北京大學
PEKING UNIVERSITY

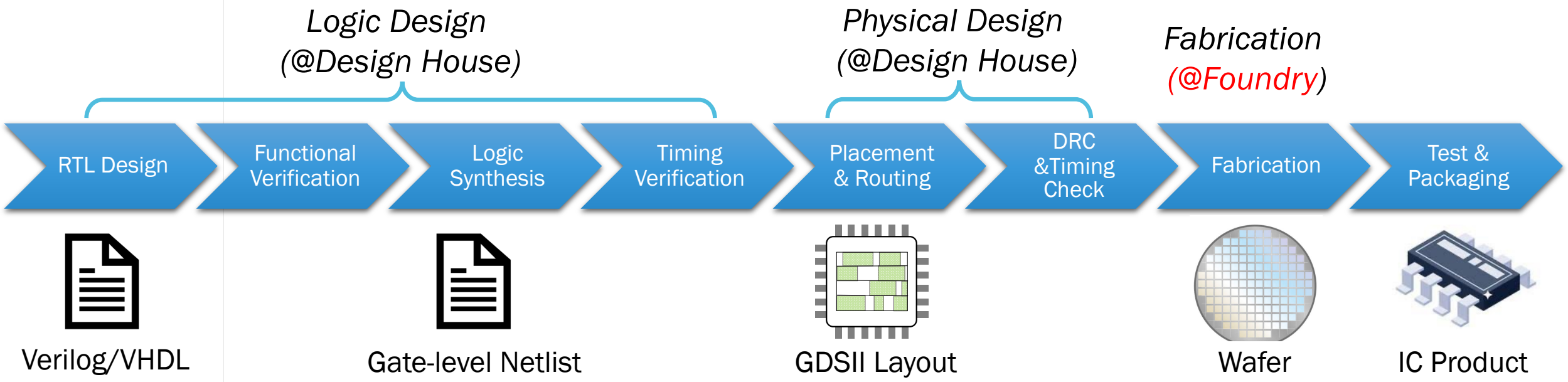
GDSII-Guard: ECO Anti-Trojan Optimization with Exploratory Timing-Security Trade-Offs

Xinming Wei, Jiaxi Zhang, Guojie Luo

Peking University

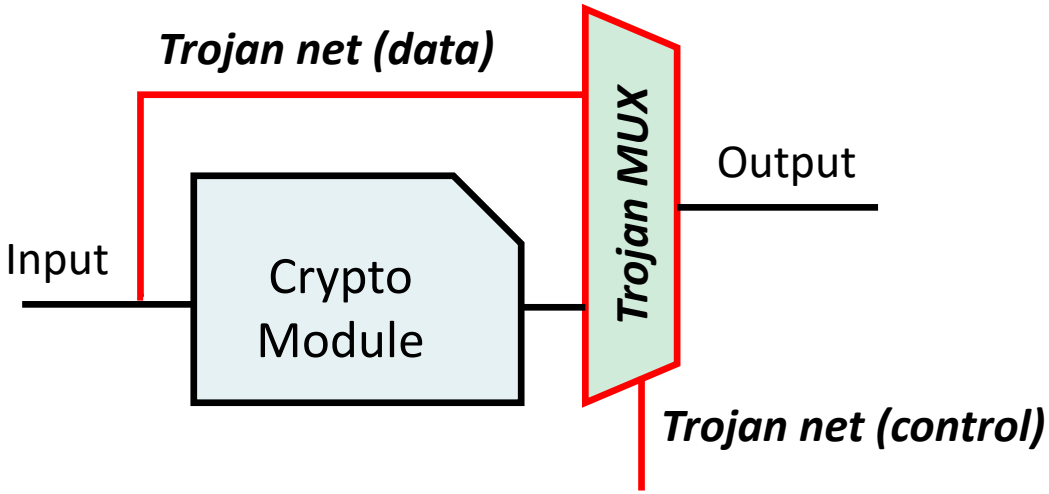
Fabrication-Time Trojan Attacks

- IC design flows are mostly ***Fabless***
  - Should the foundry be trusted?



Fabrication-Time Trojan Attacks

- Hardware Trojan effects
  - Functional change, error injection, or system failure
  - Performance degradation
  - Leakage of sensitive information
  - ……



Challenges in Trojan Defenses

- Post-Silicon detection-based defenses
  - Logic test
  - Side-channel detections

Limitations

Low Reliability
- Stealthy Trojans have small footprint

Low Testability
- Stealthy Trojans are only triggered by rare events

Unpatchability
- No remedy for vulnerabilities detected in ICs after manufacturing

Challenges in Trojan Defenses

- *Security-by-Design* defenses
  - Layout density increasing: ICAS [T. Trippel *et al.*, S&P'20]
  - Layout filling with independent logic: BISA [K. Xiao *et al.*, HOST'13], [P. Ba *et al.*, ISVLSI'16]

Limitations

Low Reliability

- Cannot provide complete confidence against diverse Trojan attacks.

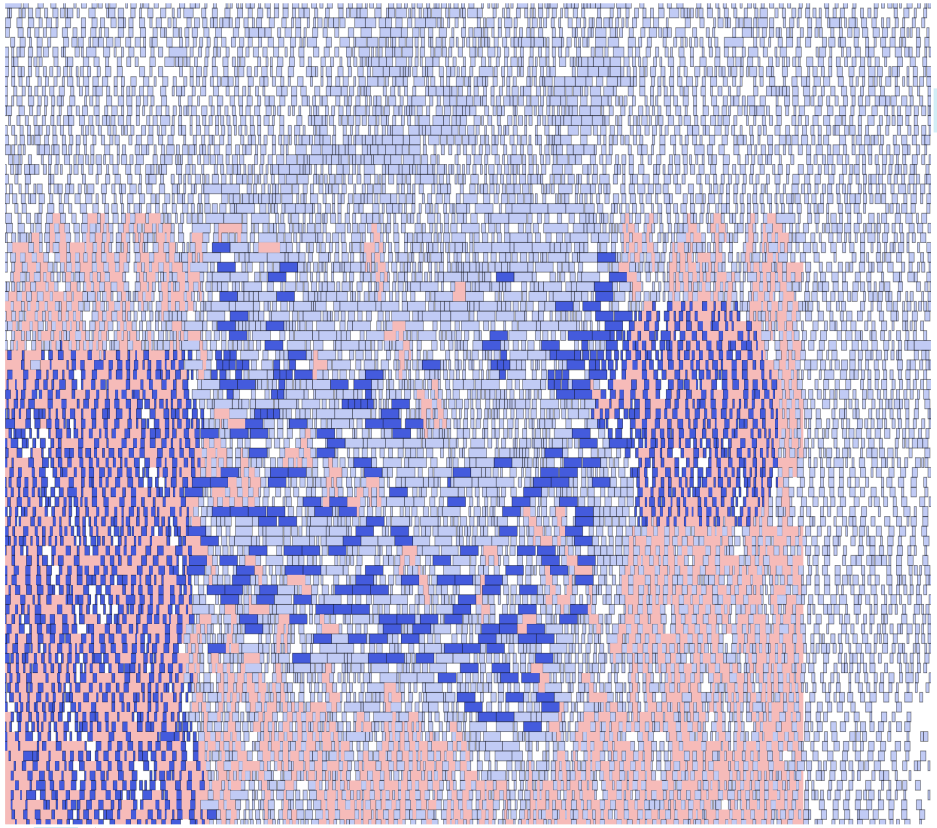
PPA-Agnostic

- Design overheads brought by defenses are not explicitly demonstrated

GDSII-Guard: Timing-aware ECO Enhancement

- Post-layout ECO enhancement against fabrication-time Trojans
- Minimized design performance, power, and DRC overheads
- Significant security improvement with modest costs

Security Metrics



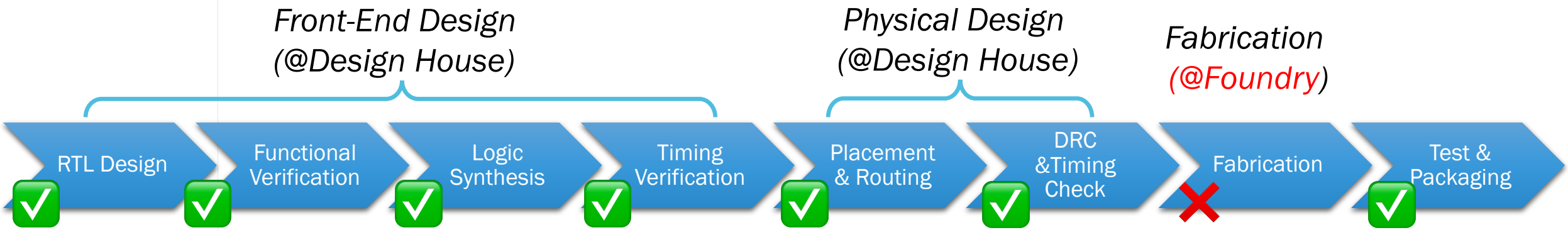
Exploitable Regions*

- Free placement sites
- Free routing tracks

*J. Knechtel *et al.*, “Benchmarking security closure of physical layouts: ISPD 2022 contest,” in *ISPD*, 2022.

Threat Model

- Focus on fabrication-time Trojans, assuming all other phases are trusted
- Attackers can inject *additive* Trojans
  - No resizing, shifting, or removing existing instances
- Attackers cannot extend the metal layers or the size of the layout



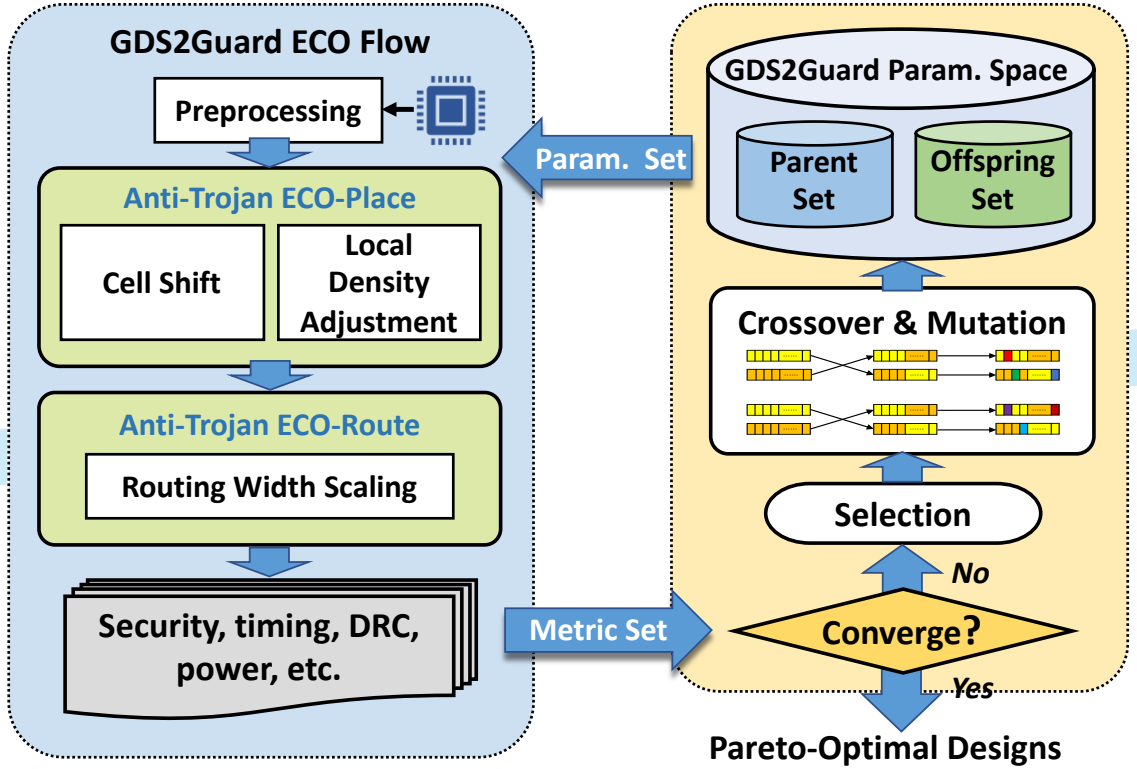
Problem Formulation

- Input: $\mathbf{L}_{base}$, security-critical assets list, timing specifications
- Output: $\mathbf{L}_{opt} = f(\mathbf{L}_{base}; x)$
- Objective:

$$\begin{aligned} &\min && \text{Security}(\mathbf{L}_{opt}) \\ &\min && -\text{TNS}(\mathbf{L}_{opt}) \\ &\text{s.t.} && \text{DRC\_viol}(\mathbf{L}_{opt}) \le N_{DRC} \\ & && \text{Power}(\mathbf{L}_{opt}) \le \beta_{power} \cdot \text{Power}(\mathbf{L}_{base}) \end{aligned}$$

$\mathbf{L}$: Layout
$f(\cdot\,; x)$: GDSII-Guard flow with param. config x,
$\text{Security}(\cdot)$: Normalized free sites/tracks by original layout (to minimize)

Framework Overview



ECO P&R Flow

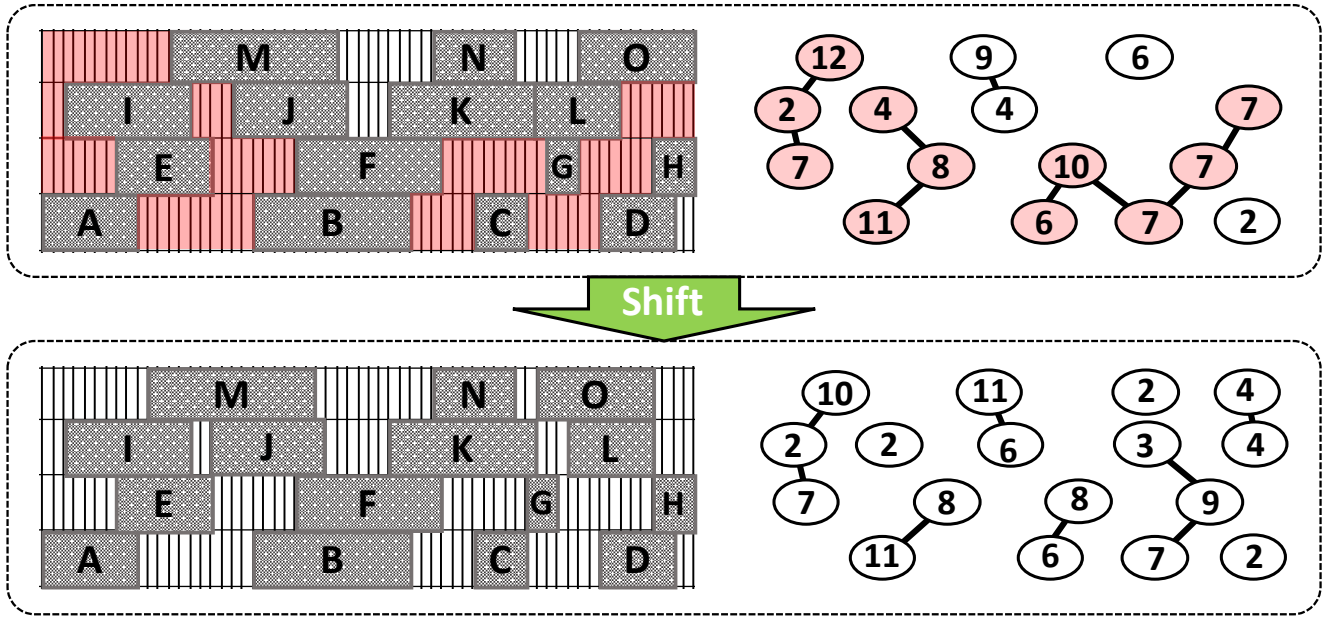
- ✓ Two alternative ECO placement operators
- ✓ One ECO routing operator
- ✓ Return a set of design metrics

Flow Parameter Tuning

- ✓ Explore security-timing trade-offs
- ✓ Return Pareto-Optimal designs

Anti-Trojan ECO P&R

- Placement: **Cell Shift**
- Algorithm takeaways
  - ✓Objective: Eliminate exploitable regions with minimized moving distances
  - ✓Graph modeling of empty regions
  - ✓Greedy-based
  - ✓Row-wise manner



Anti-Trojan ECO P&R

- Placement: **Dynamic Local Density Adjustment**
  - Algorithm takeaways
    - ✓ Designed for low-density layouts
    - ✓ “Kick” empty spaces away from security-critical assets
    - ✓ Divide layout into tiles, manages local density of tiles w/ placement blockages
- Routing: **Routing Width Scaling**
  - Algorithm takeaways
    - ✓ Further reduce free routing resources
    - ✓ Increase wire width of different metal layers selectively

Multi-Objective Flow Parameter Tuning

- Capture trade-offs between security and performance
- Parameter space size: 945k (given 10 routing layers)

Parameter Name	Description	Candidate Values
`op_select`	The selected ECO-place operator	"CS", "LDA"
`LDA::N`	#Grids in a row/column	2, 4, 8, 16, 32
`LDA::n_iter`	#Density adjustment iterations	1, 2, 3
`RWS::scale_M[i]`	Routing width scale factor of metal i $(i = 1, \ldots, K)$	1.0, 1.2, 1.5

Parameter space of GDSII-Guard flow

CS: Cell Shift
LDA: Local Density Adjustment
RWS: Routing Width Scaling

Experimental Results

Setup

- CPU: 2-way 24-core Intel Xeon Gold 6248R @3.0GHz
- RAM: 512GB DDR4
- Using multi-processing to accelerate flow tuning

Implementation

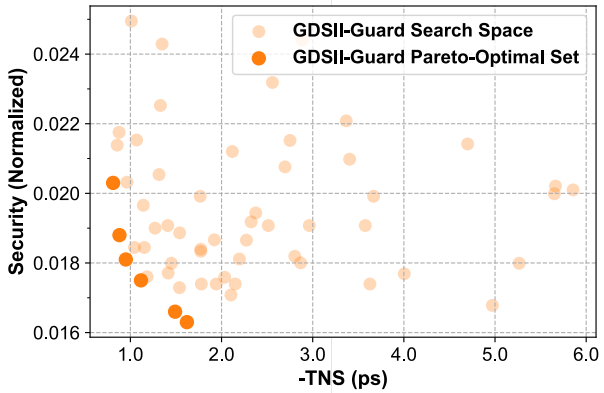
- Frontend: Python&Tcl scripts
- Backend: Cadence® Innovus™ 19.12

Baselines

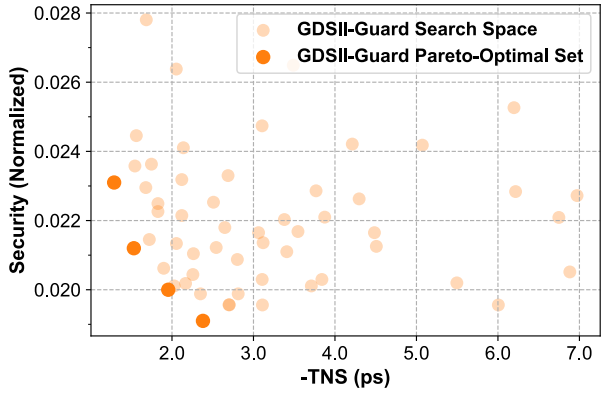
- Original design (w.o. security optimization)
- ICAS [T. Trippel *et al.*, S&P'20]
  Tune EDA params (e.g., density, slew, frequency)
- BISA [K. Xiao *et al.*, HOST'13]
  Fill empty sites with tamper-evident logic
- Ba+ [P. Ba *et al.*, ISVLSI'16]
  Improve BISA by prioritizing critical empty spaces

Experimental Results

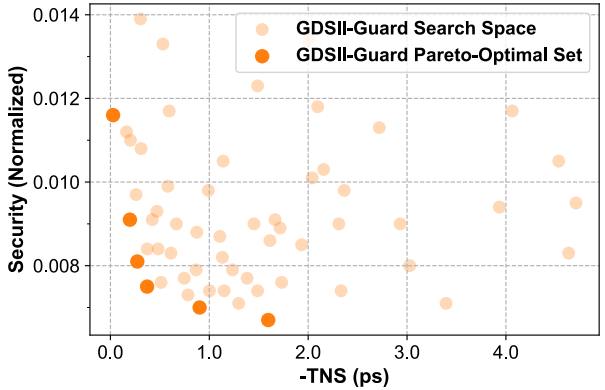
- Effectiveness of multi-objective optimization



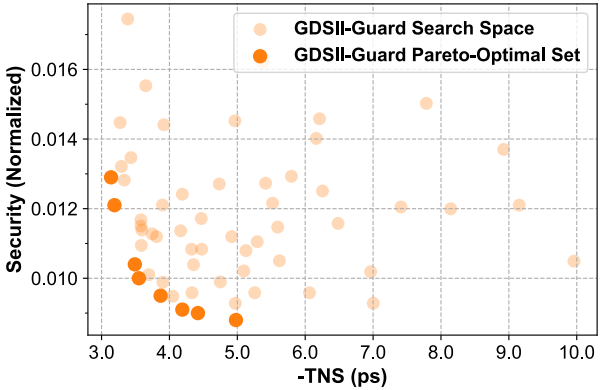
AES_1



AES_3



MISTY

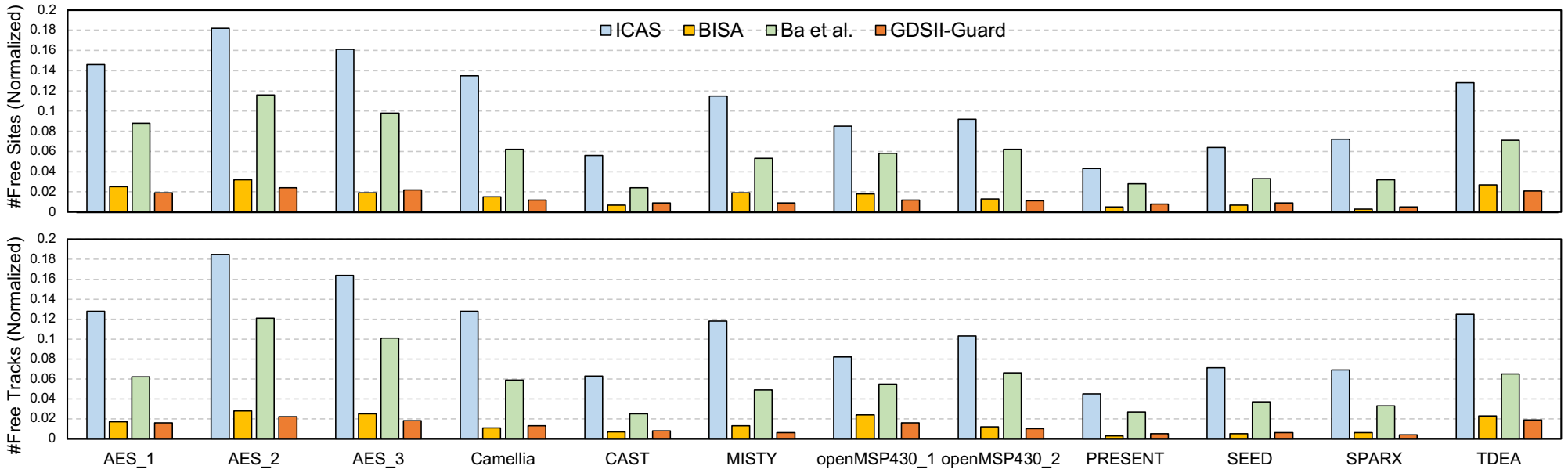


openMSP430_2

Expored Pareto fronts with GDSII-Guard on 4 designs

Experimental Results

- Comparison with state-of-the-art: Security analysis



  - Lowers the risk of Trojan insertion by ***98.8%*** on average.
  - Obtain the best overall security results.

Experimental Results

- Comparison with state-of-the-art: Overhead analysis

TNS(ps)	AES_1	AES_2	AES_3	Camellia	CAST	MISTY	openMSP430_1	openMSP430_2	PRESENT	SEED	SPARX	TDEA
Original Design	-0.998	-2.577	-1.432	0	-6.693	0	0	-2.946	0	-6.693	0	0
ICAS [10]	-1.657	-2.737	-3.356	0	-7.73	-0.414	0	-4.281	0	-8.025	0	-0.012
BISA [11]	-4.256	-9.731	-8.367	-1.23	-25.324	-4.257	-1.582	-7.768	0	-21.205	-1.432	-2.87
Ba *et al.* [12], [13]	-1.818	-3.47	-2.285	0	-10.589	-0.356	-0.021	-4.875	0	-8.924	0	-0.56
GDSII-Guard	-1.116	-2.893	-1.954	0	-8.035	-0.371	0	-3.548	0	-5.978	0	0

Power(mW)	AES_1	AES_2	AES_3	Camellia	CAST	MISTY	openMSP430_1	openMSP430_2	PRESENT	SEED	SPARX	TDEA
Original Design	66.667	68.906	67.72	1.691	4.596	3.302	0.375	1.161	0.377	4.596	2.252	1.482
ICAS [10]	69.807	70.092	73.863	1.634	6.274	3.141	0.372	1.186	0.41	4.615	2.253	1.458
BISA [11]	81.752	91.424	84.35	2.554	9.124	5.848	0.473	2.069	0.483	6.172	3.065	1.927
Ba *et al.* [12], [13]	75.403	77.38	74.583	2.104	5.973	3.954	0.388	1.536	0.434	4.892	2.266	1.503
GDSII-Guard	71.874	72.782	70.548	1.812	5.168	3.893	0.394	1.214	0.395	4.678	2.249	1.533

#DRC	AES_1	AES_2	AES_3	Camellia	CAST	MISTY	openMSP430_1	openMSP430_2	PRESENT	SEED	SPARX	TDEA
Original Design	0	12	0	0	0	0	0	0	0	0	0	0
ICAS [10]	0	15	0	0	0	0	0	0	0	9	0	0
BISA [11]	11	57	5	3	45	0	0	18	0	24	0	13
Ba *et al.* [12], [13]	5	41	0	0	19	0	0	3	0	11	0	0
GDSII-Guard	0	16	0	0	3	0	0	0	0	0	0	0

- Minimal overall timing, power and design quality downgradation
- Strick a good balance between security and timing

Conclusion

- ECO layout enhancement
  - ✓Multi-objective (security, PPA) optimization formulation
  - ✓Flexible ECO anti-Trojan P&R flow
  - ✓Efficient flow parameter tuning
- The results show that
  - ✓GDSII-Guard significantly improves layout security
  - ✓GDSII-Guard reduces timing, DRC, power side effects brought by security measures

Thank You!

Welcome to my poster for more details

weixinmming@pku.edu.cn