A New Low-Complexity Cipher Class for Clone-Resistant Identities

Saleh Mulhem, Maen Mohammad and Wael Adi
Institute of Computer and Network Engineering, Technical University of Braunschweig, Braunschweig, Germany
{s.mulhem, w.adi}@tu-bs.de

Abstract - A new large cipher class based on new two-variable self-inverse-permutation deploying Golden S-Boxes is presented. The mapping has particular properties, in that it is both self-inverse and uses arithmetic over the ring of integers modulo 2\(^a\). The key contribution of such cipher structures is in activating the use of passive hard-core multipliers (Math-Blocks) in modern FPGA devices. Such multipliers are often available for free when not utilized in for the system tasks. Standard ciphers do not usually use multiplications due to their high implementation complexity. The proposed cipher class is reactivating such free multipliers to create good quality ciphers at very low cost. The target application of such ciphers is in creating the so-called Secret Unknown Ciphers (SUCs). Such SUCs can serve as highly-resilient clone-resistant digital-identity-modules in future smart self-reconfiguring non-volatile FPGA devices. The security level of the resulting ciphers is relatively high and scalable. The main future application areas of such structures are expected to be for vehicular security applications. A sample implementation prototype demonstrates the complexity of the resulting physical identity and its performance.

Keywords - Secret Unknown Ciphers; Physical Unclonable Function; Golden S-Boxes.

I. INTRODUCTION

Since the software-based device identities can be easily cloned and manipulated, several clone-resistant physical approaches were proposed. Unclonable physical properties are much harder to attack and require often very expensive invasive attack techniques. Many physical identification solutions were proposed based on just checking a stored secret key in an embedded non-volatile memory (NVM) [1]. Such technologies has early fallen short against low-complexity physical attacks [2]. Two decades ago, Physical Unclonable Functions (PUFs), often realized as embedded structures in VLSI devices were proposed to serve as better uncloneable physical identities [3]. The key idea behind PUFs is to extract unique hard-to-clone binary sequences from highly nonlinear unknown born properties of some VLSI physical structures in electronic devices. PUFs exhibit born identification properties which are essentially impossible to clone similar to DNA chains in human beings.

However, due to the varying operation conditions as temperature, supply voltage, and other effects, PUFs suffer from inconsistency/repeatability of their identity response. The PUF’s input-output response exhibits therefore high inconsistency resulting with re-identification errors [1]. To counteract inconsistency drawbacks, fuzzy extractors using Helper Data Algorithm (HDA) were proposed as an approach to mitigate this problem. Therefore, most of the proposed PUFs still have the same difficulties in being complex and costly to implement and use in modern technology applications.

Furthermore, PUFs have been proved to be vulnerable to modeling attacks. Such attacks exploit the bias and correlations in PUF’s input-output or so-called challenge-response pairs (CRPs) to construct a machine learning algorithm with high prediction rates approaching 99% [4]. Any effort to overcome modeling attacks makes PUFs more expensive and complex.

Various protocols utilizing PUFs has been envisaged to provide a lightweight entity authentication. In [1], nineteen proposals have been studied. The results show that most of the PUFs require multiple communication transactions with the server to attain a stable response, and PUFs also exhibit a small response space that requires expansion to be sufficiently large for the entity authentication.

The Secret Unknown Cipher (SUC) was introduced as a new alternative to PUF initially in [5]. SUC is defined as a randomly self-created crypto-function which is embedded in a post-fabrication process within off-shelf FPGA devices. Furthermore, the realization of SUC-concept as a pure digital structure essentially ensures the consistency of its input-output pairs. On the other hand, SUC concept satisfies a manufacturer resistant deployment. Furthermore, the SUC-creation concept do not allow producing two equal SUCs/identities.

The main contributions of this paper are first to design a new class of Feistel-like ciphers by replacing the XOR operation by a new powerful self-inverse mapping. The new mapping is based on simple arithmetic using addition and multiplication over \( \mathbb{Z}_2 \). The keyidea for using such unusual arithmetic is that it is often available for free (as unused units) in many modern FPGA applications. In other words, the new cipher structure is a novel recycling of dead arithmetic units for creating good ciphers. Multipliers are otherwise usually not-attractive for ciphering operations due to their inherent high-complexity. The resulting new cipher-class is usable for self-creating of Secret Unknown Ciphers SUCs which were proposed to “digitally-mutate” future programmable VLSI devices into physically clone-resistant units at relatively low cost.
The rest of this paper is organized as follows. In Section II, a short summary covering several Digital PUFs (D-PUFs) designs and SUC’s proposals are presented. Section III introduces the concept of SUC as a D-PUF and points to the target implementation environment. Section IV gives SUC design strategy and a new class of mathematical involutions. In section V, a hardware implementation is provided and evaluated. Section VI shows a security analysis of the proposed SUC.

II. RELATED WORK

Several PUF designs have been introduced in the literature [3] [1]. Within the scope of this paper, D-PUFs are discussed and reviewed. A PUF is called digital when it is silicon-based, and it is extracted from special unique variations of a chip’s intrinsic characteristics. This deviation occurs randomly and cannot be controlled during the assembly process. Moreover, the PUF is called strong when it can support a large number of CRPs [1]. Though PUFs are assessed insusceptible to invasive physical attacks because it would destroy the secret through damaging the PUF, they fall short against the side channel analysis which is a non-invasive physical attack. A series of successful attacks has been done on Arbiter PUF [6], SRAM PUF [7], Ring Oscillator PUF [4].

A tremendous amount of research was conducted on PUF as a permutation mapping. For instance, PUF-based block cipher is introduced in [8]. This integrated approach defines a new concept so-called Physical Unclonable Pseudo Random Permutation (PUPRP). Where the integration of PUFs with confusion/diffusion properties of a block cipher enhances the temper-resilience of the overall design [9]. Wu and et al [9] deployed the integrated approach to construct PUPRP, which combines 4×4 PUFs into Feistel cipher. Unfortunately, every 4×4 PUFs require HDA to attain a stable response for every round. That increases the hardware complexity to implement such a proposal. In [10], public D-PUF is presented based on delay PUF that is utilized as a key generator to initialize a Boolean function imprinted in FPGA fabric (LUTs). The purpose of the public D-PUF exploits the time gap between the D-PUF execution and its simulation. Moreover, Hardware- Software Digital PUF (HW-SW DPUF) was first proposed in [11] as a cascade of randomly chosen functions from a large class of random cryptographic functions. The random selection of functions is performed by using a bit stream of a True Random Generator (TRG). The authors only utilized Feistel cipher as a function of such cascade. All previous described D-PUFs are reducing the typical disadvantages of analog PUFs against operational effects at relatively high overhead complexity.

Regarding the previous presented issues, SUC is proposed as an alternative to PUFs for lightweight authentication entity. Unlike the conventional PUFs, SUCs use only-digital-mappings making all aging and other operational factors without effect during the whole device life cycle of the device. Additionally, it was proved in previous work that the SUCs offer an easy to scale digital response space [12]. Furthermore, several proposals and applications of SUC recently investigated and published. For instance, a classical generalized Feistel network deploying Golden S-boxes is presented in [13] to realize the SUC-concept. In [12], SUC-based “Key Generation Entropy” is modeled and compared with strong traditional PUFs. The key differences between the previous proposals [12] and this work, are that FPGA hard-core multipliers are involved for both confusion and diffusion in this new SUC creation proposal. In addition to that, the golden S-Boxes are additionally used as confusion blocks. The resulting Feistel Network is further optimized in complexity and cryptographic performance compared to [12]. However, SUCs are deployed in [11] as a lightweight cipher to provide an electronic device with an identity. In [14], Adi et al. presented a SUC-based lightweight protocol that enables efficient two-way communications for low-cost physical authentication.

III. SUC CONCEPT AND THE TARGETED TECHNOLOGY

Since “the only secret which can be kept unrevealed is the one which nobody knows”, the unknown function concept was introduced in [5]. The concept of Secret Unknown Cipher (SUC) theoretically combines between secret cryptographic key principle and a cascade of unknown symmetric-ciphers. The SUC concept is practically based on randomly self-creating such unknown hard-wired ciphers in a cascade. In other words, the main idea behind SUC is to trigger a random event process that generates a combined Hardware-Software module embedded in a System-on-Chip (SoC) unit[11]. This combination is non-reversible and very hard to predict.

A. Concept of SUC Creation and Personalization

Fig.1 illustrates the creation process of SUC. In step 1, a smart software cipher designer program so-called “GENIE” is uploaded by a trusted authority (TA) into an off-shelf SoC FPGA. In step 2, the GENIE starts a single-non-repeatable event to generate one unknown and unpredictable cipher SUC, with the help of True Random Generator (TRG). In step 3, the GENIE is completely removed from the SoC device. Then, the device with a unique permanent SUC is physically locked. Therefore, non-volatile VLSI technology is required. In step 4. TA initializes the device by choosing a set \{x_1, ..., x_l\} of clear texts as random challenges and stimulates the device to generate the corresponding ciphertext set \{y_1, ..., y_l\}. The resulting challenge-response pairs of each individual device are stored in a secret record. Finally, the SoC devices should prohibit reconfiguration after generating SUC by irreversibly setting some last-fuse lock.
Now, SUC is ready to be used as an identification module to any entity. Note that self-reconfiguration technology is expected to emerge in the flash-based non-volatile technology in the near future.

B. Target Technology Environment

The only non-volatile flash-based FPGA with switching fabrics and programmable cells is available by Microsemi Smart-Fusion®2. The FPGA fabric incorporates an integrated ARM Cortex-M3 processor together with powerful/high-performance arithmetic Mathblocks (MACCs), including multipliers, all integrated into this chip. The integrated MACCs are optimized to efficiently perform 18x18 multiplication with zero hardware cost as shown in Fig.2. To avoid complex modular arithmetic, the ring of integers arithmetic modulo 2^18 is adopted as the basic cipher algebra in \( \mathbb{Z}_{2^{18}} \) (that is \( n=18 \) in Fig.2).

Fig.3 illustrates a possible functional layout after generating SUC in FPGA which uses MACCs interacting with logic components implemented in FPGA fabric. This combination between MACCs and logic implemented components results with the desired SUC.

To improve the security level of SUC, an FPGA technology, that can be kept the cipher location random and unknown, is required. Note that the random and individual location of each SUC makes physical attack very difficult, even the adversary tries to get some information by probing points inside the chip [15].

C. SUC Basic Use in Physical Identification Protocol

Fig.4 shows a generic 2-way-protocol for authenticating a SUC unit which proceeds as follows:

1) TA randomly selects a pair \((x_i, y_i)\) from the record of SUC. TA then sends cryptogram \( y_i \) to SUC device.

2) SUC responds by sending decrypted clear text \( x_i' \). If \( x_i' = x_i \), then the unit SUC is authentic. The pair \( x_i, y_i \) is marked as used and never used again.

IV. CIPHER DESIGN STRATEGY

A huge class of cryptographically-significant mappings is required to select one of them as a randomly selected SUC. Therefore, in the best-case scenario, the cardinality of all possible usable mappings should approach infinity.

A. Golden 4-bit S-Boxes as Primitive Building Elements

In [16], Saarinen showed that there are only four classes of 4-bit bijection S-Boxes which can affinely transform the resistance properties against linear cryptanalysis (LC) and Differential Cryptanalysis (DC) to all members of classes that are called golden S-Boxes.

TABLE I shows four 4-bit golden S-Boxes seeds \( G_S \), where \( k=0,1,2,3 \), which generate 4-classes of S-Boxes fulfilling all the ideal and cryptographically significant properties.

| GS Seed Classes | 4-bit input combinations | DC | LC
|-----------------|--------------------------|----|----
| \( G_{S0} \): 4-bit outputs | 035860CAE41FB2 | \( \frac{1}{4} \) | \( \frac{1}{4} \)
| \( G_{S1} \): 4-bit outputs | 03586B79EADF214 | \( \frac{1}{4} \) | \( \frac{1}{4} \)
| \( G_{S2} \): 4-bit outputs | 03586AF4ED9217CB | \( \frac{1}{4} \) | \( \frac{1}{4} \)
| \( G_{S3} \): 4-bit outputs | 03586CB7A9EF12D | \( \frac{1}{4} \) | \( \frac{1}{4} \)

The equivalence relation for class-generator is defined based on two binary permutation matrices \( P_a, P_b \), two 4-bit vectors \( a, b \in \mathbb{F}_2^4 \) and XOR-operations as follows:

\[ S(x)_{i\times4} = G_S \left( \left[ \begin{array}{c} x_{i\times4} \end{array} \right] \left[ \begin{array}{c} P \end{array} \right] \right) = \left[ \begin{array}{c} a_{i\times4} \end{array} \right] \left[ \begin{array}{c} P \end{array} \right]_{i\times4} \oplus \left[ \begin{array}{c} b_{i\times4} \end{array} \right] \] (1)

Fig.5 shows the corresponding block diagram for realizing the mapping described in (1). The number of the resulting S-Boxes is \( 4^4 \times 24^2 = 2^{17.1} \) for each \( G_S \). And the cardinality of Golden S-Box class is \( 4^{2\cdot17.1} = 2^{19.1} \).
Figure 5. Hardware Sketch of the Golden S-Box Generators [13].

The SUC cipher creator “GENIE” can easily use this formula for creating a class of $2^{10\cdot 1}$ possible different golden S-boxes [13].

B. New Involution-Mapping in Two Variables

A polynomial $P : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ in two variables $(L,R)$ is defined as a special mapping having two inputs and one output in $\mathbb{Z}_2^n$ as the ring of integers mod $2^n$, as follows, 

$$P(L,R) = a \cdot L + b \cdot R$$

(2)

Where, $a,b \in \mathbb{Z}_2^n$.

The target of this work is to create self-inverse functions with respect to only one variable such as $L$.

**Definition 1.** The polynomial $P$ in two variables $L$ and $R$ on the ring $\mathbb{Z}_2^n$ is considered as a self-inverse polynomial with respect to $L$, if the following holds:

$$P(P(L,R),R) \mod 2^n = L$$

(3)

For any $L$ and $R$.

The following lemma presents the important properties of the modular arithmetic over $\mathbb{Z}_2^n$. Note that $x = x_{n-1} \cdots x_0 \in \mathbb{Z}_2^n$ is a $n$-bit vector, where $x_i \in \mathbb{Z}_2$, for every $i \geq 0$ and $1$ denotes 0 or 1.

**Lemma 1.** Let $a,b \in \mathbb{Z}_2^n$,

- If $a = 1 \cdots 1$, then $a^2 \mod 2^n = 1$.
- If $a = 1 \cdots 1 \cdot 0 \cdots 0$, and $v = 1 \cdots 1 \cdot 0 \cdots 0$, then $u \cdot v = 1 \cdots 1 \cdot 0 \cdots 0$, where $i,j \leq n$.
- If $b = 1 \cdots 1 \cdot 0 \cdots 0$, then $b^k \mod 2^n = 0$ for $k \cdot r \geq n$.

The proofs are straightforward through the modular arithmetic over $\mathbb{Z}_2^n$.

The following theorem determines the conditions required to reach such self-inverse polynomials in two variables $(L,R)$ with respect to $L$ over $\mathbb{Z}_2^n$.

**Theorem 1.** Let $n \geq 2$ and $P(L,R)=aL+bR$ be a polynomial in two variables $(L,R)$ over $\mathbb{Z}_2^n$. $P$ is a self-inverse polynomial with respect to $L$ if all the following conditions are satisfied:

1. $a = 1 \cdots 1$.
2. $b = 1 \cdots 1 \cdot 0 \cdots 0$, where $r \geq \frac{n}{2}$ and $n$ is even.
3. $b = 1 \cdots 1 \cdot 0 \cdots 0$, where $r \geq \frac{n}{2}$ and $n$ is odd.

**Proof:**

First, let’s prove that if $n$ is even and $a = 1 \cdots 1 = 2^n - 1$, then $P(L,R)=aL+bR$ is a self-inverse polynomial with respect to $L$ over $\mathbb{Z}_2^n$. Another case can be proven in a similar fashion.

For $r \geq \frac{n}{2}$,

$$P(P(L,R),R) = a(aL+bR)+bR$$

And,

$$P(P(L,R),R) = a^2L+b(a+1)R$$

Now,

$$P(P(L,R),R) = a^2L+b(2^n - 1 + 1)R$$

Yielding,

$$P(P(L,R),R) = a^2L+2^n bR$$

Applying mod $2^n$ and from Lemma 1 results with,

$$P(P(L,R),R) \mod 2^n = L$$

□

Note that a self-inverse polynomial in two variables with respect to one variable defines a new $n$-bit mapping so-called $\pi$-mapping as shown in Fig.6, where $\pi(L) = (aL+bR) \mod 2^n$. It is very simple to prove that the $\pi$-mapping is an involution for any $R$.

Figure 6. The New $\pi$-Involusion used as a arithmetic operation.

In [17], Patel et al replaced XOR-operation in Feistel network by the addition $(L+R) \mod 2^n$ to define a $2n$-bit permutation. The results showed that the three-round variant of such a cipher is a pseudorandom permutation. Therefore, in Fig.7, replacing the XOR-operation in...
Feistel network by \( \pi(L) \) results with a new mapping
\[ \psi(L, R) = (P(L, F(R)), R) \]
which is also an involution.

Figure 7. The New \( \psi \)-Involution as XOR Replacement

The following corollary determines the number of all district self-inverse polynomials with respect to \( L \).

**Corollary 1.** For \( n \geq 3 \), the cardinality of the class \( \psi(L, R) = (P(L, F(R)), R) \) over \( \mathbb{Z}_2 \) is:

\[
\text{Card}[\psi] = \text{Card}[P(L, R)] = 2^{\frac{n}{2}+1}; \quad n = 2k
\]

\[
\text{Card}[\psi] = \text{Card}[P(L, R)] = 2^{\frac{n}{2}+1}; \quad n = 2k + 1
\]

(4)

Where, \( k \in \mathbb{N} \).

V. PROPOSED CIPHER-CLASS AND ITS COMPLEXITY

In this section, a new cipher design of SUC and its hardware implementation are presented.

A. Proposed Cipher Structure

Referring to Fig. 8, the proposed 15-rounds cipher as a modified Feistel cipher by deploying the mapping \( \pi(L, R) \) to replace the classical XOR-mapping resulting with Feistel-like \( \psi \)-Involution.

Figure 8. A Sample 64-bit SUC-Cipher Structures.

The mapping’s input data is 64 bits that splits into two 32-bit branches \( (L, R) \) in the first round. A 32-bit key is XORed with the left round branch \( L \). The involution \( \pi \)-mapping as \( (aL + bF(R)) \) is applied on \( L \) and the output of the inner function \( F \). The mapping \( F \) uses the 32-bit \( P_2 \) input and splits it into four 8-bit branches. \( F \) consists of a nonlinear layer of two-horizontal-blocks using four golden S-Boxes together with a rotation-permutation layer. The involution \( \pi \)-mapping is used recursively again in 8-bit size.

Moreover, \( F \) is composed of a recursive \( r \)-rounds repeating the usage of the same outer Feistel-similar structure. The example of Fig. 8 proposes to take \( r = 6 \) rounds as a minimum-number of rounds required to reach full diffusion in that S-Boxes iteration rounds as shown in [18]. The used golden S-Boxes are randomly selected according to (1) or Fig. 5. The outer round-structure is selected to have 3-involutions namely: XOR with a key followed by \( \psi \)-involution and terminated by swapping-involution. The 15-outer rounds are using the same 3-involutions each time with a different 32-bit-key.

B. A Possible Hardware Implementation Structure

To implement a possible compact version of the proposed cipher, the architecture of Fig. 9 is proposed as a successive round-based implementation [19]. Iterating one cipher-round (includes the said 3-involutions) is deployed as the core of the hardware design structure. A state register of 64-bit and a 64-bit multiplexer completes the state machine structure to run the 15-cipher rounds, where, each cipher-round is executed in one clock-cycle. In this implementation, additional clock 6-cycles are required for computing of inner function \( F \).

Furthermore, a new technique of key scheduling is presented in Fig. 9 storing the 16-round-keys in 32 LUTs. The keys are selected fully randomly by the GENIE. The proposed key schedule compared to Khudra and other ciphers [18] differs in that our 16-keys are fully independently and randomly generated. Note that the key entropy in our case is \( 2^4 \times 32 = 2^{12} = 512 \) bit instead of only 32-bits in the other cipher structure deploying key-schedule generating the sub-keys out of only 32-bit input-key.

Table II shows the resulting hardware complexity of the sample proposed SUC implementation in a SmartFusion®2 SoC FPGA:

**Table II: Hardware Complexity Using SmartFusion®2 M2S025T FPGA**

<table>
<thead>
<tr>
<th>Hardware Resources</th>
<th># LUTs</th>
<th># D-FFs</th>
<th># MACCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>The proposed SUC</td>
<td>208</td>
<td>113</td>
<td>8</td>
</tr>
</tbody>
</table>

VI. SECURITY ANALYSIS AND EVALUATION

According to Kerckhoffs’s principle: “An attacker knows all details of the used cipher structure except the cipher-key which is kept secret”. To increase the security of the cipher, the idea of using a block cipher with secret
components is early investigated. For instance, Biryukov and Shamir [20] cryptanalyzed the so-called AES-like cipher that is defined as two and a half rounds of AES-128 with secret 8-bits S-Boxes and secret affine mapping. In such architecture, the attack requires only 2^{16} chosen plaintexts to determine all secret S-Box components.

In SUC- attack model, an attacker theoretically needs to recover the secret key and then to predict the randomly-chosen golden S-Boxes and the coefficients a, b of each mappings \( \pi(LR) = aL+bR \) of the SUC. The successful attack is possible with a complexity of the order \( (2^{71.8} \cdot 2^{23} \cdot 2^{16.9}) \approx 2^{121.7} \). Where, \( 2^{71.8} \) is the number of distinct choices for selecting 4 different golden S-Boxes from a class of \( 2^{19.1} \), \( 2^{23} \) is the number of choosing one 32 bits \( \pi(LR) \) out of all possible mappings, and \( 2^{16.9} \) is the number of choosing two different 8 bits \( \pi(LR) \) out of \( 2^{8} \) possibilities according to (4). The attack complexity may be reduced by using a novel differential-style attack on a block cipher with secret components as given in [21]. However, this is only possible if the attacker gets access to each output of a round function which is prohibited in SUC structure model.

Furthermore, the selected S-Boxes are golden S-Boxes and their differential behavior is known (see TABLE I). In [13], an exhaustive search algorithm has showed that at least 6 “active S-Boxes” need to be crypto-analyzed in the inner function \( F \) for both differential and linear cryptoanalysis. These S-boxes have a differential probability of \( p = \frac{1}{2^6} \) and a linear approximation characteristic probability of \( e = \frac{1}{2^4} \). In this case, the inner function \( F \) exhibits a differential and linear time complexity of \( 2^{26} = 2^{12} \). Therefore, the proposed SUC with at least 15 rounds has neither differential nor linear characteristics whose complexities are less than \( 2^{152.14} \approx 2^{168} \). This discussion proves that even if the GENIE is published or somehow found, then the proposed SUC has an acceptable level of security. Otherwise, an attacker is only able to collect the input combinations and save the corresponding outputs in the term of the generic attacks with respect to a black-box attack model, where, the probability of guessing/predicting the secret parameters and then recovering the secret key approaches the products of both previous complexities, that is \( 2^{168} \cdot 2^{121.7} \approx 2^{289.7} \). Therefore, ongoing research is conducted to answer the following open question: whether the three-round variant of such a cipher behaves like a pseudorandom permutation [17].

VII. CONCLUSION

A new self-creatable large cipher class based on multiplicative two-variables self-inverse mappings together with golden S-Box mappings is presented. The resulting ciphers can serve as low-complexity Secret Unknown Ciphers (SUCs) as a clone-resistant digital PUFs. The low-complexity results from recycling dead math-blocks in some FPGA applications. As a result, highly-resilient digital PUF may be created for possibly negligible-costs in existing applications using the unused MACCs (math-blocks) in their FPGA units. The resulting digital-PUF’s security level is scalable and can even cope with post-quantum security requirements.

REFERENCES