The Impact of Discharge Inversion Effect on Learning SRAM Power-up Statistics

Joint Work with Zhonghao Liao, George Amariucai, and Raymond Wong

Yong Guan

Department of Electrical and Computer Engineering
Associate Director for Research, Information Assurance Center
NIST Center of Excellence in Forensic Sciences - CSAFE
Iowa State University

csafe
Center for Statistics and Applications in Forensic Evidence

A fundamental weakness of securing cyber space is Hardware Security!!!

Sensitive data required to be stored and processed on licensing platforms.

- Identification and authentication of integrated circuits (ICs)
- Anti-counterfeiting – device fingerprints, PUF

Outline

- Motivation & Problem Definition
- Data Collection - Sampling
- In-Depth Study of Discharge Inversion Effect (DIE)
- Discussions
- Summary and Future Work

Device Fingerprints

- Motivation & Problem Definition

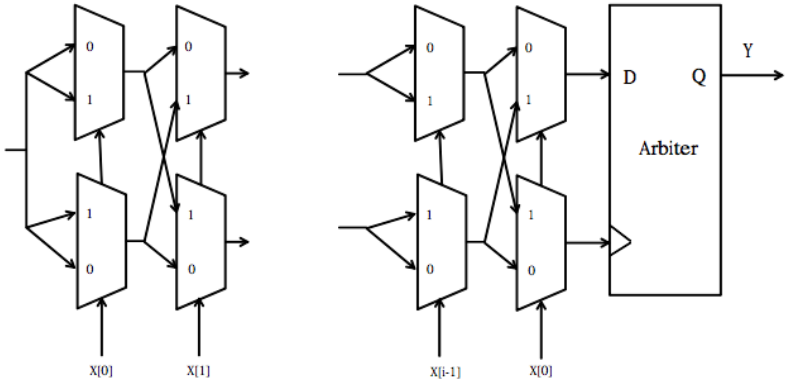
- Physical Unclonable Function (PUF) was proposed in 2002 by Gassend et al. [3] and R. Pappu et al.
  - The output of PUF, a specific binary pattern, is determined by the fabrication variance and can be used as a fingerprint for the device.

- Challenge-response scheme requires the preferential patterns and responses

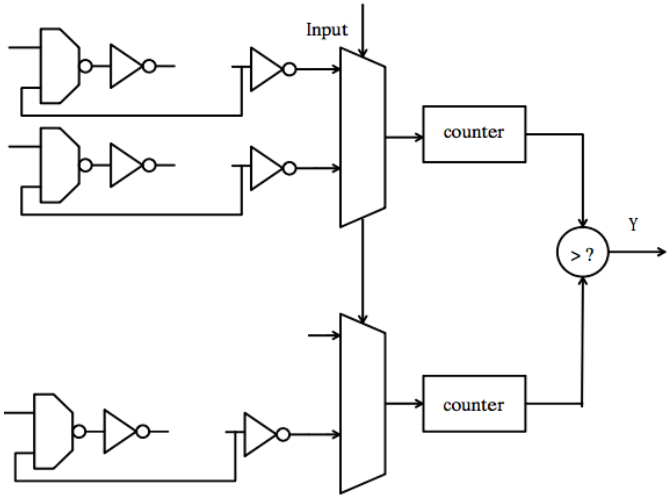
  Treating observed data as if they were gathered independently could lead to an incorrect assessment of the preferential patterns, and of their statistics.

PUFs are increasingly Used

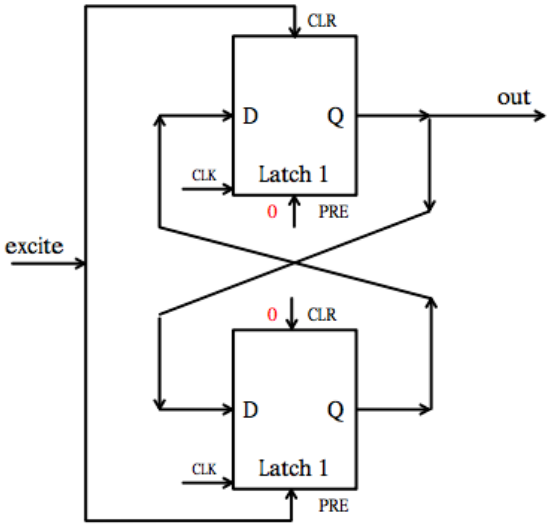
Easily evaluated by physical systems, but difficult to reproduce or predict.



Arbiter PUF



Ring Oscillator PUF



Butterfly PUF

csafe
Center for Statistics and Applications in Forensic Evidence

SRAM Based PUF

- Sampling of power-up states is indispensable

Limitations:

- Collection schemes are often not detailed:
  - Temperature setting
  - Sampling interval
  - Pin process during chip is off
- Data remanence is ignored
  - Temporal dependency might lead to an incorrect assessment of the power-up states

Our Contributions

- Experimental study reveals the possible assessment errors and interesting and abnormal phenomenons
  - A careful statistical analysis of serial reading results of power-up states of SRAM chips
  - A conjecture of DIE and corresponding verification analysis
- We have developed a novel modified sampling method that removes temporal dependency.

Experimental Setup

- The power-up streaming data was collected by the Arduino Mega 2560 microcontroller board.
- The positive and negative power supply pins and all control pins (e.g. chip enable (CE) pin and output enable (OE) pin) of SRAM chips were connected by separate electromagnetic relays.
- For temperature control, testing board and Arduino were put into the ESPEC TSE-12-A thermal chamber.

Data Collection - Sampling Scheme

- Goals of sampling scheme:
  - Minimize sampling period
  - Minimize temporal dependency

- Settings when sampling:
  - Keep a constant temperature (20ºC) – close to room temperature
  - Sampling interval is minimized as 10 sec
  - Short power pins and control pins during chip power-off

Test Procedure

Algorithm 1 SRAM power-up states sampling

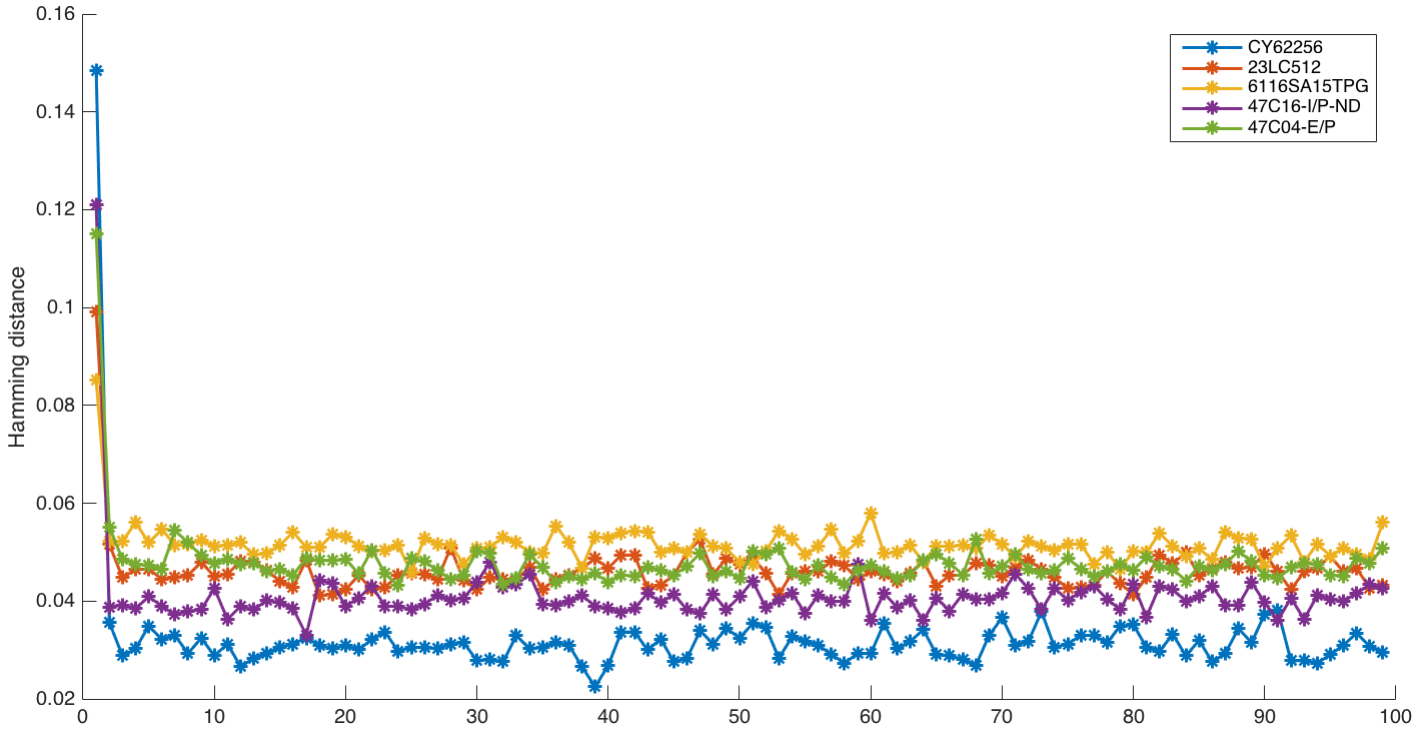
1: **for** $i = 1 \rightarrow 100$ **do**
2: Apply power supply
3: Read the power-up state of SRAM chip
4: Remove power supply; keep pins floating (condition 1) or shorted to ground (condition 2)
5: Wait for 10 seconds
6: **end for**

Temporal Correlation Results

Model	TC with pins floating	TC with pins shorted to ground
CY62256NLL-70PXC	0.2925	0.0082
23LC512	0.1635	-0.0026
6116SA15TPG	0.2327	0.0047
47C16-I/P-ND	0.1920	0.0060
47C04-E/P	0.2147	-0.0036

- The turn-off measures have a great influence on the temporal autocorrelation values.
- The result of Lag – 1 autocorrelations based on each sampling
- Power pins and control pins should be shorted during chip power-off: helps to remove the remaining charges inside the chips

Discovery of Discharge Inversion Effect



- Hamming distance of two adjacent power-up states: A large gap between first and second reading

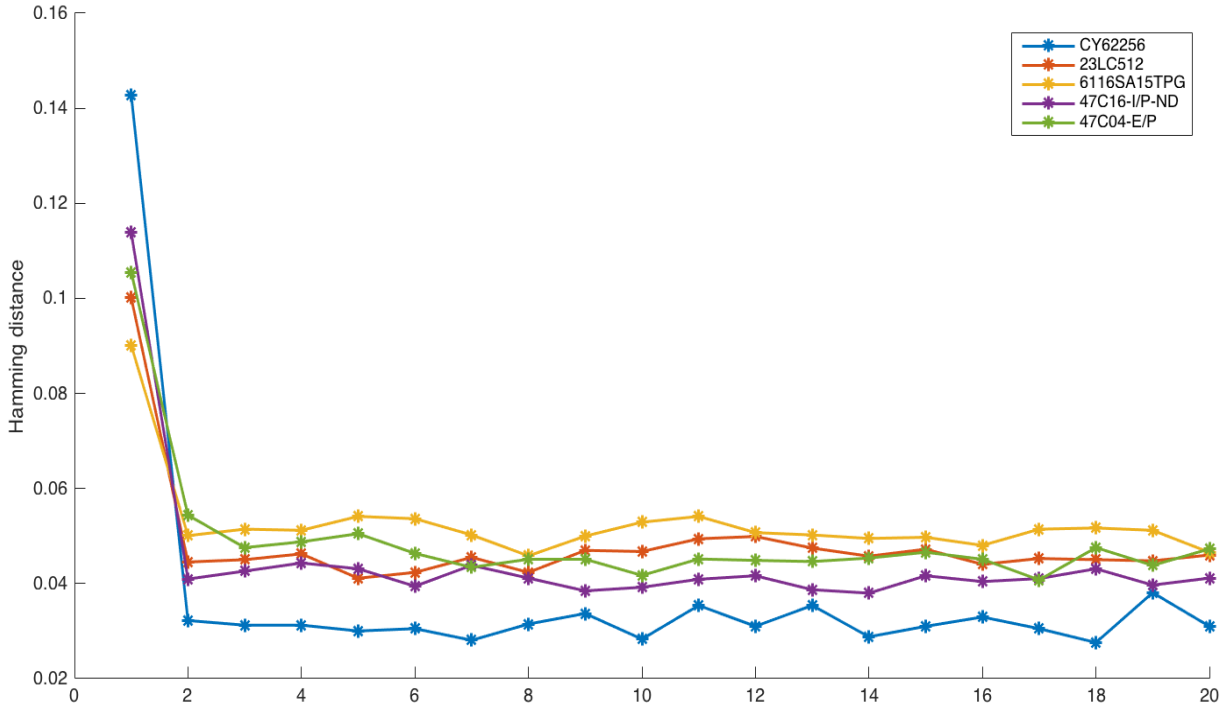
Conjecture of DIE

- Possible reasons:
  - Heating effect that appears only after the first reading
  - Residual charge after the first power-off, causing a reoccurrence of the first state
  - Differences in the discharge phenomena between the two inverters that make up the SRAM cell.

Experimental Designs for In-depth Study of DIE

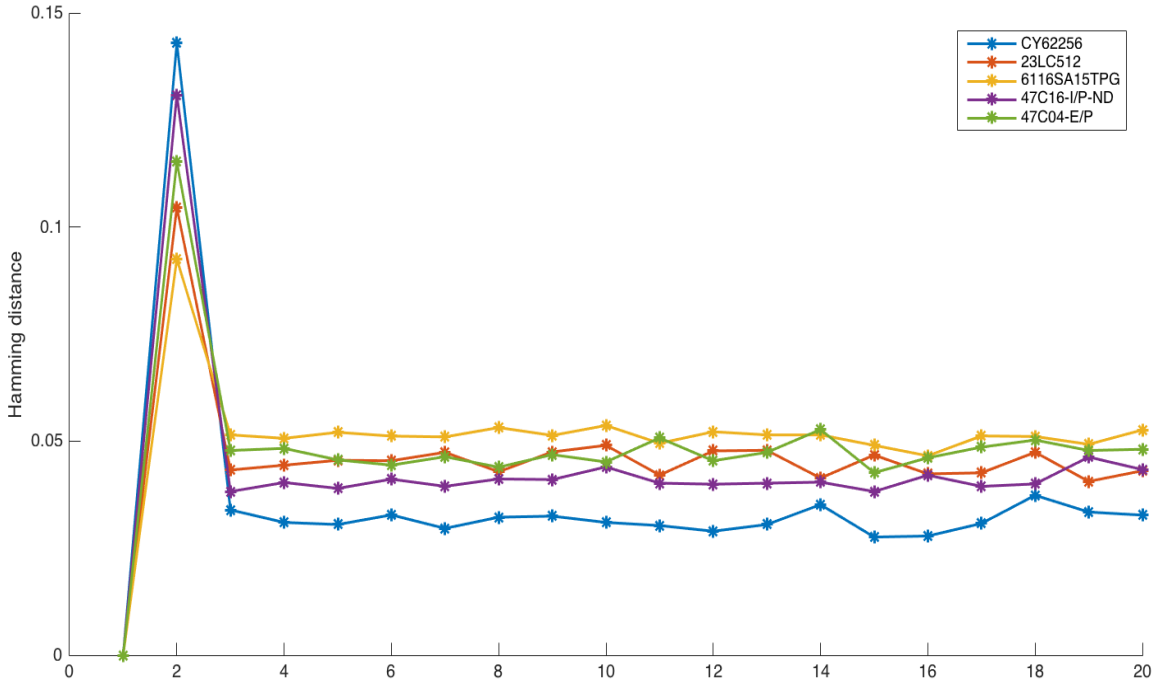
- Corresponding tests:
  - Intermittent sampling analysis: Read blocks with interrupt
  - Heating effect analysis: Power up without reading for first block
  - Uninterrupted sampling analysis: Read blocks without interrupt
- Initial state recovery time analysis:
  - Wait enough time between two samples to reproduce large HD gap
- Use same chips & temperature settings as aforementioned

Intermittent Sampling Analysis Results



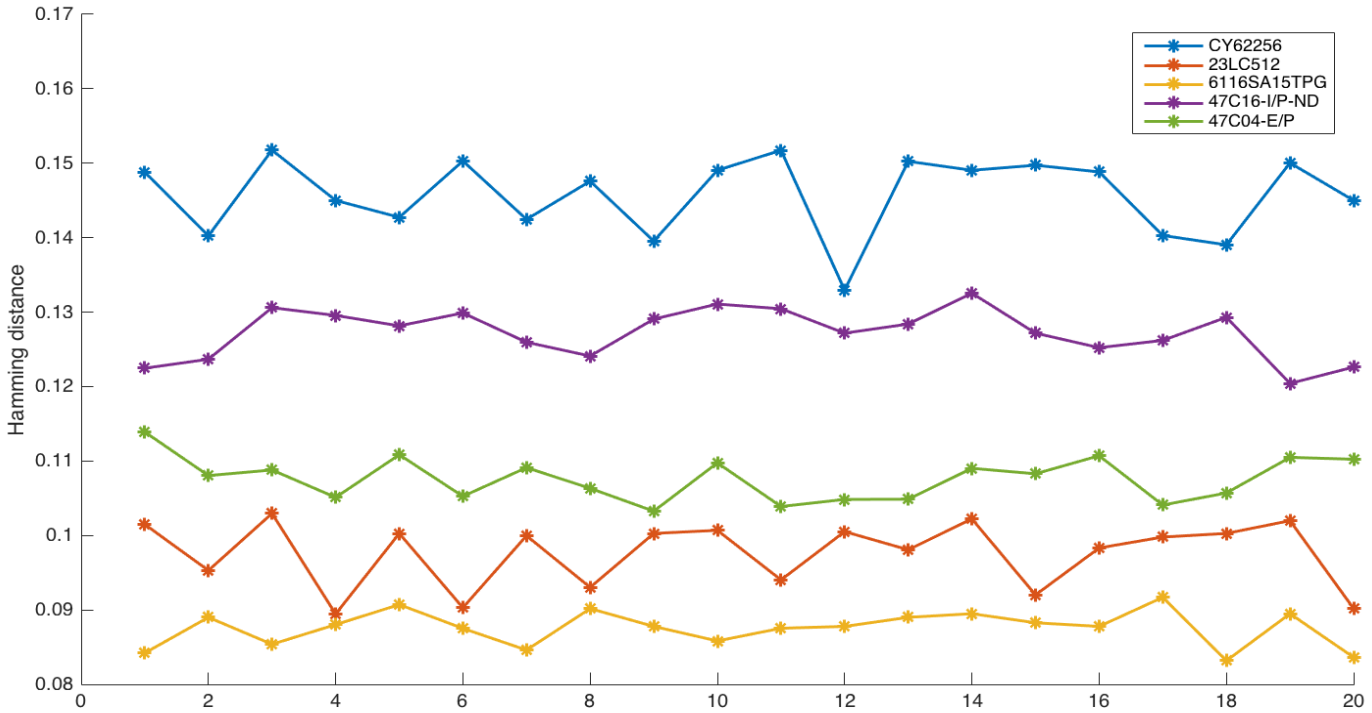
- Hamming distance of two Adjacent power-up states
- The address of bits will not influence the result of this test

Heating Effect Analysis Results



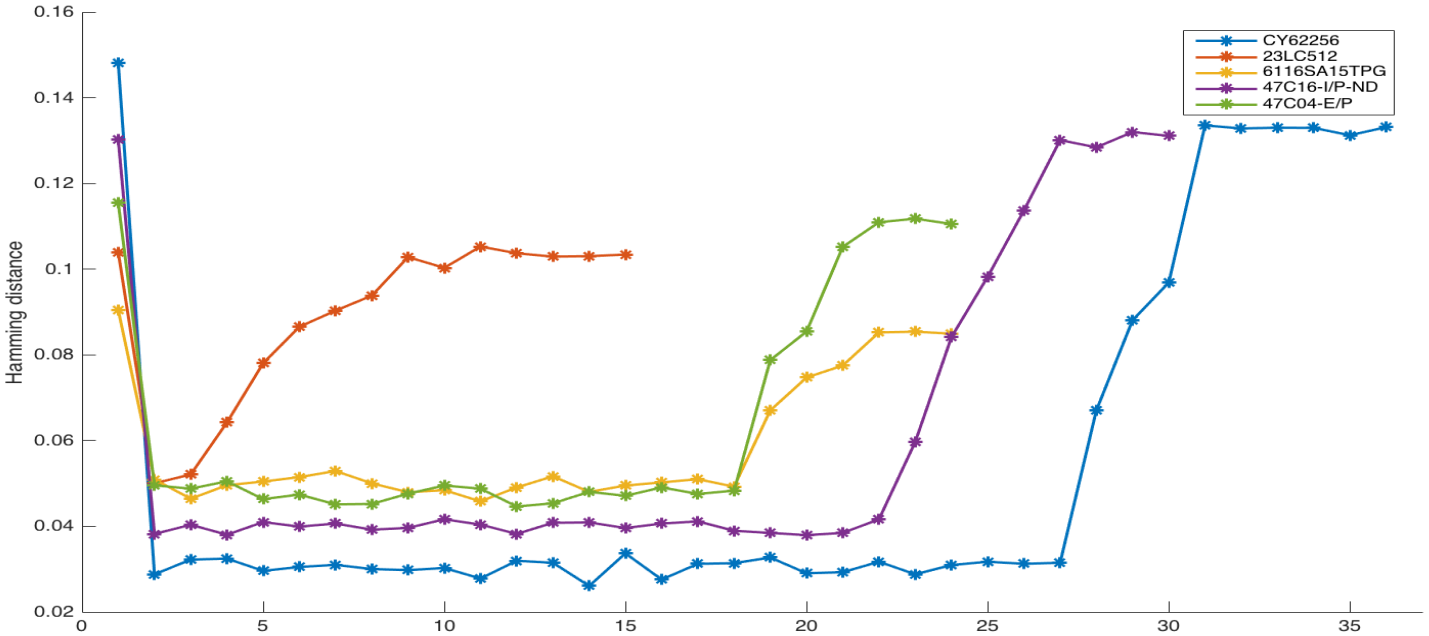
- Hamming distance of two Adjacent power-up states
- The decline of Hamming distance is not due to the heating effect of SRAM chips

Uninterrupted Sampling Analysis Results



- Hamming distance of two Adjacent power-up states
- Due to the first sampling rather than the address and size of tested bits or the heating effect

Recovery Time Analysis Results



- After a certain waiting time between two pairs of sampling, the Hamming distance increases rapidly.
- Different types of SRAM chips have different recovery time, ranging from 1 ~ 4 minutes

Summary and Future Works

- Temporal dependency can be removed using the proposed scheme.
  - The drop of Hamming distance is due to the first sampling of the SRAM chip, rather than the address and size of tested bits or the heating effect.
- Two different power-up states- *initial state* and the *subsequent state* can be observed
  - Secret key is closer to the *subsequent state*
  - Intuitive solution: Ignore first sample
- Future work:
  - Evaluate spatial correlation inside the SRAM chip
  - Design an improved SRAM PUF based on this discovery

csafe

Center for Statistics and Applications in Forensic Evidence

SRAM Based PUF

- Sampling of power-up states is indispensable

Limitations:

- Collection schemes are often not detailed:
  - Temperature setting
  - Sampling interval
  - Pin process during chip is off
- Data remanence is ignored
  - Temporal dependency might lead to an incorrect assessment of the power-up states

SRAM Based PUF

- Sampling of power-up states is indispensable

Limitations:

- Collection schemes are often not detailed:
  - Temperature setting
  - Sampling interval
  - Pin process during chip is off
- Data remanence is ignored
  - Temporal dependency might lead to an incorrect assessment of the power-up states

Questions?

Thank you.

Yong Guan
guan@iastate.edu