Questions to be asked:

1. What are some of the anti-ageing techniques used in SRAM PUFs?
2. Papers available in the IEEE portals only mentioned that successful reconstruction of keys is achieved by correcting up to 15% of bit values. However, Broadkey claims to achieve successful key reconstruction at 25%. How is BroadKey’s error correction algorithm different from other error correction algorithms such that it is able to achieve this figure of 25%? Is there any way that we could test this out?
3. We are using SRAM to secure the boot process. Due to the fact that turning the SRAM on for very long period of time could wear off the SRAM and clear its data, do we need the SRAM after the boot process or could they be turned off after verification?
4. For bk\_create\_private\_key function, there are 3 sources. Source 1 is actually derived based on the device fingerprint and the activation code of the cryptographic instance. However sources 2 and 3 are based on a random source and from user defined sources respectively. Therefore can the private keys generated from the random source be re-generated? If not, what is the purpose for this random source?
5. For the bk\_compute\_public\_from\_private\_key, is the same public key being generated each time this function is called or are the public keys different?
6. It has been stated in the paper that the bk\_generate\_cryptogram function can be used to achieve confidentiality, integrity, non-replayability and authenticity of the sender. In this function, we are including the sender\_private\_key\_code and receiver\_public key code as parameters. Furthermore, for bk\_process\_cryptogram, the sender\_public\_key\_code and the receiver’s private\_key\_codes are required. When this is the case, how does sender/receiver authentication take place? Sender encrypts using his private key and uses the receiver’s public key to authenticate. Receiver uses the sender’s public key to decrypt. Then why do we need the receiver’s private key as parameter for bk\_process\_cryptogram?
7. Can I re-generate more than 1 pair of private public key pairs without having to store in the non-volatile memory?
8. I came across in a paper that side channel attacks could be applied to error correction processes and even extractor functions in PUFs. They perform these attacks by monitoring the chip’s power consumption, its electromagnetic emanation ect. How secure are BroadKey’s error correction processes from these kinds of attacks? Have any tests been conducted?

Concerns (are they really physically unclonable) sources (<https://silicontrust.files.wordpress.com/2013/06/cloning.pdf>, <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8118417>,

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7560198> ):

* There are fault attacks done on helper data generated by the PUF function. Fault attack methods include alpha radiation, laser or electromagnetic localized impulses, X-rays, beta ray and UV-irradiation, temperature exposure or gas diffusion to induce permanent changes.)
* Side channel attacks could be applied to error correction processes or extractor functions used in PUF implementations. – By observing the chip’s power consumption, its electromagnetic emanation, local optical emission or laser voltage probing, an attacker can spy out confidential data.
* Error correction and extraction circuits are possible targets for snooping data.
* PUF are only physically unclonable, but mathematically, they are still clonable; if a reaction of a PUF circuit to an unknown input is predictable, the attacker could implement his own solution to generate such data and produce cloned chips. 🡪 Leads to a phenomenon called the modeling attack where input and output data are first collected and then mathematically analyzed. Computer model is generated that could give a prognosis for the PUF behavior to an unknown data. Therefore, modeling attacks can be done using machine learning and logistic regression techniques.
* Machine learning attack occurs by collecting several challenge response pairs and then trying to predict responses to unknown challenges. Machine learning attacks can predict PUF responses to unknown challenges with high probability (but not completely).
* SRAM PUFs are harder to read out invasively but they are weak PUFs as they only involve simple, single challenge response. Purely numerical modeling attacks are not relevant for weak PUFs with only one challenge. However, SRAM PUF is susceptible to side-channel attacks. Most importantly, SRAM is subjected to wearout attacks that could even change the state of the most stable bits. This is done through the use of accelerated stress using elevated voltage and temperature.
* The SRAM PUFs in this report (<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7560198> ) were subjected to accelerated stress (temperature of 120 degree celcius and Vdd of 7V). Therefore, using the results that were obtained from this report, if the SRAM remains powered on while storing its startup value (digital fingerprint) then it would most likely to experience greatest loss of data. 15% recovery failure rate (maximum percentage of bit errors that are allowed so that the reconstruction of keys could take place). Under accelerated conditions, the percentage remained well above 15% even after not subjecting to stress for a month (no natural way of restoring it). Therefore, if an SRAM is allowed to remain powered on while storing its startup value (digital fingerprint), it could cause equal damage to erasing the fingerprint. Data that has been previously encrypted will not be available/cannot be retrieved 🡪 Total loss of data.
* If there is complete loss of data, the loss of data can be reversed by using a negative voltage. In this way, permanent loss of data can be reduced or even be eliminated. Therefore, there is still a way for the original PUF to be used again with the original enrollment information.
* This paper (<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7560198>) suggests that an SRAM PUF should not be used as data storage once identification is complete, and that it should be powered down immediately afterward, as the most effective way to erase its fingerprint is to stress it while storing its most probable state at power-on (its fingerprint).

Some additional notes:

* The main mechanism that increases the noise in the SRAM PUF is the silicon-aging phenomenon. If nothing is done about the degradation levels, the noise levels in the PUF may become impossible to be corrected.