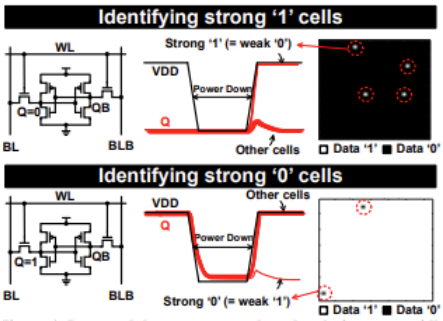
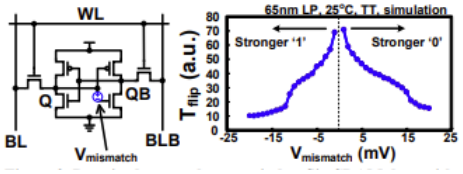
UNIVERSITY OF MINNESOTA
Driven to Discover℠

The Data Remanence Technique for enhanced data encryption

A data remanence based approach for reliable key extraction from SRAM memory cells.





IP Status: US Patents Issued; Patent No. 11,769,548 & 11,309,018

Applications

- Cybersecurity
- Data encryption

Technology Overview

In the pursuit of secure and unclonable encryption key generation, SRAM (Static Random-Access Memory) cells have emerged as an exceptional candidate. Their unique, random, and unclonable nature, stemming from inherent process mismatch among transistors, makes SRAM an attractive choice. However, the primary challenge facing SRAM-based key generation has been its susceptibility to instability in the presence of random noise, temperature variations, voltage fluctuations, and device aging.

To address this challenge, Researchers at the University of Minnesota have developed a data remanence based approach known as the Data Remanence Technique. This innovative approach simplifies the identification of stable SRAM cells for reliable key generation by reducing testing time and hardware requirements. Unlike previous methods, such as Temporal Majority Voting (TMV), which are resource-intensive and time-consuming, the Data Remanence Technique only requires two remanence tests, simplifying the process. It works by initially writing the entire SRAM array with '1' or '0', followed by a momentary power shutdown until a few cells flip. The technique leverages the fact that the cells that are easily flipped are the most robust cells when written with the opposite data, offering a unique and efficient solution for stable key generation. Experimental studies demonstrate that the 256-bit keys generated using this approach from a 512 kbit SRAM exhibit 100% stability under varying conditions, including temperature fluctuations, power ramp-up times, and device aging. The Data Remanence Technique is an innovative solution for secure key generation, leveraging the inherent

Technology ID

20180041

Category

Software & IT/Algorithms
Software & IT/Cloud Computing
Software & IT/Communications & Networking
Software & IT/Cyber Security
Software & IT/Data Mining
Software & IT/Databases

View online

unpredictability of SRAM cells to ensure that encryption keys remain resilient despite external challenges, ultimately safeguarding critical data assets.

Phase of Development

TRL: 3-4
The Data Remanence Technique has been experimentally verified in commercial SRAM chips.

Desired Partnerships

This technology is now available for:

- License
- Sponsored research
- Co-development

Please contact our office to share your business' needs and learn more.

Researchers

- **Chris Kim, PhD** Distinguished McKnight University Professor, Department of Electrical and Computer Engineering
- **Keshab Parhi, PhD** Distinguished McKnight University Professor, Department of Electrical and Computer Engineering

References

1. Muqing Liu; Chen Zhou; Qianying Tang; Keshab K. Parhi; Chris H. Kim(2017) , https://doi.org/10.1109/ISLPED.2017.8009192, https://ieeexplore.ieee.org/document/8009192, 1-6