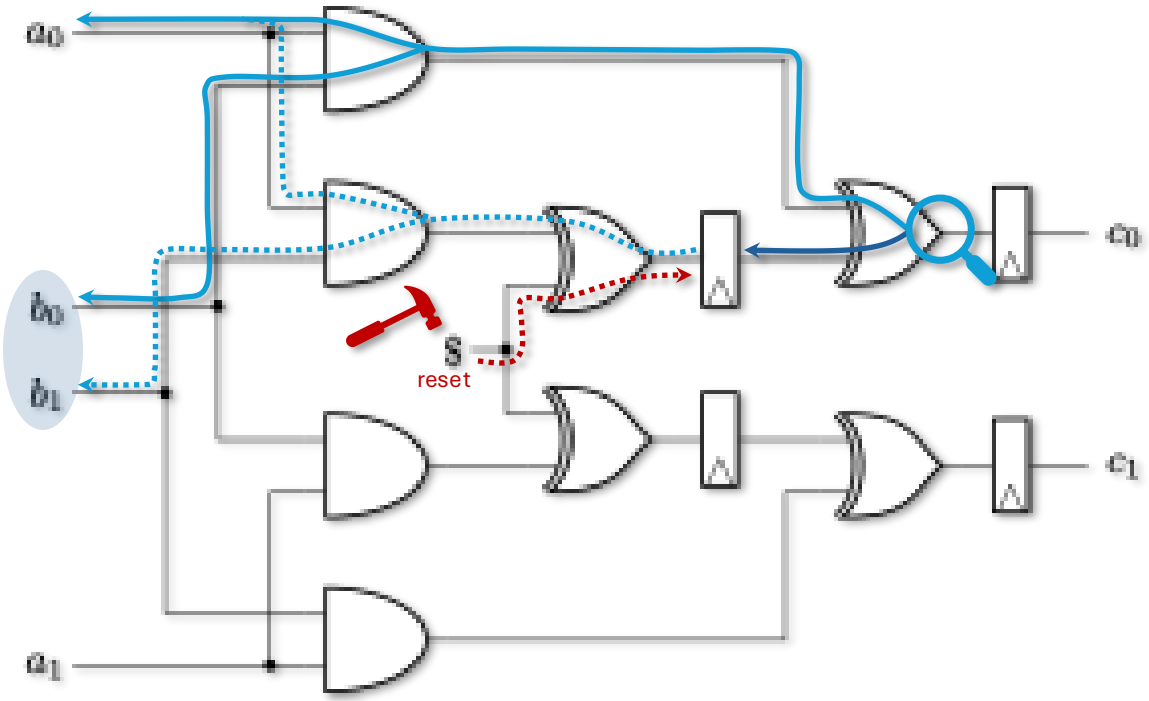
SECURITY DEFINITION: (d,k)-COMBINED SECURITY
Faulty behavior can be detected/corrected at the output (integrity) and the distribution of the adversarial observation (probes) in the faulty circuit can be simulated without access to any secret (confidentiality).

BACKGROUND | MASKING & REPLICATION



PROTECTION MECHANISM: MASK-THEN-REPLICATE
Combination of countermeasures is non-trivial, due to reciprocal effects, e.g., **removal of entropy** and **conditional fault propagation**.

BACKGROUND | REMOVAL OF ENTROPY

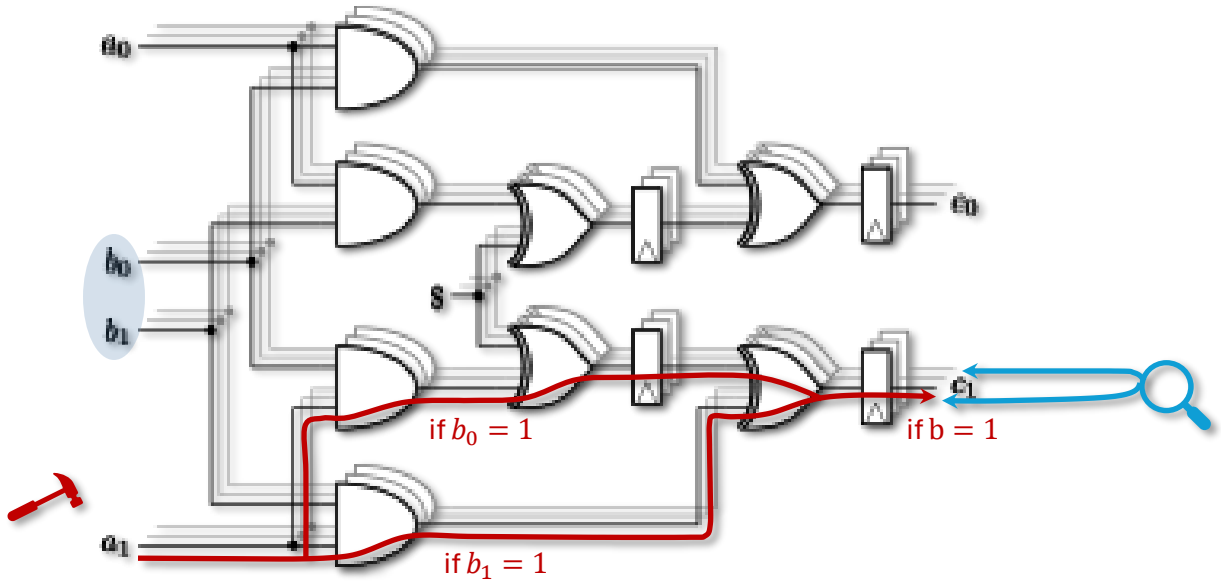


THE REMOVAL OF ENTROPY (THROUGH FAULTS) CAN RESULT IN

ENHANCEMENT OF PROBE PROPAGATION

(LEAKAGE INFORMATION FLOW).

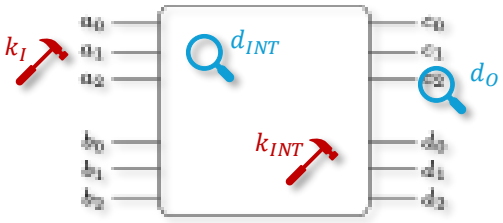
BACKGROUND | CONDITIONAL FAULT PROPAGATION



CONDITIONAL FAULT PROPAGATION CAN RESULT IN

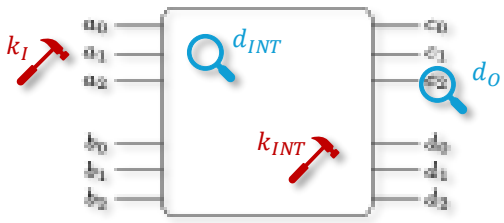
LEAKAGE THAT IS OBSERVABLE THPROUGH THE EFFECTIVENESS OF FAULTS.

BACKGROUND | COMBINED COMPOSABILITY



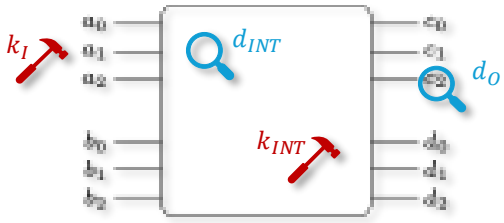
CNI [DN20]
COMBINED NON-INTERFERENCE

$$d_{INT} + d_O + k_I + k_{INT} \leq d$$
$$k_I + k_{INT} \leq k$$



CSNI [DN20]
COMBINED STRONG NON-INTERFERENCE

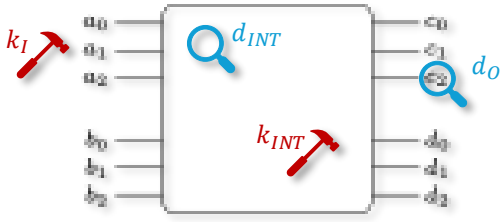
$$d_{INT} + d_O + k_I + k_{INT} \leq d$$
$$k_I + k_{INT} \leq k$$



CINI [FRS+22]
COMBINE-ISOLATING NON-INTERFERENCE

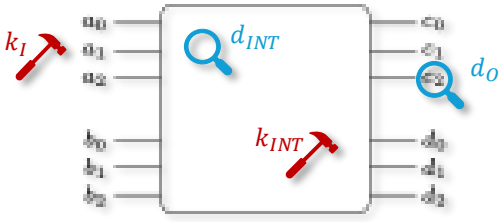
$$d_{INT} + d_O + k_I + k_{INT} \leq d$$
$$k_I + k_{INT} \leq k$$

COMBINED COMPOSABILITY NOTIONS DEFINE **RULES FOR THE CORRECT AND SECURE COMPOSITION OF GADGETS** UNDER PROBE PROPAGATION AND FAULT PROPAGATION (INFORMATION FLOW).



ICSNI [DN20]
INDEPENDENT COMBINED STRONG NON-INTERFERENCE

$$d_{INT} + d_O \leq d$$
$$k_I + k_{INT} \leq k$$



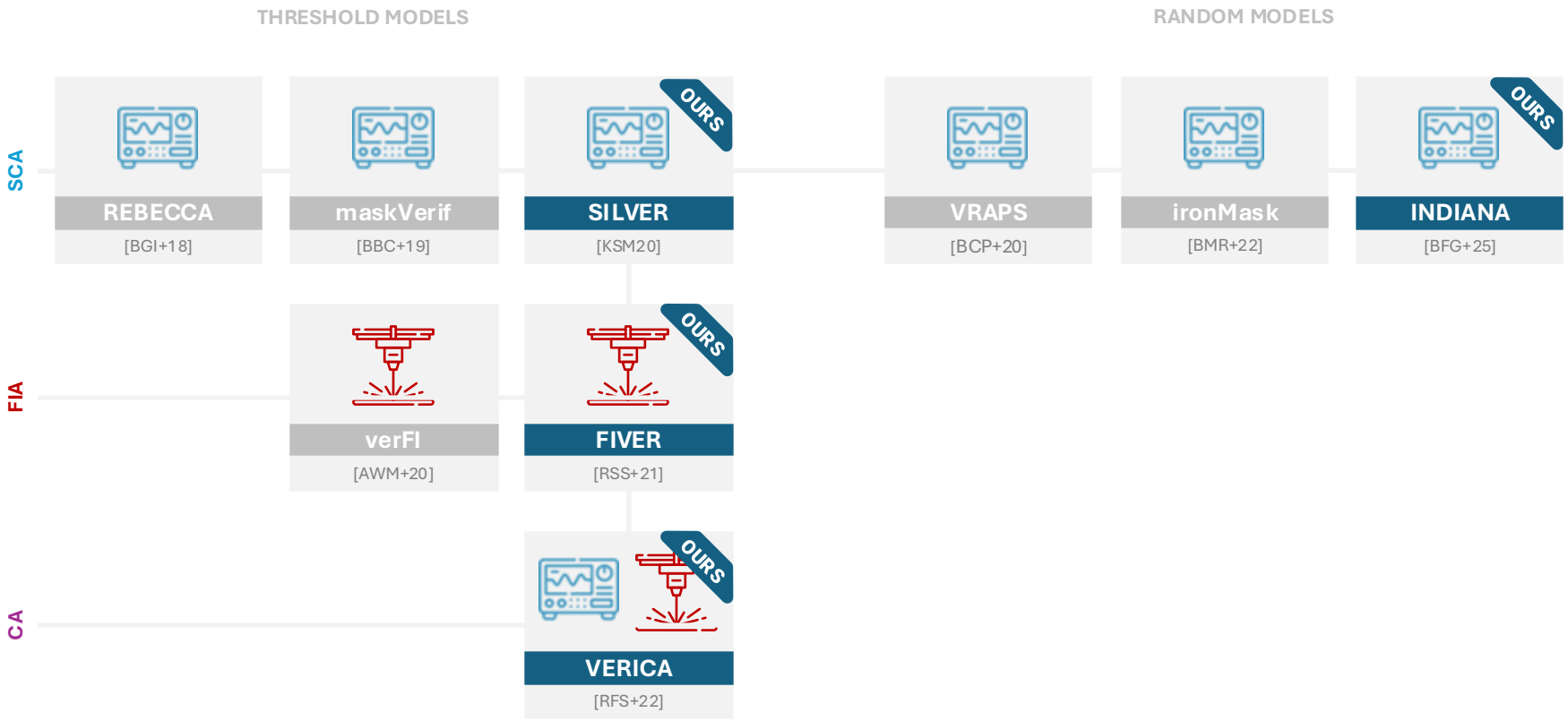
ICINI [FRS+22]
INDEPENDENT COMBINE-ISOLATING NON-INTERFERENCE

$$d_{INT} + d_O + k_I + k_{INT} \leq d$$
$$k_I + k_{INT} \leq k$$

AGENDA

1. **WHO WE ARE**
2. **MOTIVATION** | WHY SECURITY VERIFICATION?
3. **BACKGROUND** | SECURITY MODELS
4. **VERIFICATION** | TECHNIQUES AND TOOLS
5. **RESULTS** | CASE STUDIES
6. **CONCLUSION**

VERIFICATION | TOOL LANDSCAPE



DUE TO THE INCREASING COMPLEXITY OF THE SECURITY MODELS,

STATE-OF-THE-ART REASONING TOOLS ARE **MOSTLY RESTRICTED TO THE THRESHOLD MODELS**

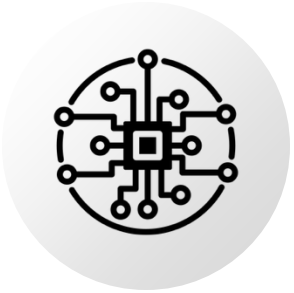
WHILE ONLY VERY FEW TOOLS CONSIDER THE RANDOM MODELS.

VERIFICATION | GENERAL CONCEPT

DESIGN SPECIFICATION

GATE-LEVEL NETLIST (VERILOG)

CIRCUIT MODEL



DIRECTED ACYCLIC GRAPH (DAG)

SYMBOLIC SIMULATION

BINARY DECISION DIAGRAMS (BDDS)

VERIFICATION

STATISTICAL INDEPENDENCE / INDISTINGUISHABILITY

OUR PRACTICAL IMPLEMENTATION OF SECURITY VERIFICATION IS

A MULTI-STAGE PROCESS THAT IS BASED ON

SPECIAL DATA STRUCTURES AND THE REFORMULATION OF SECURITY PROPERTIES.

$$\Pr[\textbf{Probes}|\textbf{Secret}] = \Pr[\textbf{Probes}]$$

A CIRCUIT C WITH SECRET INPUT IS d-THRESHOLD PROBING SECURE, IF AND ONLY IF FOR ANY COMBINATION OF UP TO d PROBED WIRES, THE PROCESSED SECRET IS **STATISTICALLY INDEPENDENT** OF THE OBSERVATION.

VERIFICATION | BINARY DECISION DIAGRAMS (BDDS)

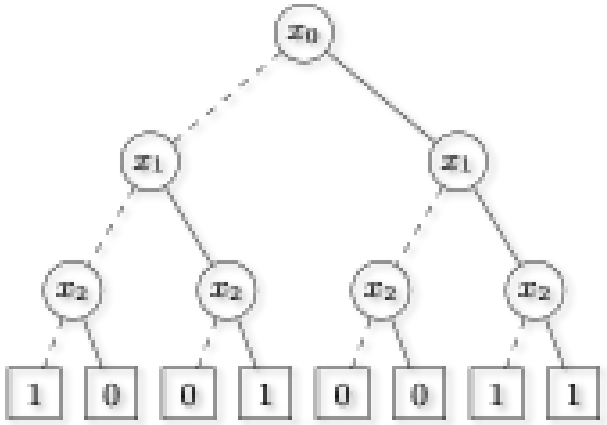
BOOLEAN FUNCTION

$$f = \overline{x_0} \cdot \overline{x_1} \cdot \overline{x_2} + x_0 \cdot x_1 + x_1 \cdot x_2$$

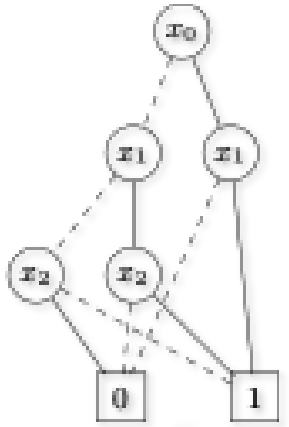
TRUTH TABLE

x_0	x_1	x_2	f
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

BINARY DECISION TREE



(REDUCED, ORDERED)
BINARY DECISION DIAGRAM

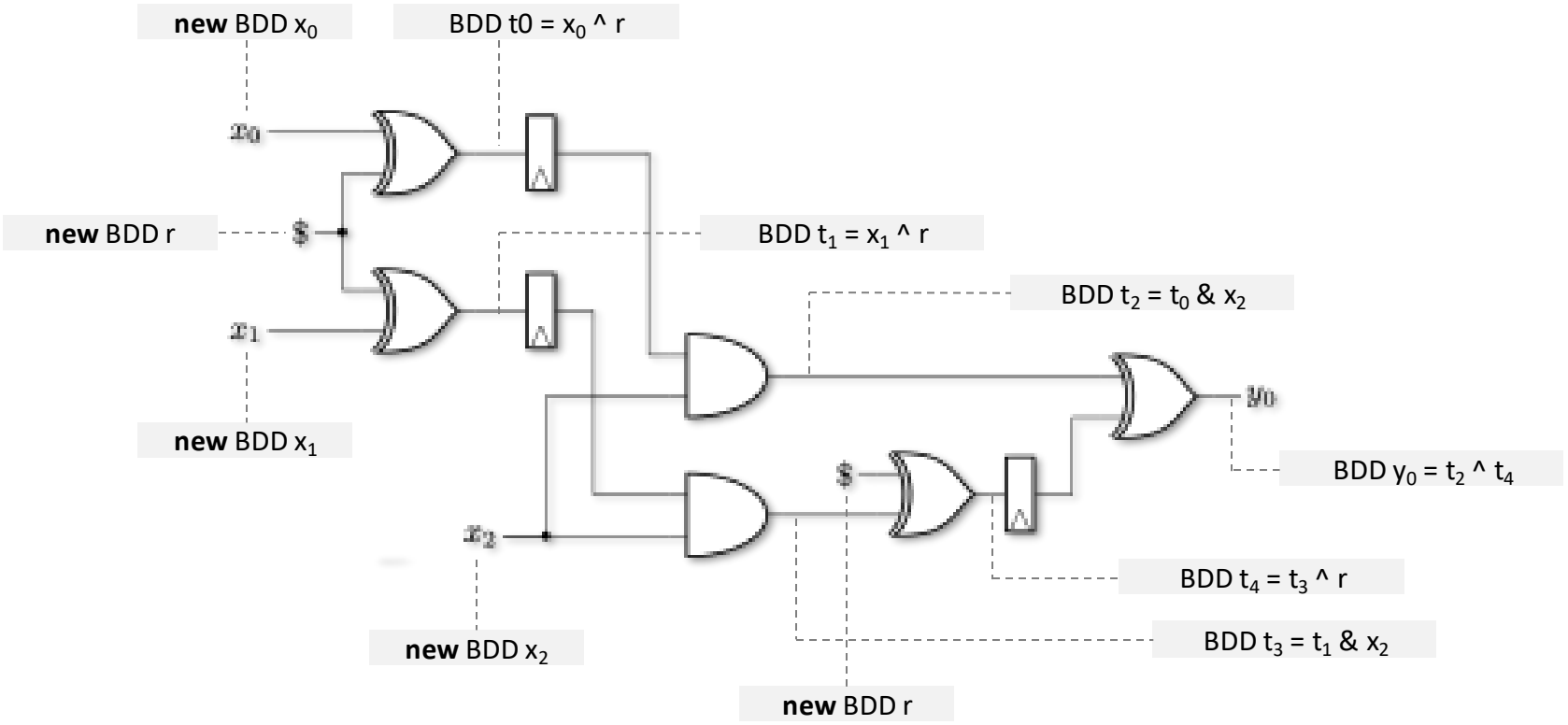


(REDUCED, ORDERED) BINARY DECISION DIAGRAMS ARE A CONCISE DATA STRUCTURE TO

STORE, MANIPULATE, SIMULATE, AND EVALUATE

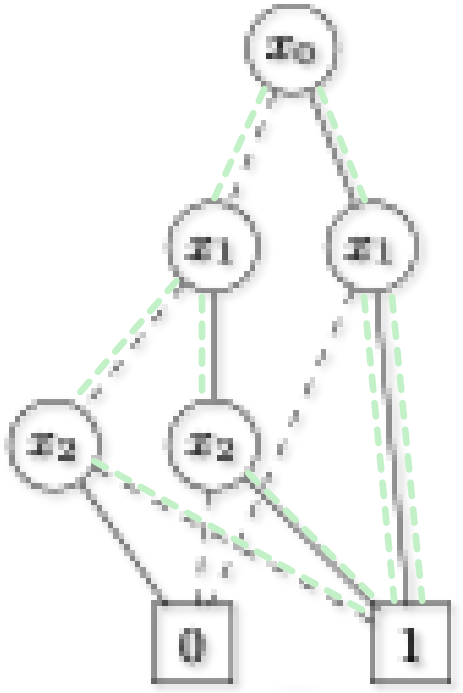
BOOLEAN FUNCTIONS.

VERIFICATION | SYMBOLIC SIMULATION OF CIRCUITS (USING BDDS)



VERIFICATION | CHECKING STATISTICAL INDEPENDENCE WITH BDDS

SATCOUNT OPERATION
COUNTING SATISFYING ASSIGNMENTS



SATCOUNT(f) = 4

STATISTICAL INDEPENDENCE
FOR TWO BINARY RANDOM VARIABLES

$$\Pr[X = 1, Y = 1] = \Pr[X = 1] \cdot \Pr[Y = 1]$$
$$\Pr[X = 1, Y = 0] = \Pr[X = 1] \cdot \Pr[Y = 0]$$
$$\Pr[X = 0, Y = 1] = \Pr[X = 0] \cdot \Pr[Y = 1]$$
$$\Pr[X = 0, Y = 0] = \Pr[X = 0] \cdot \Pr[Y = 0]$$

BDDS AS BINARY RANDOM VARIABLES
COMPUTING PROBABILTIES USING BDDS

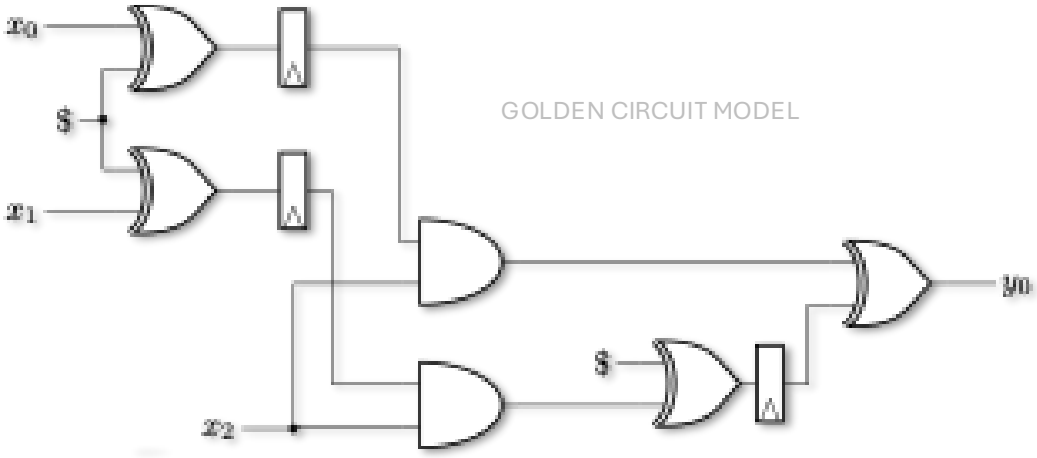
$$\Pr[X = 1] = \frac{\text{SATCOUNT(X)}}{\text{\#ASSIGNMENTS(X)}}$$
$$\Pr[X = 0] = 1 - \Pr[X = 1]$$

$$\Pr[X = 1, Y = 1] = \frac{\text{SATCOUNT(X \& Y)}}{\text{\#ASSIGNMENTS(X \& Y)}}$$
$$\Pr[X = 1, Y = 0] = \frac{\text{SATCOUNT(X \& !Y)}}{\text{\#ASSIGNMENTS(X \& !Y)}}$$
$$\Pr[X = 0, Y = 1] = \frac{\text{SATCOUNT(!X \& Y)}}{\text{\#ASSIGNMENTS(!X \& Y)}}$$

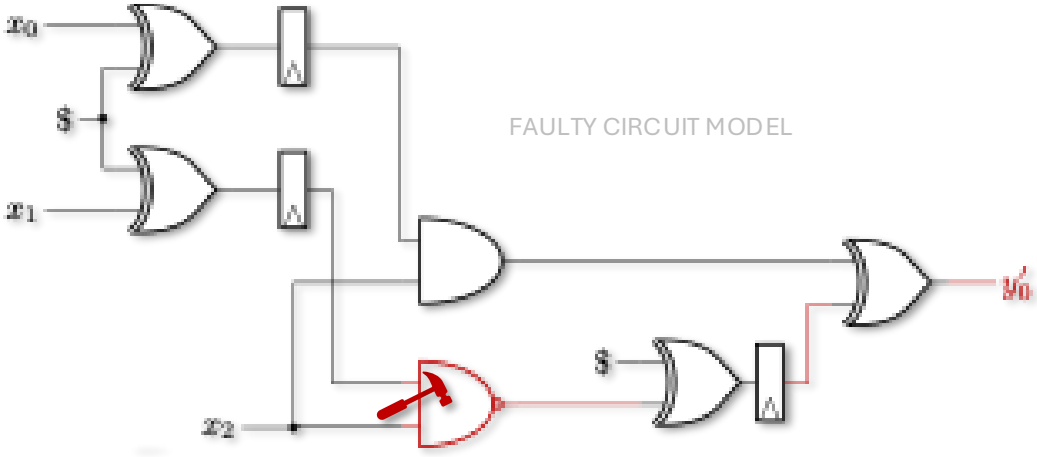
$$\mathbf{Circuit}_{golden}(X) \oplus \mathbf{Circuit}_{faulty}(X) = 0$$

A CIRCUIT C IS k-THRESHOLD FAULT SECURE (UNDER FAULT CORRECTION), IF AND ONLY IF
FOR ANY COMBINATION OF UP TO k FAULTED GATES,
THE CORRECT AND FAULTY RESULTS ARE **INDISTINGUISHABLE**.

VERIFICATION | CHECKING INDISTINGUISHABILITY WITH BDDS



GOLDEN CIRCUIT MODEL



FAULTY CIRCUIT MODEL

BDD $check_0 = y_0 \wedge y_0'$

THE NUMBER EFFECTIVE FAULTS CORRESPONDS TO THE

NUMBER OF SATISFYING ASSIGNMENTS

OF THE CHECK FUNCTION.

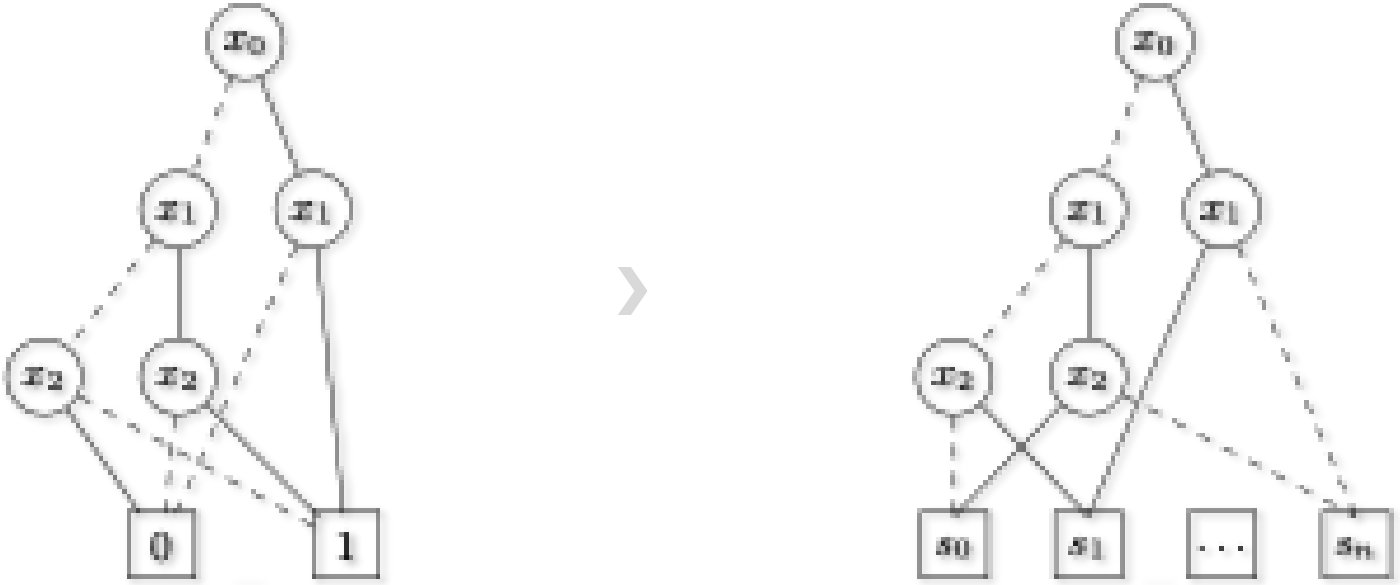
COMBINED SECURITY (SIMPLIFIED DEFINITION)

A CIRCUIT C IS COMBINED SECURE IF AND ONLY IF

FOR ANY SET OF UP TO k FAULTS, AND ANY SET OF UP TO d PROBES,

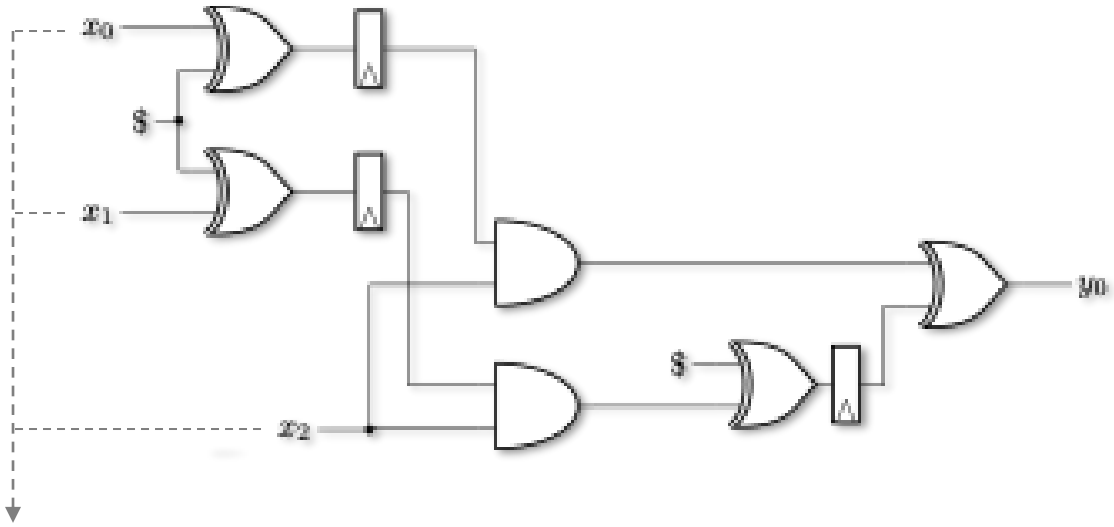
CONFIDENTIALITY AND **INTEGRITY** IS ENSURED.

VERIFICATION | MULTI-TERMINAL BINARY DECISION DIAGRAMS (MTBDDS)

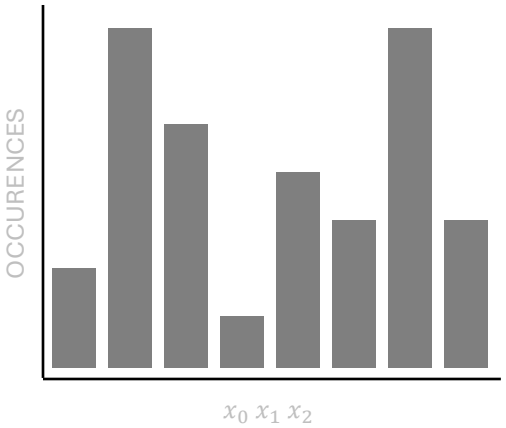


MULTI-TERMINAL BINARY DECISION DIAGRAMS EXTEND BINARY DECISION DIAGRAMS AND ARE USED TO SYMBOLICALLY REPRESENT A BOOLEAN FUNCTION WHOSE CODOMAIN IS AN ARBITRARY FINITE SET S.

VERIFICATION | ENCODING PROBABILITY DISTRIBUTIONS WITH MTBDDS



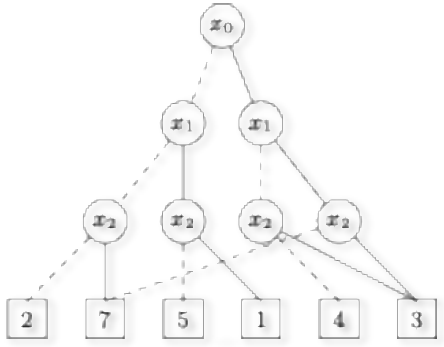
DISCRETE PROBABILITY DISTRIBUTION



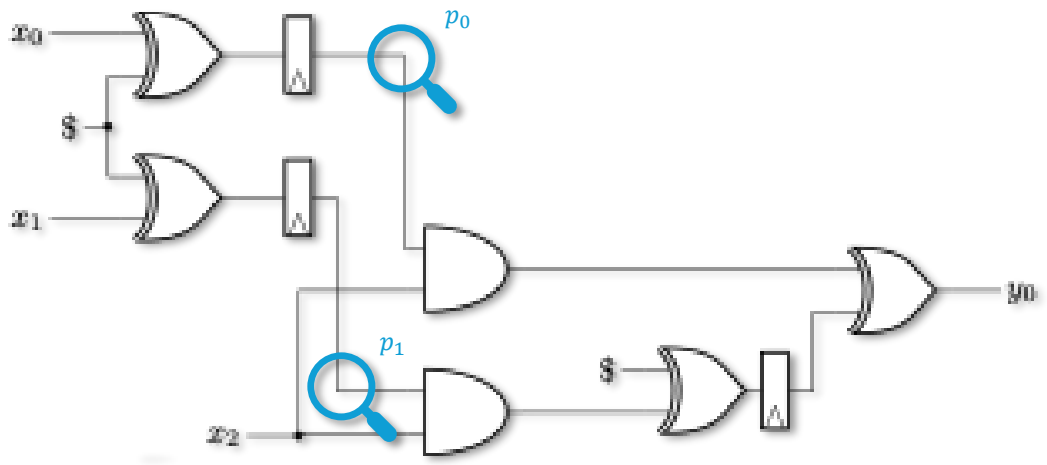
VECTOR OF OCCURENCES

$$\begin{matrix} 0\,0\,0 \\ 0\,0\,1 \\ 0\,1\,0 \\ 0\,1\,1 \\ 1\,0\,0 \\ 1\,0\,1 \\ 1\,1\,0 \\ 1\,1\,1 \end{matrix} \begin{pmatrix} 2 \\ 7 \\ 5 \\ 1 \\ 4 \\ 3 \\ 7 \\ 3 \end{pmatrix}$$

MULTI-TERMINAL BINARY DECISION DIAGRAM



VERIFICATION | ENCODING TRANSITIONS AS BINARY DECISION DIAGRAMS



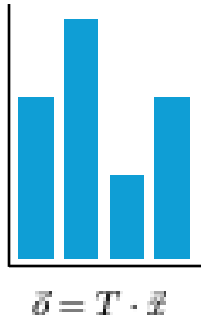
TRANSITION RELATION

x_0	x_1	r		p_0	p_1
0	0	0	→	0	0
0	0	1	→	1	1
0	1	0	→	0	1
0	1	1	→	1	0
1	0	0	→	1	0
1	0	1	→	0	1
1	1	0	→	1	1
1	1	1	→	0	0

TRANSITION FUNCTION

$$T(x_0, x_1, r, p_0, p_1) = \begin{cases} 1 & \text{valid transition} \\ 0 & \text{else} \end{cases}$$

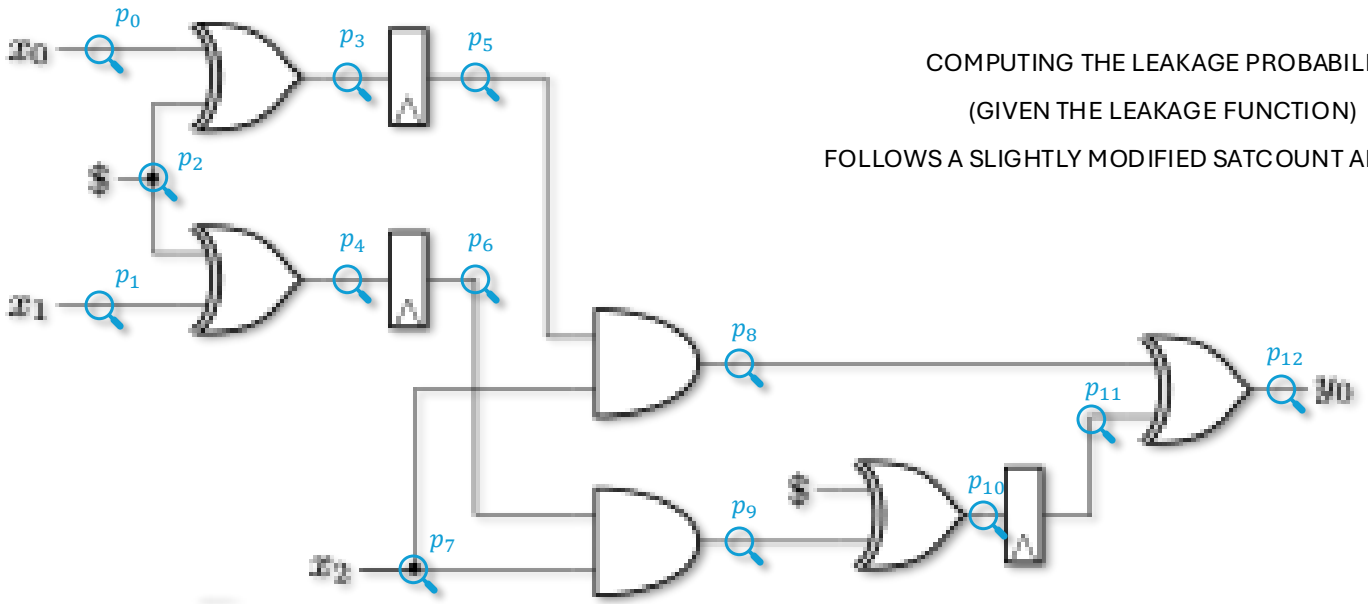
ADVERSARIAL OBSERVATION



WE ENCODE VALIT TRANSITIONS BETWEEN INPUTS AND OBSERVATIONS (PROBES) AS

TRANSITION FUNCTION AND STORE IT AS BINARY DECISION DIAGRAM.

VERIFICATION | DERIVING THE LEAKAGE FUNCTION

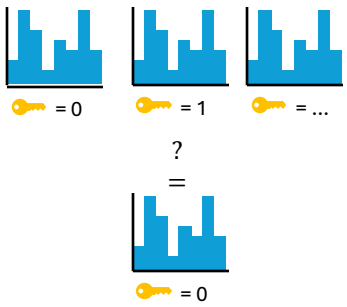


COMPUTING THE LEAKAGE PROBABILITY

(GIVEN THE LEAKAGE FUNCTION)

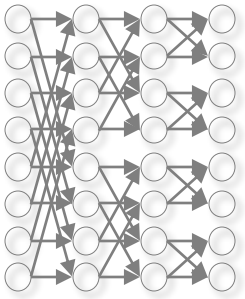
FOLLOWS A SLIGHTLY MODIFIED SATCOUNT ALGORITHM.

SECRET-DEPENDENT OBSERVATIONS



$$D_{H,x}(y) := |H_x^{-1}(y)| - |H_0^{-1}(y)|$$

FOURIER-HADAMARD TRANSFORM



$$\hat{f} : \mathbb{F}_2^m \to \mathbb{R}, \beta \mapsto \sum_{y \in \mathbb{F}_2^m} (-1)^{\langle \beta, y \rangle} f(y)$$

LEAKAGE FUNCTION

$$\mathcal{L}(p_0, p_1, \ldots, p_{12}) = \begin{cases} 1 & \text{combination leaks} \\ 0 & \text{else} \end{cases}$$

AGENDA

1. **WHO WE ARE**
2. **MOTIVATION** | WHY SECURITY VERIFICATION?
3. **BACKGROUND** | SECURITY MODELS
4. **VERIFICATION** | TECHNIQUES AND TOOLS
5. **RESULTS** | CASE STUDIES
6. **CONCLUSION**

RESULTS | THRESHOLD PROBING MODEL (SILVER)

Scheme	Pos.†	d	Probing		NI		SNI		PINI		Unif.
			std.	rob.	std.	rob.	std.	rob.	std.	rob.	
Gadgets											
DOM [29]	19	1	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	✓[0.0 s]
DOM [29]	42	2	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	✓[0.0 s]
DOM [29]	74	3	$^{3}\checkmark$[0.2 s]	$^{3}\checkmark$[1.2 s]	$^{3}\checkmark$[2.5 s]	$^{3}\checkmark$[24.4 s]	$^{3}\checkmark$[3.7 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	✓[0.0 s]
DOM SNI [26]	21	1	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	✓[0.0 s]
DOM SNI [26]	45	2	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	✓[0.0 s]
DOM SNI [26]	78	3	$^{3}\checkmark$[0.1 s]	$^{3}\checkmark$[1.5 s]	$^{3}\checkmark$[2.4 s]	$^{3}\checkmark$[39.4 s]	$^{3}\checkmark$[3.7 s]	$^{3}\checkmark$[39.4 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	✓[0.0 s]
PARA1 [5]	22	1	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	✓[0.0 s]
PARA2 [5]	45	2	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.1 s]	$^{2}\checkmark$[0.1 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	✓[0.0 s]
PARA3 [5]	68	3	$^{3}\checkmark$[0.1 s]	$^{3}\checkmark$[0.5 s]	$^{3}\checkmark$[1.6 s]	$^{3}\checkmark$[12.1 s]	$^{3}\times$/$^{2}\checkmark$[0.8 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	✓[0.0 s]
PARA3 SNI [5]	82	3	$^{3}\checkmark$[0.2 s]	$^{3}\checkmark$[1.2 s]	$^{3}\checkmark$[2.8 s]	$^{3}\checkmark$[33.0 s]	$^{3}\checkmark$[4.1 s]	$^{3}\checkmark$[38.7 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	✓[0.0 s]
PINI1 [17]	21	1	$^{1}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	✓[0.0 s]
PINI2 [17]	51	2	$^{2}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	✓[0.0 s]
HPC1 [16]	22	1	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	✓[0.0 s]
HPC1 [16]	52	2	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	✓[0.0 s]
HPC2 [16]	32	1	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	✓[0.0 s]
HPC2 [16]	75	2	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	✓[0.0 s]
ISW SNI REF [26]	26	1	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	$^{1}\checkmark$[0.0 s]	✓[0.0 s]
ISW SNI REF [26]	65	2	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	✓[0.0 s]
CMS3 [36]	104	3	$^{3}\times$/$^{2}\checkmark$[0.2 s]	$^{3}\times$/$^{2}\checkmark$[0.4 s]	$^{3}\times$/$^{2}\checkmark$[1.2 s]	$^{3}\times$/$^{2}\checkmark$[2.9 s]	$^{3}\times$/$^{2}\checkmark$[1.7 s]	$^{3}\times$/$^{2}\checkmark$[4.6 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	✓[0.0 s]
UMA2 [36]	81	2	$^{2}\times$/$^{1}\checkmark$[0.0 s]	$^{2}\times$/$^{1}\checkmark$[0.0 s]	$^{2}\times$/$^{1}\checkmark$[0.0 s]	$^{2}\times$/$^{1}\checkmark$[0.0 s]	$^{2}\times$/$^{1}\checkmark$[0.0 s]	$^{2}\times$/$^{1}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{1}\times$[0.0 s]	✓[0.0 s]
DOM2 DEP‡ [36]	56	2	$^{2}\checkmark$[0.0 s]	$^{2}\times$/$^{1}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\times$/$^{1}\checkmark$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{1}\times$[0.0 s]	$^{2}\checkmark$[0.0 s]	$^{2}\times$/$^{1}\checkmark$[0.0 s]	✓[0.0 s]

VERIFICATION | THRESHOLD FAULTING MODEL (FIVER)

Redundancy (Capability*) [bits]	Verification Parameter $\zeta(n,t,l)$	Variate	Complexity Reduction	Design Properties Comb. Gates	Seq. Gates	Logic Stages	Analysis Results Combinations	Time [s]	Security
CRAFT – 1 round (detection)									
1 (1)	$\zeta(1,\tau_{bf},cs)$	univariate	no	845	80	2	766	0.021	✓
1 (1)	$\zeta(2,\tau_{bf},cs)$	univariate	no	845	80	2	151 561	0.769	✗
3 (2)	$\zeta(2,\tau_{bf},cs)$	univariate	no	1 410	112	2	329 730	1.496	✓
3 (2)	$\zeta(3,\tau_{bf},cs)$	univariate	no	1 410	112	2	64 320 469	441	✗
4 (3)	$\zeta(3,\tau_{bf},cs)$	univariate	no	1 679	128	2	91 737 144	2 937	✓
			yes	1 679	128	2	4 665 200	360	✓
CRAFT – 2 rounds (detection)									
1 (1)	$\zeta(1,\tau_{bf},cs)$	univariate	no	1 571	160	3	1 491	0.378	✓
1 (1)	$\zeta(2,\tau_{bf},cs)$	univariate	no	1 571	160	3	417 882	62	✗
3 (2)	$\zeta(2,\tau_{bf},cs)$	univariate	no	2 526	224	3	868 500	157	✓
3 (2)	$\zeta(3,\tau_{bf},cs)$	univariate	no	2 526	224	3	250 984 950	∞	–
			yes	2 526	224	3	7 364 279	408	✗
CRAFT – 2 rounds – multivariate (detection)									
1 (1)	$\zeta(1,\tau_{bf},cs)$	bivariate	no	1 720	160	3	682 832	140	✓
1 (1)	$\zeta(1,\tau_{bf},cs)$	trivariate	yes	1 720	160	3	99 542 528	26 955	✓
3 (2)	$\zeta(2,\tau_{sr},s)$	bivariate	no	2 915	224	3	38 651 200	81 897	✓
CRAFT – 1 round (correction)									
3 (1)	$\zeta(1,\tau_{bf},cs)$	univariate	no	2 868	112	2	2 788	0.081	✓
3 (1)	$\zeta(2,\tau_{bf},cs)$	univariate	no	2 868	112	2	3 201 690	22	✗
7 (2)	$\zeta(2,\tau_{bf},cs)$	univariate	no	17 460	176	2	129 651 034	3 543	✓
			yes	17 460	176	2	10 923 888	130	✓
LED-64 – 1 round (detection)									
1 (1)	$\zeta(1,\tau_{bf},cs)$	univariate	no	1 541	0	1	1 301	0.064	✓
1 (1)	$\zeta(2,\tau_{bf},cs)$	univariate	no	1 541	0	1	846 951	9.558	✗
3 (2)	$\zeta(2,\tau_{bf},cs)$	univariate	no	2 435	0	1	1 730 730	27	✓
3 (2)	$\zeta(3,\tau_{bf},cs)$	univariate	no	2 435	0	1	1 072 477 550	12 722	✗
4 (3)	$\zeta(3,\tau_{bf},cs)$	univariate	no	2 916	0	1	1 654 087 449	17 348	✓
			yes	2 916	0	1	3 983 413	94	✓
AES-128 – 1 round (detection)									
1 (1)	$\zeta(1,\tau_{bf},cs)$	univariate	no	24 864	0	1	24 432	22	✓
4 (2)	$\zeta(2,\tau_{bf},cs)$	univariate	no	34 159	0	1	298 473 528	∞	–
			yes	34 159	0	1	56 632 584	471 281	✓

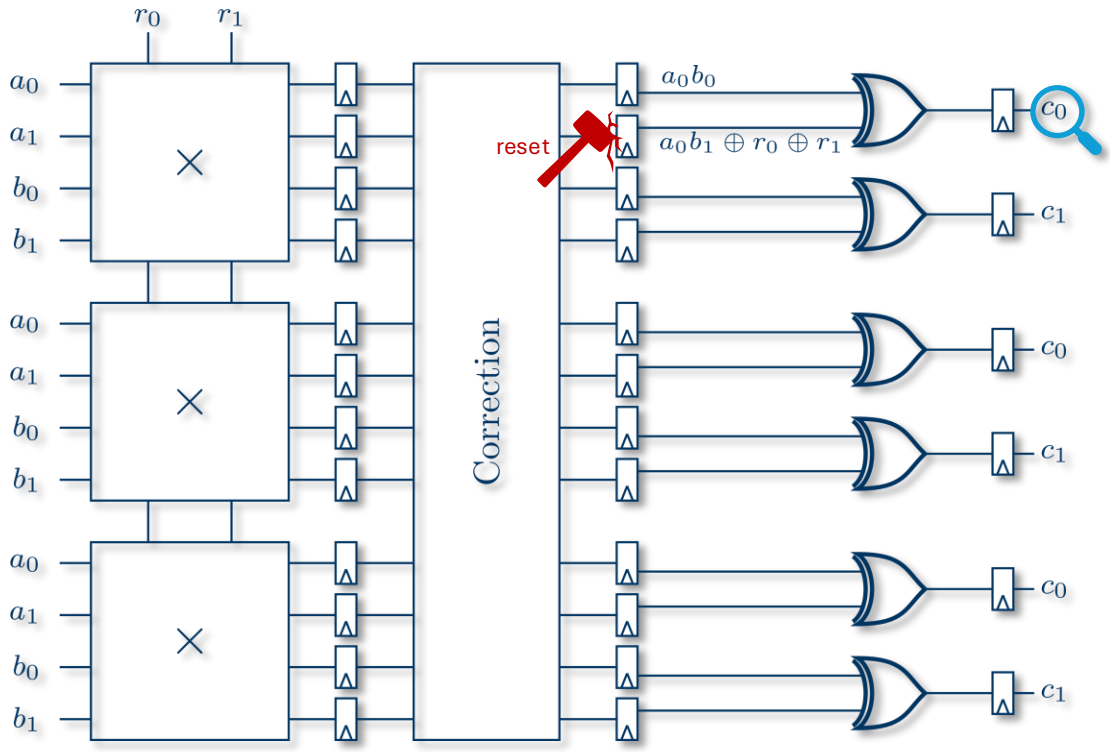
* The capability determines the maximum number of faults that can be detected or corrected by the corresponding countermeasure.

VERIFICATION | THRESHOLD COMBINED MODEL (VERICA)

Gadget	Design					SCA			FIA			Combined			
	d	k	rand.	comb.	memory	PNI	PSNI	Time	FNI	FSNI	Time		(d,k)		Time
NINA	1	1	0	4	0	1✓	–	0.460 s	1✓	–	0.429 s	CNI	$(1,1)^{\checkmark}$		0.430 s
NINA	1	2	0	6	0	1✓	–	0.455 s	2✓	–	0.445 s		$(1,2)^{\checkmark}$		0.492 s
NINA	2	1	0	6	0	2✓	–	0.471 s	1✓	–	0.451 s		$(2,1)^{\checkmark}$		0.436 s
NINA	2	2	0	9	0	2✓	–	0.442 s	2✓	–	0.444 s		$(2,2)^{\checkmark}$		0.442 s
SNINA	1	1	1	22	16	–	1✓	0.476 s	–	1✓	0.449 s	CSNI	$(1,1)^{\checkmark}$		0.473 s
SNINA	1	2	1	38	26	–	1✓	0.451 s	–	2✓	0.500 s		$(1,2)^{\checkmark}$		0.519 s
SNINA	2	1	3	57	33	–	2✓	0.566 s	–	1✓	0.456 s		$(2,1)^{\times}/(1,1)^{\checkmark}$		0.592 s
SNINA	2	2	3	96	54	–	2✓	0.821 s	–	2✓	0.673 s		$(2,2)^{\times}/(1,1)^{\checkmark}$		1.062 s
SININA	1	1	2	90	30	–	1✓	0.450 s	–	1✓	0.461 s	ICSNI	$(1,1)^{\times}/(0,0)^{\checkmark}$		0.456 s
SININA	1	2	3	360	50	–	1✓	0.555 s	–	2✓	1.395 s		$(1,2)^{\times}/(0,0)^{\checkmark}$		17.985 s
SININA	2	1	6	207	63	–	2✓	1.334 s	–	1✓	0.511 s		$(2,1)^{\times}/(0,0)^{\checkmark}$		73.574 s
SININA*	2	2	9	825	105	–	2✓	76.030 s	–	2✓	5.300 s		$(2,2)^{\times}/(0,0)^{\checkmark}$		>2.7 h

* Due to the high verification complexity, we interrupted the combined analysis after testing $(2,1)$-SININA where VERICA already reported a failure.

VERIFICATION | THRESHOLD COMBINED MODEL (VERICA)



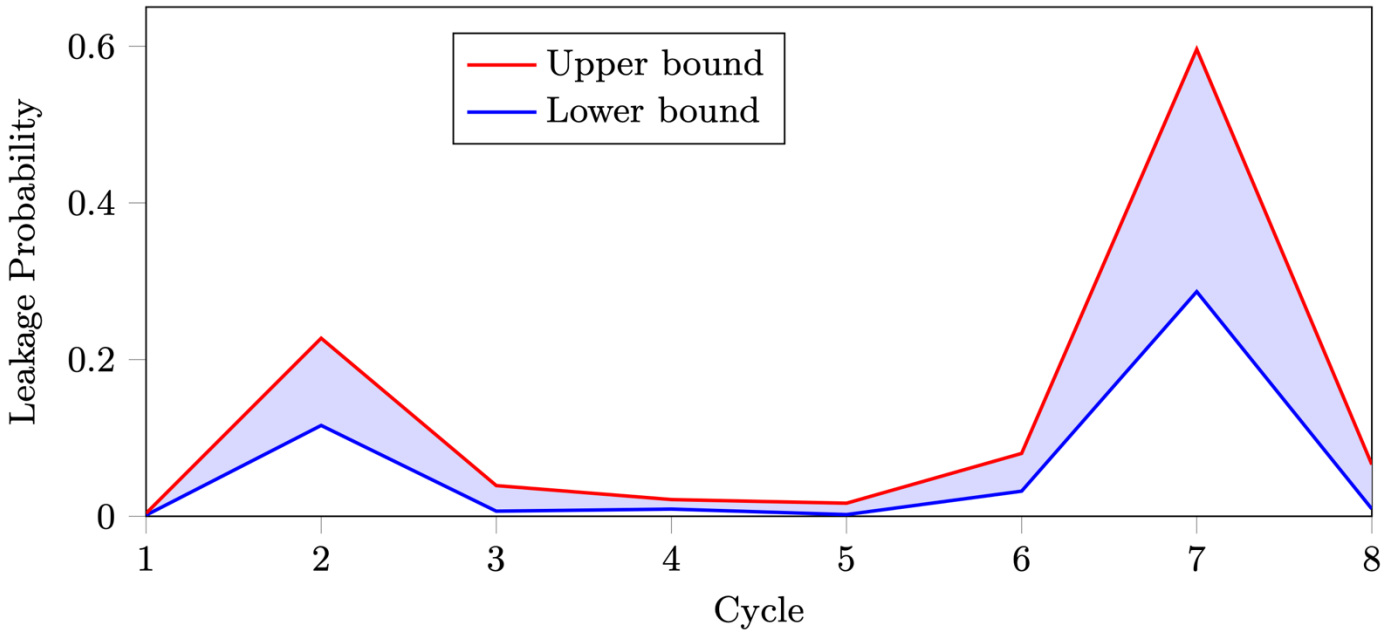
RESULTS | RANDOM PROBING MODEL (INDIANA)

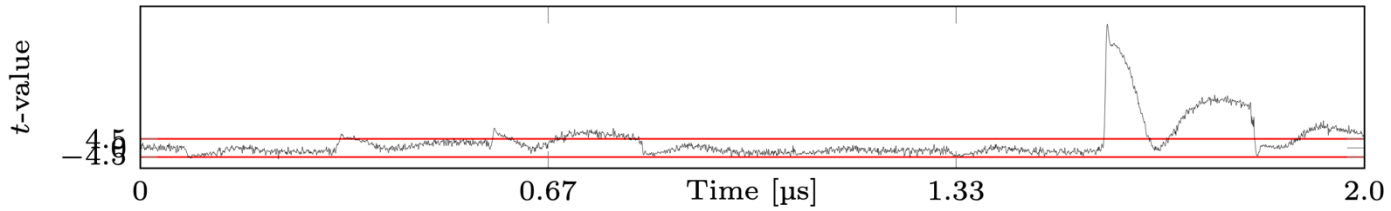
VERIFICATION OF A FULL AES ROUND (PIPELINED, 16 S-BOXES IN PARALLEL)

Cycle	Positions part. × wires	Probes part. × probes	Samples part. × samples	Leakage min. / max.	Time totally elapsed
1	16×72	16×2	16×2556	$0.056/0.458$	1.20 min
2	16×138	16×2	16×9453	$0.785/0.966$	6.25 min
3	16×72	16×2	16×2556	$0.099/0.472$	39.33 min
4	16×52	16×2	16×1326	$0.145/0.296$	39.43 min
5	16×52	16×2	16×1326	$0.034/0.236$	39.53 min
6	16×92	16×2	16×4186	$0.406/0.738$	39.79 min
7	16×304	16×2	16×46056	$0.992/0.999$	3.33 h
8	16×102	16×2	16×5151	$0.149/0.767$	3.58 h
9	4×324	16×2	4×52326	$0.051/0.981$	3.76 h

RESULTS | RANDOM PROBING MODEL (INDIANA)

VERIFICATION OF A SINGLE AES S-BOX IN THE RANDOM PROBING MODEL





PRACTICAL 2-ND ORDER TVLA RESULTS

AGENDA

1. **WHO WE ARE**
2. **MOTIVATION** | WHY SECURITY VERIFICATION?
3. **BACKGROUND** | SECURITY MODELS
4. **VERIFICATION** | TECHNIQUES AND TOOLS
5. **RESULTS** | CASE STUDIES
6. **CONCLUSION**

CONCLUSION | SUMMARY OF THIS TALK

SECURITY MODEL AND DEFINITIONS

- probing, faulting and combined models
- composability notions for gadget-based protection

VERIFICATION TECHNIQUES AND TOOLS

- Binary Decision Diagrams and Multi-Terminal BDDs
- statistical independence leakage verification (SILVER)
- golden and faulty circuits comparison (FIVER)
- indistinguishability analysis and leakage functions (INDIANA)

THANK YOU FOR YOUR ATTENTION!

DO YOU HAVE ANY QUESTIONS?

pascal.sasdrich@rub.de

LITERATURE

[AWM+20] Victor Arribas, Felix Wegener, Amir Moradi, Svetla Nikova. Cryptographic Fault Diagnosis using VerFI. HOST 2020.

[BBC+19] Gilles Barthe, Sonia Belaïd, Gaëtan Cassiers, Pierre-Alain Fouque, Benjamin Grégoire, François-Xavier Standaert. maskVerif: Automated Verification of Higher-Order Masking in Presence of Physical Defaults. ESORICS 2019.

[[BBD+15] Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, Pierre-Yves Strub. Verified Proofs of Higher-Order Masking. EUROCRYPT 2015.

[BBD+16] Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, Pierre-Yves Strub, Rébecca Zucchini. Strong Non-Interference and Type-Directed Higher-Order Masking. CCS 2016.

[BCP+20] Sonia Belaïd, Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain, and Abdul Rahman Taleb. Random Probing Security: Verification, Composition, Expansion and New Constructions. CRYPTO 2020.

[BFG+24] Sonia Belaïd, Jakob Feldtkeller, Tim Güneysu, Anna Guinet, Jan Richter-Brockmann, Matthieu Rivain, Pascal Sasdrich, Abdul Rahman Taleb: Formal Definition and Verification for Combined Random Fault and Random Probing Security. ASIACRYPT 2024.

[BFG+25] Christof Beierle, Jakob Feldtkeller, Anna Guinet, Tim Güneysu, Gregor Leander, Jan Richter-Brockmann, Pascal Sasdrich. INDIANA - Verifying (Random) Probing Security Through Indistinguishability Analysis. EUROCRYPT 2025.

[BGI+18] Roderick Bloem, Hannes Groß, Rinat Iusupov, Bettina Könighofer, Stefan Mangard, Johannes Winter. Formal Verification of Masked Hardware Implementations in the Presence of Glitches. EUROCRYPT 2018.

[BMR+22] Sonia Belaïd, Darius Mercadier, Matthieu Rivain, Abdul Rahman Taleb. IronMask: Versatile Verification of Masking Security. IEEE SP 2022.

[CS20] Gaëtan Cassiers, François-Xavier Standaert. Trivially and Efficiently Composing Masked Gadgets With Probe Isolating Non-Interference. IEEE TIFS 2020.

[DDF14] Alexandre Duc, Stefan Dziembowski, and Sebastian Faust. Unifying Leakage Models: from Probing Attacks to Noisy Leakage. EUROCRYPT 2014.

[DN20] Siemen Dhooghe and Svetla Nikova. My Gadget Just Cares for Me – How NINA Can Prove Security Against Combined Attacks. CT-RSA 2020.

[DN23] Siemen Dhooghe, Svetla Nikova: The Random Fault Model. SAC 2023.

[FGM+18] Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, and Francois-Xavier Standaert. Composable Masking Schemes in the Presence of Physical Defaults & the Robust Probing Model. IACR TCHES 2018.

[FRS+22] Jakob Feldtkeller, Jan Richter-Brockmann, Pascal Sasdrich, and Tim Güneysu. CINI MINIS: Domain Isolation for Fault and Combined Security. CCS, 2022

[IPS+06] Yuval Ishai, Manoj Prabhakaran, Amit Sahai, David A. Wagner. Private Circuits II: Keeping Secrets in Tamperable Circuits. EUROCRYPT 2006.

[ISW03] Yuval Ishai, Amit Sahai, and David A. Wagner. Private Circuits: Securing Hardware against Probing Attacks. CRYPTO 2003.

[KSM20] David Knichel, Pascal Sasdrich, Amir Moradi. SILVER - Statistical Independence and Leakage Verification. ASIACRYPT 2020.

[RFS+22] Jan Richter-Brockmann, Jakob Feldtkeller, Pascal Sasdrich, Tim Güneysu. VERICA - Verification of Combined Attacks: Automated formal verification of security against simultaneous information leakage and tampering. IACR TCHES 2022.

[RSG23] Jan Richter-Brockmann, Pascal Sasdrich, Tim Güneysu. Revisiting Fault Adversary Models - Hardware Faults in Theory and Practice. IEEE TC 2023.

[RSS+21] Jan Richter-Brockmann, Aein Rezaei Shahmirzadi, Pascal Sasdrich, Amir Moradi, Tim Güneysu. FIVER - Robust Verification of Countermeasures against Fault Injections. IACR TCHES 2021.