Reviewer 2:

Please see modification in the manuscript marked in blue.

General comments:

1. In the SUC creation step, a larger class of ciphers need to be created. Does the number of cipher have the influence on the performance?

   The cipher class-size has no influence at all on the created SUC performance. However the class-size may increase the run-time for the GENIE as cipher creator and its complexity. On the other hand, if the number σ of all possible SUCs is very large, then the search space of an adversary to identify the chosen cipher is correspondingly larger. Therefore, we added the following sentence in the lines 239-240:

   “The SUC design proposal is targeting HCRE > 500 bits, that is the cloning complexity is larger than 2^500 cycles and/or memory bits.”

2. How many ciphers are used in the paper, 600? Do we need to save these ciphers?

   The number of possible ciphers in the paper is $2^{649}$ different ciphers. There in no need to store them. The proposed GENIE in the paper requires 896 TRNG random unknown bits to generate randomly one cipher out of $2^{649}$ possibilities.

   Therefore, we added a new description in the lines 513 till 520.

3. In page 6, the authors wrote "A Trusted Authority (TA) injects into a System on Chip (SoC) device a single event the software package “GENIE”, for a short time." What does a short time mean?

   Short time means as much time as required to create an unknown cipher, usually few milliseconds.

   We rewrote the whole paragraph referring to Fig. 4 again to make it clearer. Please check the lines 176 till 186.

4. Will it has risk to be attacked during the time of using GENIE? What is the kind of software package “GENIE”? It should be a public or private part in the scheme?

   No risk as SUC creation is assumed to be processed in a secure environment by end-manufacturer as a trusted authority TA which would not act against itself. Notice that TA cannot even create two units with the same serial number as TA has no control and access at all on what happens inside the unit during SUC creation. The device is only
cloneable if the random TRNG bits stream can be leaked out or stored during the few creation microseconds in the assumed TA secure environment.

5. The authors claim that the proposed scheme is a possible zero-cost scheme in conclusion. Could you please give more details about the complexity, memory requirement for this scheme?

Most FPGA applications do not consume the whole FPGA resources. In particular powerful and complex multiplier cores. The ultimate goal of the SUC design is to embed the SUC in the FPGA without cutting resources from the functional FPGA duties. The reason is that, embedding SUCs and personalization is processed at the very late stage by the end-manufacturer before releasing the products to the market. This allows the end-manufacturer to attain the highest security as all sub-contractors would have no influence on the security management. In other words, end manufacturer can easily produce his different components outside his factory without having any fear that the sub-contractor would be able to clone his products as sub-contractors are fully out of the security process. Any produced component cannot be used without the SUC-approval of the end-manufacturer. Cloning by pirate companies or sub-contractors is then prohibited and the original products royalties are then fully protected.

Zero-Cost aspects: The cipher design is deploying mainly hard-core (complex) multipliers as major building blocks which may be available unused in modern System on Chip SoC FPGA devices. The ultimate target of the cipher design is to allow “reanimating” spare unused multiplier-cores to convert devices into clone-resistant units at possibly zero-cost. Zero-cost is assumed to be attained, when embedding such a SUC module in a device does not consume any area cut from the usual application resources.

This text is added to the updated version of the conclusion lines 641 to 659. Many thanks to the reviewer for this hint.

Minor comments:

Secret Unknown Ciphers SUCs should be changed to Secret Unknown Ciphers or SUCs. They are the same words. For example, in page 2, line 59 and page 1, line 19. Fig. 19 should be explained with more details. What do the different markers and the bigger blue circles mean?.

We took your notes into consideration and rewrote the description of Fig. 19 as follows:

Figure 19 illustrates an experimental security analysis on 20 000 randomly selected different ciphers from the proposed class to figure out the minimum number of differentially active GSs. It was found that after 4 rounds and for all 20 000 ciphers, at least 12 to 18 GSs (out of 32) were differentially active (shown as colored circles). After increasing the number of rounds the active GSs increased proportionally. The ciphers having only 12 active GSs after 4 rounds mostly stayed in the bottom in their number of active boxes (marked as bold blue circles) but never divert far away from
the remaining sample ciphers. After 10 rounds, at least 48 GSs (out of 80) were active. The security analysis is made based on the worst case active GSs.

Please check the lines 597 till 604.