An Analysis of the Effects of Temperature on the Performance of ReRAM-Based TRNGs

Nico Mexis
Faculty of Computer Science and Mathematics
University of Passau
Passau, Germany
nico.mexis@uni-passau.de
ORCID: 0000-0003-0181-7648

Nikolaos Athanasios Anagnostopoulos
Faculty of Computer Science and Mathematics
University of Passau
Passau, Germany
nikolaos.anagnostopoulos@uni-passau.de
ORCID: 0000-0003-0243-8594

Stefan Katzenbeisser
Faculty of Computer Science and Mathematics
University of Passau
Passau, Germany
stefan.katzenbeisser@uni-passau.de
ORCID: 0009-0005-3608-874X

Tolga Arul
Faculty of Computer Science and Mathematics
University of Passau
Passau, Germany
tolga.arul@uni-passau.de
Department of Computer Science
Technical University of Darmstadt
Darmstadt, Germany
arul@rbg.informatik.tu-darmstadt.de
ORCID: 0000-0002-2078-3976

***Abstract*—In this work, we propose a simple implementation of a True Random Number Generator (TRNG) based on Resistive Random Access Memory (ReRAM) and evaluate its practicability at different ambient temperatures.**

***Index Terms*—Commercial Off-The-Shelf (COTS), Resistive Random Access Memory (ReRAM), runtime-accessible, True Random Number Generator (TRNG)**

I. Introduction

Random number generation is one of the most important areas of modern cryptography. For this reason, the search for True Random Number Generators (TRNGs) is still a prevalent research topic. In this abstract, we shortly introduce a simple implementation of a Resistive Random Access Memory (ReRAM)-based TRNG and evaluate its applicability at different temperature conditions.

II. Technical Background and Results

ReRAM is a type of non-volatile memristor-based memory that stores bits by changing the resistance of the underlying material. Our ReRAM-based TRNG uses the entropy of the write latency to derive random bits. This is done by selecting three values: $addr$, $byte_1$, and $byte_2$. The value $byte_1$ is written first at address $addr$ to the ReRAM. Then the ReRAM status register is read in a loop and, on each iteration, the `WIP` (Write In Progress) bit is checked. This process is called *WIP polling* and the corresponding bit is set (`1`) as long as the write process continues. Once the `WIP` bit clears (`0`), the writing is finished. After that, the value $byte_2$ is written to the same cell $addr$ in order to overwrite the current value $byte_1$. Again, WIP polling is performed, but this time the number of performed polls is recorded. The least significant bit of this number of polls is unstable and fluctuates as the writes take different amounts of time. Effectively, a random bit is generated through two write instructions. In our implementation, the von Neumann extractor algorithm [1] is additionally used in order to eliminate potential biases.

In our experiments we are using two different ReRAM models: the Adesto RM25C512C-LTAI-T [2] and the Fujitsu MB85AS4MTPF-G-BCERE1 [3]. Four different modules of each type are examined in order to provide conclusive results.

Our results indicate that the bitrate of both models is highly dependent on the ambient temperature. At room temperature the bit rate is at around 500 bits/s for the Fujitsu-based and 50 bits/s for the Adesto-based TRNG while it can be as low as 50 bits/s and 35 bits/s under adverse conditions, respectively.

This work has been partially funded by the Interreg VI-A Programme Germany/Bavaria–Austria 2021–2027 – Programm INTERREG VI-A Bayern–Österreich 2021–2027, as part of Project BA0100016: "CySeReS-KMU: Cyber Security and Resilience in Supply Chains with focus on SMEs", co-funded by the European Union, and by the German Research Foundation – Deutsche Forschungsgemeinschaft (DFG), under Project P03: "Hardware-Entangled Cryptography" of Collaborative Research Center (CRC) – SonderForschungsBereich (SFB) 1119: "CROSSING — Cryptography-Based Security Solutions: Enabling Trust in New and Next Generation Computing Environments", as well as under Projects 440182124: "PUFMem: Intrinsic Physical Unclonable Functions from Emerging Non-Volatile Memories", and 439892735: "NANOSEC: Tamper-Evident PUFs Based on Nanostructures for Secure and Robust Hardware Security Primitives" of the Priority Program – SchwerPunktProgramme (SPP) 2253: "Nano Security: From Nano-Electronics to Secure Systems". The authors would also like to thank Johannes Hölzlwimmer for his work within the framework of his Bachelor's Thesis "Wenn die Temperatur den Zufall beeinflusst: Eine Untersuchung von Resistive Random-Access Memory-basierten Zufallszahlengeneratoren".

III. Conclusion

It can be concluded that although the ReRAM-based TRNG is a promising approach to random number generation, it is susceptible to a simple temperature-based attack. Future work should investigate whether there are countermeasures against this exploitable behaviour.

References

[1] J. Von Neumann, "Various Techniques Used in Connection With Random Digits," *National Bureau of Standards: Applied Mathematics Series*, vol. 12, pp. 36–38, 1951, Summary written by George E. Forsythe.

[2] Adesto Technologies, *RM25C512C-L Preliminary Datasheet*, 2017. [Online]. Available: http://web.archive.org/web/20200221101215/https://www.adestotech.com/wp-content/uploads/DS-RM25C512C_079.pdf

[3] Fujitsu Semiconductor, *DS501-00045-1v0-E Data Sheet*, 2016. [Online]. Available: https://www.fujitsu.com/tw/Images/MB85AS4MT-DS501-00045-1v0-E.pdf