Provably Secure Higher-Order Masking of AES

Matthieu Rivain[1] and Emmanuel Prouff[2]

[1] CryptoExperts
matthieu.rivain@cryptoexperts.com
[2] Oberthur Technologies
e.prouff@oberthur.com

Abstract. Implementations of cryptographic algorithms are vulnerable to Side Channel Analysis (SCA). To counteract it, masking schemes are usually involved which randomize key-dependent data by the addition of one or several random value(s) (the *masks*). When dth-order masking is involved (*i.e.* when d masks are used per key-dependent variable), the complexity of performing an SCA grows exponentially with the order d. The design of generic dth-order masking schemes taking the order d as security parameter is therefore of great interest for the physical security of cryptographic implementations. This paper presents the first generic dth-order masking scheme for AES with a provable security and a reasonable software implementation overhead. Our scheme is based on the hardware-oriented masking scheme published by Ishai *et al.* at Crypto 2003. Compared to this scheme, our solution can be efficiently implemented in software on any general-purpose processor. This result is of importance considering the lack of solution for $d \geqslant 3$.

1 Introduction

Side Channel Analysis exploits information that leaks from physical implementations of cryptographic algorithms. This leakage (*e.g.* the power consumption or the electro-magnetic emanations) may indeed reveal information on the data manipulated by the implementation. Some of these data are *sensitive* in the sense that they are related to the secret key, and the leaking information about them enables efficient key-recovery attacks [7, 18].

Due to the very large variety of side channel attacks reported against cryptosystems and devices, important efforts have been done to design countermeasures with provable security. They all start from the assumption that a cryptographic device can keep at least some secrets and that only computation leaks [24]. Based on these assumptions, two main approaches have been followed. The first one consists in designing new cryptographic primitives inherently resistant to side channel attacks. In [24], a very powerful side channel adversary is considered who has access to the whole internal state of the ongoing computation. In such a model, the authors show that if a *physical* one-way permutation exists which does not leak any information, then it can be used in the pseudo-random number generator (PRNG) construction proposed in [4] to give a PRNG provably secure against the aforementioned side channel adversary. Unfortunately,

S. Mangard and F.-X. Standaert (Eds.): CHES 2010, LNCS 6225, pp. 413–427, 2010.

no such leakage-resilient one-way permutation is known at this day. Besides, the obtained construction is quite inefficient since each computation of the one-way permutation produces one single random bit. To get more practical constructions, further works focused on designing primitives secure against a *limited* side channel adversary [13]. The definition of such a limited adversary is inspired by the *bounded retrieval model* [10, 21] which assumes that the device leaks a limited amount of information about its internal state for each elementary computation. In such a setting, the block cipher based PRNG construction proposed in [29] is provably secure assuming that the underlying cipher is *ideal*. Other constructions were proposed in [13, 30] which do not require such a strong assumption but are less efficient [39]. The main limitations of these constructions is that they do not enable the choice of an initialization vector (otherwise the security proofs do not hold anymore) which prevents their use for encryption with synchronization constraints or for challenge-response protocols [39]. Moreover, as they consist in new constructions, these solutions do not allow for the protection of the implementation of standard algorithms such as DES or AES [14, 15].

The second approach to design countermeasures provably secure against side channel attacks consists in applying *secret sharing schemes* [2, 38]. In such schemes, the sensitive data is randomly split into several shares in such a way that a chosen number (called the *threshold*) of these shares is required to retrieve any information about the data. When the SCA threat appeared, secret sharing was quickly identified as a pertinent protection strategy [6, 16] and numerous schemes (often called *masking schemes*) were published that were based on this principle (see for instance [1, 3, 17, 22, 25, 28, 33, 37]). Actually, this approach is very close to the problem of defining Multi Party Communication (MPC) schemes (see for instance [9, 12]) but the resources and constraints differ in the two contexts (*e.g.* MPC schemes are often based on a *trusted dealer* who does not exist in the SCA context). A first advantage of this approach is that it can be used to secure standard algorithms such as DES and AES. A second advantage is that *dth-order masking schemes*, for which sensitive data are split into $d+1$ shares (the threshold being $d+1$), are sound countermeasures to SCA in *realistic leakage model*. This fact has been formally demonstrated by Chari *et al.* [6] who showed that the complexity of recovering information by SCA on a bit shared into several pieces grows exponentially with the number of shares. As a direct consequence of this work, the number of shares (or equivalently of masks) in which sensitive data are split is a sound security parameter of the resistance of a countermeasures against SCA.

The present paper deals with the problem of defining an efficient masking scheme to protect the implementation of the AES block cipher [11]. Until now, most of works published on this subject have focussed on first-order masking schemes where sensitive variables are masked with a single random value (see for instance [1, 3, 22, 25, 28]). However, this kind of masking have been shown to be efficiently breakable in practice by *second-order SCA* [23, 26, 41]. To counteract those attacks, *higher-order masking schemes* must be used but a very few have been proposed. A first method has been introduced by Ishai *et al.* [17] which

enables to protect an implementation at any chosen order. Unfortunately, it is not suited for software implementations and it induces a prohibitive overhead for hardware implementations. A scheme devoted to secure the software implementation of AES at any chosen order has been proposed by Schramm and Paar [37] but it was subsequently shown to be secure only in the second-order case [8]. Alternative second-order masking schemes with provable security were further proposed in [33], but no straightforward extension of them exist to get efficient and secure masking scheme at any order. Actually, at this day, no method exists in the literature that enables to mask an AES implementation at any chosen order $d \geqslant 3$ with a practical overhead; the present paper fills this gap.

2 Preliminaries on Higher-Order Masking

2.1 Basic Principle

When higher-order masking is involved to secure the physical implementation of a cryptographic algorithm, every sensitive variable x occurring during the computation is randomly split into $d+1$ shares $x_0, \ldots, x_d$ in such a way that the following relation is satisfied for a group operation $\perp$:

$$x_0 \perp x_1 \perp \cdots \perp x_d = x \ . \tag{1}$$

In the rest of the paper, we shall consider that $\perp$ is the exclusive-or (XOR) operation denoted by $\oplus$. Usually, the d shares $x_1, \ldots, x_d$ (called *the masks*) are randomly picked up and the last one x_0 (called *the masked variable*) is processed such that it satisfies (1). When d random masks are involved per sensitive variable the masking is said to be *of order d*.

Assuming that the masks are uniformly distributed, masking renders every intermediate variable of the computation statistically independent of any sensitive variable. As a result, classical side channel attacks exploiting the leakage related to a single intermediate variable are not possible anymore. However, a dth-order masking is always theoretically vulnerable to $(d+1)$*th-order SCA* which exploits the leakages related to $d+1$ intermediate variables at the same time [23, 36, 37]. Indeed, the leakages resulting from the $d+1$ shares (i.e. the masked variable and the d masks) are jointly dependent on the sensitive variable. Nevertheless, such attacks become impractical as d increases, which makes higher-order masking a sound countermeasure.

2.2 Soundness of Higher-Order Masking

The soundness of higher-order masking was formally demonstrated by Chari *et al.* in [6]. They assume a simplified but still realistic leakage model where a bit b is masked using d random bits $x_1, \ldots, x_d$ such that the masked bit is defined as $x_0 = b \oplus x_1 \oplus \cdots \oplus x_d$. The adversary is assumed to be provided with observations of $d+1$ leakage variables L_i, each one corresponding to a share x_i. For every i, the leakage is modelled as $L_i = x_i + N_i$ where the noises

N_i's are assumed to have Gaussian distributions $\mathcal{N}\left(\mu, \sigma^2\right)$ and to be mutually independent. Under this leakage model, they show that the number of samples q required by the adversary to distinguish the distribution $(L_0, \ldots, L_d | b = 0)$ from the distribution $(L_0, \ldots, L_d | b = 1)$ with a probability at least α satisfies:

$$q \geqslant \sigma^{d+\delta} \tag{2}$$

where $\delta = 4 \log \alpha / \log \sigma$. This result encompasses all the possible side-channel distinguishers and hence formally states the resistance against every kind of side channel attack. Although the model is simplified, it could probably be extended to more common leakage models such as the Hamming weight/distance model. The point is that if an attacker observes noisy side channel information about $d + 1$ shares corresponding to a variable masked with d random masks, the number of samples required to retrieve information about the unmasked variable is lower bounded by an exponential function of the masking order whose base is related to the noise standard deviation. This formally demonstrates that higher-order masking is a sound countermeasure especially when combined with noise. Many works also made this observation in practice for particular side channel distinguishers (see for instance [36, 37, 40]).

2.3 Higher-Order Masking Schemes

When dth-order masking is involved in protecting a block cipher implementation, a so-called *dth-order masking scheme* (or simply a *masking scheme* if there is no ambiguity on d) must be designed to enable computation on masked data. In order to be complete and secure, the scheme must satisfy the two following properties:

- *completeness*: at the end of the computation, the sum of the d shares must yield the expected ciphertext (and more generally each masked transformation must result in a set of shares whose sum equal the correct intermediate result),
- *dth-order SCA security*: every tuple of d or less intermediate variables must be independent of any sensitive variable.

If the dth-order security property is satisfied, then no attack of order lower than $d + 1$ is possible and we benefit from the security bound (2).

Most block cipher structures (*e.g.* AES or DES) alternate several rounds composed of a key addition, one or several linear transformation(s), and a non-linear transformation. The main difficulty in designing masking schemes for such block ciphers lies in masking the nonlinear transformations. Many solutions have been proposed to deal with this issue but the design of a dth-order secure scheme for $d > 1$ has quickly been recognized as a difficult problem by the community. As mentioned above, only three methods exist in the literature that have been respectively proposed by Ishai, Sahai and Wagner [17], by Schramm and Paar [37] (secure only for $d \leqslant 2$) and by Rivain, Dottax and Prouff [33] (dedicated to $d = 2$). Among them, only [17] can be applied to secure a non-linear transformation at any order d. This scheme is recalled in the next section.

2.4 The Ishai-Sahai-Wagner Scheme

In [17], Ishai *et al.* propose a higher-order masking scheme (referred to as ISW in this paper) enabling to secure the hardware implementation of any *circuit* at any chosen order d. They describe a way to transform the circuit to protect into a new circuit (dealing with masked values) such that no subset of d of its *wires* reveals information about the unmasked values[1]. For such a purpose, they assume without loss of generality that the circuit to protect is exclusively composed of NOT and AND gates. Securing a NOT for any order d is straightforward since $x = \bigoplus_i x_i$ implies $\mathrm{NOT}(x) = \mathrm{NOT}(x_0) \oplus x_1 \cdots \oplus x_d$. The main difficulty is therefore to secure the AND gates. To answer this issue, Ishai *et al.* suggest the following elegant solution.

Secure logical AND. Let a an b be two bits and let c denote $\mathrm{AND}(a, b) = ab$. Let us assume that a and b have been respectively split into $d+1$ shares $(a_i)_{0 \leqslant i \leqslant d}$ and $(b_i)_{0 \leqslant i \leqslant d}$ such that $\bigoplus_i a_i = a$ and $\bigoplus_i b_i = b$. To securely compute a $(d+1)$-tuple $(c_i)_{0 \leqslant i \leqslant d}$ s.t. $\bigoplus_i c_i = c$, Ishai *et al.* perform the following steps:

1. For every $0 \leqslant i < j \leqslant d$, pick up a random bit $r_{i,j}$.
2. For every $0 \leqslant i < j \leqslant d$, compute $r_{j,i} = (r_{i,j} \oplus a_i b_j) \oplus a_j b_i$.
3. For every $0 \leqslant i \leqslant d$, compute $c_i = a_i b_i \oplus \bigoplus_{j \neq i} r_{i,j}$.

Remark 1. The use of brackets indicates the order in which the operations are performed, which is mandatory for security of the scheme.

The completeness of the solution follows from:

$$\bigoplus_i c_i = \bigoplus_i \big(a_i b_i \oplus \bigoplus_{j \neq i} r_{i,j}\big) = \bigoplus_i \big(a_i b_i \oplus \bigoplus_{j>i} r_{i,j} \oplus \bigoplus_{j<i} (r_{j,i} \oplus a_i b_j \oplus a_j b_i)\big)$$
$$= \bigoplus_i \big(a_i b_i \oplus \bigoplus_{j<i} (a_i b_j \oplus a_j b_i)\big) = \big(\bigoplus_i a_i\big)\big(\bigoplus_i b_i\big) \ .$$

In [17] it is shown that the AND computation above is secure against any attack of order lower than or equal to $d/2$. As stated in Section 4 (and proven the full version of the paper [35]) this scheme is actually dth-order secure.

Practical issues. Although the ISW scheme is an important theoretical result, its practical application suffers few issues. Firstly, it induces an important overhead in silicon area for the masked circuit. Indeed, every single AND gate is encoded using $(d+1)^2$ AND gates plus $2d(d+1)$ XOR gates, and it requires the generation of $d(d+1)/2$ random bits at every clock cycle. As an illustration, masking the compact circuit for the AES S-box described in [5] would multiply its size (in terms of number of gates) by 7 for $d = 2$, by 14 for $d = 3$ and by 22 for $d = 4$ (without taking the random bits generation into account). Secondly,

[1] Considering wires as intermediate variables, this is equivalent to the security property given in Section 2.3.

masking at the hardware level is sensitive to glitches, which induces first-order flaws although in theory every internal wire carries values that are independent of the sensitive variables [19, 20]. Preventing glitches in masked circuits imply the addition of synchronizing elements (*e.g.* registers or latches) which still significantly increases the circuit size (see for instance [31]).

Since software implementations of masking schemes do not suffer area overhead and are not impacted by the presence of glitches at the hardware level, a straightforward approach to deal with the practical issues discussed above could be to implement the ISW scheme in software. Namely, we could represent each non-linear transformation S to protect by a tuple of Boolean functions $(f_i)_i$ usually called *coordinate functions* of S, and evaluate the f_i's with the ISW scheme by processing the AND and XOR operations with CPU instructions. However, this approach is not practical since the timing overhead would clearly be prohibitive. The present paper follows a different approach: we generalize the ISW scheme to secure any finite field multiplication rather than a simple multiplication over $\mathbb{F}_2$ (*i.e.* a logical AND). We apply this idea to design a secure higher-order masking scheme for the AES and we show that its software implementation induces a reasonable overhead.

3 Higher-Order Masking of AES

The AES block cipher iterates a round transformation composed of a key addition, a linear layer and a nonlinear layer which applies the same substitution-box (S-box) to every byte of the internal state. As previously explained, the main difficulty while designing a masking scheme for such a cipher is the masking of the nonlinear transformation, which in that case lies in the masking of the S-box. Our method for masking the AES S-box is presented in the next section.

In what follows, we shall consider that a random generator is available which on an invocation $\mathsf{rand}(n)$ returns n unbiased random bits.

3.1 Higher-Order Masking of the AES S-Box

The AES S-box S is defined as the right-composition of an affine transformation Af over $\mathbb{F}_2^8$ with the power function $x \mapsto x^{254}$ over the field $\mathbb{F}_{2^8} \equiv \mathbb{F}_2[x]/(x^8+x^4+x^3+x+1)$. Since the affine transformation is straightforward to mask, our scheme mainly consists in a method for masking the power function at any order d. Our solution consists in a secure computation of the exponentiation to the power 254 over $\mathbb{F}_{2^8}$. Such an approach has already been described by Blömer *et al.* for $d = 1$ [3]. The core idea is to apply an exponentiation algorithm (*e.g.* the square-and-multiply algorithm) on the first-order masked input while ensuring the mask correction step by step. Compared to Blömer *et al.* 's solution, our exponentiation algorithm is able to operate on dth-order masked inputs and it achieves dth-order SCA security for any value of d. To perform such a secure

exponentiation, we define hereafter some methods to securely compute a squaring and a multiplication over $\mathbb{F}_{2^8}$ at the dth order.

Masking the field squaring. Since we operate on a field of characteristic 2, the squaring is a linear operation and we have $x_0^2 \oplus x_1^2 \oplus \cdots \oplus x_d^2 = x^2$. Securely computing a squaring can hence be carried out by squaring every share separately. More generally, for every natural integer j, raising x to the power 2^j can be done securely by raising each x_i to the 2^j separately.

Masking the field multiplication. For the usual field multiplication we use the ISW scheme recalled in Section 2.4. Even if it has been described to securely compute a logical AND (that is a multiplication over $\mathbb{F}_2$), it can actually be transposed to secure a multiplication over any field of characteristic 2: variables over $\mathbb{F}_2$ are replaced by variables over $\mathbb{F}_{2^n}$, binary multiplications (*i.e.* ANDs) are replaced by multiplications over $\mathbb{F}_{2^n}$ and binary additions (*i.e.* XORs) are replaced by addition over $\mathbb{F}_{2^n}$ (that are n-bit XORs). This keep unchanged the completeness of the scheme recalled in Section 2.4. The whole secure multiplication over $\mathbb{F}_{2^n}$ is depicted in the following algorithm.

Algorithm 1. SecMult - dth-order secure multiplication over $\mathbb{F}_{2^n}$

INPUT: shares a_i satisfying $\bigoplus_i a_i = a$, shares b_i satisfying $\bigoplus_i b_i = b$
OUTPUT: shares c_i satisfying $\bigoplus_i c_i = ab$

1. **for** $i = 0$ **to** d **do**
2. **for** $j = i + 1$ **to** d **do**
3. $r_{i,j} \leftarrow \mathsf{rand}(n)$
4. $r_{j,i} \leftarrow (r_{i,j} \oplus a_i b_j) \oplus a_j b_i$
5. **for** $i = 0$ **to** d **do**
6. $c_i \leftarrow a_i b_i$
7. **for** $j = 0$ **to** d, $j \neq i$ **do** $c_i \leftarrow c_i \oplus r_{i,j}$

Masking the power function. Now we have a secure squaring and a secure multiplication over $\mathbb{F}_{2^8}$ it remains to specify an exponentiation algorithm. It is clear from Algorithm 1 that the running time of a secure multiplication is huge compared to that of a secure squaring. A secure squaring indeed requires $d + 1$ squarings while a secure multiplication requires $(d + 1)^2$ field multiplications, $2d(d + 1)$ XORs and the generation of $d(d + 1)/2$ random 8-bit values. Our goal is therefore to design an exponentiation algorithm using the least possible multiplications which are not squares. It can be checked that an exponentiation to the power 254 requires at least 4 such multiplications. The exponentiation algorithm presented hereafter achieves this lower bound and requires few additional squares. It involves three intermediate variables denoted y, z and w (note that x and y may be associated to the same memory address).

Algorithm 2. Exponentiation to the 254

INPUT: x
OUTPUT: $y = x^{254}$

1. $z \leftarrow x^2$ $[z = x^2]$
2. $y \leftarrow zx$ $[y = x^2 x = x^3]$
3. $w \leftarrow y^4$ $[w = (x^3)^4 = x^{12}]$
4. $y \leftarrow yw$ $[y = x^3 x^{12} = x^{15}]$
5. $y \leftarrow y^{16}$ $[y = (x^{15})^{16} = x^{240}]$
6. $y \leftarrow yw$ $[y = x^{240} x^{12} = x^{252}]$
7. $y \leftarrow yz$ $[y = x^{252} x^2 = x^{254}]$

As argued in the full version of this paper [35], for the dth-order security to hold, it is important that the masks $(a_i)_{i \geqslant 1}$ and $(b_i)_{i \geqslant 1}$ in input of the SecMult algorithm are mutually independent. That is why we shall refresh the masks at some points during the secure exponentiation by calling a procedure RefreshMasks[2]. The whole exponentiation to the power 254 over $\mathbb{F}_{2^8}$ secure against dth-order SCA is depicted in the following algorithm.

Algorithm 3. SecExp254 - dth-order secure exponentiation to the 254 over $\mathbb{F}_{2^8}$

INPUT: shares x_i satisfying $\bigoplus_i x_i = x$
OUTPUT: shares y_i satisfying $\bigoplus_i y_i = x^{254}$

1. **for** $i = 0$ **to** d **do** $z_i \leftarrow x_i^2$ $[\bigoplus_i z_i = x^2]$
2. RefreshMasks$(z_0, z_1, \ldots, z_d)$
3. $(y_0, y_1, \ldots, y_d) \leftarrow$ SecMult$\big((z_0, z_1, \ldots, z_d), (x_0, x_1, \ldots, x_d)\big)$ $[\bigoplus_i y_i = x^3]$
4. **for** $i = 0$ **to** d **do** $w_i \leftarrow y_i^4$ $[\bigoplus_i w_i = x^{12}]$
5. RefreshMasks$(w_0, w_1, \ldots, w_d)$
6. $(y_0, y_1, \ldots, y_d) \leftarrow$ SecMult$\big((y_0, y_1, \ldots, y_d), (w_0, w_1, \ldots, w_d)\big)$ $[\bigoplus_i y_i = x^{15}]$
7. **for** $i = 0$ **to** d **do** $y_i \leftarrow y_i^{16}$ $[\bigoplus_i y_i = x^{240}]$
8. $(y_0, y_1, \ldots, y_d) \leftarrow$ SecMult$\big((y_0, y_1, \ldots, y_d), (w_0, w_1, \ldots, w_d)\big)$ $[\bigoplus_i y_i = x^{252}]$
9. $(y_0, y_1, \ldots, y_d) \leftarrow$ SecMult$\big((y_0, y_1, \ldots, y_d), (z_0, z_1, \ldots, z_d)\big)$ $[\bigoplus_i y_i = x^{254}]$

For completeness, we describe the RefreshMasks algorithm hereafter.

Algorithm 4. RefreshMasks

INPUT: shares x_i satisfying $\bigoplus_i x_i = x$
OUTPUT: shares x_i satisfying $\bigoplus_i x_i = x$

1. **for** $i = 1$ **to** d **do**
2. $\quad tmp \leftarrow$ rand(8)
3. $\quad x_0 \leftarrow x_0 \oplus tmp$
4. $\quad x_i \leftarrow x_i \oplus tmp$

[2] Note that the masks resulting from the SecMult algorithm are independent of the input masks.

Table 1. Complexity of SecExp254

order	nb. XORs	nb. mult.	nb. ^2^	nb. rand. bytes	memory (bytes)
1	20	16	6	6	7
2	56	36	9	16	12
3	108	64	12	20	18
4	176	100	15	48	25
5	260	144	18	70	33
d	$8d^2 + 12d$	$4d^2 + 8d + 4$	$3d + 3$	$2d^2 + 4d$	$\frac{1}{2}d^2 + \frac{7}{2}d + 3$

Algorithm 3 involves of $8d(d+1) + 4d$ XORs, $4(d+1)^2$ multiplications (over $\mathbb{F}_{2^8}$), $d+1$ squares, $d+1$ raising to the 4 and $d+1$ raising to the 16. It uses $3(d+1) + d(d+1)/2$ bytes of memory[3] and it requires the generation of $2d(d+1) + 2d$ random bytes (see illustrative values in Table 1). In comparison, the 2nd-order countermeasures previously published [33, 37] require at least 512 look-ups and 512 XORs and have a memory consumption of at least 256 bytes (see [32, 34] for a detailed comparison).

Masking the full S-box. The affine transformation is straightforward to mask. After recalling that the additive part of Af equals `0x63`, it can be checked that we have:

$$Af(x_0) \oplus Af(x_1) \oplus \cdots \oplus Af(x_d) = \begin{cases} Af(x) & \text{if } d \text{ is even,} \\ Af(x) \oplus \texttt{0x63} & \text{if } d \text{ is odd.} \end{cases}$$

Masking the affine transformation hence simply consists in applying it to every input share separately and, in case of an even d, in adding `0x63` to one of the share afterward. The full S-box computation secure against dth-order SCA is summarized in the following algorithm.

Algorithm 5. SecSbox

INPUT: shares x_i satisfying $\bigoplus_i x_i = x$

OUTPUT: shares y_i satisfying $\bigoplus_i y_i = \mathrm{S}(x)$

1. $(y_0, \ldots, y_d) \leftarrow$ SecExp254$(x_0, \ldots, x_d)$
2. **for** $i = 0$ **to** d **do** $y_i \leftarrow Af(y_i)$
3. **if** $(d \bmod 2 = 1)$ **then** $y_0 \leftarrow y_0 \oplus$ `0x63`

Implementation aspects. Multiplications over $\mathbb{F}_{2^8}$ are typically implemented in software using log/alog tables (see for instance [11]). Note that for security reasons, such an implementation must avoid conditional branches in order to ensure a constant operation flow. The squaring and raisings to the 4 and 16 may be looked-up. Different time-memory tradeoffs are possible. If not much ROM is available, the squaring can be implemented using logical shifts and

[3] $3(d+1)$ bytes for the shares y_i's, z_i's and w_i's (Algorithm 3), and $d(d+1)/2$ for the intermediate variables $r_{i,j}$'s (Algorithm 1).

XORs (see for instance [11]), and the raising to the 2^j, $j \in \{2, 4\}$, can then be simply processed by j sequential squarings. Otherwise, depending on the amount of ROM available, one can either use one, two or three look-up table(s) to implement the raisings to 2^j, $j \in \{1, 2, 4\}$.

Remark 2. For the implementations presented in Section 5, we chose to implement the squaring by a look-up table, getting the raising to the 4 (resp. 16) by accessing this table sequentially 2 (resp. 4) times.

Our scheme may also be implemented in hardware. The sensitive part is the implementation of the SecMult algorithm (see Algorithm 1) which may be subject to glitches and which should incorporate synchronizing elements. In particular, the evaluation of the c_i shares should not start before the evaluation of all the $r_{i,j}$'s has been fully completed. Another approach would be to enhance the software implementation of the scheme with special purpose hardware instructions. For instance, the multiplication, squaring and raisings to powers 4 and 16 over $\mathbb{F}_{2^8}$ could be added to the instructions set of the processor.

3.2 Higher-Order Masking of the Whole Cipher

In the previous section, we have shown how the AES S-box can be masked at any chosen order d. Since the S-box is actually the most difficult part of AES to mask, and due to length constraints, we do not detail the masking of the whole AES cipher here. This description is given in the full version of this paper [35].

4 Security Analysis

In this section, we give a sketch of the security proof of our scheme. We first formally define the notion of *dth-order SCA security* and we introduce afterward our main security result (Theorem 1). The complete security proof is given in the full version of the paper [35].

We consider a *randomized encryption algorithm* $\mathcal{E}$ taking a plaintext p and a (randomly shared) secret key k as inputs[4] and performing a deterministic encryption of p under the secret key k while randomizing its internal computations by means of an external random number generator (RNG). The RNG outputs are assumed to be perfectly random (uniformly distributed, mutually independent and independent of the plaintext and of the secret key). Any variable that can be expressed as a deterministic function of the plaintext and the secret key, which is not constant with respect to the secret key, is called a *sensitive variable* with the exception of the ciphertext $\mathcal{E}_k(p)$ or any deterministic function of it. Note that every intermediate variable computed during an execution of $\mathcal{E}$ (except the plaintext and the ciphertext) can be expressed as a deterministic function of a sensitive variable and of the RNG outputs.

[4] The secret key k is assumed to be split into $d+1$ shares $k_0, k_1, \ldots, k_d$ such that $\bigoplus_i k_i = k$ and every d-tuple of k_i's is uniformly distributed and independent of k.

We shall consider the plaintext, the secret key and the intermediate variables of $\mathcal{E}$ as random variables. The distributions of the intermediate variables are induced by the algorithm inputs (p and k) distributions and by the uniformity of the RNG outputs. The joint distribution of all the intermediate variables of $\mathcal{E}$ thus depends on (p, k). On the other hand, some subsets of intermediate variables may be jointly independent of (p, k). This leads us to the following formal definition of *dth-order SCA security.*

Definition 1. *A randomized encryption algorithm is said to achieve* dth-order SCA security *if every d-tuple of its intermediate variables is independent of any sensitive variable.*

Equivalently, an encryption algorithm achieves dth-order SCA security if any d-tuple of its intermediate variables, except the plaintext and the ciphertext (or any function of one of them), is independent of the algorithm inputs (p, k).

The most sensitive part of our scheme is the masked multiplication algorithm based on the generalized ISW scheme (Algorithm 1). The theorem hereafter states that it achieves dth-order SCA security.

Theorem 1. *Let a and b be two sensitive variables. Let $(a_i)_{0 \leqslant i \leqslant d}$ and $(b_i)_{0 \leqslant i \leqslant d}$ be two families of intermediate variables in input of Algorithm 1 satisfying $a = \bigoplus_{0 \leqslant i \leqslant d} a_i$ and $b = \bigoplus_{0 \leqslant i \leqslant d} b_i$ with $(a_i)_{i \geqslant 1}$ and $(b_i)_{i \geqslant 1}$ being RNG outputs. Then, the distribution of every tuple of d or less intermediate variables in Algorithm 1 is independent of (a, b).*

Theorem 1 states that the generalized ISW scheme achieves dth-order SCA security whereas in [17] it is only proven that the ISW scheme achieves $(d/2)$th-order SCA security. This improvement is of practical interest since it enables to double the security order for any chosen complexity (in terms of timing and/or silicon area).

The proof of Theorem 1 as well as the security proof of our whole dth-order masking scheme for AES are given in the full version of the paper [35].

5 Implementation Results

To compare the efficiency of our proposal with that of other methods proposed in the literature, we applied them to protect an implementation of the AES-128 algorithm in encryption mode. We have implemented our new countermeasure for $d \in \{1, 2, 3\}$, namely to counteract either first-order SCA ($d = 1$) or second-order SCA ($d = 2$) or third-order SCA ($d = 3$). Among the numerous methods proposed in the literature to thwart first-order SCA we chose to implement only that having the best timing performance (the *table re-computation method* [22]) and that offering the best memory performance (the *tower field method* [27]). In the second-order case, we implemented the only two existing methods: the one proposed in [37][5] and the one proposed [33]. Eventually, since no countermeasure

[5] Initially, the method of [37] was devoted to thwart dth-order SCA for any chosen order d but it has been shown insecure for $d \geqslant 3$ [8].

Table 2. Comparison of secure AES implementations

Method	Reference	cycles	RAM (bytes)	ROM (bytes)
Unprotected Implementation				
No Masking	Na.	2×10^3	32	1150
First Order Masking				
Re-computation	[22]	10×10^3	$256 + 35$	1553
Tower Field in $\mathbb{F}_4$	[27, 28]	77×10^3	42	3195
Our scheme for $d = 1$	This paper	129×10^3	73	3153
Second Order Masking				
Double Re-computations	[37]	594×10^3	$512 + 90$	2336
Single Re-computation	[33]	672×10^3	$256 + 86$	2215
Our scheme for $d = 2$	This paper	271×10^3	79	3845
Third Order Masking				
Our scheme for $d = 3$	This paper	470×10^3	103	4648

against 3rd-order SCA was existing before that introduced in this paper, it is the single one in its category.

We wrote the codes in assembly language for an 8051-based 8-bit architecture. The implementations only differ in their approaches to protect the S-box computations. In Table 2, we list the timing/memory performances of the different implementations.

As expected, in the first-order case the countermeasures introduced in [22] and [27, 28] are much more efficient than ours. This is a consequence of the generic character of our method which is not optimized for one choice of d but aims to work for any d.

In the second-order case, our proposal becomes much more efficient than the existing solutions. It is 2.2 times faster than the countermeasure proposed in [37] with a RAM memory requirement divided by around 10. It is also 2.5 times faster than the countermeasure in [33] and requires 5.3 times less RAM. Memory allocation differences are merely due to the fact that the methods [37] and [33] generalize the table re-computation method and thus require the storage of one (for [33]) or two (for [37]) randomized representation(s) of the AES S-box. The differences in timing performances come from the fact that the methods in [37] and [34] process one loop over all the 256 elements of the S-box look-up table (each loop iteration processing itself a few elementary operations), which is more costly than the 36 field multiplications and 56 bitwise additions involved in our method (see Table 1).

Eventually, in the third-order case our method has acceptable timing/memory performances. For comparison, it stays faster than the second-order countermeasures proposed in [37] and [33] and it still requires much less RAM memory. For a chip running at 31MHz (which is today quite usual) an AES encryption of one block requiring 470×10^3 cycles, takes 91ms. For some use cases where the size of the message to encrypt/decrypt is not too long such a timing performance is acceptable (*e.g.* challenge-response protocols, Message Authentication Codes for one-block messages as in banking transactions).

6 Conclusion

In this paper, we have presented the first masking scheme dedicated to AES which is provably secure at any chosen order and which can be implemented in software at the cost of a reasonable overhead. We provided implementation results showing the practical interest of our scheme as well as its efficiency compared to the existing second-order masking schemes. In the full version of this paper [35], we further give a formal security proof of our scheme including an improved security proof for the scheme published by Ishai *et al.* at Crypto 2003.

References

1. Akkar, M.-L., Giraud, C.: An Implementation of DES and AES, Secure against Some Attacks. In: Ko**c**c, **c**C.K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 309–318. Springer, Heidelberg (2001)
2. Blakely, G.: Safeguarding cryptographic keys. In: National Comp. Conf., New York, June 1979, vol. 48, pp. 313–317. AFIPS Press (1979)
3. Blömer, J., Merchan, J.G., Krummel, V.: Provably Secure Masking of AES. In: Matsui, M., Zuccherato, R. (eds.) SAC 2004. LNCS, vol. 3357, pp. 69–83. Springer, Heidelberg (2004)
4. Blum, M., Micali, S.: How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits. SIAM J. Comput. 13(4), 850–864 (1984)
5. Canright, D.: A Very Compact S-Box for AES. In: Rao, J., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 441–455. Springer, Heidelberg (2005)
6. Chari, S., Jutla, C., Rao, J., Rohatgi, P.: Towards Sound Approaches to Counteract Power-Analysis Attacks. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 398–412. Springer, Heidelberg (1999)
7. Chari, S., Rao, J., Rohatgi, P.: Template Attacks. In: Kaliski Jr., B., Ko**c**c, **c**C.K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 13–28. Springer, Heidelberg (2003)
8. Coron, J.-S., Prouff, E., Rivain, M.: Side Channel Cryptanalysis of a Higher Order Masking Scheme. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 28–44. Springer, Heidelberg (2007)
9. Cramer, R., Damgård, I., Ishai, Y.: Share Conversion, Pseudorandom Secret-Sharing and Applications to Secure Computation. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 342–362. Springer, Heidelberg (2005)
10. Crescenzo, G.D., Lipton, R.J., Walfish, S.: Perfectly Secure Password Protocols in the Bounded Retrieval Model. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 225–244. Springer, Heidelberg (2006)
11. Daemen, J., Rijmen, V.: The Design of Rijndael. Springer, Heidelberg (2002)
12. Damgård, I., Keller, M.: Secure Multiparty AES (full paper). Cryptology ePrint Archive, Report 20079/614 (2009), `http://eprint.iacr.org/`
13. Dziembowski, S., Pietrzak, K.: Leakage-resilient cryptography. In: FOCS, pp. 293–302. IEEE Computer Society, Los Alamitos (2008)
14. FIPS PUB 197. Advanced Encryption Standard. National Institute of Standards and Technology (November 2001)
15. FIPS PUB 46-3. Data Encryption Standard (DES). National Institute of Standards and Technology (October 1999)

16. Goubin, L., Patarin, J.: DES and Differential Power Analysis – The Duplication Method. In: Ko**c**c, **c**C.K., Paar, C. (eds.) CHES 1999. LNCS, vol. 1717, pp. 158–172. Springer, Heidelberg (1999)
17. Ishai, Y., Sahai, A., Wagner, D.: Private Circuits: Securing Hardware against Probing Attacks. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 463–481. Springer, Heidelberg (2003)
18. Kocher, P., Jaffe, J., Jun, B.: Differential Power Analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
19. Mangard, S., Popp, T., Gammel, B.M.: Side-Channel Leakage of Masked CMOS Gates. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 351–365. Springer, Heidelberg (2005)
20. Mangard, S., Pramstaller, N., Oswald, E.: Successfully Attacking Masked AES Hardware Implementations. In: Rao, J., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 157–171. Springer, Heidelberg (2005)
21. Maurer, U.: A provably-secure strongly-randomized cipher. In: Damgård, I. (ed.) EUROCRYPT 1990. LNCS, vol. 473, pp. 361–388. Springer, Heidelberg (1991)
22. Messerges, T.: Securing the AES Finalists against Power Analysis Attacks. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 150–164. Springer, Heidelberg (2001)
23. Messerges, T.: Using Second-order Power Analysis to Attack DPA Resistant Software. In: Paar, C., Ko**c**c, **c**C.K. (eds.) CHES 2000. LNCS, vol. 1965, pp. 238–251. Springer, Heidelberg (2000)
24. Micali, S., Reyzin, L.: Physically Observable Cryptography (Extended Abstract). In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 278–296. Springer, Heidelberg (2004)
25. Nikova, S., Rijmen, V., Schläffer, M.: Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches. In: Lee, P.J., Cheon, J.H. (eds.) ICISC 2008. LNCS, vol. 5461, pp. 218–234. Springer, Heidelberg (2009)
26. Oswald, E., Mangard, S., Herbst, C., Tillich, S.: Practical Second-order DPA Attacks for Masked Smart Card Implementations of Block Ciphers. In: Pointcheval, D. (ed.) CT-RSA 2006. LNCS, vol. 3860, pp. 192–207. Springer, Heidelberg (2006)
27. Oswald, E., Mangard, S., Pramstaller, N.: Secure and Efficient Masking of AES – A Mission Impossible? Cryptology ePrint Archive, Report 2004/134 (2004)
28. Oswald, E., Mangard, S., Pramstaller, N., Rijmen, V.: A Side-Channel Analysis Resistant Description of the AES S-box. In: Gilbert, H., Handschuh, H. (eds.) FSE 2005. LNCS, vol. 3557, pp. 413–423. Springer, Heidelberg (2005)
29. Petit, C., Standaert, F.-X., Pereira, O., Malkin, T., Yung, M.: A block cipher based pseudo random number generator secure against side-channel key recovery. In: Abe, M., Gligor, V.D. (eds.) Symposium on Information, Computer and Communications Security – ASIACCS 2008, pp. 56–65. ACM, New York (2008)
30. Pietrzak, K.: A Leakage-Resilient Mode of Operation. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 462–482. Springer, Heidelberg (2010)
31. Popp, T., Kirschbaum, M., Zefferer, T., Mangard, S.: Evaluation of the Masked Logic Style MDPL on a Prototype Chip. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 81–94. Springer, Heidelberg (2007)
32. Rivain, M.: On the Physical Security of Cryptographic Implementations. PhD thesis, University of Luxembourg (September 2009)
33. Rivain, M., Dottax, E., Prouff, E.: Block Ciphers Implementations Provably Secure Against Second Order Side Channel Analysis. In: Baignères, T., Vaudenay, S. (eds.) FSE 2008. LNCS, vol. 5086, pp. 127–143. Springer, Heidelberg (2008)

34. Rivain, M., Dottax, E., Prouff, E.: Block Ciphers Implementations Provably Secure Against Second Order Side Channel Analysis. Cryptology ePrint Archive, Report 2008/021 (2008), http://eprint.iacr.org/
35. Rivain, M., Prouff, E.: Provably Secure Higher-Order Masking of AES. Cryptology ePrint Archive (2010), http://eprint.iacr.org/
36. Rivain, M., Prouff, E., Doget, J.: Higher-Order Masking and Shuffling for Software Implementations of Block Ciphers. In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 171–188. Springer, Heidelberg (2009)
37. Schramm, K., Paar, C.: Higher Order Masking of the AES. In: Pointcheval, D. (ed.) CT-RSA 2006. LNCS, vol. 3860, pp. 208–225. Springer, Heidelberg (2006)
38. Shamir, A.: How to Share a Secret. ACM Commun. 22(11), 612–613 (1979)
39. Standaert, F.-X., Pereira, O., Yu, Y., Quisquater, J.-J., Yung, M., Oswald, E.: Leakage resilient cryptography in practice. Cryptology ePrint Archive, Report 2009/341 (2009), http://eprint.iacr.org/
40. Standaert, F.-X., Veyrat-Charvillon, N., Oswald, E., Gierlichs, B., Medwed, M., Kasper, M., Mangard, S.: The World is Not Enough: Another Look on Second-Order DPA. Cryptology ePrint Archive, Report 2010/180 (2010), http://eprint.iacr.org/
41. Tillich, S., Herbst, C.: Attacking State-of-the-Art Software Countermeasures-A Case Study for AES. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 228–243. Springer, Heidelberg (2008)