Bertrand Cambou – Northern Arizona University, Flagstaff AZ 86011, USA – 2/20/2022

Tamper resistance with ternary ReRAM-based PUFs and TAPKI

Summary. Resistive Random Access Memory (ReRAM) operating in the pre-forming range as root of trust, combined with Ternary Addressable Public Key Infrastructure (TAPKI) schemes breaking away from generic binary logic, are designed to provide additional of tamper resistance to sensitive asset. The ReRAMs can operate at exceptionally low levels of power, in the 1 femto Joule per bit range, which allow the design of physical unclonable functions (PUFs) generating cryptographic keys . In this range of power, ReRAMs operating below electronic noise levels, can be naturally tamper-resistant, and extremely hard to read by opponents, even when the components are under their control. The TAPKI protocol masks the marginal cells, and allows concurrent generation by the server, and client devices, of highly secure private keys from Ternary ReRAMs with very low bit error rates (BERs). The response based cryptography (RBC), combined with TAPKI, eliminates the need to use cumbersome error detection, and error correction schemes, thereby handling the natural drifts, and exposure to environmental variations of the T-PUFs. Additional methods to enhance tamper resistance include: i) sensing schemes within the ReRAM array detecting intrusion; ii) self-destruct mode of the arrays when under attack; iii) ability to store-read-erase the challenges in the array for key recovery; iv) noise injections in the ternary protocol associated with High Performance computing (HPC), can strengthen security by preventing opponents equipped with inferior computing power to participate. Pre-formed ReRAM-based TAPKI schemes, with post quantum cryptography (PQC), can target various use-cases, including secure communication through public networks, the protection of digital files with key recovery, and mobile server in zero-trust environment.

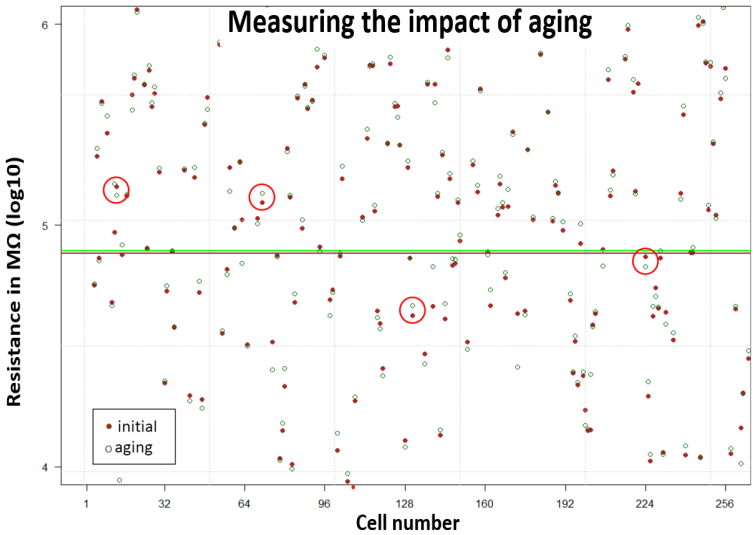
1- ReRAM's physical properties at low power.

We designed PUFs with arrays of pristine ReRAM cells (un-formed). Small currents are injected during challenge-response cycles to generate cryptographic keys. With injected currents in the 1 nA to 1µA range, the resistance values of the cells drop to the 0.1 MΩ to 20 MΩ range; after measurement, the resistance values return to the original values of the pristine state, typically 100 MΩ or higher. The conduction is thereby ephemeral and reversible. The resistance of each ReRAM cell is unique to that cell and depends on the number, location, and density of defects within the dielectric layer along with the precise thickness and area between electrodes. We measured the resistance at variable injected currents of thousands of cells manufactured (source: **Crossbar** 1.a test chips) with various fabrication batches and observed large and random cell-to-cell variations, while the variations of the resistance values measured on each cell are extremely small. Resistance values can be used to design PUFs for the following reasons:

i. The cell-to-cell random variations in resistance values are large. Typically, inter-PUF standard variations are in the 50% range of the median values. Each ReRAM array is unique for key generation.

ii. Small intra-PUF variations: The intra-PUF relative standard variations are in the 2% range of the median resistance values.

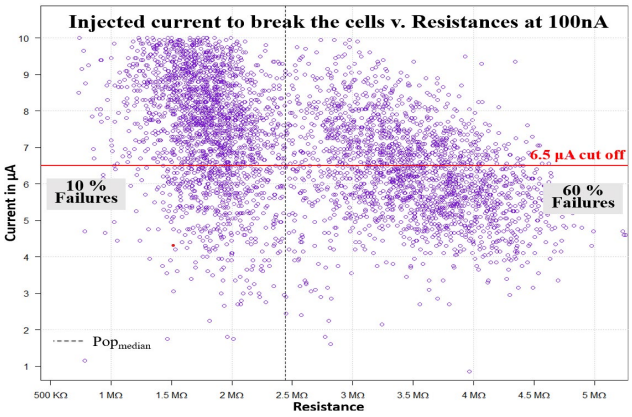
iii. As shown on the right, the resistances of each cell are stable overtime, because the measurements do not disturb the physical properties.



AFRL-RV, who is equipped with the exact same set up than NAU confirmed these measurements and results. Samples 1a. from Crossbar were tested at NAU, then retested by **AFRL-RV**, resulting in a perfect correlation between the two sites. AFRL-RV also submitted the samples to a battery of ionizing radiation tests, demonstrating that the ReRAM technology is radhard when operating in the pre-forming range. We recommend the readers to contact **Bill Kemp** for further details on the work done by RV, characterizing pre-formed ReRAMs.

2- Sensing elements with Pre-formed ReRAM-based PUFs.

The breakdown of the ReRAM cells operating under constant current is caused by the non-reversible partial forming of conductive filaments. The cells with higher resistances see higher voltage drop at the same injected current, therefore the breakdown occurs at lower injected current. This physical property can be used as a feature to detect third parties reading the resistance values of the PUFs.



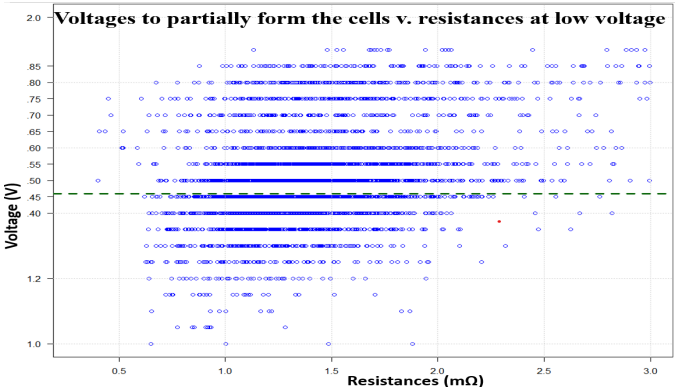
a. ***Enrollment***: The resistance of each cell is characterized at low current (~100 nA). Only 50% of the cells with low resistances are kept for the enrollment protocol. This constitutes the strong cell population (SCP). A stress of 6.5 µA is then applied to SCP cells, which result in breaking about 10% of this population, see graph enclosed measured in the 1a wafers from Crossbar.

b. ***Key generation***: The ternary protocols generating keys only address the cells belonging to 90% of the SCP cells that survived the stress of 6.5 µA, randomly injecting currents below that level.

The keys generated by such a PUF are varying with the level of injected current in the cells. An opponent having access to the device will not be able to randomly read the resistance values in the 1 to 6.5 µA range without damaging about 60% of the cell population with high resistance, called vulnerable cell population (VCP). One possible protocol is to regularly explore at low current the cells of the VCP, and check that cells kept high resistance values.

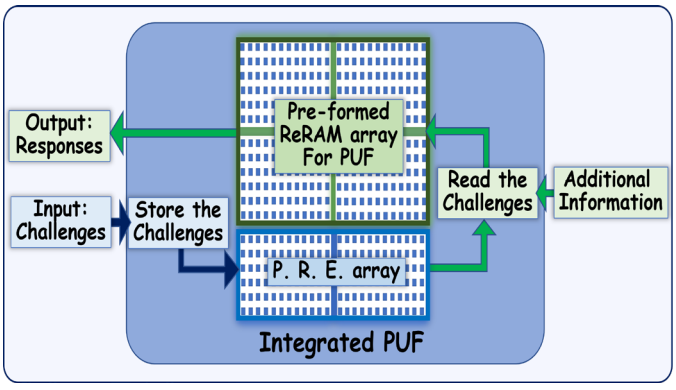
3- Ability to damage the pre-formed ReRAM-based PUFs at low power.

It could be desirable to be able to intentionally damage a PUF when the device has been compromised. One of the advantages of using pre-formed ReRAMs is the ability to form conductive filaments with only a 2 volt stress. Only partial forming cycles are needed to permanently damage a pre-formed ReRAM-based PUF, so we conducted an experimental analysis on crossbar's 1a samples to develop a reliable method, see results enclosed. Here, there is no need to damage all cells, as long as enough cells are destroyed. We concluded that applying only 1.45 volt for about 100 µs is enough to damage about 40% of the cells of the 4096 bit array. The ratio of the cells damaged at 1.45 volt for the cells with lower resistances, the SVP, is conveniently higher at 55%.

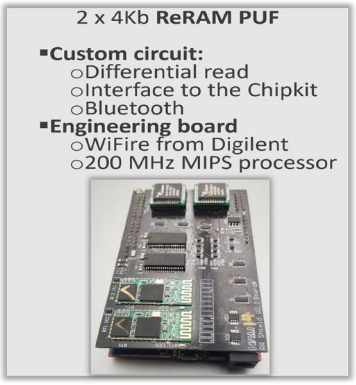


4- Protection of the PUF challenges during key recovery cycles.

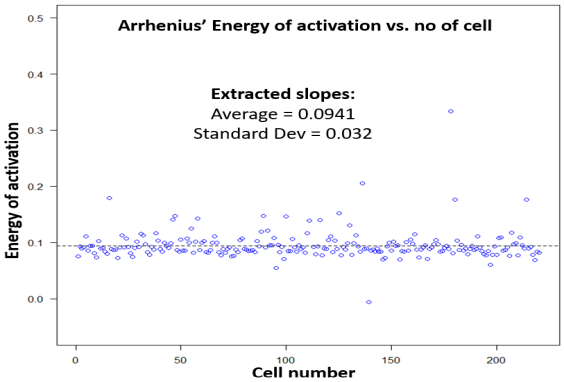
A challenge-response-pair mechanism can generate cryptographic keys from a PUF. Rather than storing an encrypted key in the non-volatile memory of a device, we can store the challenges to retrieve the PUF responses and the keys, which are encrypted with the responses. With TAPKI, the challenges are combined with ternary instructions keeping track of the "bad" cells such as the fuzzy cells, and the ones part of the VCP. These instructions can be communicated by a third party, on demand. Using for example a technology developed by [Crossbar](), it is possible to store the challenges in the pre-formed array, in such a way that these challenges can only be read once in a program-read-erase (PRE) operation, see on the enclosed diagram. The responses used to encrypt the cryptographic key can be generated only once, and need the additional information provided externally, thereby enhancing tamper resistance.



5- Design of addressable PUF generators with pre-formed ReRAM.



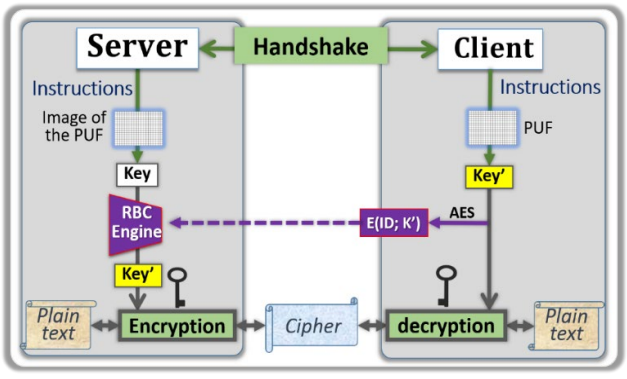
The objective of the design is to be able to send a set of addresses in the pre-formed array, at a particular injected current (i.e., the challenges), and to get a stream of "0" or a "1" (i.e., the responses). Such a function is called APG for addressable PUF generator. Crossbar designed an ASIC, called the 1b., that was integrated into the circuit designed by NAU operating as APG. The high level description of the 1b. ASIC is a 4096 ReRAM array integrated with the control circuitry allowing the read of a particular cell, at a particular current. The input of the ASIC is one address in the ReRAM array and one value of the injected current between 100 nA and 15 µA; the output of the chip is a voltage drop across the ReRAM cell proportional to the resistance value of the cell. A steam of addresses at a given current results in a stream of resistance values. We encourage the readers interested by the detail of the ASIC to contact Ashish Pancholy from Crossbar . In order to turn the ASIC into an APG, NAU designed a custom board with voltage comparator fed by two ASICs. The PUF challenges consist of the addresses of a pair of cells with the value of the injected current, each cell located in one of the ASIC. The TAPKI masks the cells that are fuzzy or vulnerable. The enclosed pic is showing the custom APG board designed by NAU, the circuit handle 128 million possible pairs. The two ReRAM arrays are read separately during enrollment and mounted in a circuit that only allow the comparative read of pairs of cells. We estimate that two ReRAM arrays of 16 Kbytes will be tamper resistant: the trillions of pairs require 9 years to be read in the field.



Such a differential method has resulted into highly reliable APGs with bit error rates (BERs) below 1 part per million. The impact of temperature is negligible because most cells track each other well, as shown in the enclosed Arrhenius plot, measuring the energy of activation from -25°C to +125°C. The small differences are masked by the TAPKI protocol, only using the pairs with large differences in resistance value.

6- TAPKI with Response Based Cryptography (RBC).

The TAPKI allows the implementation of pre-formed ReRAM-based PUFs, as described above. A server with an image of the PUF generates the challenges and the mask with ternary positions. The handshake allows the concurrent generation of the responses from the PUF, and cryptographic key generation. A man-in-the-middle would not be able to send a "working" handshake without knowing the position of the fuzzy and VCP cells. The handshakes can be shared openly as they have no value without the PUF. We developed an RBC engine to recover the key when errors are generated by the PUF due to drift, noise, or environmental interferences, see the diagram enclosed. Such a method eliminates the need to implement error correcting codes at the client level, and thereby enhance the tamper resistance when the terminal is in a zero-trust environment. A noise injection technique coupled with high performance computing (HPC) at the server level was designed to provide additional levels of protections. The RBC is able to handle noisy keys with BERs as high as 20%, that can only be handled with HPCs.

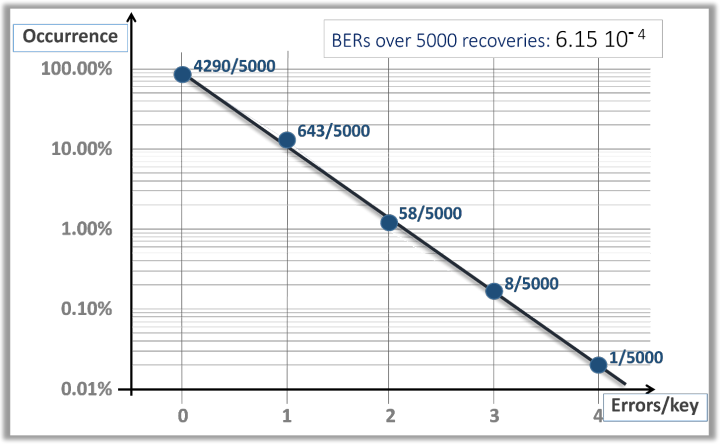


The architecture is encryption agnostic. Any symmetrical or asymmetrical schemes are directly implementable. To use public key infrastructure, a key pair is generated from the PUF responses. We completed prototypes with elliptic curves, EC-DSA, and post quantum cryptographic schemes (Dilithium, Saber, …). Layers of multi-factor authentications have been developed and tested on the TAPKI. In particular we developed a pseudo-homomorphic method allowing the users to never disclose its passwords, while verifying the authentication of a server in a zero-trust network. Such an authentication is folded in the TAPKI protocol to deliver stronger two-way protections.

Experimental validation. For each key generation cycle with the TAPKI protocol, 512 pairs of cells are randomly selected in the ReRAM arrays, of which 256 pairs act as a buffer, to only keep the 256 pairs having resistance values further apart. The injected current is also randomly changed at each cycle from 100 nA to 800 nA . The potential errors due the PUF are corrected by the RBC. The listing below is showing a succession of key generation cycles. The 256-bit long keys generated from the look-up table are on the left, those from the ReRAM-PUF are on the right, followed by the count of errors. Here, we only observed one error, during the key generation cycle number 26, which could be due to the instability of the ReRAM or noise in the electronic system. Each cycle lasted less than 1 second.

```
PS C:\Users\bertr\OneDrive\Desktop\7-Demo> .\bin\challenge_demo.exe -p 13 --embed --protocol=cellpairing
dbf-f105-41e8-a4d4-402e17aedfb5\die1.puf .\enroll\7257cdbf-f105-41e8-a4d4-402e17aedfb5\die2.puf
Connecting to 'COM13'... Connected!
Using 80 reads for enrollment, with a validation timeout of 10 seconds...
Initializing enrollment... Done!
UUID: 7257cdbf-f105-41e8-a4d4-402e17aedfb5
Count: Server Key:                                   Key:                                    Errors: Current
1   vrK+/Pan+/5wcO53J/hf2HIlY+x3hb5mG9XnvCufxXE=  vrK+/Pan+/5wcO53J/hf2HIlY+x3hb5mG9XnvCufxXE=  0  688
2   X/3+265X/v+u5pbr83f/NU386//Z2/+7rvifu7H9sfg=  X/3+265X/v+u5pbr83f/NU386//Z2/+7rvifu7H9sfg=  0  608
3   4cHVLz1Br/PqxduTVqp61wf8uo//T+77/ry89CU//z8=  4cHVLz1Br/PqxduTVqp61wf8uo//T+77/ry89CU//z8=  0  503
4   BINw4AAQUClwmUYWgCqLt6xgI5AJACASASBRCQG5hIA=  BINw4AAQUClwmUYWgCqLt6xgI5AJACASASBRCQG5hIA=  0  608
5   EbQyEJ5hzBds1pdNHrQdeF2ZRqsopVgBQLKB3jZqSt4=  EbQyEJ5hzBds1pdNHrQdeF2ZRqsopVgBQLKB3jZqSt4=  0  794
6   vWHTXBMVk43pqpd87fDMHlUHZcHWZP2a9UdHKtl/gDs=  vWHTXBMVk43pqpd87fDMHlUHZcHWZP2a9UdHKtl/gDs=  0  794
7   0/z/I37fW//Ddt4/wP3wvv8/7e9++zt9/dzuTj5xffY=  0/z/I37fW//Ddt4/wP3wvv8/7e9++zt9/dzuTj5xffY=  0  304
8   EpwDawBCYgA1EASGcUxwQoYESIsGICiREiEKAKrA4Cw=  EpwDawBCYgA1EASGcUxwQoYESIsGICiREiEKAKrA4Cw=  0  503
9   qU3QJYBrB5jRfgFJVlIgkrOSAYJQSfgpbaTVG6JAoBg=  qU3QJYBrB5jRfgFJVlIgkrOSAYJQSfgpbaTVG6JAoBg=  0  688
10  P+PAr8abPm1/EN4O/b9e8h7tR27TYzm/PXzmffnMKd8=  P+PAr8abPm1/EN4O/b9e8h7tR27TYzm/PXzmffnMKd8=  0  688
11  dO7wUQoPkiSjdRO1FfmPUGgG7DtcG6jYTfH+5sznWFO=  dO7wUQoPkiSjdRO1FfmPUGgG7DtcG6jYTfH+5sznWFO=  0  794
12  DSMIGXYAAkACMJh10iCgFmgQEQE3AsqlSoScBIMBwEA=  DSMIGXYAAkACMJh10iCgFmgQEQE3AsqlSoScBIMBwEA=  0  304
13  qAAAAAAEEAAQACAAAGAAAAACQUAgAACIAMCAkAABEBA=  qAAAAAAEEAAQACAAAGAAAAACQUAgAACIAMCAkAABEBA=  0  106
14  AMAAoABIFgEMAAAIEgIBACEQAIAAAAgAAAABAAgBEAA=  AMAAoABIFgEMAAAIEgIBACEQAIAAAAgAAAABAAgBEAA=  0  106
15  6/v/5/77rarP5n/d+/22+ze//u/Ub7rrf6fL/+5v5ec=  6/v/5/77rarP5n/d+/22+ze//u/Ub7rrf6fL/+5v5ec=  0  304
16  NEDAGFSCxYBaICTKTRQhRZByhDOGCGIhwAGBETIJkCU=  NEDAGFSCxYBaICTKTRQhRZByhDOGCGIhwAGBETIJkCU=  0  503
17  cuOCPWz/MTtVA40WVmDwtGua37XyTCfWvyK7aEsNPPk=  cuOCPWz/MTtVA40WVmDwtGua37XyTCfWvyK7aEsNPPk=  0  794
18  zjnmhXnrF3qLqR53PcxeH/ObfW1trXrukvLdFp7okn8=  zjnmhXnrF3qLqR53PcxeH/ObfW1trXrukvLdFp7okn8=  0  397
19  sHGAQAAAQJEAxCQQgwCzggrqwGBBIYCQQgUAooARAAA=  sHGAQAAAQJEAxCQQgwCzggrqwGBBIYCQQgUAooARAAA=  0  304
20  YAACOCSKJBQQ4GJAkChBGYQAaIV5SETRAQFIMVSZhCo=  YAACOCSKJBQQ4GJAkChBGYQAaIV5SETRAQFIMVSZhCo=  0  608
21  AAABCADAAAAASIgACIQEAAAgEAgQgIAAAACAACAEBQE=  AAABCADAAAAASIgACIQEAAAgEAgQgIAAAACAACAEBQE=  0  106
22  P5s7ldnzdpcYPIV1ofdtbDwg3FJSmQrsIxvO7yxVODE=  P5s7ldnzdpcYPIV1ofdtbDwg3FJSmQrsIxvO7yxVODE=  0  794
23  /1ovrX4O0wyzvs/t5pxu/77/u/u+fM1F293/ed38//8=  /1ovrX4O0wyzvs/t5pxu/77/u/u+fM1F293/ed38//8=  0  304
24  CAAhgAAhAIAAKAUBQQDIAAAAAAASAAAAkCEAGIAIAAA=  CAAhgAAhAIAAKAUBQQDIAAAAAAASAAAAkCEAGIAIAAA=  0  106
25  QEmAUWJgaC7AAOKhgnAQY4gOzUBgXNAIJihh5qKCMiY=  QEmAUWJgaC7AAOKhgnAQY4gOzUBgXNAIJihh5qKCMiY=  0  503
26  AXXD+HCX/m+e7/Sqqa8qW9mpzb55z868v/O5K9X3f38=  AXXD+HCX/m+f7/Sqqa8qW9mpzb55z868v/O5K9X3f38=  1  688
27  0U6XHP6+cGWHtHc/C298TfeiX/Ol7O54L5wnKeUfNj8=  0U6XHP6+cGWHtHc/C298TfeiX/Ol7O54L5wnKeUfNj8=  0  688
28  9u3G8bf/uOP/fr73n77yg/+x/L9L3r3Wn++3/2+9//4=  9u3G8bf/uOP/fr73n77yg/+x/L9L3r3Wn++3/2+9//4=  0  304
29  e258rc/J/94Pcj/5/4r/fX9z3+N/vx893eXJ+8/fZvI=  e258rc/J/94Pcj/5/4r/fX9z3+N/vx893eXJ+8/fZvI=  0  304
30  +N85m/3/+v+f819v5vf1vz5P9cq3/73S923vY5mfnfO=  +N85m/3/+v+f819v5vf1vz5P9cq3/73S923vY5mfnfO=  0  304
```

Session key recovery cycle. We tested a protocol recommended by [Lockheed Martin](): a session key recovery cycle driven by a single device. Such a protocol is challenging because the reference responses are the result of a single read of the PUF, the session keys are encrypted by the PUF responses. BERs were evaluated by performing 5000 successive cycles. Shown enclosed is the probability of occurrence as a function of the numbers of errors for 256-bit long keys. The average BERs observed in this experiment are 6.148 10^{-4}. The PUF created 787 errors out of the 5000x256 bits. All errors were corrected by the RBC; the keys were recovered 100% of the time. Further optimization of the BERs can be achieved by increasing the enrollment cycles and identifying more cells that are unstable.



Conclusion and future work. The work presented in this white paper is providing encouraging results on ternary PUFs designed with pre-formed ReRAM arrays and driven by the TAPKI protocol. The 1a samples, as well as the ASIC, provided by Crossbar, had extremely low rates of defects, encouraging tamper resistance properties, and excellent reliability. This allowed the design, and test of APGs with low BERs, and the fabrication of prototypes demonstrating end-to-end cryptographic protocols. A second phase of this research effort is needed to integrate the components designed around the engineering board. Such an integration should further enhance tamper resistance, and to allow the development of use cases for a variety of applications, such as the ones with radhard environment as suggested by AFRL-RV, key recovery from single device as suggested by LM, mobile servers operating in zero-trust environment, PKI with digital signatures, and infrastructure for secure supply chain.

Reference papers available on demand: bertrand.cambou@nau.edu