Washington University in St. Louis
Office of Technology Management

DATA SECURITY FOR IOT AND MOBILE DEVICES USING BIT2RNG RANDOM NUMBER GENERATOR WITH NO ADDITIONAL HARDWARE

Yan, Wei, Zhang, Xuan "Silvia"

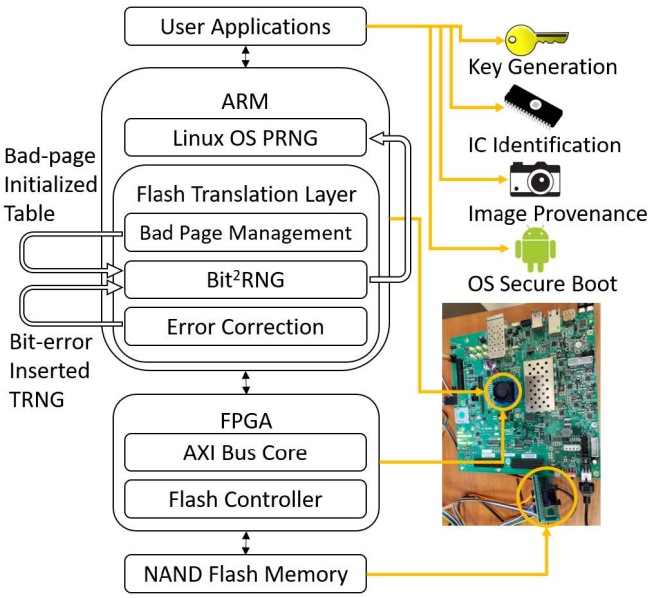
Carter, Paul

T-019418

Technology Description

Engineers in Prof. Xuan “Silvia” Zhang’s laboratory have developed a robust true random number generator (RNG) designed to be used as a low-resource security system for mobile and internet-of-things (IoT) devices. This technology, called “Bit^{2}RNG”, provides entropy without any hardware modifications to the memory chip or flash controller by leveraging the randomness and uniqueness intrinsic to MLC NAND flash.

Overview of Zync SoC Demo for Bit^{2}RNG



Current data security primitives often require additional computational power or hardware components. These requirements can increase production costs and limit implementation on IoT, mobile and other resource-constrained devices. Bit^{2}RNG solves this problem by seeding RNG-based security through bad pages and bit errors - two intrinsic physical characteristics in standard NAND flash memories. Because these characteristics are required in the flash translation layer, a flash controller makes these high-level sources of information readily available to users with no additional hardware modification. Experimental results indicate that Bit^{2}RNG is a practical solution with better system performance trade-off than other state-of-the-art TRNG techniques. Therefore, this technology has the potential to be widely adopted in billions of flash-based devices with in a variety of end-user applications such as key cryptography and device identification.

Stage of Research:

The inventors demonstrated Bit^{2}RNG's utility in commodity flash systems with several lightweight IoT applications that leverage the unique strength of the primitives: chip identification via aging estimation; image provenance/tamper protection via unforgeable randomness from bad flash pages; and secure boot. Intra-chip and inter-chip measurements proved the randomness and uniqueness of the proposed system.

Applications

- **Security for low resource mobile and IoT devices** – replace or supplement true random number generator or key cryptography in devices with NAND flash memory for end-user applications such as device identification and data provenance

Key Advantages

- **Low resource costs**:
  - no extra entropy source is needed apart from the onboard NAND flash memory
  - no increased device production cost because there are no hardware modifications to memory chip or flash controller
  - compatible with standard flash interfaces and devices and therefore can be applied to existing legacy infrastructure instead of requiring new deployment
  - random source is derived from high-level intrinsic system information observable at the user level (bad pages and bit errors in commodity, off-the-shelf NAND flash memory)
  - simple software computation that consumes no additional system memory space
- **Versatile and robust**:
  - guarantees a secure randomness source for a variety of security functions
  - no measurable false positives or false negatives detected in the experiments (also theoretically proven)
  - aging enables non-forgeable identification with OTP technology
  - provides sufficient entropy and with reasonable throughput

Publications: W. Yan, H. Zhu, Z. Yu, F. Tehranipoor, J. Chandy, N. Zhang, X. Zhang, Bit2RNG: Leveraging Bad-page Initialized Table with Bit-error Insertion for True Random Number Generation in Commodity Flash Memory, IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2020

Patents: Application filed

Related Web Links: Zhang Lab