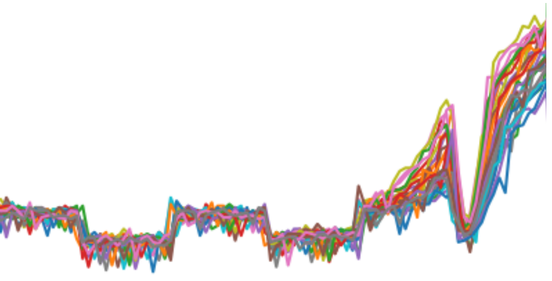
NC STATE UNIVERSITY

Department of Physics



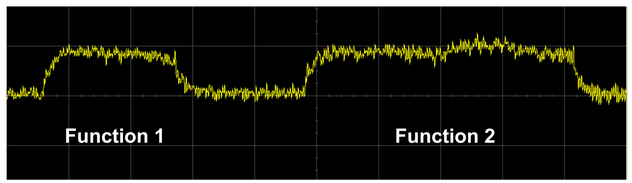
Analyzing the Robustness of Chaos Computing Against Power-Analysis Side-Channel Attacks

Jack Lynch, Nonlinear Artificial Intelligence Lab (NAIL)

Power Analysis Attacks

Although modern cybersecurity software is continually evolving, it is much more difficult to regulate **the emissions of computer *hardware***, which broadcast information continuously.

- Power Analysis attacks uncover a computer's operations by **monitoring the power consumption of its logic gates**.
- Simple Power Analysis (SPA) involves visually distinguishing between **distinct power signatures** to glean operational information.



Power signatures corresponding to two different functions. [1]

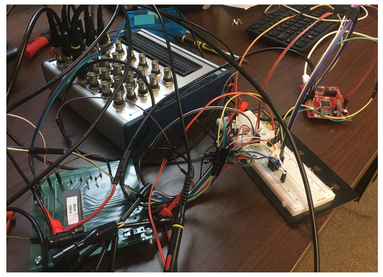
Chaos Computing

The Applied Nonlinear Artificial Intelligence Lab at NC State (NAIL) is developing chaos-based reconfigurable logic gates that implement **all digital functions with a single architecture**.

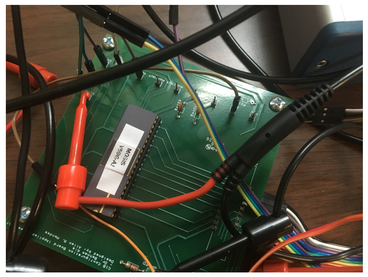
Because they use the same circuit for every function, it was posited that chaos computers might produce relatively uniform power signatures and thus be **resistant to Power Analysis attacks**.

Methods

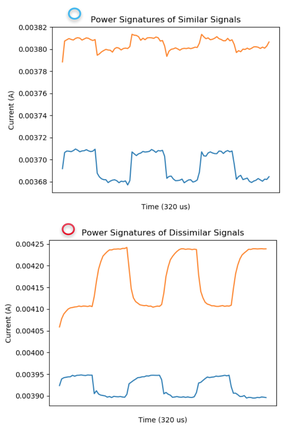
The power consumption of a chaos-based logic gate was recorded while it applied a variety of **different functions to binary input pairs**. Thousands of power signatures were recorded for each circuit configuration and pair of input bits, using LabVIEW and an MSP430 microcontroller. Signatures were then processed in Python.



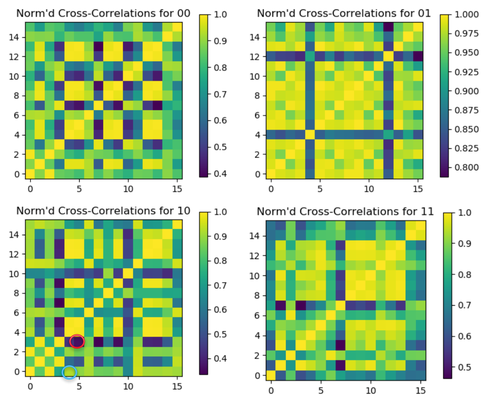
The testing setup



The chaos-based logic gate



Similar-shape power signatures (top) and dissimilar-shape signatures (bottom).

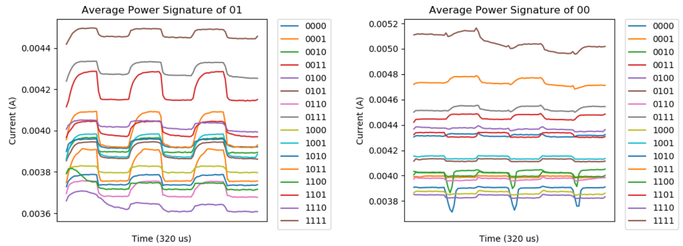


Signature similarities between different circuit configurations. Yellow indicates higher similarity.

Results

Recorded data indicates that chaos-based logic gates exhibit **a variety of different power signatures** for different functions and inputs, with **groups of similar operation/data signatures**.

The plot below shows that signature shape similarities change with function and input pairs.



Here, switching one of the circuit's input bits from 0 to 1 has a noticeable effect on the shape of the power signatures for most (but not all) possible circuit configurations.

Conclusions

Results indicate that chaos computers are not *entirely* invulnerable to Power Analysis attacks, but do contain some inherent robustness.

Further analysis could be done in other domains and phase spaces, and with signal classification via deep learning (CNN, RNN, LSTM, etc).

References

[1] Wikipedia, "Power Analysis" (GPL)