International Journal of Multimedia and Ubiquitous Engineering
Vol.10, No.11 (2015), pp.173-186
http://dx.doi.org/10.14257/ijmue.2015.10.11.17

# An Ultra-Lightweight Side-Channel Resistant Crypto for Pervasive Devices

Weijian Li

*School of Computer Science & Engineering,*
*South China University of Technology, Guangzhou, China*
*weijianlee@126.com*

***Abstract***

*Lightweight cryptography is equipped as security component, to secure those pervasive devices that are security and privacy sensitive. It has been conclusively proven that unprotected cryptographic implementations are vulnerable to side-channel attacks. In practice, area resource smaller than 3,000GE (5,000GE sometimes) may be available for security components in pervasive devices. This paper presents an ultra-lightweight first-order side-channel resistant crypto of KLEIN, which is a new family of lightweight block cipher that has advantages in both of software and hardware performances. The serial implementation of masked KLEIN requires 2102GE, while parallel implementation requires 4451GE, which are suitable for resource-constrained pervasive devices. Experimental results show that it is secure under First-order Power Analysis Attack, but still vulnerable to High-order Side-channel Attacks, with an exponential increase of the SCA data complexity.*

***Keywords:*** *Lightweight cipher, KLEIN, First-order masking, High-order Side-channel Attacks*

## 1. Introduction

Internet of Things (IoT) is a novel paradigm that is rapidly gaining ground in information technology. The basic idea of this concept is the pervasive devices around us, which are able to interact with each other and cooperate with their neighbors to reach common goals, through unique addressing schemes. Increasingly everyday items are enhanced to pervasive devices by embedding computing power, such as Radio-Frequency Identification (RFID) tags, sensors, ASICs and smart cards, which have harsh cost constraints in terms of area, memory, computing power, battery supply. Although the mass deployment of pervasive devices promises many benefits, when it comes to many applications that are security and privacy sensitive (military and financial applications, *etc.*), security and privacy are striving issues. Lightweight cryptography is equipped as security component, to secure such applications.

For resource-constrained devices, traditional block ciphers such as DES and AES, could be too expensive. Therefore, topic of lightweight ciphers is a pressing issue, and several lightweight ciphers have been published so far, such as PRESENT, LED and KLEIN. KLEIN [1] is a new family of lightweight block ciphers that is designed for resource- constrained devices such as wireless sensors and RFID tags. To meet the requirement of limited resources, lightweight cryptography is much simpler and serialized. Even worse, pervasive devices are deployed in a hostile environment, i.e. an adversary has physical access to or control over the devices, which poses a serious practical threat to these security components [2-3].

After over 15 years' research, it has been conclusively proven that unprotected cryptographic implementations are vulnerable to side-channel attacks. Power analysis attacks exploit the dependency between the instantaneous power consumption of a

ISSN: 1975-0080 IJMUE

cryptographic device and the data it processes and/or the operation it performs. Differential Power Analysis is a statistical test which examines a large number of power consumption traces to retrieve secret keys. Differential Power Analysis is one of the effective methods to retrieve secret keys, which includes mono-bit DPA [4] , multi-bit DPA[5, 6] and Correlation Power Analysis (CPA) [7-10].

During the last ten years, there have been many endeavors to develop effective countermeasures against DPA attacks, including two major countermeasures: hiding [11-12] and masking [13-17]. The latter is the most widespread, thanks to its relatively low overhead, low performance loss and robustness against first-order attacks.

To construct the masking scheme, the most important consideration has been to mask the S-box operation. Commonly, there are two strategies [19]:

1. The precomputation look-up table [13, 18, 19]: this method re-computes the masked S-box as a pre-computed look-up table, and stores it in RAM or ROM. The look-up table $MS-box(A \oplus M) = S-box(A) \oplus q$ is pre-computed according to the intermediate value $A$ and one or several random value(s) $M$. The value of $q$ could be different for different masking schema, in a simplified version, $q$ is equal to $M$, which is sufficient to prevent from first-order SCA.

2. The S-box secure calculation [15-17]: the S-box outputs are computed on-the- fly by using a mathematical (*e.g*. polynomial) representation of the *S-box*. Each time the masked value has to be computed, an algorithm is executed. The computation of algorithm is split into elementary operations (bitwise addition, bitwise multiplication, *etc*.) performed by accessing one or several look-up table(s).

Pervasive devices are strongly cost-driven, which prohibits expensive countermeasures. In practice, area resource smaller than 3,000GE (5,000GE sometimes) may be available for security components in pervasive devices [3]. Precomputation look-up table based masking countermeasure is low-cost and secure against first-order DPA, therefore is more suitable for lightweight ciphers in resource-constrained devices. In this article, we aim at First-order Side-Channel Resistant Crypto that is smaller than 3,000GE and 5,000GE, which is suitable for pervasive devices. Moreover, for the sake of practical use, its SCA Security will be discussed in the paper.

The remainder of this paper is organized as follows. Section 2 gives a brief description of KLEIN, as well as the security of unprotected KLEIN under first-order power analysis attacks. A brief and low-cost implementation of masking countermeasure is proposed in Section 3. Section 4 evaluates the security of our proposed masked KLEIN under first-order power analysis attacks, and second-order power analysis attack. Section 5 concludes the paper.

## 2. Side-Channel Attacks Against KLEIN

### 2.1. Algorithmic Description of KLEIN

The structure of KLEIN is a typical Substitution-Permutation Network (SPN), which is also used in many advanced block ciphers, *e.g*. AES and PRESENT. It has both block and key size of 64, 80 and 96 bits, referred to as KLEIN-64, KLEIN-80 and KLEIN-96, respectively. Number of rounds NR is 12/16/20 for KLEIN-64/80/96 respectively. A high-level description of the KLEIN encryption is described in Figure 1.

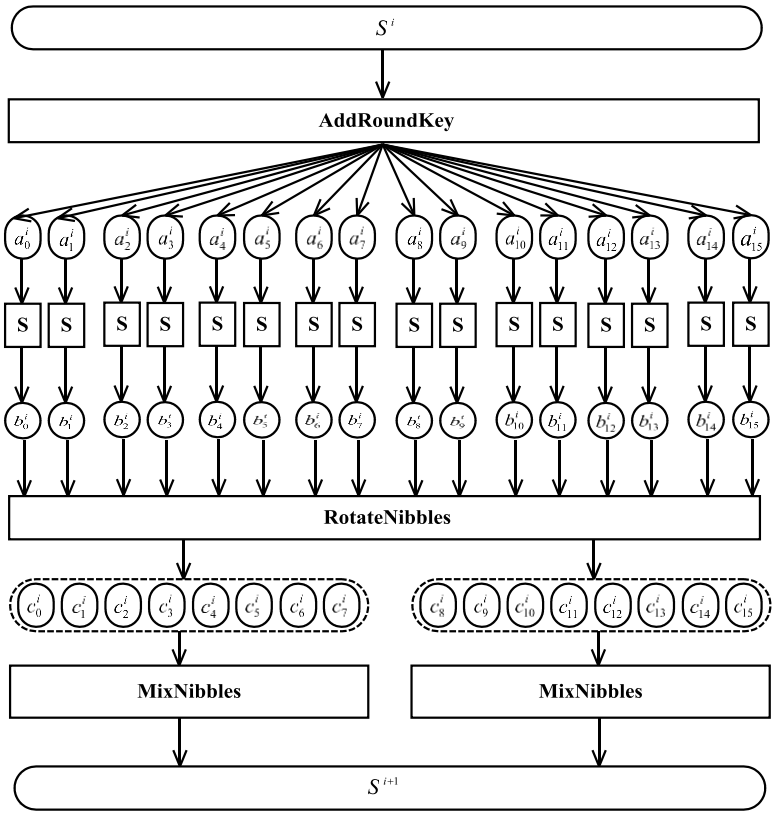



**Figure 1. One Round of the Encryption Process of KLEIN**

1. SubNibbles Step

In the SubNibbles step, the XORed results will be divided into 16 of 4-bit nibbles and input to the same 16 S-boxes. The KLEIN *S-box S* is a $4 \times 4$ involutive permutation described in table 1.

**Table 1. 4-Bit S-Box Used in KLEIN**

| Input | 0 1 2 3 4 5 6 7 8 9 A B C D E F |
|---|---|
| Output | 7 4 A 9 1 F B 0 C 3 2 6 8 E D 5 |

2. RotateNibbles Step

After the SubNibbles step, 16 nibbles $b_0^i, b_1^i, ..., b_{15}^i$ will be rotated left two bytes during the *i*-th round where $i \in [1, NR]$.

3. MixNibbles Step

The *i*-th round input nibbles $c_0^i, c_1^i, ..., c_{15}^i$ will be divided into 2 tuples, The tuples of the state are considered as polynomials over $F_2^8$ and multiplied modulo $x^4+1$ with a fixed polynomial , described in equation 1.

Where $s_0^i, s_1^i, ..., s_{15}^i$ is the output of the MixNibbles step.

$$\begin{bmatrix} s_0^{i+1} \| s_1^{i+1} \\ s_2^{i+1} \| s_3^{i+1} \\ s_4^{i+1} \| s_5^{i+1} \\ s_6^{i+1} \| s_7^{i+1} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} c_0^i \| c_1^i \\ c_2^i \| c_3^i \\ c_4^i \| c_5^i \\ c_6^i \| c_7^i \end{bmatrix}, \begin{bmatrix} s_8^{i+1} \| s_9^{i+1} \\ s_{10}^{i+1} \| s_{11}^{i+1} \\ s_{12}^{i+1} \| s_{13}^{i+1} \\ s_{14}^{i+1} \| s_{15}^{i+1} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} c_8^i \| c_9^i \\ c_{10}^i \| c_{11}^i \\ c_{12}^i \| c_{13}^i \\ c_{14}^i \| c_{15}^i \end{bmatrix} \quad (1)$$

## 2.2. Power Analysis Attacks against KLEIN

It has been conclusively proven that unprotected cryptographic implementations are vulnerable to side-channel attacks. This subsection demonstrates first-order Power Analysis Attacks against unprotected KLEIN [20].

When designing a DPA/CPA attack against a new cryptographic algorithm, there are several aspects that have to be considered: power leakage model, selection functions *D*(*C*,*K*) and statistical methods.

1) Selection Functions

We found that the Hamming-weight of S-box input can be utilized to reveal the secret key in our experiments. At the first round, the power consumption of KLEIN *S-box* is

$$P(t) = \varepsilon \cdot HW(S-box\_IN) + L = \varepsilon \cdot HW(P \oplus sk^1) + L \quad (2)$$

Therefore $D(P \oplus sk^1) = P \oplus sk^1$ is our selection function.

2) Statistical Methods

Statistical methods are used to compare hypothetical power consumption with power traces to reveal the secret key. There exist many statistical methods, mono-bit DPA, multi-bit DPA, CPA and PPA *etc*.

a) Messerges' multi-bit DPA[5]

Messerges' multi-bit DPA can be expressed in equation (3), where $T_i$ is the power consumption of plaintext $P_i$, $C_i$ is partial plaintext $P_i$, and $K_s$ is partial key hypothesis. $\Delta_s(b)$ is called DPA trace, representing the difference between the mean powers for selection function $D(C_i, K_s) < d/2$ and selection function $D(C_i, K_s) \geq d/2$ respective. In theory, if the key hypothesis $K_s$ is correct, $\Delta_s(b) \neq 0$ at the instant when intermediate value is handled, which means that there will be a peak in the DPA trace. Otherwise, $\Delta_s(b)$ tends to be 0, and no obvious peak appears. At other instants when intermediate value is not handled, $\Delta_s(b)$ tends to be 0 too .We are therefore able to distinguish correct key from other wrong key hypothesis.

$$\begin{aligned} G_0 &= \{T_i, i \in 1,2,\ldots,N \mid HW(D(C_i, K_s)) < d/2\} \\ G_1 &= \{T_i, i \in 1,2,\ldots,N \mid HW(D(C_i, K_s)) \geq d/2\} \\ \Delta_s(b) &= \frac{\sum_{G_{1,s}} T_i}{|G_{1,s}|} - \frac{\sum_{G_{0,s}} T_i}{|G_{0,s}|} \end{aligned} \quad (3)$$

b) Correlation Power Analysis (CPA) [7]

Correlation Power Analysis is considered to be the most powerful methods, which exploits the Pearson correlation coefficient to measure the linear correlation between power consumption of the device and hypothetical power consumption. The correlation coefficients are computed by equation 4, where *T* is a vector with composition *i* equal to $T_i$, *H* is a vector with composition *i* equal to $HW(D(C_i, K_s))$. $\sigma_{TH}$ ranges from -1 to +1, and if the key hypothesis $K_s$ is correct, $\sigma_{TH}$ tends to ±1 at the instant when intermediate value is handled, which means that there will be a peak in the CPA trace. Otherwise, $\sigma_{TH}$ tends to be 0, and no obvious peak appears. At other instants when intermediate value is

not handled, $\sigma_{TH}$ tends to be 0 too .We are therefore able to distinguish correct key from other wrong key hypothesis.

$$\sigma_{TH} = \frac{\mathrm{cov}(T,H)}{\sigma_T \sigma_H} = \frac{E(TH) - E(T)\cdot E(H)}{\sigma_T \sigma_H} = \frac{\sum_{i=0}^{n-1}(T_i - E(T))(H_i - E(H))}{\sqrt{\sum_{i=0}^{n-1}(T_i - E(T))^2}\sqrt{\sum_{i=0}^{n-1}(H_i - E(H))^2}} \quad (4)$$

The CPA attack against unprotected KLEIN is described by Algorithm CPA below.

**Algorithm CPA**

**1) for** key guess k = 0 : $2^s$-1

/* Calculate hypothetical power consumption with key guess *k* and known plaintexts *p*[1,...,*N*] */

$hw[k,:] = HW(p[:] \oplus k)$;

**2) for** *i* = 0 : *sp*-1

/* Compare the Pearson correlations(Equ 4) between hypothetical power Consumption matrix and measurement matrix for each candidate key *k* and all possible sample positions */

*cortmp*(*i*) = *corrcoef*(*hw*[*k*,:],measurement[:,*i*]);

**end** 2);

*cor*(*k*) = *max*(cortmp);

**end** 1);

candidate *key* = *indexofmax*(*cor*);

### 2.3. Experimental Results of DPA and CPA against Unprotected KLEIN

Figure 2(a) demonstrates the result of DPA attack against unprotected KLEIN, where the black DPA trace corresponds to the correct key hypothesis, while the other gray traces correspond to the wrong key hypotheses. It is obvious that after approximately 1400 plaintexts, one byte of correct key guess is distinguished from a wrong guess.

Result of CPA attack against unprotected KLEIN is much better than that of DPA. As shown in Figure 2(b), after approximately 600 plaintexts, one byte of correct key guess is distinguished from a wrong guess. Therefore CPA attack is successful after about 600 plaintexts, much less than that of DPA.

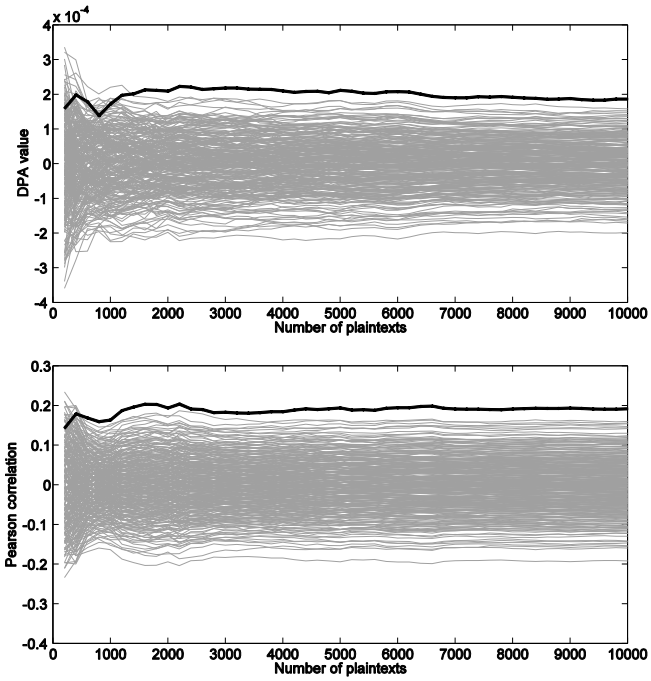



**Figure 2. Results of DPA and CPA Attacks against Unprotected KLEIN, Black Trace for Correct Key Hypothesis and Gray Traces for Wrong Key Hypotheses**

Figure 3 shows the success rates of DPA and CPA, along with the increasing number of Plaintexts. Black trace corresponds to correct key hypothesis and gray traces correspond to wrong key hypotheses.

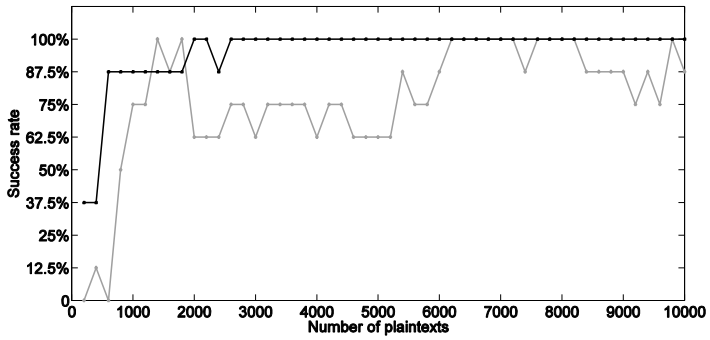



**Figure 3. Success Rates of DPA (Gray) and CPA (Black) Attacks against KLEIN-64**

## 3. An Ultra-Lightweight Side-Channel Resistant Crypto for Pervasive Devices

Unprotected KLEIN is vulnerable to side-channel attacks, as shown in section 2. A side-channel countermeasure of KLEIN is required when put into practice. Since pervasive devices are resource-constrained, power, energy, and area requirements of algorithms must be kept to a minimum, the DPA countermeasure of KLEIN must be smaller than 3,000GE or 5,000GE. Therefore an ultra-lightweight first-order side-channel resistant masked KLEIN is designed for pervasive devices, which masks *S-box* to randomize the intermediate values at the algorithm level.

To randomize the intermediate values, the plaintext *P* is masked by a random value *M* at the beginning of the algorithm, and at the end of the algorithm the mask must be removed to reestablish the expected value of cipher. Thus the implementation of KLEIN must be changed to meet this requirement. The only non-linear operation of KLEIN is SubNibbles *S-box*: $S-box(x \oplus y) \neq S-box(x) \oplus S-box(y)$ . Consequently, to construct the masking scheme, the most important consideration has been to mask the *S-box* operation. *S-box* should be rewritten for the masking countermeasures. For the purpose of ultra-lightweight, pre-computed look-up table *MS-box* is designed in such way that $MS-box(A \oplus M, M) = S-box(A) \oplus M$ , where $A$ is intermediate value $p \oplus k$ , $M$ is the random mask. Figure 4 illustrates this low-cost precomputed table for masked *S-box*. *S-box* will be rewritten from $4 \times 4$ *S-box* to $8 \times 4$ *MS-box*, as shown in table 2, where *x* and *y* are input and output of *MS-box* respectively.

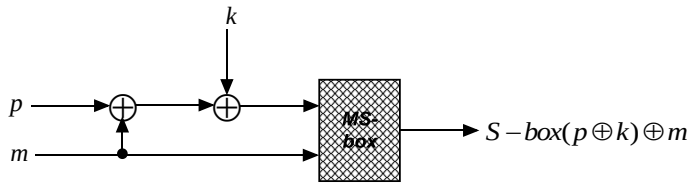



**Figure 4. Masked S-Box as Pre-Computed Look-Up Table**

Figure 5 describes one round of the encryption process of our proposed masked KLEIN, using the masked *S-box* shown in Figure 4 and Table 2.

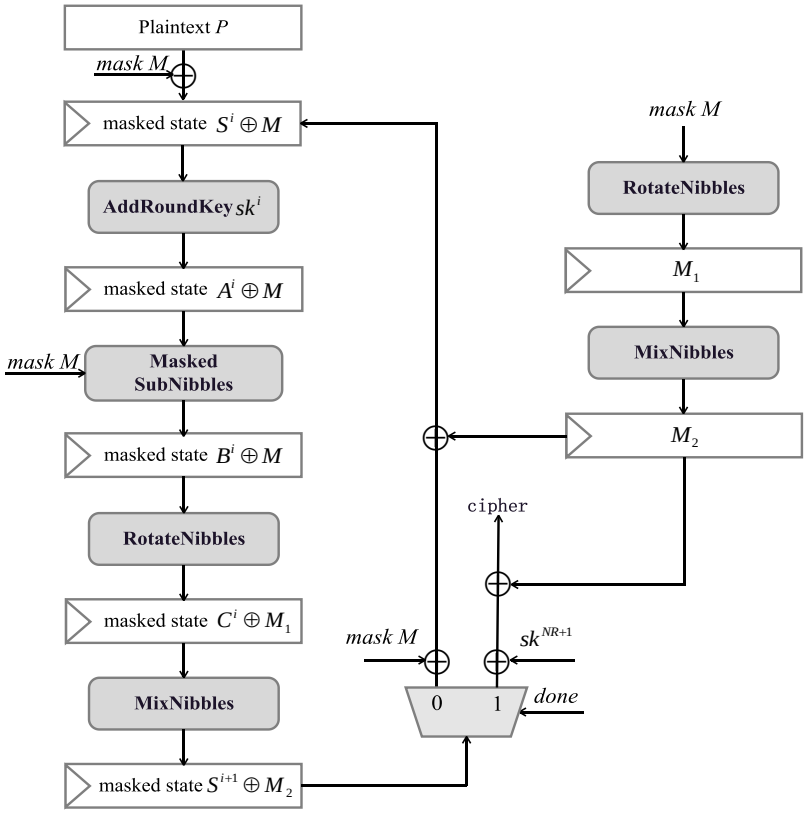



**Figure 5. One Round of the Encryption Process of Proposed Masked KLEIN**

**Table 2.** $8 \times 4$ ***MS-Box*** **Used in Proposed Masked KLEIN**

| x | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| y | 7 | 5 | 8 | A | 5 | A | D | 7 | 4 | A | 8 | D | 4 | 3 | 3 | A |
| x | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 1A | 1B | 1C | 1D | 1E | 1F |
| y | 4 | 6 | B | 9 | B | 4 | 6 | C | B | 5 | C | 9 | 2 | 5 | B | 2 |
| x | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 2A | 2B | 2C | 2D | 2E | 2F |
| y | A | 8 | 5 | 7 | F | 5 | 7 | 8 | A | F | 6 | 8 | 1 | 8 | 6 | 1 |
| x | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 3A | 3B | 3C | 3D | 3E | 3F |
| y | 9 | B | 6 | 4 | 4 | E | 9 | 6 | E | B | 9 | 7 | 9 | 0 | 0 | 7 |
| x | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 4A | 4B | 4C | 4D | 4E | 4F |
| y | 1 | E | 9 | 3 | 3 | 1 | C | E | 0 | 7 | 7 | E | 0 | E | C | 9 |
| x | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 5A | 5B | 5C | 5D | 5E | 5F |
| y | F | 0 | 2 | 8 | 0 | 2 | F | D | 6 | 1 | F | 6 | F | 1 | 8 | D |
| x | 60 | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 6A | 6B | 6C | 6D | 6E | 6F |
| y | B | 1 | 3 | C | E | C | 1 | 3 | 5 | C | 2 | 5 | E | B | 2 | C |
| x | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 7A | 7B | 7C | 7D | 7E | 7F |
| y | 0 | A | D | 2 | D | F | 2 | 0 | D | 4 | 4 | 3 | A | F | D | 3 |
| x | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 8A | 8B | 8C | 8D | 8E | 8F |
| y | C | 2 | 0 | 5 | C | B | B | 2 | F | D | 0 | 2 | D | 2 | 5 | F |
| x | 90 | 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 9A | 9B | 9C | 9D | 9E | 9F |
| y | 3 | D | 4 | 1 | A | D | 3 | A | C | E | 3 | 1 | 3 | C | E | 4 |
| x | A0 | A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 | A9 | AA | AB | AC | AD | AE | AF |
| y | 2 | 7 | E | 0 | 9 | 0 | E | 9 | 2 | 0 | D | F | 7 | D | F | 0 |
| x | B0 | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | BA | BB | BC | BD | BE | BF |
| y | 6 | 3 | 1 | F | 1 | 8 | 8 | F | 1 | 3 | E | C | C | 6 | 1 | E |
| x | C0 | C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | C9 | CA | CB | CC | CD | CE | CF |
| y | 8 | F | F | 6 | 8 | 6 | 4 | 1 | 9 | 6 | 1 | B | B | 9 | 4 | 6 |
| x | D0 | D1 | D2 | D3 | D4 | D5 | D6 | D7 | D8 | D9 | DA | DB | DC | DD | DE | DF |
| y | E | 9 | 7 | E | 7 | 9 | 0 | 5 | 7 | 8 | A | 0 | 8 | A | 7 | 5 |
| x | E0 | E1 | E2 | E3 | E4 | E5 | E6 | E7 | E8 | E9 | EA | EB | EC | ED | EE | EF |
| y | D | 4 | A | D | 6 | 3 | A | 4 | 3 | 9 | B | 4 | 6 | 4 | 9 | B |
| x | F0 | F1 | F2 | F3 | F4 | F5 | F6 | F7 | F8 | F9 | FA | FB | FC | FD | FE | FF |
| y | 5 | C | C | B | 2 | 7 | 5 | B | 8 | 2 | 5 | A | 5 | 7 | A | 8 |

One round of the encryption process of proposed masked KLEIN-64 is described as follows:

1. The Initial Step. At the beginning of algorithm, a random 64-bit mask *M* is generated inside the device, and XORed with plaintext *P* as masked plaintext, which is stored into state register *S*.

2. The AddRoundKey Step. Since operation of AddRoundKey is a linear function, it holds that $S^i \oplus M \oplus sk^i = (S^i \oplus sk^i) \oplus M = A^i \oplus M$ , where $A^i = \{a_0^i, a_1^i, ..., a_{15}^i\}$ in Figure 1, and $sk^i$ is the *i*-th round key.

3. The Masked SubNibbles Step. According to the definition of *MS-box*, $MS-box(A^i \oplus M, M) = S-box(A^i) \oplus M = B^i \oplus M$ , where $B^i = \{b_0^i, b_1^i, ..., b_{15}^i\}$ in Figure 1.

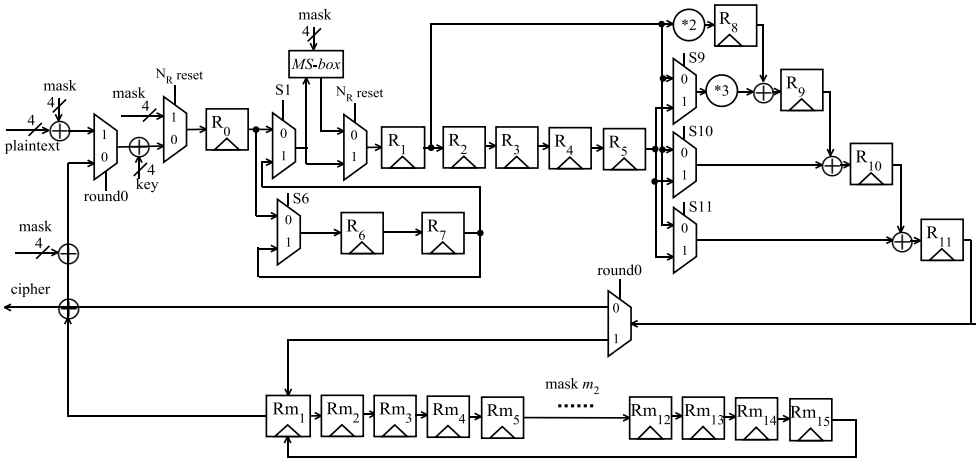
4. The RotateNibbles Step. Since operation of RotateNibbles is a linear function, it holds that $\mathrm{RotateNibbles}(B^i \oplus M) = \mathrm{RotateNibbles}(B^i) \oplus \mathrm{RotateNibbles}(M) = C^i \oplus M_1$ , where $C^i = \{c_0^i, c_1^i, ..., c_{15}^i\}$ in Figure 1, and $M_1$ = RotateNibbles(*M*).

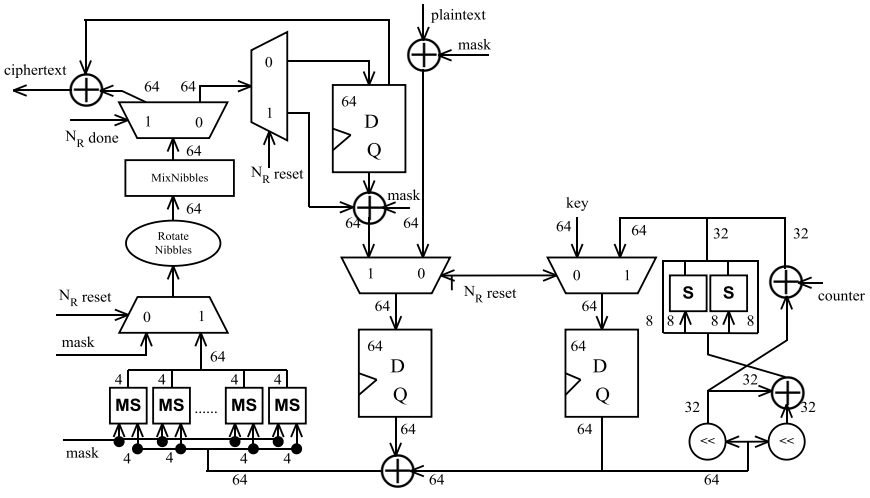
5. The MixNibbles Step. Since operation of MixNibbles is a linear function, it holds that $\mathrm{MixNibbles}(C^i \oplus M_1) = \mathrm{MixNibbles}(C^i) \oplus \mathrm{MixNibbles}(M_1) = S^{i+1} \oplus M_2$, where $M_2$ = MixNibbles($M_1$) = MixNibbles(RotateNibbles($M$)).

6. The Testing Step. If it is the last round, mask state $S^{NR+1} \oplus M_2$ will be XORed with last round key $sk^{NR+1}$, and XORed with $M_2$ afterwards to reestablish the cipher $S^{NR+1} \oplus sk^{NR+1}$. Otherwise, mask state $S^{NR+1} \oplus M_2$ will be XORed with $M_2$ and $M$ to maintain masked state $S^{i+1} \oplus M$ for next round of encryption.

Note that our proposed masked KLEIN-64 above makes it possible for the $M_2$ to be precomputed only once at the beginning of encryption, which requires as less resources as possible.




(a) 4-Bit Datapath Serial Circuit Design of Masked KLEIN-64




(b) 64-Bit Datapath Parallel Circuit Design of Masked KLEIN-64

**Figure 6. Parallel and Serial Circuit Designs of Masked KLEIN-64**

Parallel and serial circuit designs of our proposed masked KLEIN are illustrates in Figure 6. Hardware version of masked KLEIN require only an additional RNG (Random Number Generator) to generate mask $M$. RotateNibbles and MixNibbles circuit can be reused to compute $M_2$. As demonstrated in Figure 6(a) and 6(b), using the signal of *NRreset*, masked KLEIN computes $M_2$ in the initial cycle(the first cycle), therefore

parallel implementation of our masked KLEIN only requires the same cycles as unprotected KLEIN, while serial implementation require 16 additional cycles. A 64-bit register is needed to store $M_2$.

FPGA resources required by the unprotected KLEIN and masked KLEIN implementations are listed in table 3. The resource required by *MS-box* is 66GE, twice than the resource required by S-box. Parallel masked KLEIN-64 requires 1.66 times the area of the unprotected one. Meanwhile, serial masked KLEIN-64 requires 1.61 times the area and 1.44 times the time of the unprotected one.

**Table 3. Resources Required in KLEIN and Masked KLEIN**

| Algorithm | Area(GE) | Cycles per block | Nanoseconds per cycle |
|---|---|---|---|
| *S-box* | 30 | 1 | 8 |
| *MS-box* | 66 | 1 | 8 |
| Serial Klein-64 | 1306 | 209 | 12 |
| Serial Masked Klein-64 | 2102 | 225 | 16 |
| Parallel KLEIN-64 | 2680 | 13 | 20 |
| Parallel Masked KLEIN-64 | 4451 | 13 | 20 |

## 4. SCA Security of Our Masked KLEIN

In order to evaluate the security of our proposed masked KLEIN under Power Analysis Attack, DPA and CPA Algorithms described in section 2.2 will be performed once again. We carefully simulated the deterministic power consumptions in Synopsys Primepower using dedicated power simulation libraries. PrimePower is a dynamic, full-chip power analysis tool for complex multimillion-gate designs. Its high-capacity power analysis includes gate-level average and peak power verification. PrimePower supports industry-standard synthesis libraries and comprises a powerful and flexible methodology that is fully integrated with existing design flows. It provides a high degree of accuracy, performance, ease of use and comprehensive power diagnostics. The synthesis library used is TSMC 0.18 $\mu m$ Process 1.8-Volt SAGE-X Standard Cell Library, which appears in many published papers.

### 4.1. First-Order SCA Security

*MS-box* is implemented as a pre-computed lookup table with 8 bits of input(4 bits of mask *m* and 4 bits of masked intermediate data $p \oplus k \oplus m$ ), and 4 bits of output equal to $S-box(p \oplus k) \oplus m$ . Power consumption of *MS-box* depends on the mask *m* and the masked data $p \oplus k \oplus m$ that it processes. According to the Hamming-weight power model, power consumption of *MS-box* $P_{MS-box} = \varepsilon \cdot (HW(m) + HW(p \oplus k \oplus m)) + L$ . Since random value *m* is unknown, an adversary is unable to predict the power consumption of the *MS-box*, and therefore cannot reveal the secret key through the power analysis attack described in section 2.2. It has been demonstrated in Figure 7, which illustrates the results of First-order DPA and CPA attacks against *MS-box*, using a large number of 1,000,000 power traces.

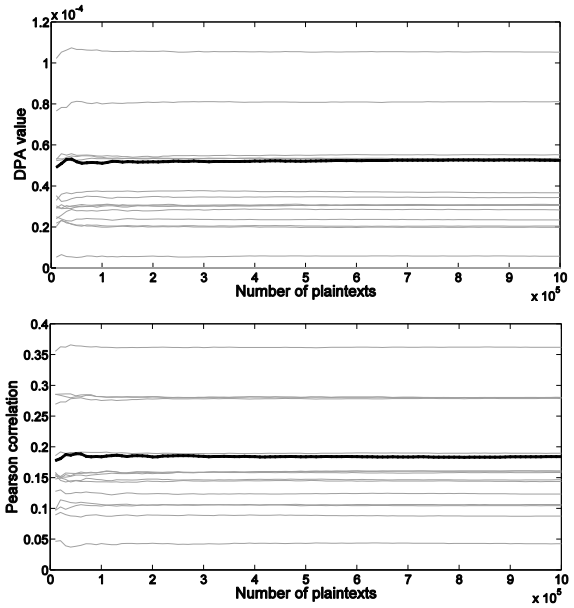
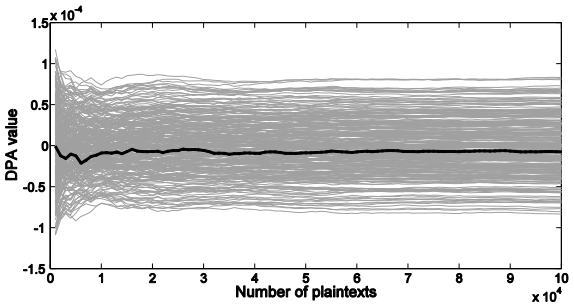



**Figure 7. First-Order DPA and CPA Attacks against Masked S-Box, Black Trace for Correct Key Hypothesis and Gray Traces for Wrong Key Hypotheses**

Figure 8(a) demonstrates the result of first-order DPA against our proposed masked KLEIN, where the black trace corresponds to the correct key hypothesis, while the other gray traces correspond to the wrong key hypotheses. Although the number of plaintexts has increased to 100,000 and even much more, the black trace cannot be distinguished from gray traces. Thus an adversary cannot reveal secret key by first-order DPA attack any more. Figure 8(b) illustrates the result of first-order CPA against our proposed masked KLEIN, which is the same result as that of DPA. Along with 100,000 plaintexts and even much more, first-order DPA and CPA attacks cannot reveal even one byte of secret key.



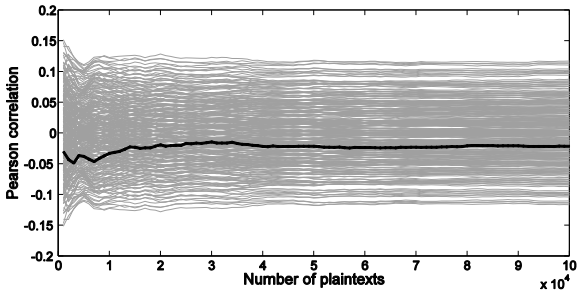



**Figure 8. First-Order DPA and CPA Attacks against Masked KLEIN. Black Trace for Correct Key Hypothesis and Gray Traces for Wrong Key Hypotheses**

### 4.2. High-Order SCA Security

Although our proposed masked KLEIN is secure under First-order Power Analysis Attack, it is still vulnerable to high-order side-channel attacks.

To simplify our discussion, we take into account only the single bit of input of *MS-box*. Table 4 shows the power consumptions of *MS-box* with different input of *p*, *k* and *m*.

**Table 4. Power Consumption of *MS-Box***

| $p \oplus k$ | $m$ | $p \oplus k \oplus m$ | $P(MS-box(m, p \oplus k \oplus m))$ | $Mean(P)$ | $Mean(P^2)$ |
|---|---|---|---|---|---|
| 0 | 0 | 0 | $2P_0$ | $P_0+P_1$ | $2P_0^2 + 2P_1^2$ |
| 0 | 1 | 1 | $2P_1$ | | |
| 1 | 0 | 1 | $P_0+P_1$ | $P_0+P_1$ | $(P_0 + P_1)^2$ |
| 1 | 1 | 0 | $P_0+P_1$ | | |

As shown in column 5 of Table 4, a first-order Power Analysis Attack is infeasible because the power consumptions are nothing different in the case of $p \oplus k = 0$ and $p \oplus k = 1$. However, quadratic mean of power consumptions in column 6 are obviously dependent on value of $p \oplus k$. In other words, if there are two power consumptions $P^{(1)}$, $P^{(2)}$ with $p \oplus k = 0$, the mask $m_1$ of $P^{(1)}$ is 0, meanwhile the mask $m_2$ of $P^{(2)}$ is 1, we have $(P^{(1)} + P^{(2)})^2 / 2 = P(p \oplus k = 0)^2 / 2 = 2(P_0^2 + P_1^2)$.

Further more, if there are *n*(*n* is even) power traces $P^{(1)}$,..., $P^{(n)}$ of $p \oplus k = 0$, with one half of *m* equal to 0, the other half of *m* equal to 1, we have $P(p \oplus k = 0)^2 / n = 2(P_0^2 + P_1^2)$. Meanwhile if there are *n*(*n* is even) power traces $P^{(1)}$,..., $P^{(n)}$ with $p \oplus k = 1$, and one half of *m* are equal to 0, while the other half of *m* are equal to 1, we have $P(p \oplus k = 1)^2 / n = 2(P_0 + P_1)^2$.

In conclusion, quadratic means of power consumptions of single bit *MS-box* are different and dependent on the value of $p \oplus k$. When considering an 8 bits *MS-box*, quadratic means of power consumptions are dependent on the number of bits of $p \oplus k = 1$ equal to 0 or 1.

A Second-order Power Analysis Attack [22] utilizing quadratic means of power traces is performed to reveal the secret key. The experimental result of Second-order Power Analysis Attack is shown in Figure 9, when $n \geq 1,000$ (*n* is the number of power traces), second-order power analysis attack correctly reveals a 4 bits secret key, which means that

at least $n \times 16 = 16,000$ power traces are required by Second-order Power Analysis Attack.

Therefore a Second-order Power Analysis Attack utilizing quadratic means of power traces is feasible to reveal the secret key of our proposed masked KLEIN, however with an exponential increase of the SCA data complexity.

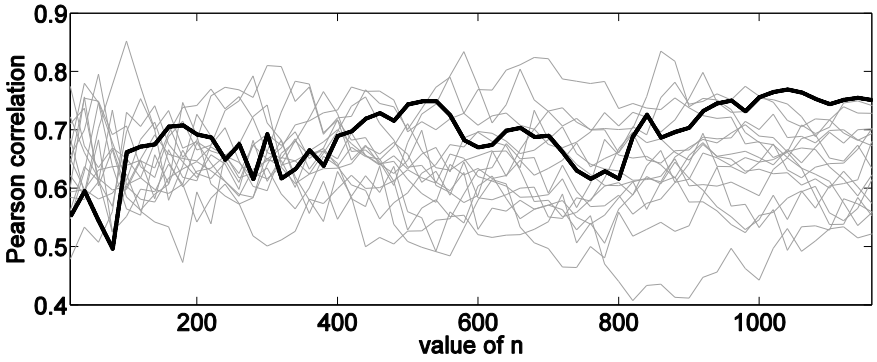



**Figure 9. Second-Order Attack against Our Proposed Masked KLEIN, Black Trace for Correct Key Hypothesis and Gray Traces for Wrong Key Hypotheses**

## 5. Conclusion

KLEIN is a new family of lightweight block cipher that has advantages in both software and hardware performances. To meet the requirement of limited resources, implementations of lightweight ciphers are much briefer and serialized. Even worse, pervasive devices are deployed in a hostile environment, *i.e.*, an adversary has physical access to or control over the devices, which poses a serious practical threat to these security components. Precomputation look-up table based masking countermeasure is low-cost and secure against first-order DPA, therefore is more suitable for lightweight ciphers in resource-constrained devices. Based on precomputation look-up table, we propose an ultra-lightweight masked KLEIN: the serial implementation of masked KLEIN requires 2102GE, and parallel implementation requires 4451GE, which makes these implementations suitable for resource-constrained pervasive devices. Experimental results show that our proposed masked KLEIN is secure under first-order DPA and CPA attacks. Second-order power analysis attack is feasible to reveal the secret key of our masked KLEIN, but with an exponential increase of the SCA data complexity.

## References

[1] Z. Gong, S. Nikova and Y. W. Law, "Klein: A new family of lightweight block ciphers. In RFID. Security and Privacy", of Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 7055, **(2012)**, pp. 1-18
[2] A. Moradi and A. Poschmann, "Lightweight cryptography and DPA countermeasures: a survey", Financial Cryptography and Data Security, **(2010)**, pp. 68-79.
[3] A. Poschmann, A. Moradi, K. Khoo, C. W. Lim, H. Wang and S. Ling, "Side-channel resistant crypto for less than 2,300 GE", Journal of cryptology, vol. 24, no. 2, **(2011)**, pp. 322-345.
[4] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis", In Advances in Cryptology CRYPTO 99, Springer, **(1999)**, pp. 789-789.
[5] T. S. Messerges, E. A. Dabbish and R. H. Sloan, "Investigations of power analysis attacks on smartcards", In USENIX workshop on Smartcard Technology, **(1999)**.
[6] T. S. Messerges, Dabbish and E. A., "Examining smart-card security under the threat of power analysis attacks", Computers, IEEE Transactions on, vol. 51, no. 5, **(2002)**, pp. 541-552.
[7] E. Brier, C. Clavier and F. Olivier, "Correlation power analysis with a leakage model", Cryptographic Hardware and Embedded Systems-CHES 2004, **(2004)**, pp. 135-152.

[8] M. Tunstall, N. Hanley, R. McEvoy, C. Whelan, C. C. Murphy, W. P. Marnane and I. Cork, "Correlation power analysis of large word sizes", In IET Irish Signals and Systems Conference (ISSC), **(2007)**.
[9] S. Aumonier, "Generalized correlation power analysis", In Proceedings of the Encrypt Workshop Tools for Cryptanalysis, **(2007)**.
[10] F. X. Standaert, S. B. Ors and B. Preneel, "Power analysis of an FPGA. Implementation of Rijndael: Is pipelining a DPA countermeasure? In Cryptographic Hardware and Embedded Systems - CHES 2004", of Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 3156, **(2004)**, pp. 30-44.
[11] C. Clavier, J. S. Coron and N. Dabbous, "Differential power analysis in the presence of hardware countermeasures", In Cryptographic Hardware and Embedded Systems-CHES 2000, Springer, **(2000)**, pp. 13-48.
[12] S. Mangard, "Hardware countermeasures against DPA-a statistical analysis of their effectiveness", Topics in Cryptology-CT-RSA 2004, **(2004)**, pp. 1998-1998.
[13] M. L. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks", In Cryptographic Hardware and Embedded Systems, CHES 2001, Springer, **(2001)**, pp. 309-318.
[14] M. L. Akkar and L. Goubin, "A generic protection against high-order differential power analysis", In Fast Software Encryption, Springer, **(2003)**, pp. 192-205.
[15] E. Oswald, S. Mangard, N. Pramstaller and V. Rijmen, "A side-channel analysis resistant description of the AES S-box", In Fast Software Encryption, Springer, **(2005)**, pp. 199-228.
[16] M. Rivain and E. Prouff, "Provably secure higher-order masking of AES", Cryptographic Hardware and Embedded Systems, CHES 2010, **(2010)**, pp. 413-427.
[17] H. S. Kim, S. Hong and J. Lim, "A fast and provably secure higher-order masking of AES S-box", Cryptographic Hardware and Embedded Systems-CHES 2011, **(2011)**, pp. 95-107.
[18] T. S. Messerges, "Securing the AES finalists against power analysis attacks", In Fast Software Encryption, of Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 1978, **(2001)**, pp. 150-164.
[19] E. Prouff and M. Rivain, "A generic method for secure SBox implementation", In Sehun Kim, Moti Yung, and Hyung-Woo Lee, editors, Information Security Applications, of Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 4867, **(2007)**, pp. 227-244.
[20] W. Li, S. Tang and Z. Gong, "Power Analysis Attacks against Hardware Implementation of KLEIN", Journal of Computational Information Systems, vol. 10, no. 8, **(2014)**, pp. 3171-3179.
[21] S. Mangard, E. Oswald and T. Popp, "Power analysis attacks: Revealing the secrets of smart cards", Springer, vol. 31, **(2007)**.
[22] F. X. Standaert, E. Peeters and J. J. Quisquater, "On the masking countermeasure and higher-order power analysis attacks", In Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on, IEEE, vol. 1, **(2005)**, pp. 562-567.