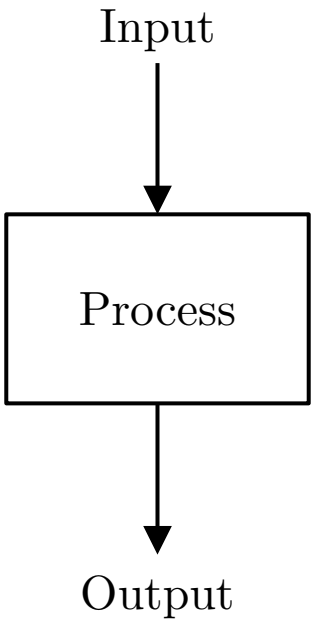
Defence Against the Unknown

Preventing Side Channel Attacks You Don't Know Exist

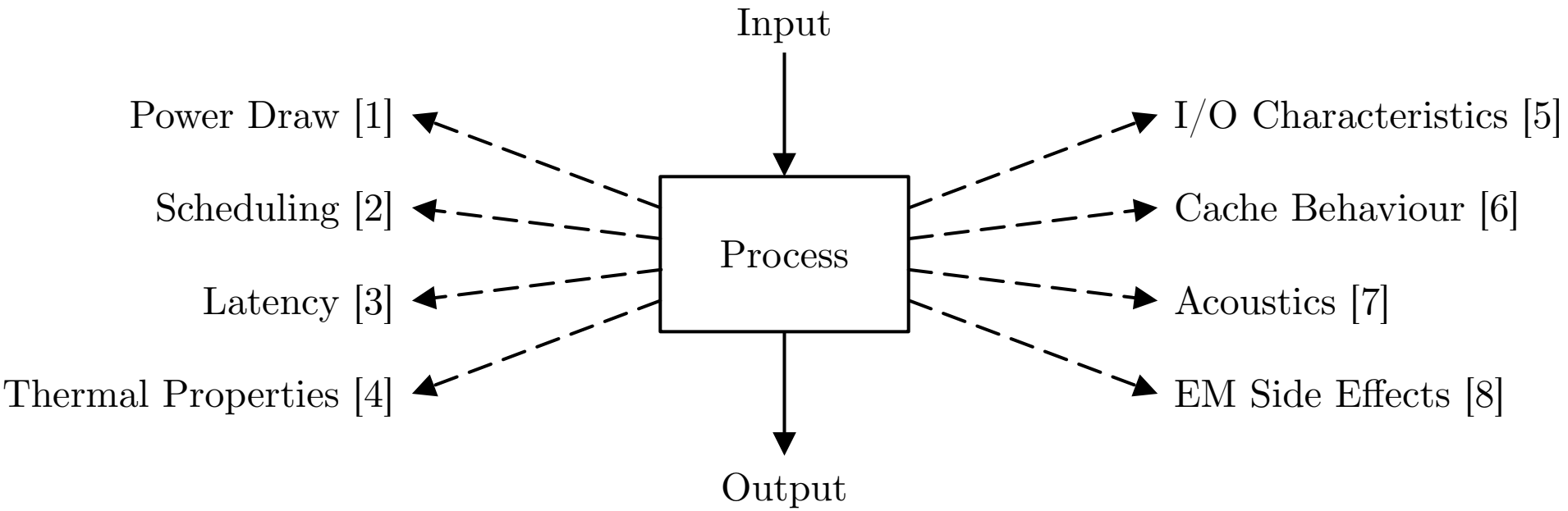
University of
St Andrews

Gregor Haywood

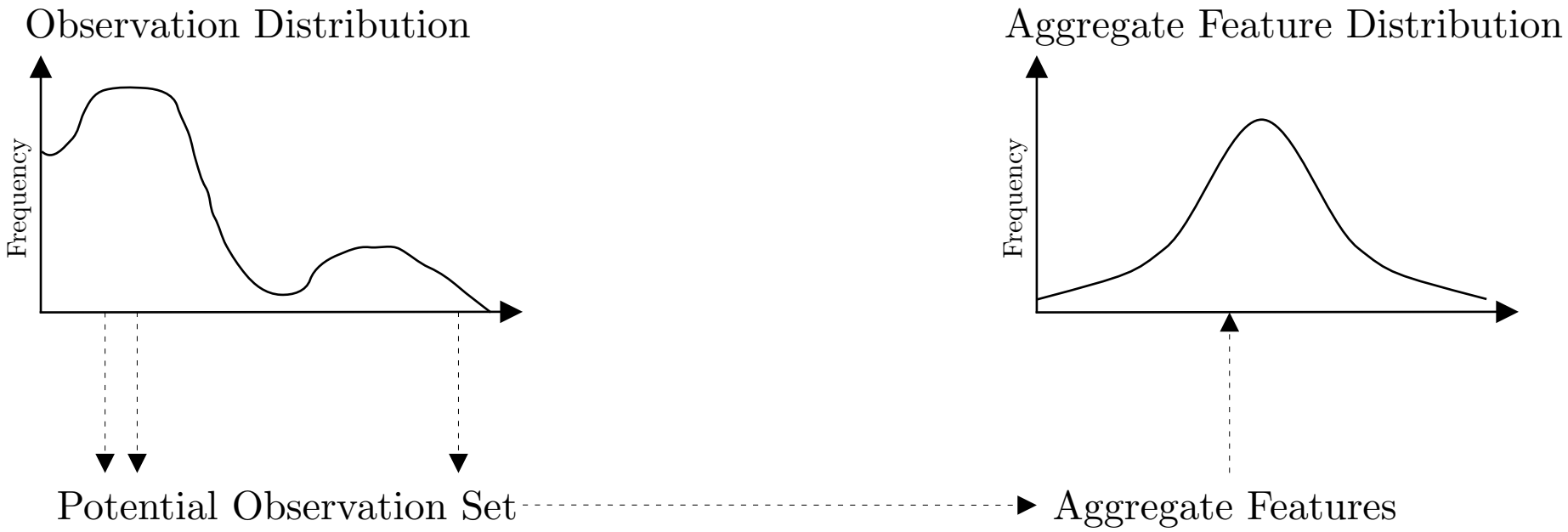
Side Channels



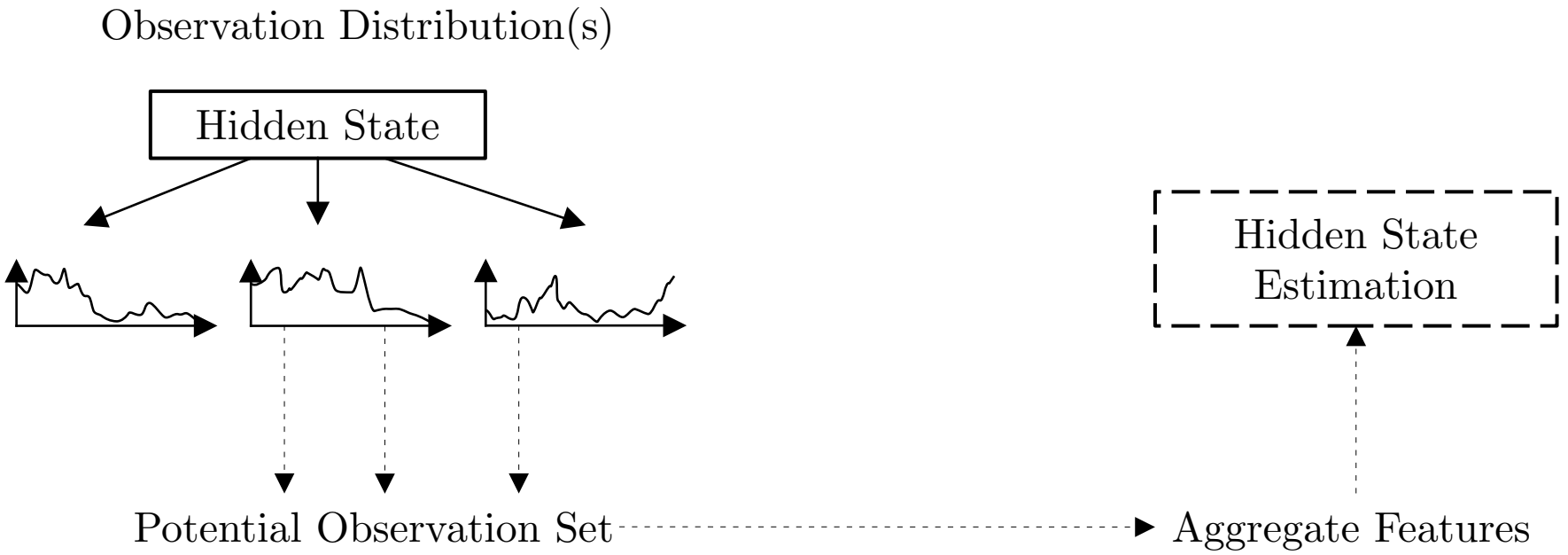
Side Channels



Stateless Information Leaks



Stateful Information Leaks

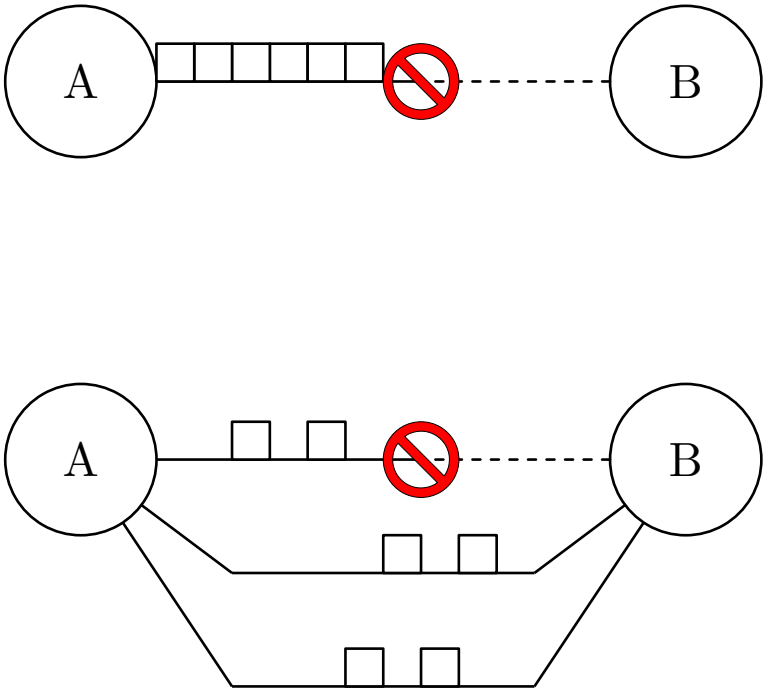


Privacy as Failure

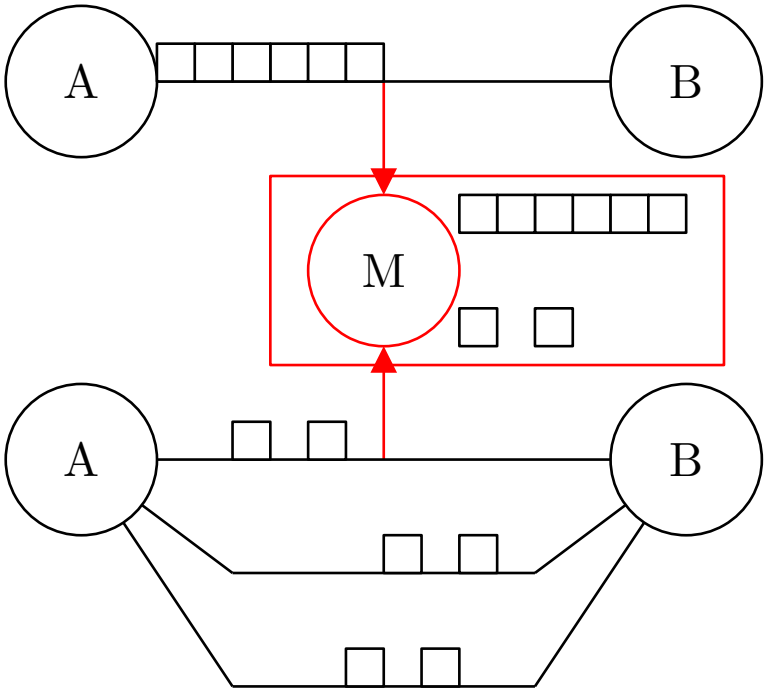
- Failure is inevitable
- Fault-tolerance:
  - Limit failure domains
  - Redundancy
- Acceptable failure rate

- Compromise is inevitable
- Compromise-tolerance:
  - Limit compromise domains
  - Redundancy
- Acceptable compromise rate

In Practice: Multipath



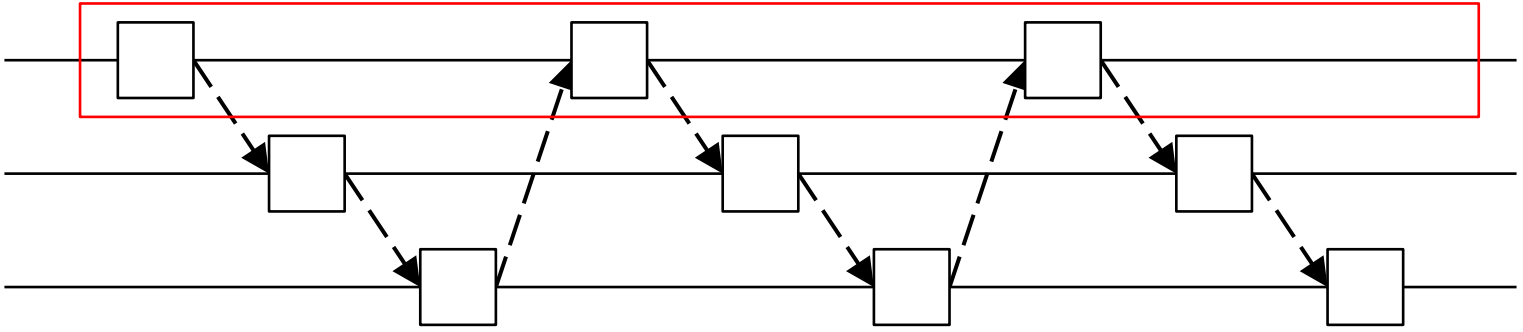
Fault Tolerance



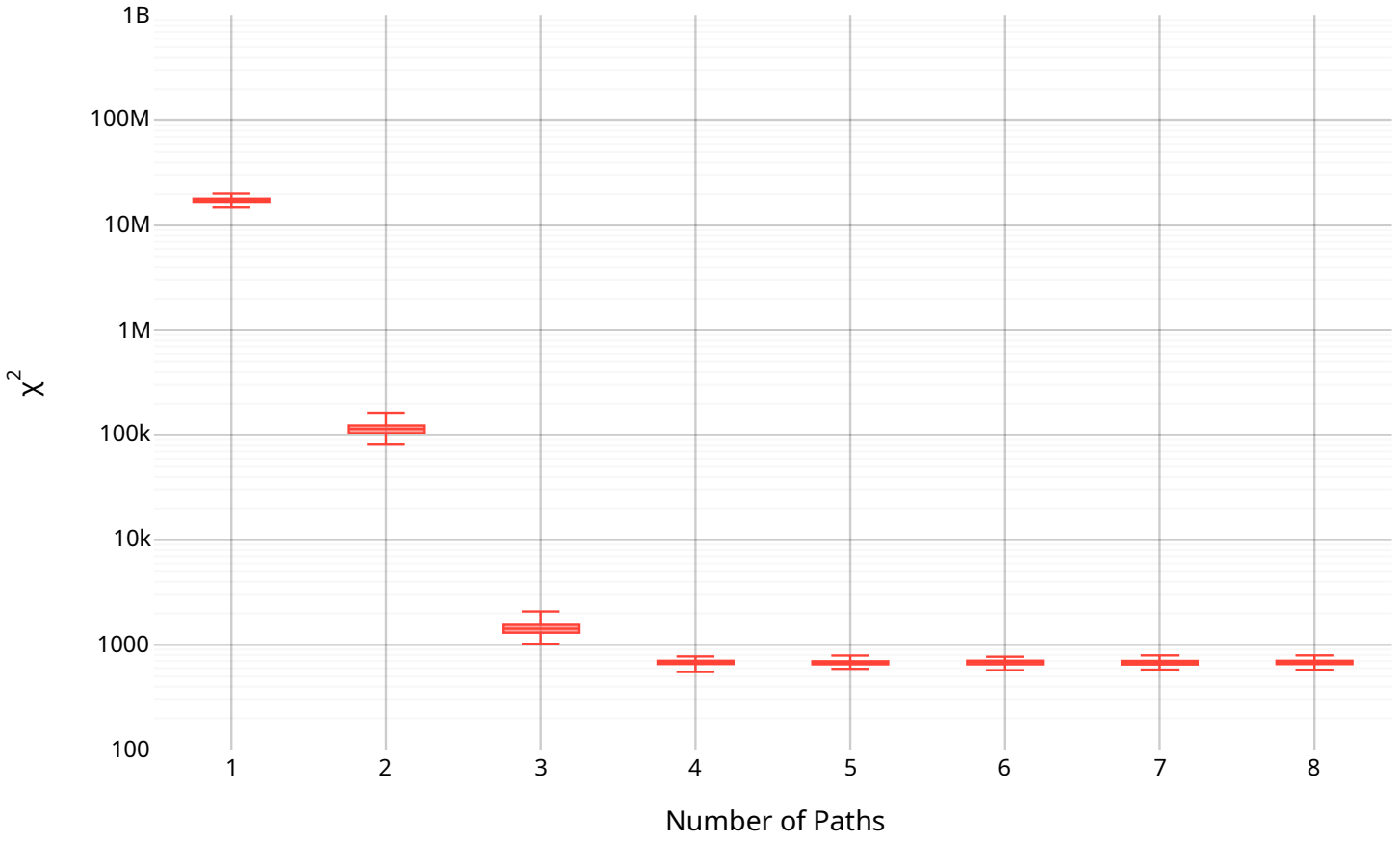
Compromise Tolerance

Partial vs Limited

- Prtl cmprms my stll b sffcnt fr th ttckr
  - **Stateful** information cascades
  - **Stateless** information does not
- Ensure limited compromise domain is stateless



Observed Bigrams vs Unigrams



General Defence

- Partial compromise of stateless domains
  - **Partial:** limited to a subset of observations
  - **Stateless:** does not cascade
- Any process!
- Any side channel!
- Does not prevent stateless attacks

Summary

- Side channel attacks can be disrupted
  - Even if they are unknown!
- Resilient to future attacks
- Performance cost is not necessary
- Implemented for round-robin multipath
- Keen to implement in other domains!

University of St Andrews

References

[1] Kocher, P., Jaffe, J., & Jun, B. (1999). Differential Power Analysis. In: Wiener, M. (eds) Advances in Cryptology — CRYPTO' 99. CRYPTO 1999. Lecture Notes in Computer Science, vol 1666. Springer, Berlin, Heidelberg.

[2] Kadloor, S., Kiyavash, N. (2014). Exploiting Timing Side Channel in Secure Cloud Scheduling. In: Han, K., Choi, BY., Song, S. (eds) High Performance Cloud Auditing and Applications. Springer, New York, NY.

[3] He, W., Zhang, W., Das, S., & Liu, Y. (2018) SGXlinger: A New Side-Channel Attack Vector Based on Interrupt Latency Against Enclave Execution, 2018 IEEE 36th International Conference on Computer Design (ICCD), Orlando, FL, USA, 2018, pp. 108-114

[4] Taneja, H., Kim, J., Xu, J. J., Van Schaik, S., Genkin, D., & Yarom, Y. (2023). Hot Pixels: Frequency, Power, and Temperature Attacks on GPUs and Arm SoCs. In 32nd USENIX Security Symposium (USENIX Security 23) (pp. 6275-6292).

[5] Song, D. X., Wagner, D., & Tian, X. (2001). Timing analysis of keystrokes and timing attacks on SSH. In 10th USENIX Security Symposium (USENIX Security 01).

[6] Kocher, P., Horn, J., Fogh, A., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., Mangard, S., Prescher, T., Schwarz, M., & Yarom, Y. 2020. Spectre attacks: exploiting speculative execution. Communications of the ACM 63, 7 (July 2020), 93–101.

[7] Deepa, G., SriTeja, G., & Venkateswarlu, S. (2013). An overview of acoustic side-channel attack. International Journal of Computer Science & Communication Networks, 3(1), 15-20.

[8] Genkin, D., Pachmanov, L., Pipman, I., Tromer, E., & Yarom, Y. (2016). ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels. In ACM Conference on Computer and Communications Security (CCS) 2016