

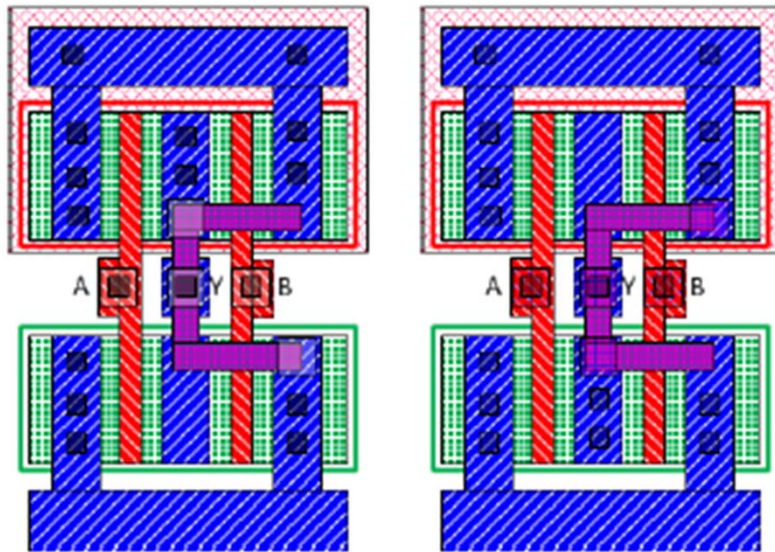


Improved Metrics for Obfuscated ICs

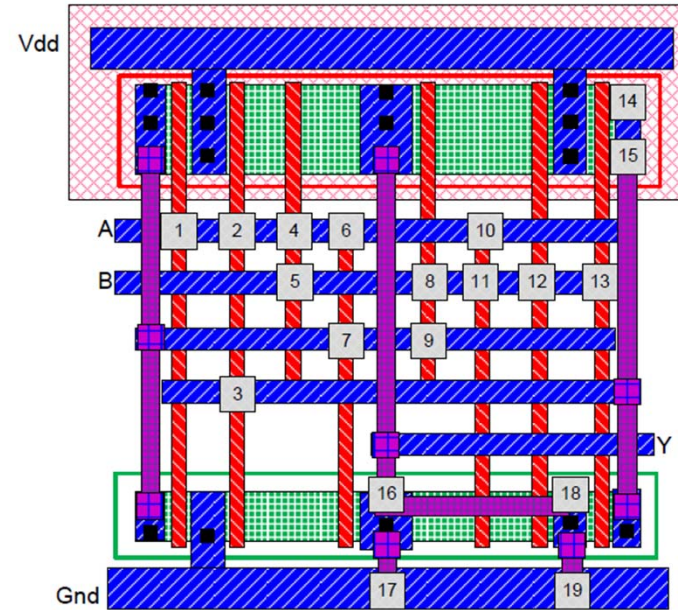
Mutian Zhu, Matthew French, and Peter A. Beerel



Introduction to Obfuscation



Obfuscated NAND and NOR gate



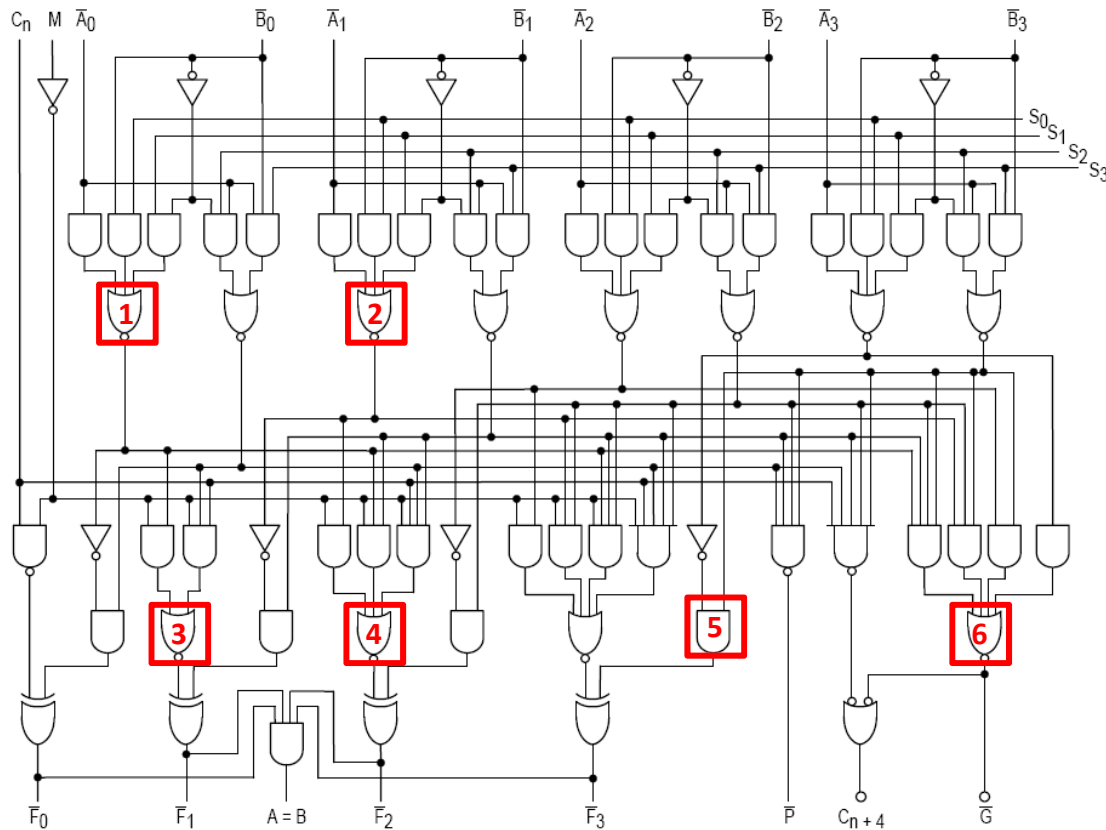
Can perform either as XOR, NAND , or NOR based on which contacts are true and dummy

- Cannot easily tell the function of an obfuscated element by observing its layout.

[J Rajendran, 2013]



Introduction to Obfuscation



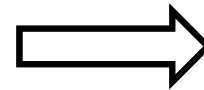
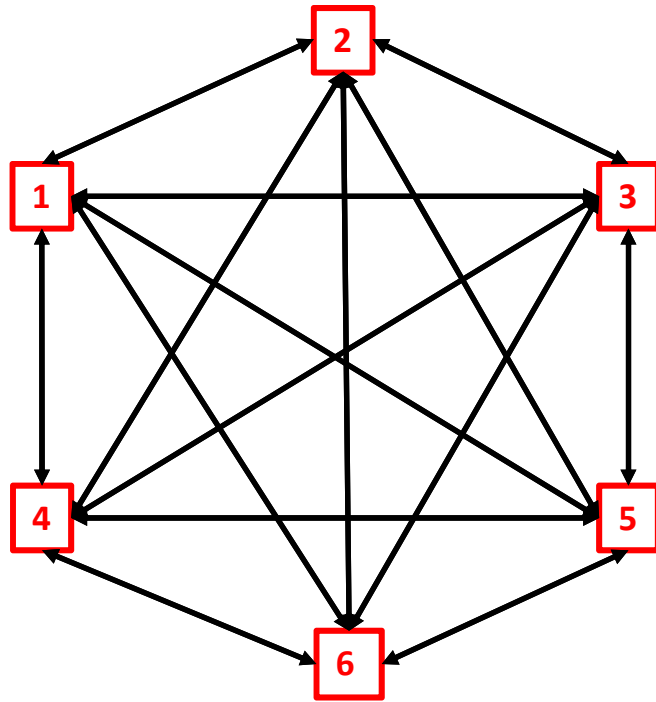
Obfuscated elements

- Obfuscation elements can be put at the key part(s) of a circuit.

[Circuit from Wikipedia]




Our Assumption: Identities may be Correlated



$$\begin{bmatrix} 1 & \rho_{12} & \dots & \rho_{15} & \rho_{16} \\ \rho_{21} & 1 & \dots & \rho_{25} & \rho_{26} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \rho_{51} & \rho_{52} & \dots & 1 & \rho_{56} \\ \rho_{61} & \rho_{62} & \dots & \rho_{65} & 1 \end{bmatrix}$$

ρ_{ij} Correlation coefficient between elements i and j

 Obfuscated elements

 Pair-wise correlation between identities of obfuscation elements exist



Expected Number of Attacks

A. Brute Force Attack

$$E[N] = 2^{n-1} + 0.5$$

n : Number of obfuscation elements

B. Correlation Driven Attack

$$E[N] = \sum_{i=1}^{2^n} i \times P_{si}$$

i : Success with i attacks, P_{si} : Probability of success with the i^{th} attack

C. Entropy Lower Bound [James L. Massey, 1994]

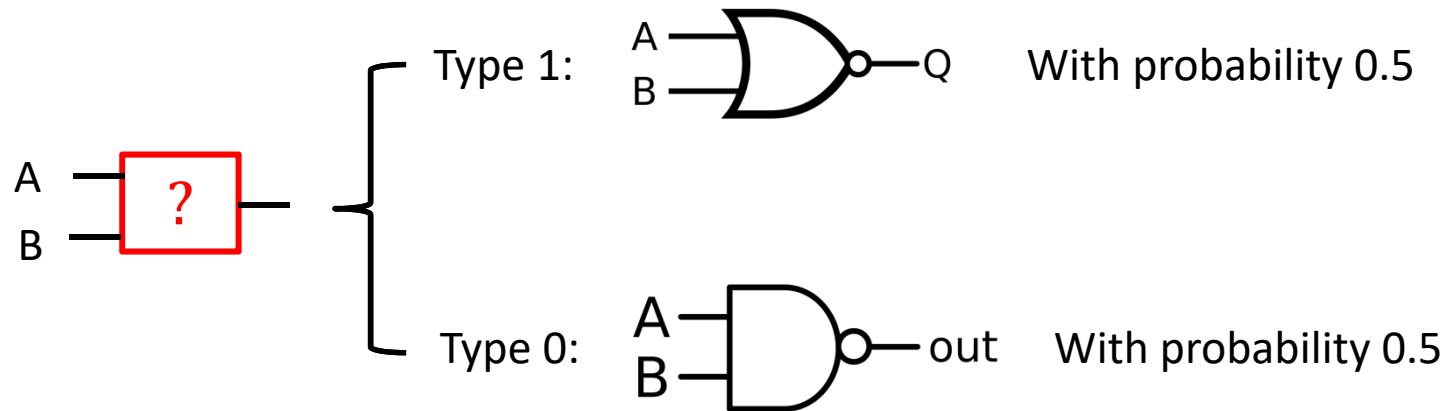
$$E[N] \geq \left(\frac{1}{4}\right) 2^{H(P)} + 1$$

P : Joint distribution of all possible key combinations.

$H(P)$: The entropy of P



Constraints on the Joint Distribution



- Then the mathematical definition of ρ_{ij} gives:

$$P_{ij}(1, 1) = \frac{1}{4} + \frac{\rho_{ij}}{4}$$

$P_{ij}(1, 1)$: Probability of obfuscation element i and j both taking type one.



Constraints on the Joint Distribution

- The definition of marginal distribution gives the system of equations:

$$\begin{cases} P_i(1) = P_{ij}(1,0) + P_{ij}(1,1) = 0.5 \\ P_j(0) = P_{ij}(0,0) + P_{ij}(0,1) = 0.5 \\ P_i(1) = P_{ij}(0,1) + P_{ij}(1,1) = 0.5 \end{cases}$$

- By solving them gives us:

$$P_{ij}(0,0) = P_{ij}(1,1) = \frac{1}{4} + \frac{\rho_{ij}}{4}$$
$$P_{ij}(1,0) = P_{ij}(0,1) = \frac{1}{4} - \frac{\rho_{ij}}{4}$$

- Each $P_{ij}(u, v)$ also satisfies

$$\sum_{k=1}^{2^n} a_k P_{12\dots n}(x_1, \dots, x_n) = P_{ij}(u, v), a_k \in \{0,1\}$$

where a_k equals one if and only if $x_i = u$ and $x_j = v$ and $u, v \in \{0,1\}^2$



Constraints on the Joint Distribution

- This yields system of linear equations:

: Obfuscated elements

$$\begin{array}{c}
 \square \times n \longrightarrow \left\{ \begin{array}{l} \rho_{12} \\ \rho_{13} \\ \vdots \\ \rho_{ij} \\ \vdots \\ \rho_{n-1n} \end{array} \right. \longrightarrow \left\{ \begin{array}{l} P_{ij}(0,0) \\ P_{ij}(0,1) \\ P_{ij}(1,0) \\ P_{ij}(1,1) \end{array} \right. \longrightarrow \sum_{k=1}^{2^n} a_k P_{12\dots n} = P_{ij}(u,v), a_k \in \{0,1\}
 \end{array}$$



$$A \times \underline{P} = b$$

A : Boolean parameter matrix of a_k 's

$$\underline{P} = \begin{bmatrix} P_{12\dots n}(0, \dots, 0) \\ \vdots \\ P_{12\dots n}(1, \dots, 1) \end{bmatrix} \qquad b = \begin{bmatrix} P_{12}(0,0) \\ \vdots \\ P_{n-1n}(1,1) \end{bmatrix}$$



Choosing the Joint Distribution

- Choose the solution with maximum entropy:

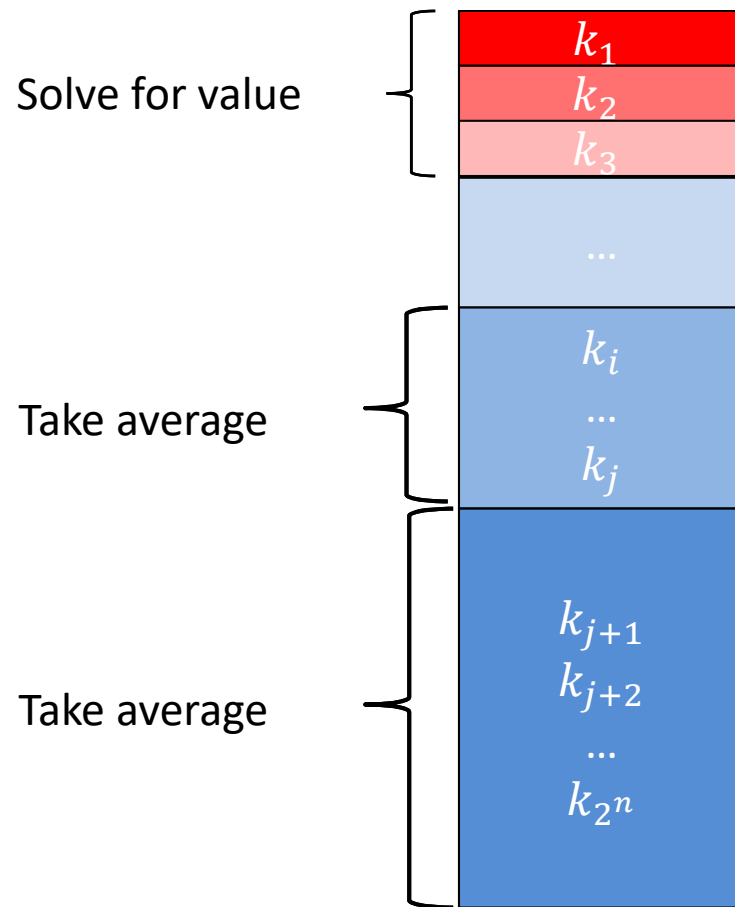
$$\underset{\underline{P}}{\operatorname{argmin}} \sum_{i=1}^{2^n} P(i) \log[P(i)]$$

$$\text{subject to } P(i) \geq 0, i = 1, 2, \dots, 2^n \\ A \times \underline{P} = b$$

- Yields the largest number of expected guesses
- Can be implemented using known optimization algorithms
 - Easily implemented
 - But limited to small n due to exponential number of constraints

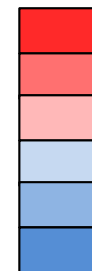


Complexity Reduction: Approximation Algorithm



- k_i : The key with i -th highest probability to be correct.

High probability



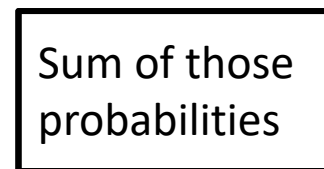
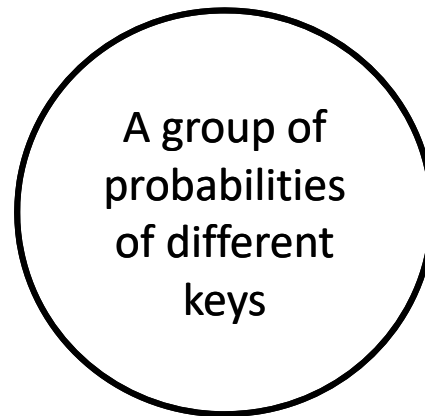
Low probability



Approximation Algorithm

- Take another look at the equation:

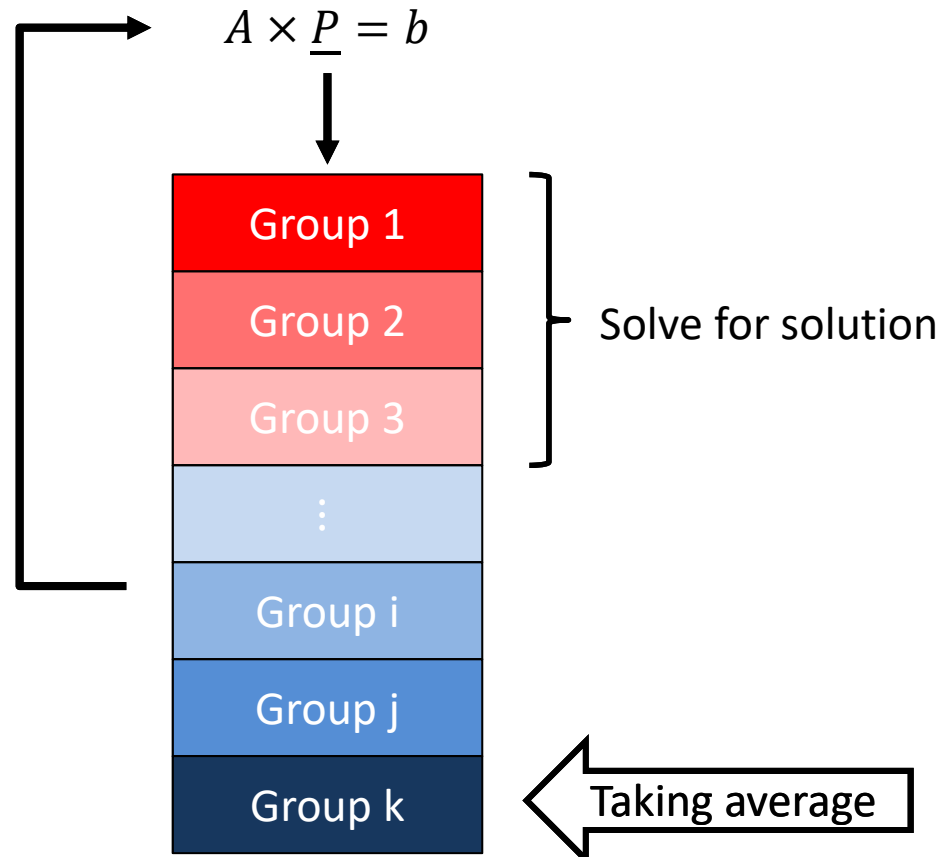
$$\sum_{k=1}^{2^n} a_k P_{12\dots n}(x_1, \dots, x_n) = P_{ij}(u, v), a_k \in \{0,1\}$$



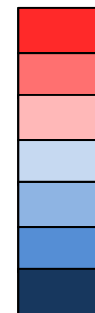


Approximation Algorithm

- Remove overlapped parts
- Update A and b



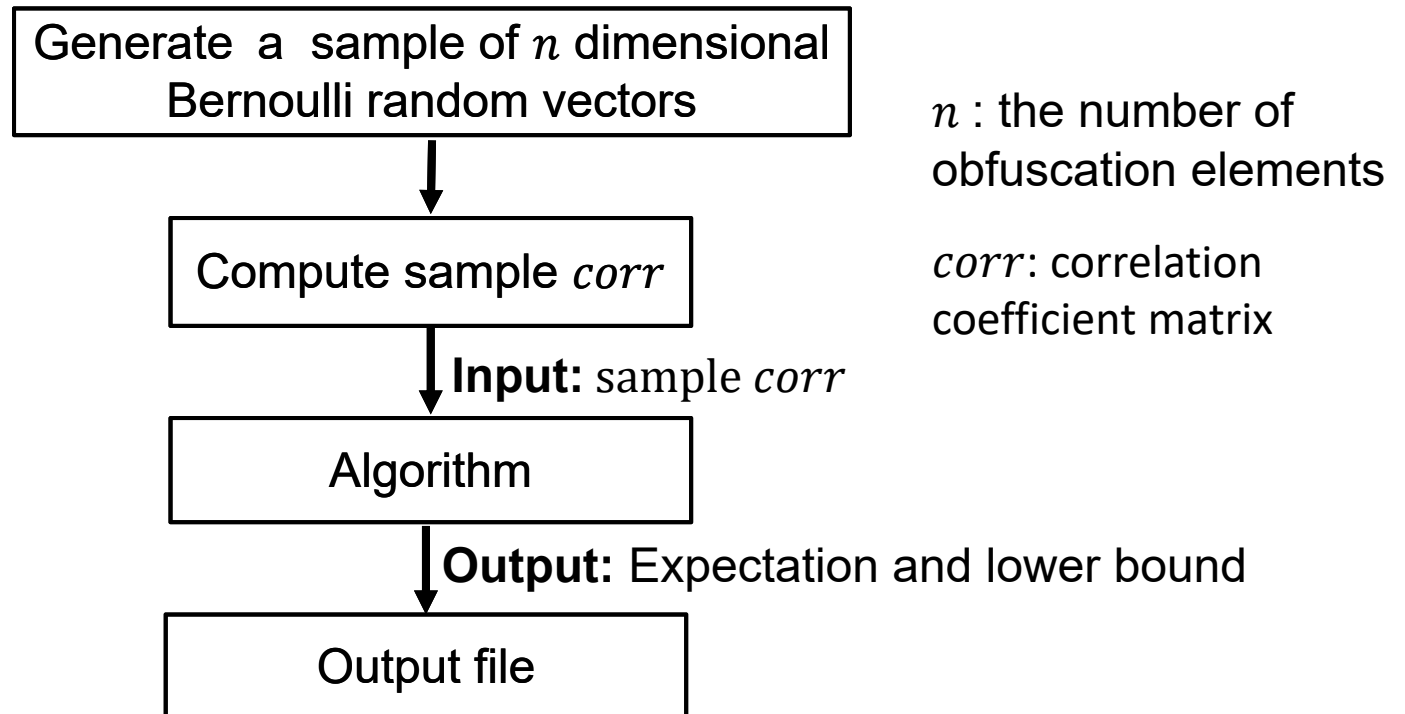
High average probability



Low average probability

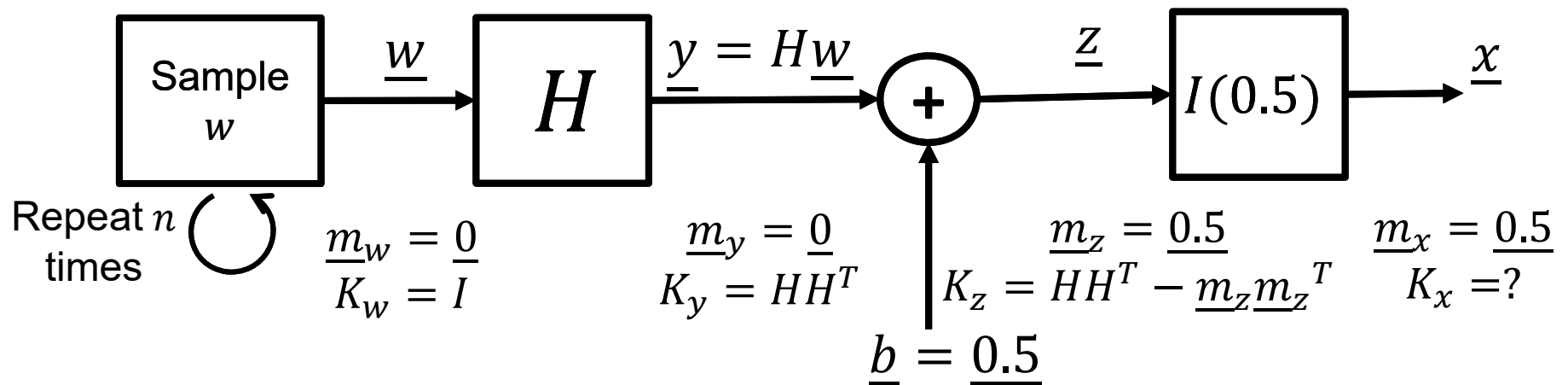


Experimental Results: Simulation





Generate a Bernoulli Random Vector



- w : follows elementary Gaussian distribution $N(0,1)$
- \underline{m} : mean vector
- K : covariance matrix.
- H : A random matrix used to create the correlations
- $I(0.5)$: Indicator function with threshold 0.5.
- \underline{x} : Sampled Bernoulli random vector with non-identity covariance matrix.



Compute Sample Correlation Coefficient Matrix

Repeatedly perform sampling procedure: $X = [\underline{x}_1, \underline{x}_2 \dots \underline{x}_S]$



Sample Correlation matrix: $\widehat{R}_x = \frac{XX^T}{S}$, Sample mean: $\widehat{m}_x = \frac{\sum_{i=1}^S x_i}{S}$



Sample covariance matrix: $\widehat{K}_x = \widehat{R}_x - \widehat{m}_x \widehat{m}_x^T$



Sample correlation coefficient: $\widehat{\rho}_{ij} = \frac{\widehat{K}_x(i, j)}{\sqrt{\widehat{K}_x(i, i)} \sqrt{\widehat{K}_x(j, j)}}$

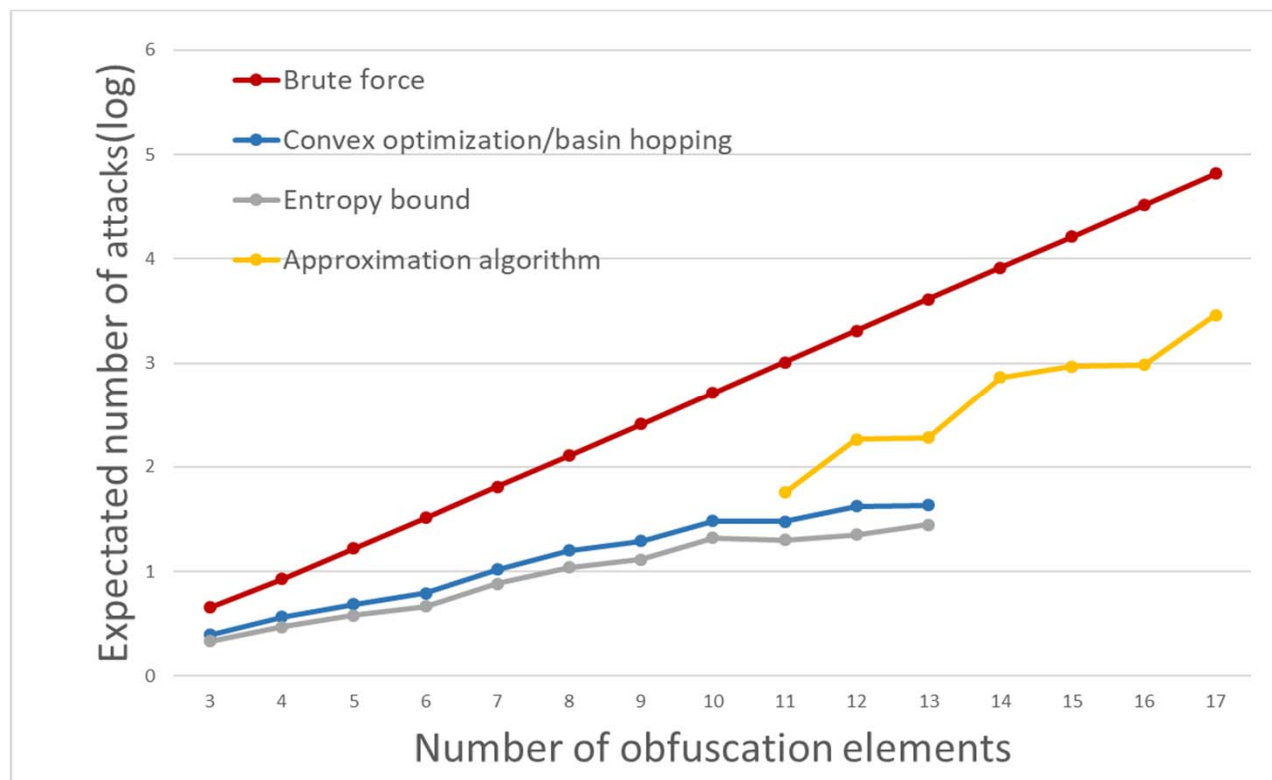


Sample correlation coefficient matrix: *corr*



Simulation Results

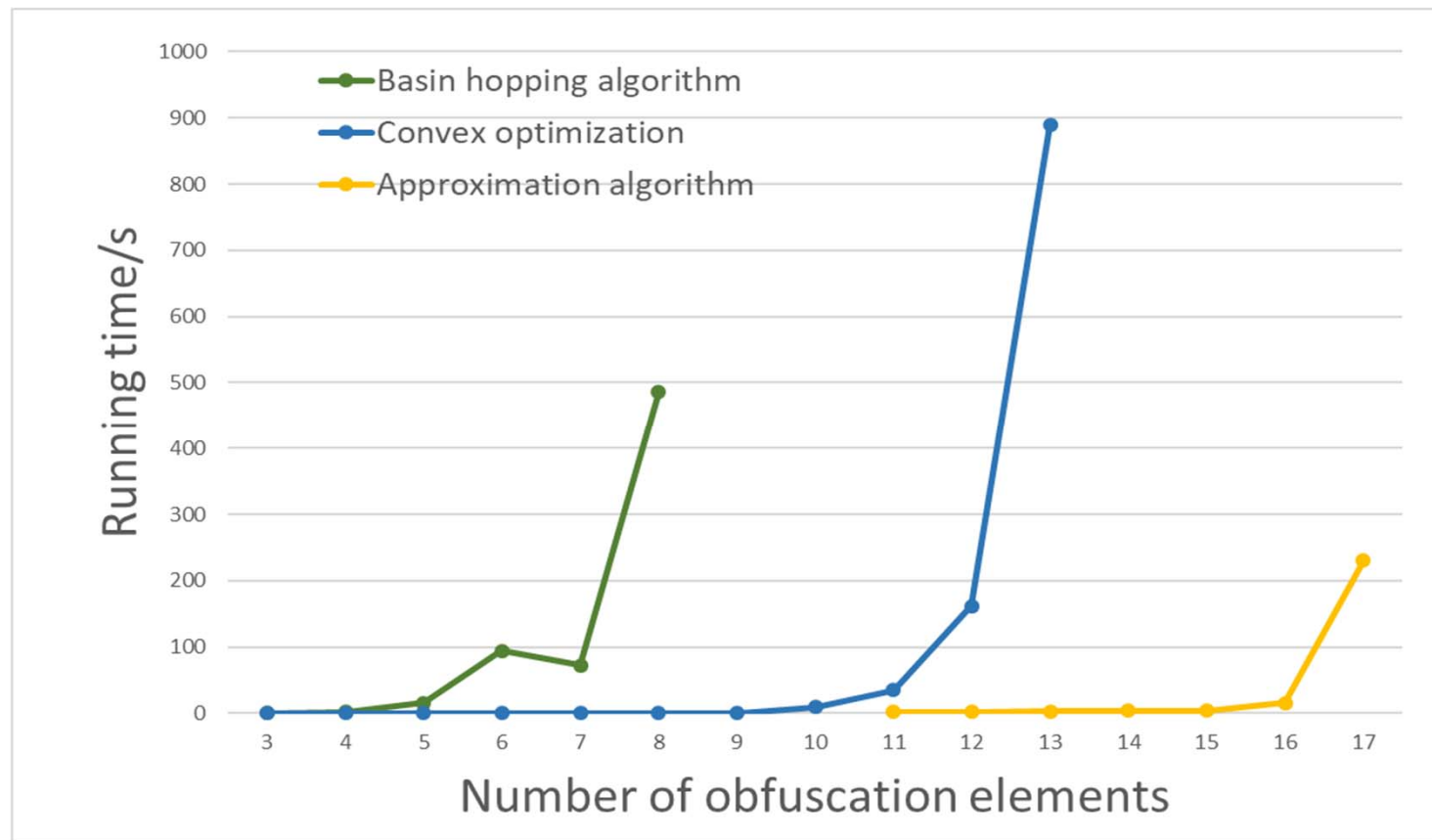
- Tested two built-in python functions to directly find the arg-min
 - Basin hopping algorithm and convex optimization solver
- Implemented approximation algorithm in python using numPy
 - Use convex optimization to solve for critical keys





Simulation Results

- The complexity is still a concern.





Summary and Conclusions

- Our metric shows that correlation information can reduce the number of attacks needed to reverse engineer a chip dramatically.
- If an attacker follows the strategy in our paper, the proposed metric represents an upper bound on the expected number of guesses.
- Complexity scaling exponentially with number of obfuscated elements is a challenge to both us and attackers.
- Addressing this complexity scaling problem is future work



Key References

- Massey, James L. "Guessing and entropy." *Information Theory, 1994. Proceedings., 1994 IEEE International Symposium on*. IEEE, 1994.
- Rajendran, Jeyavijayan, et al. "Security analysis of integrated circuit camouflaging." *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013.