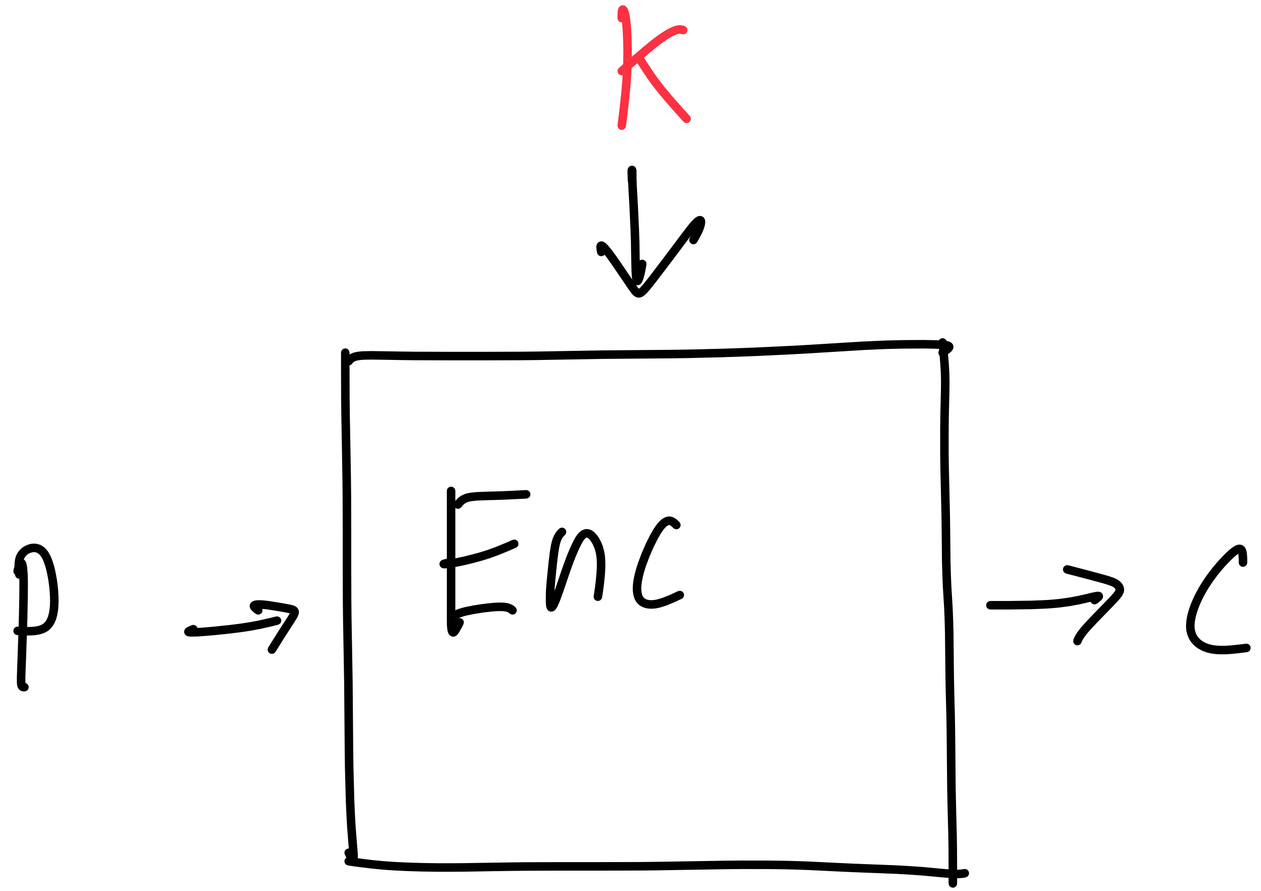
A Comparison of Graph-Inference Side-Channel Attacks Against SKINNY

CASCADE 2025

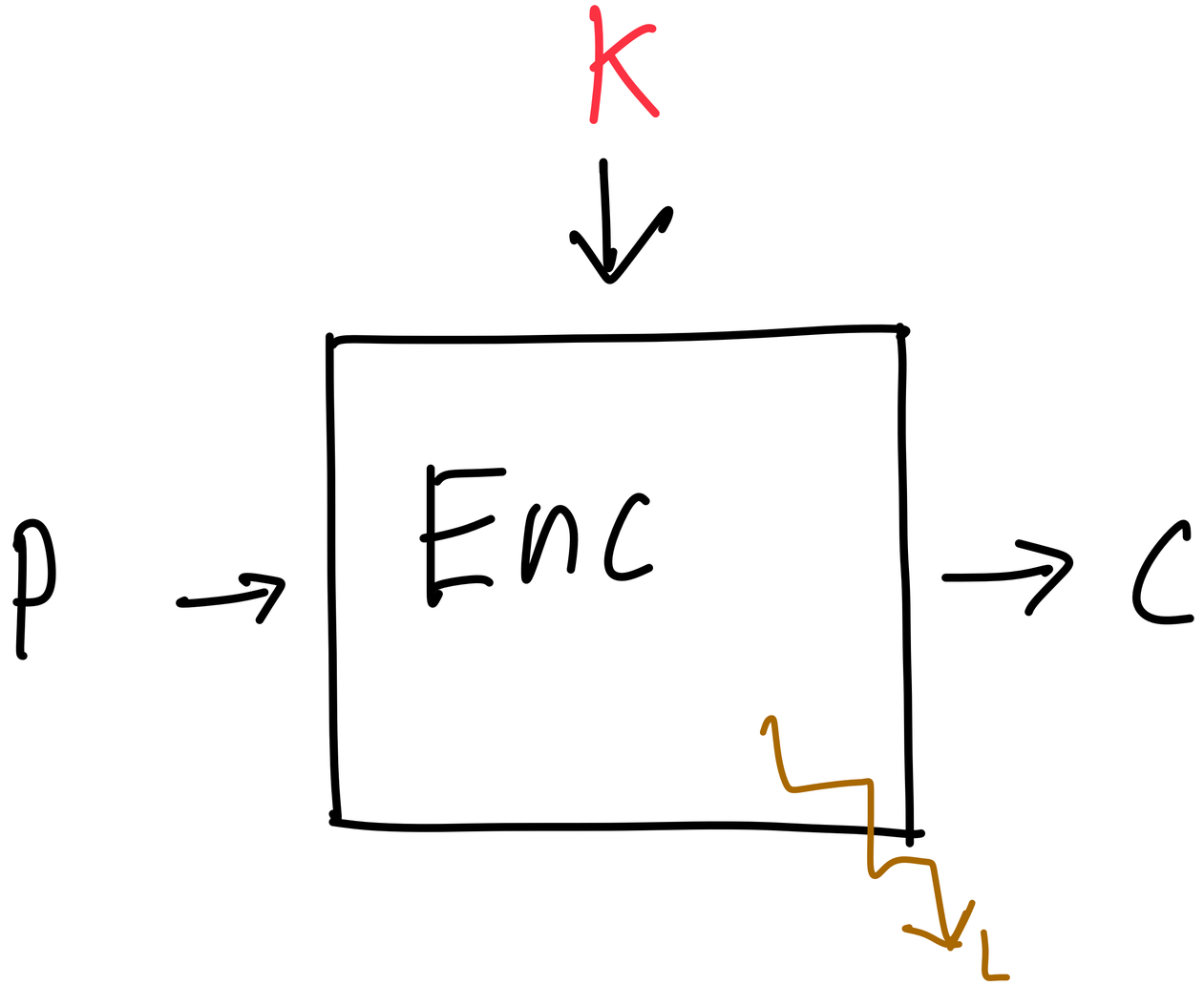
Stian Husum, Håvard Raddum and Martijn Stam

Side-Channel Analysis

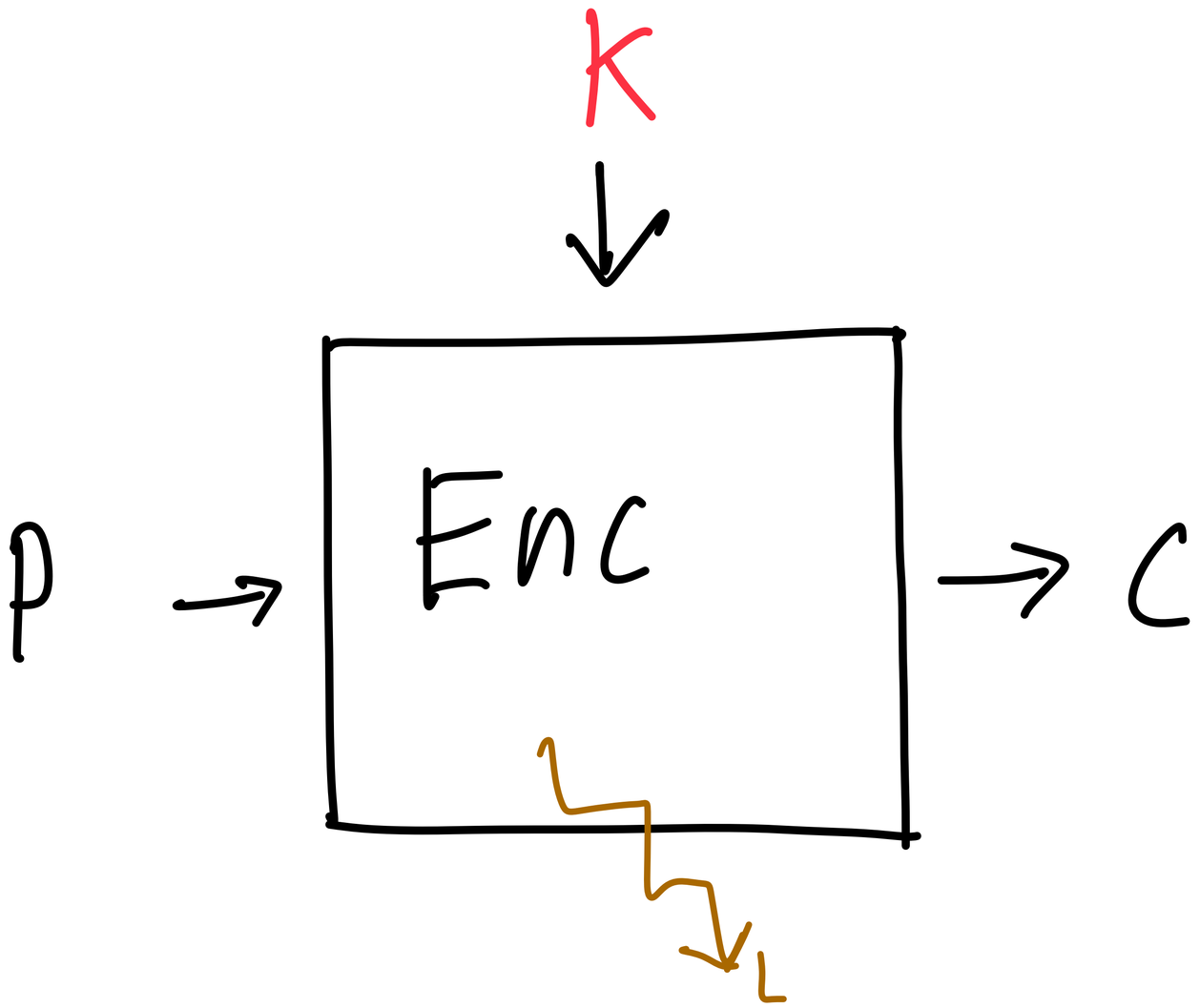
Side-Channel Analysis



Side-Channel Analysis

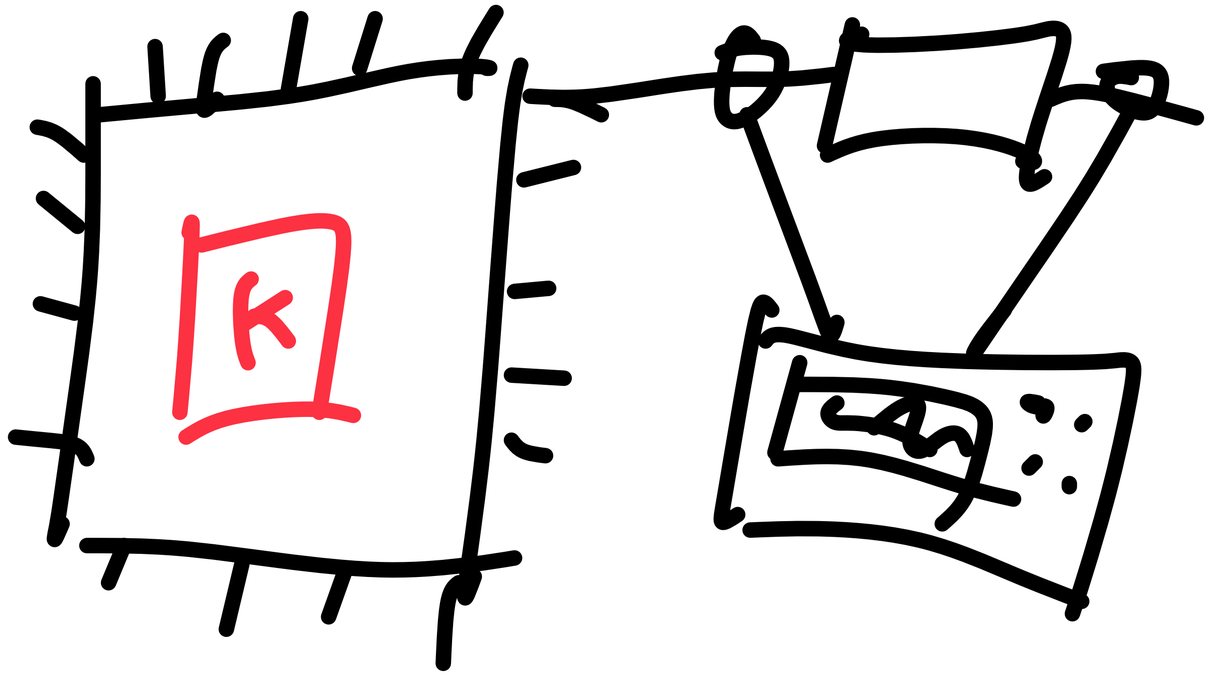


Side-Channel Analysis

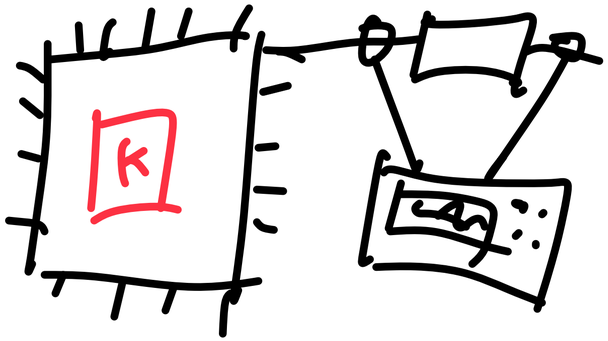


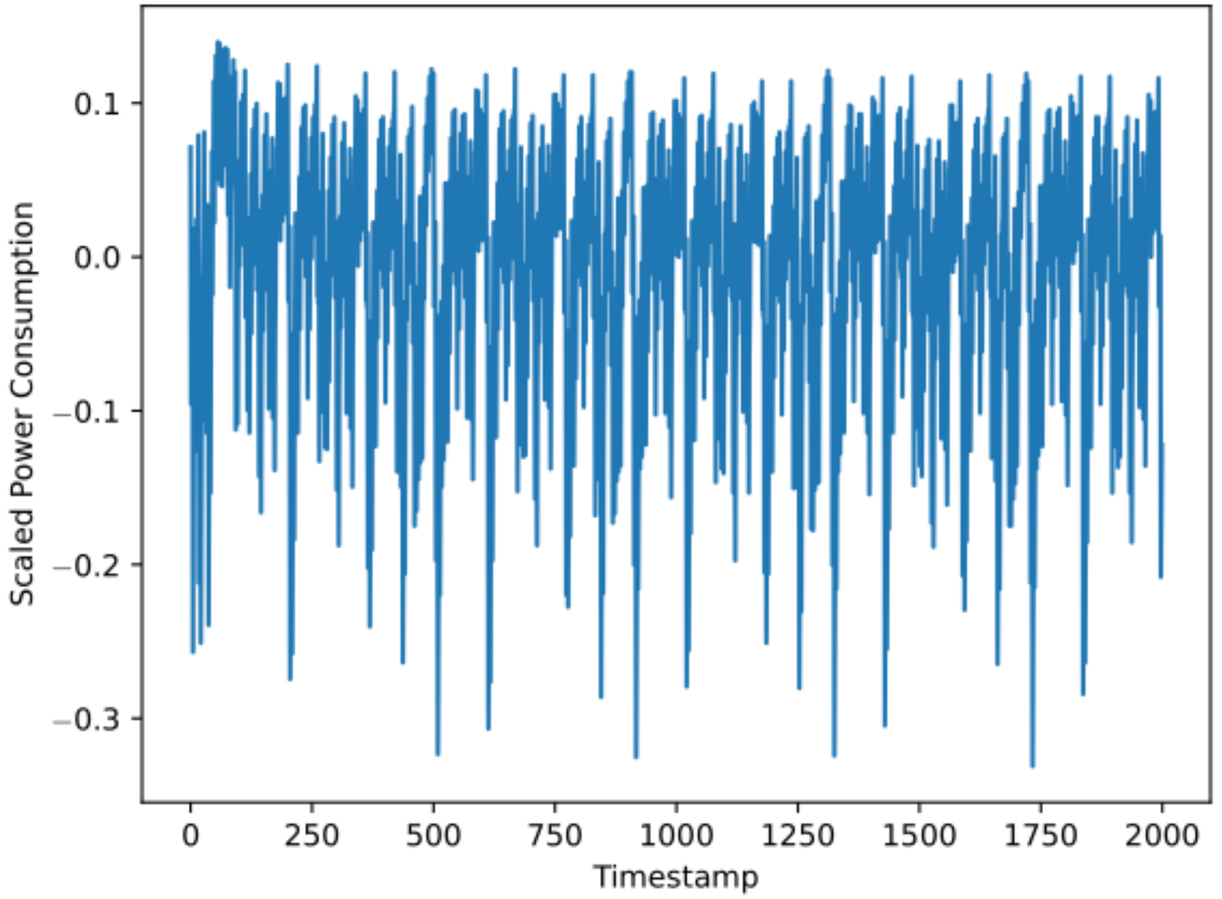
- Power Draw
- EM Radiation
- Temperature
- Sound
- Time
- Etc.

Power Analysis

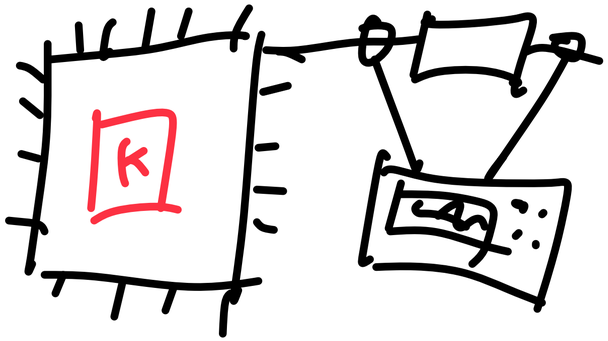


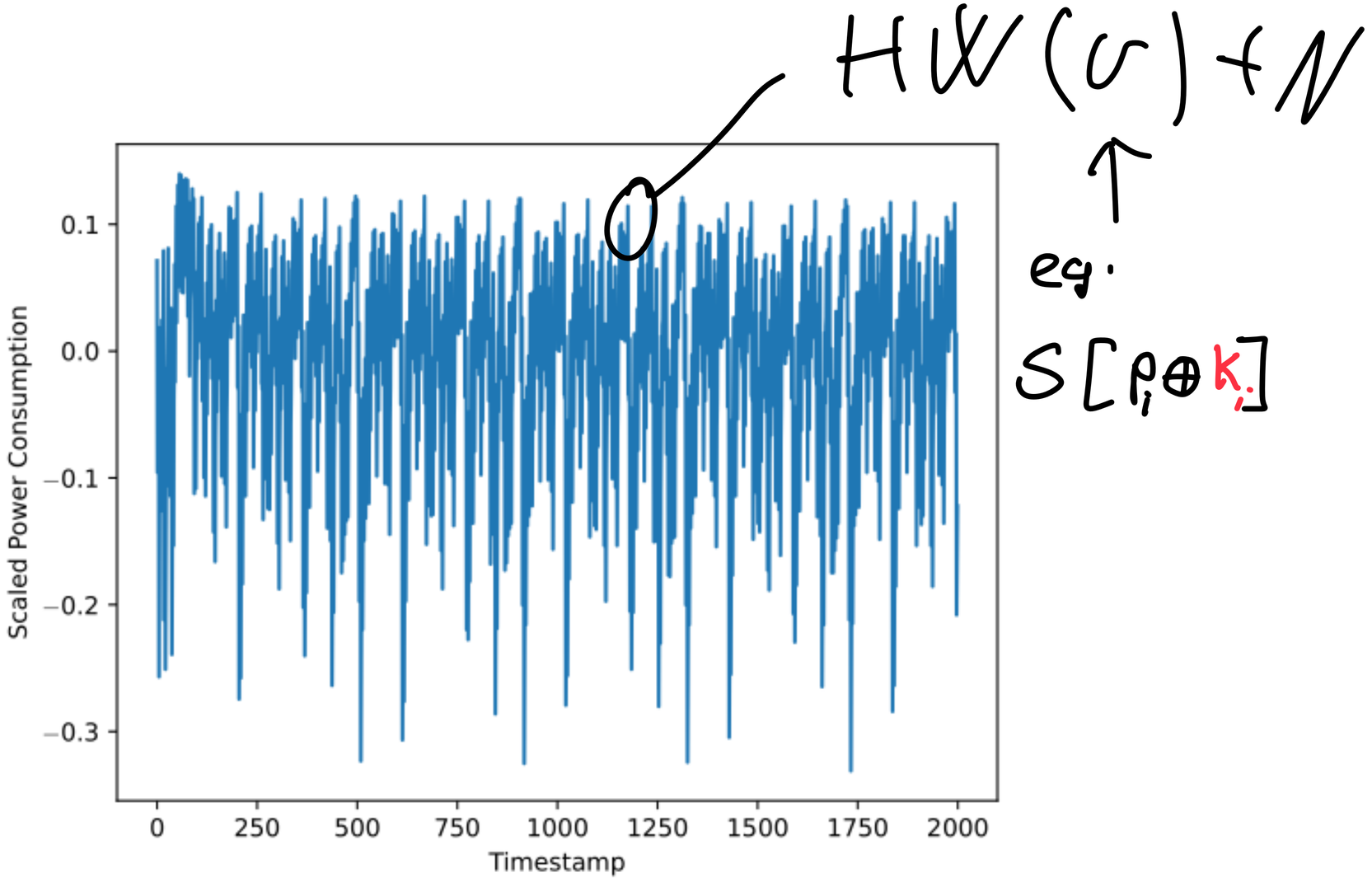
Power Analysis



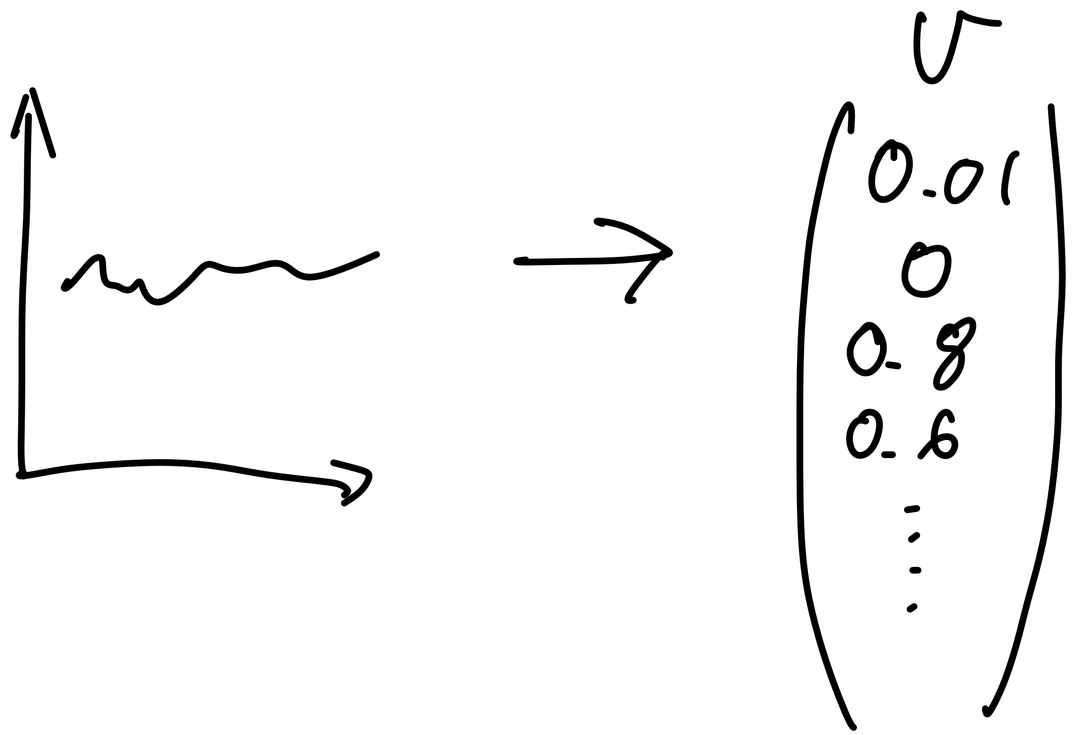


Power Analysis

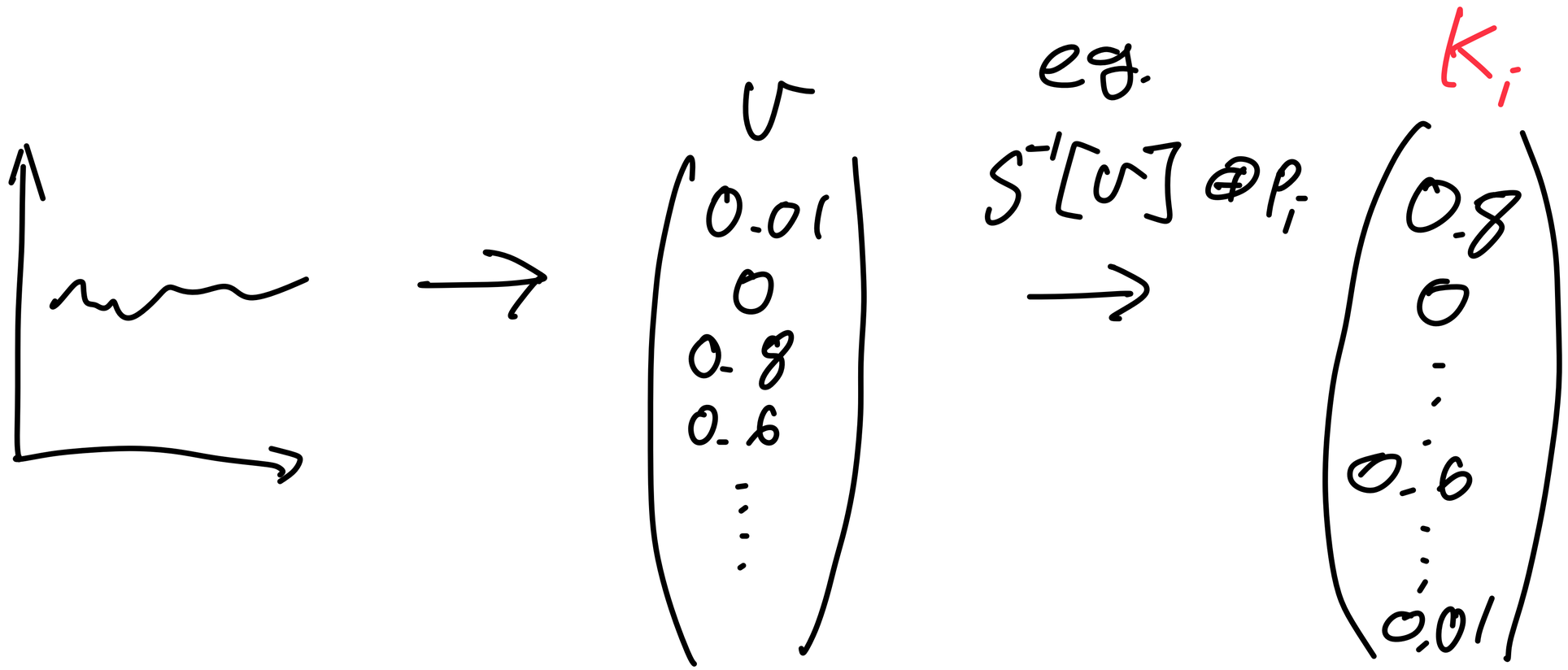




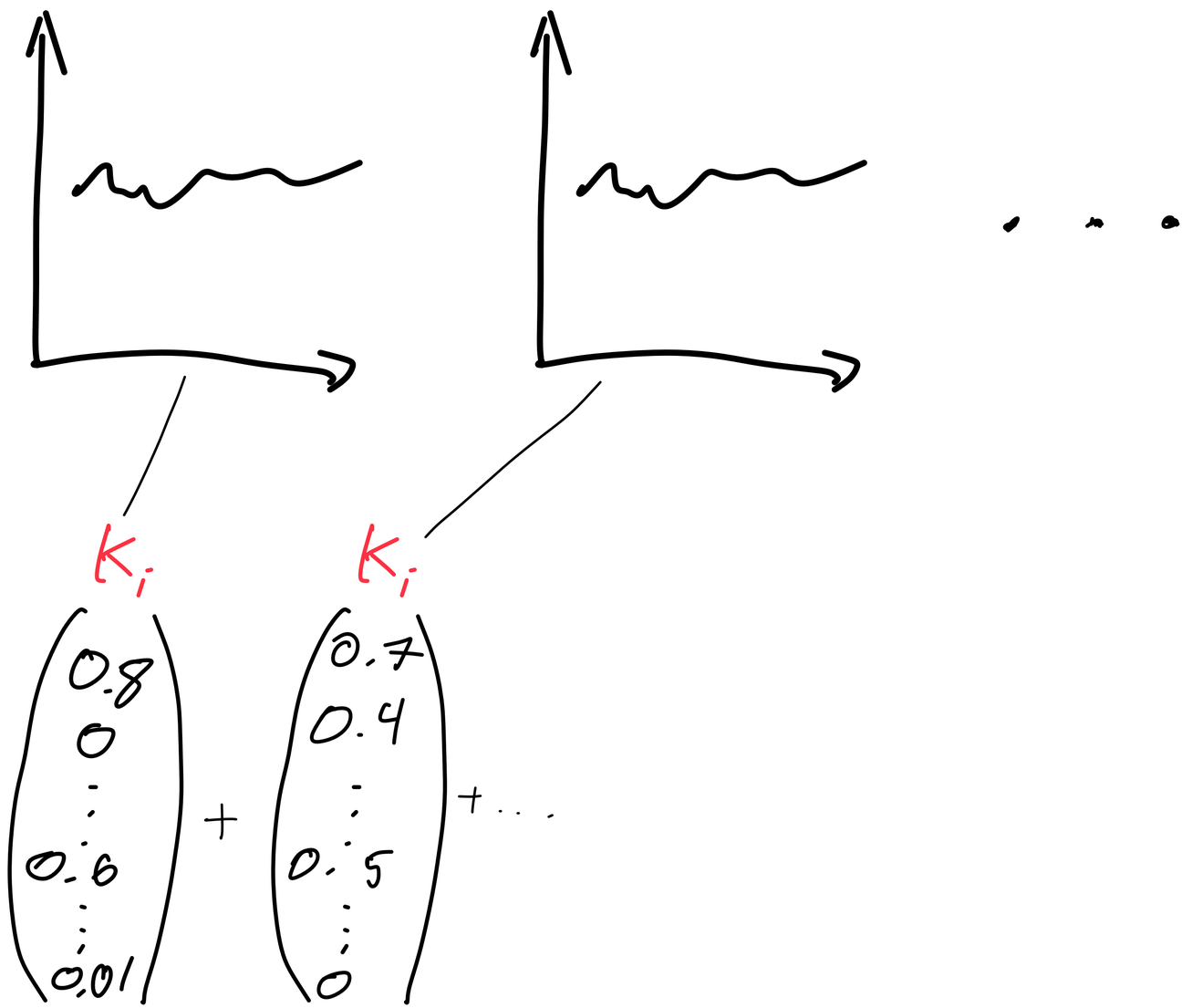
Distinguishing Scores



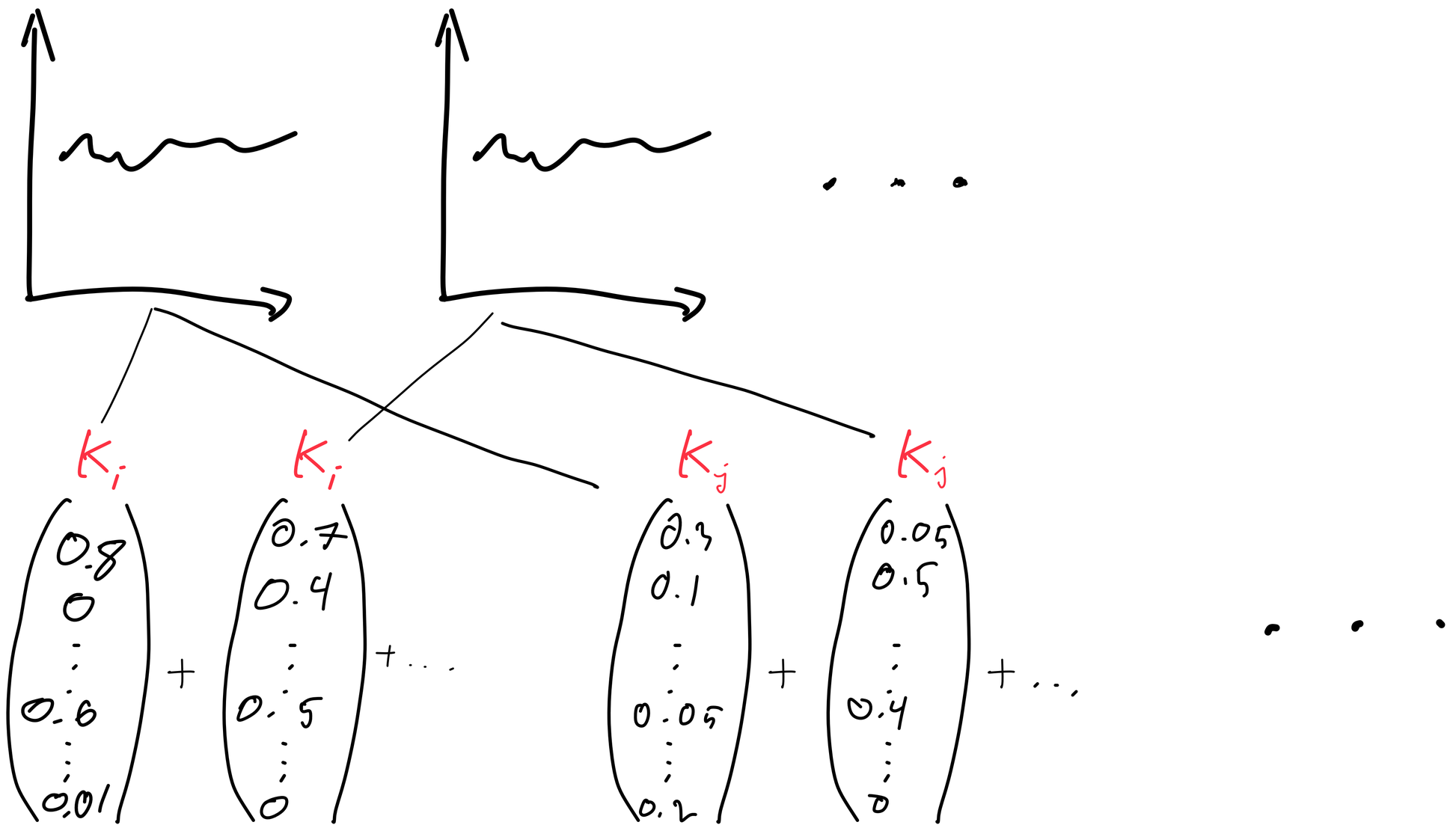
Distinguishing Scores



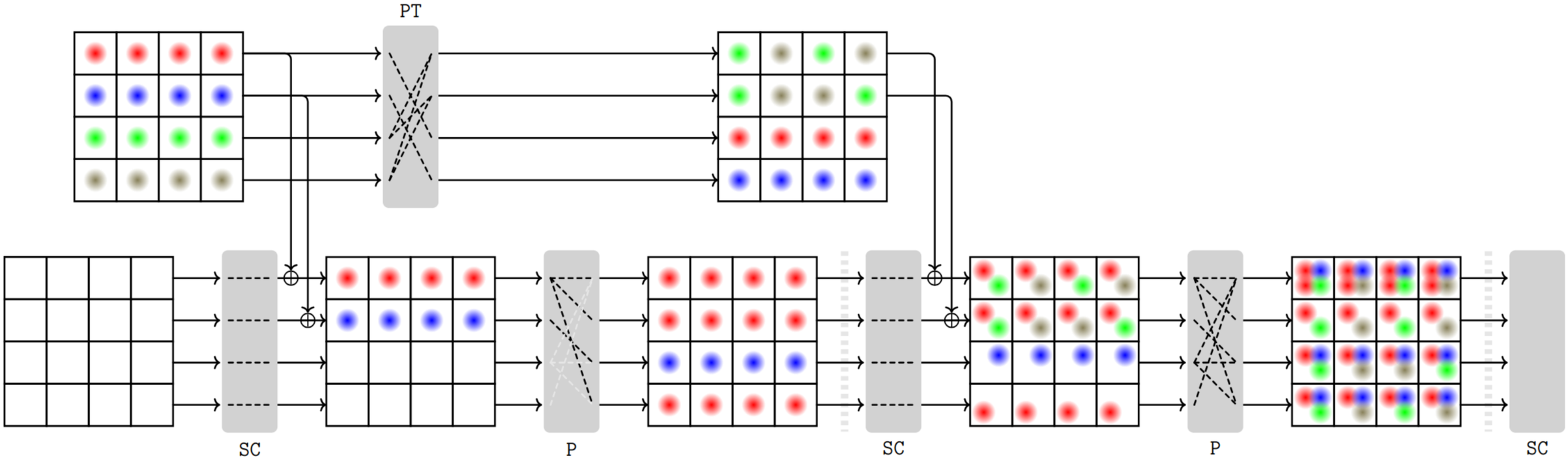
Distinguishing Scores



Distinguishing Scores

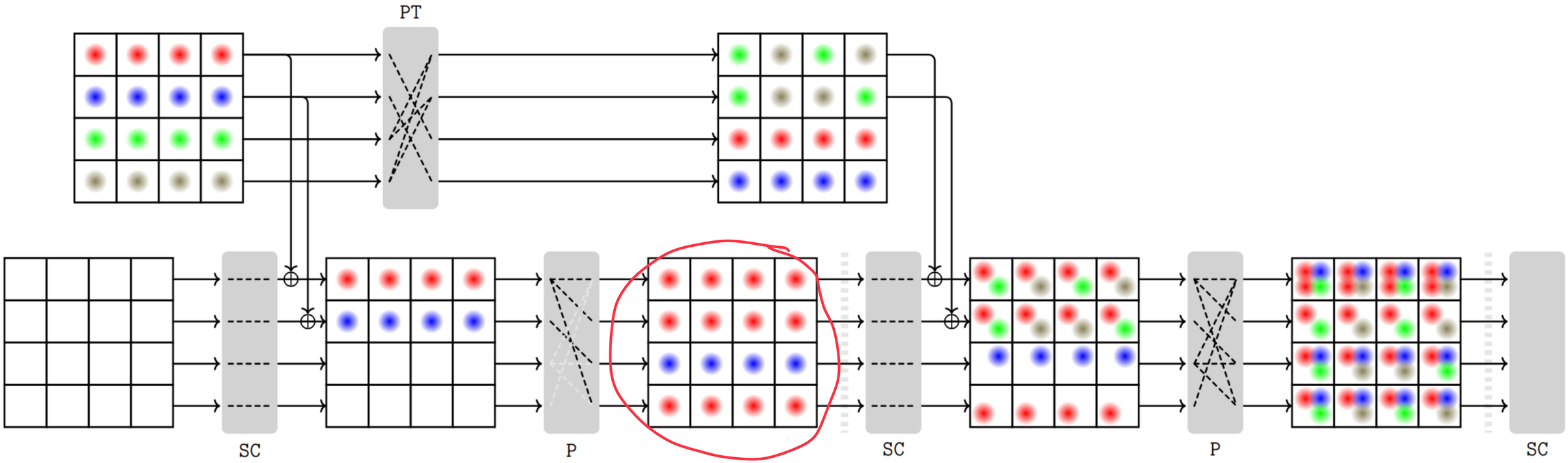


SKINNY



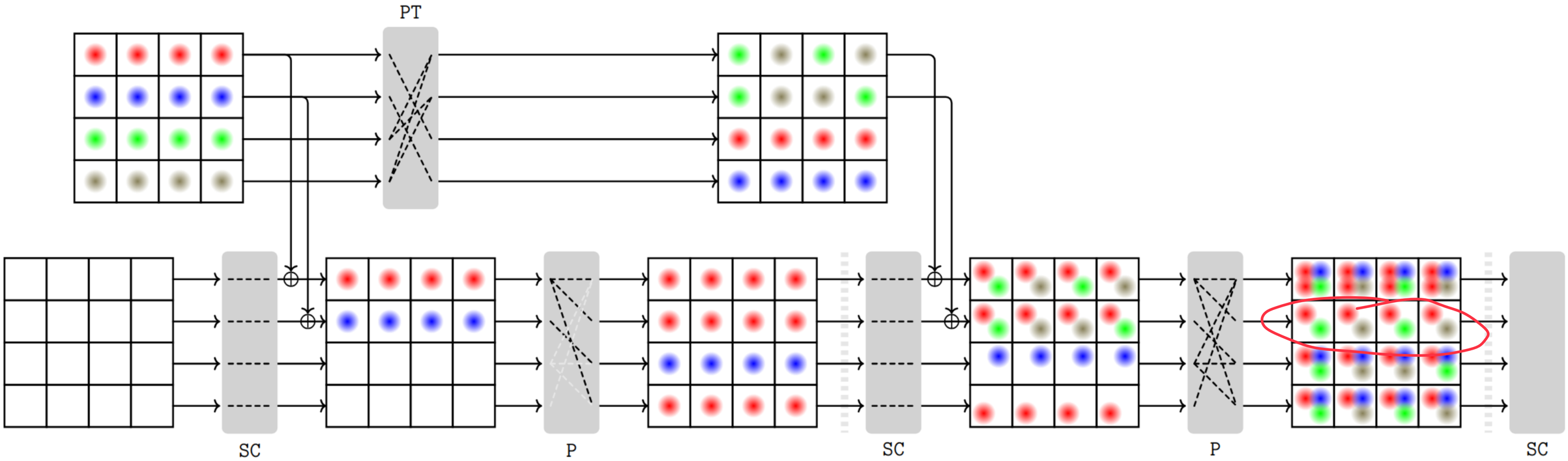
Costes, N., & Stam, M. (2023). Pincering SKINNY by Exploiting Slow Diffusion: Enhancing Differential Power Analysis with Cluster Graph Inference. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2023*(4), 460-492. https://doi.org/10.46586/tches.v2023.i4.460-492

SKINNY



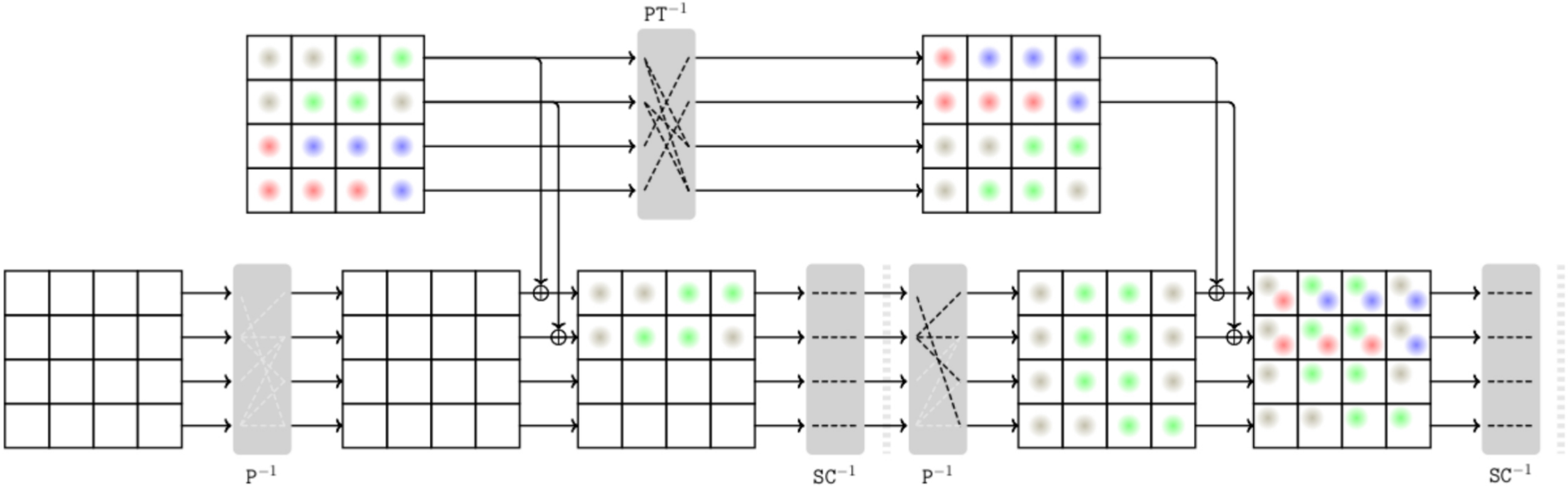
Costes, N., & Stam, M. (2023). Pincering SKINNY by Exploiting Slow Diffusion: Enhancing Differential Power Analysis with Cluster Graph Inference. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2023*(4), 460-492. https://doi.org/10.46586/tches.v2023.i4.460-492

SKINNY



Costes, N., & Stam, M. (2023). Pincering SKINNY by Exploiting Slow Diffusion: Enhancing Differential Power Analysis with Cluster Graph Inference. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2023*(4), 460-492. https://doi.org/10.46586/tches.v2023.i4.460-492

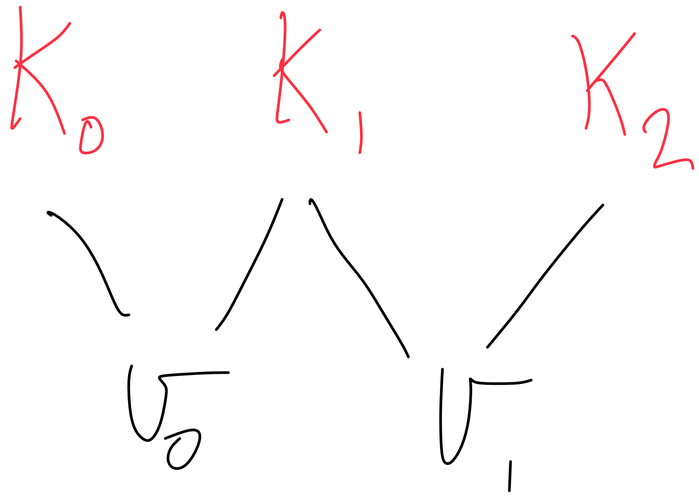
SKINNY: Last Rounds



Costes, N., & Stam, M. (2023). Pincering SKINNY by Exploiting Slow Diffusion: Enhancing Differential Power Analysis with Cluster Graph Inference. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2023*(4), 460-492. https://doi.org/10.46586/tches.v2023.i4.460-492

Central Problem

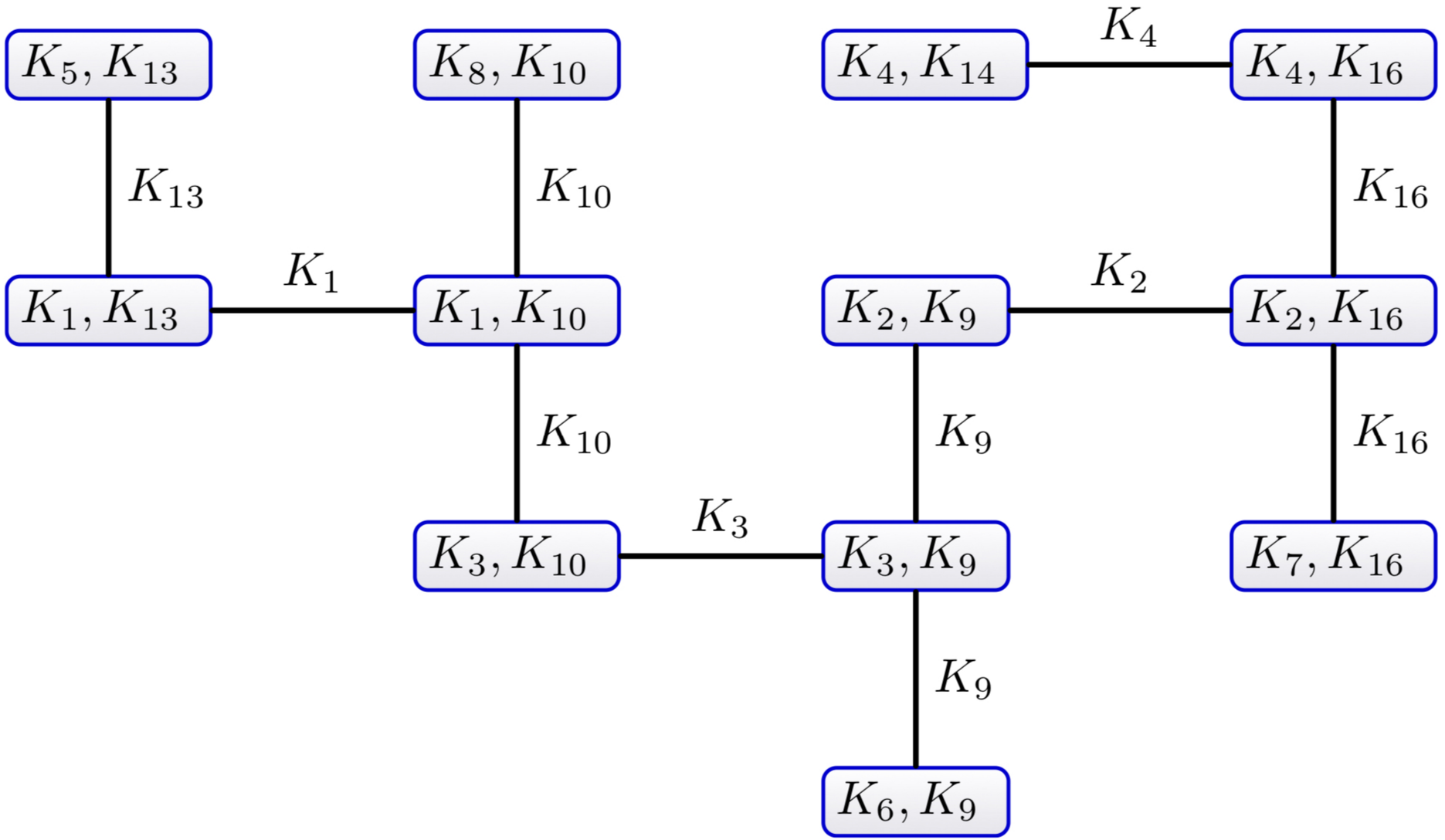
- How do we combine scores when variables depend on multiple keybytes?



Graph Inference

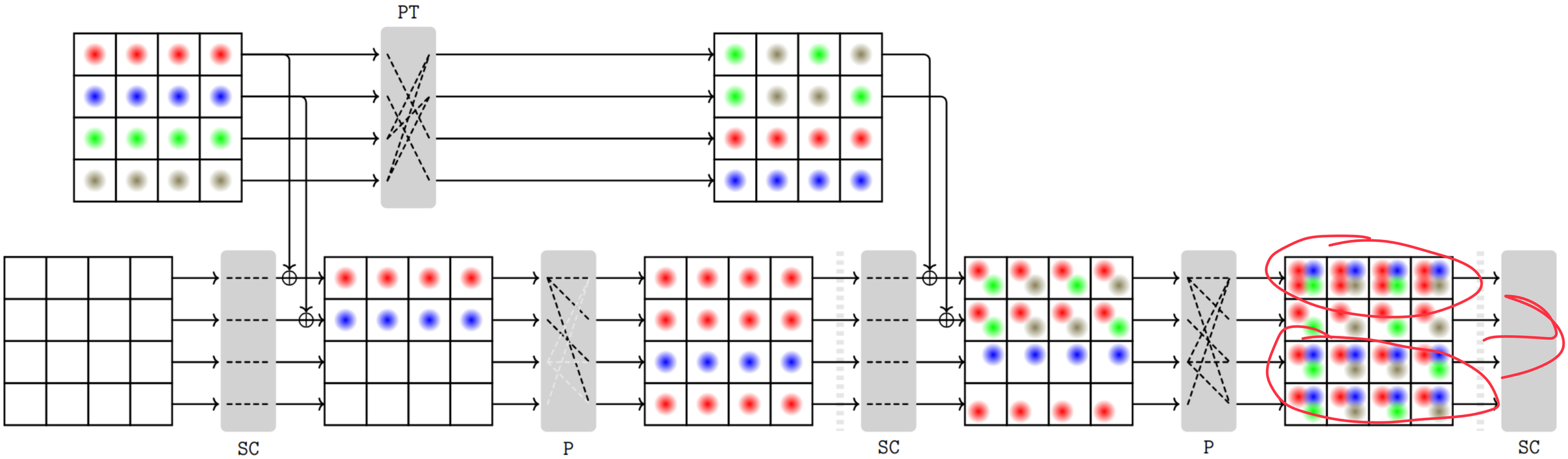
- Describe relations between variables as a graph
- Instantiate nodes with scores
- Run belief propagation on graph to consolidate scores
- Extract final scores

Cluster Graph Inference



Costes, N., & Stam, M. (2023). Pincering SKINNY by Exploiting Slow Diffusion: Enhancing Differential Power Analysis with Cluster Graph Inference. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2023*(4), 460-492. https://doi.org/10.46586/tches.v2023.i4.460-492

SKINNY

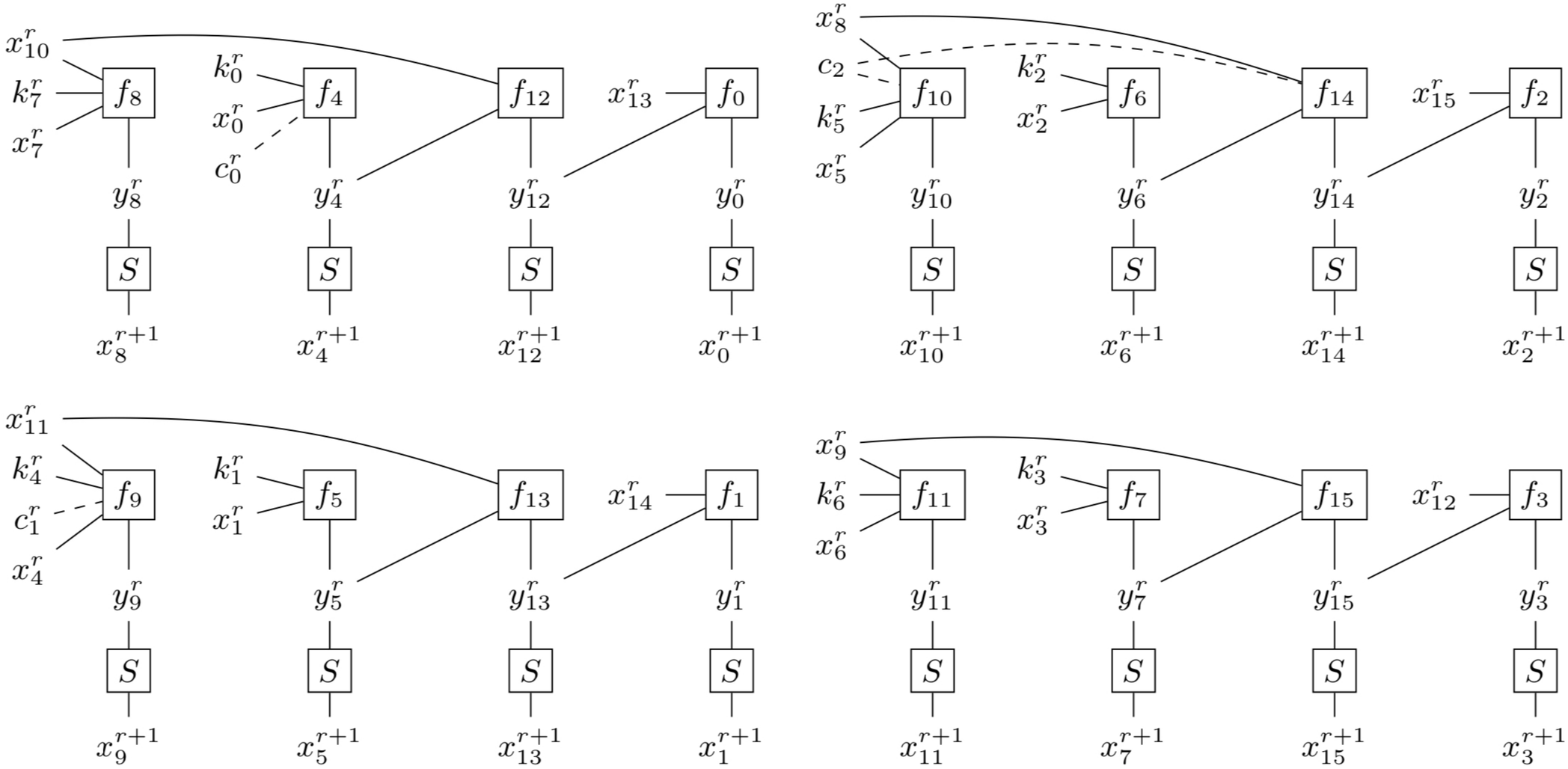


Costes, N., & Stam, M. (2023). Pincering SKINNY by Exploiting Slow Diffusion: Enhancing Differential Power Analysis with Cluster Graph Inference. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2023*(4), 460-492. https://doi.org/10.46586/tches.v2023.i4.460-492

(Large) Factor Graph Inference (LFGI, SASCA)

- Bipartite graph with:
- - Variable nodes corresponding to variables in cipher
- - Factor nodes corresponding to operations in cipher

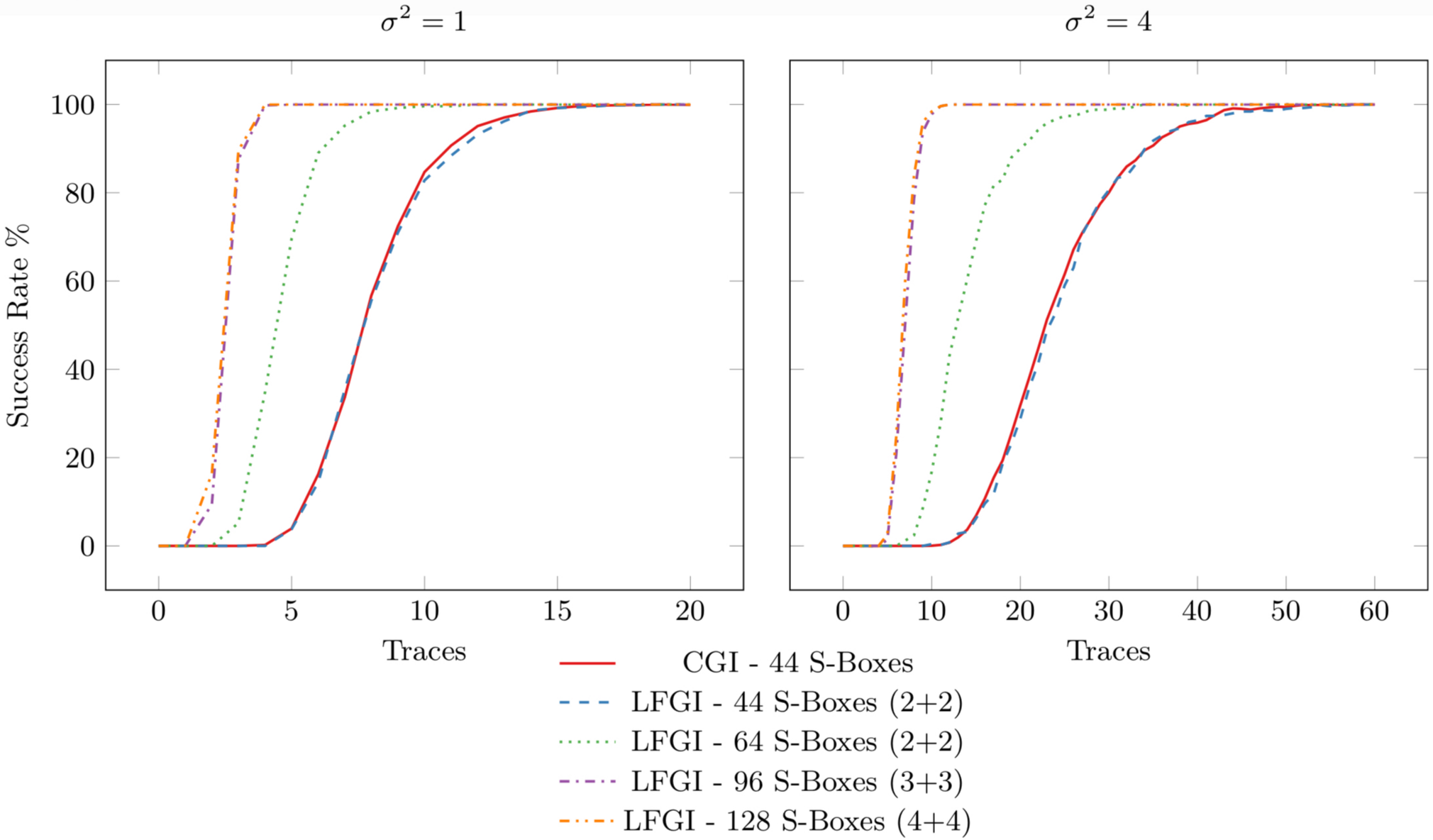
SKINNY Graph Construction



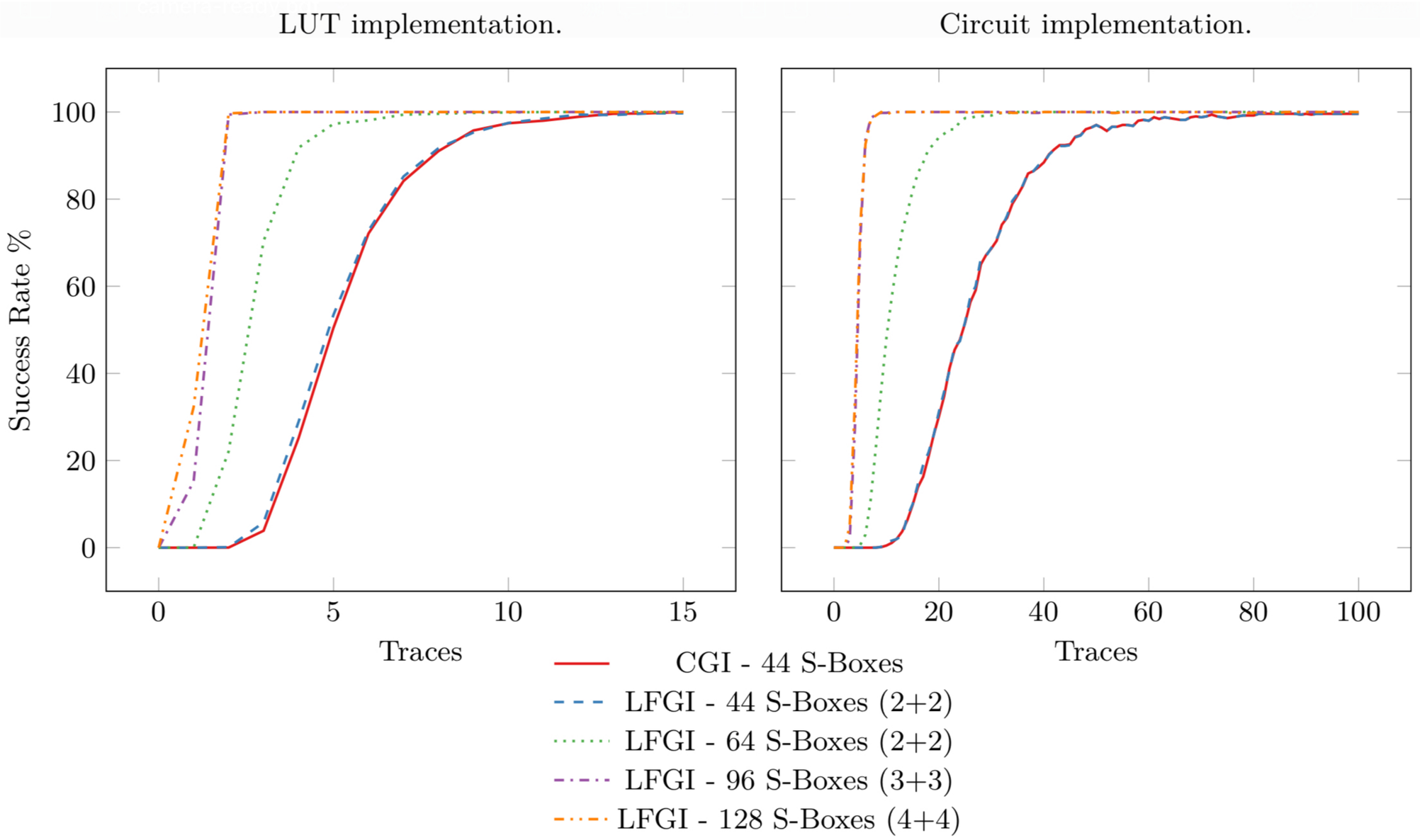
Caveats

- CGI is:
- - Acyclic and therefore inference is exact
- - Can be used with unprofied distinguishers
- FGI is:
- - Loopy and therefore inference is heuristic
- - Need an profiled distinguisher

Results: Synthetic



Results: Real Traces



Summary

- LFGI can exploit leakage deeper into the cipher compared to CGI
- LFGI is however limited to profiled attacks
- Focused on only the inference step in the attack, a tailored attack could perform even better
- Future work: Attacks against countermeasures(such as masking)

- Thanks! Questions?