Received: 14 May 2021 | Revised: 13 September 2021 | Accepted: 28 September 2021

DOI: 10.1049/ise2.12048

The Institution of Engineering and Technology WILEY

RAPID COMMUNICATION

On robust strong-non-interferent low-latency multiplications

Maria Chiara Molteni[1] | Jürgen Pulkus[2] | Vittorio Zaccaria[3]

[1]Dipartimento di Informatica "Giovanni Degli Antoni", Università degli Studi di Milano, Milano, Italy

[2]G+D Mobile Security GmbH, München, Germany

[3]Department of Electronics, Information and Bioengineering, Politecnico di Milano, Milano, Italy

Correspondence
Vittorio Zaccaria, Dipartimento di Elettronica, Informazione e Bioingegneria (DEIB), Politecnico di Milano, Piazza Leonardo da Vinci 32, 20133 Milano, Italy.
Email: vittorio.zaccaria@polimi.it

Abstract

The overarching goal of this work is to present new theoretical and practical tools to implement robust $-$ $t-$probing security. In this work, a low-latency multiplication gadget that is secure against probing attacks that exploit logic glitches in the circuit is presented. The gadget is the first of its kind to present a 1-cycle input-to-output latency while belonging to the class of *probing security by optimized composition* gadgets [6]. In particular, the authors show that it is possible to construct robust-t-strong-non-interferent gadgets without compromising on latency with a moderate increase in area. The authors provide a theoretical proof for the robustness of the gadget and show that, for $t \leq 4$, the amount of randomness required can even be reduced without compromising on robustness.

KEYWORDS
cryptography, security

1 | INTRODUCTION

In this work, we address the problem of protecting hardware implementations against side channel attacks. State-of-the-art countermeasures are typically based on masking [1] but creating a masked implementation is not trivial at all, especially when we consider adversarial scenarios such as probing attacks [2] or, more recently, glitch-extended probing attacks [3, 4]. The non-linear modules of cryptographic circuits are the most intricate to protect against such attacks. For this reason, the most studied case is the secure implementation of the logic AND, which over the years has never ceased to stimulate research since its inception [2].

In the following, we say that a gadget is $t-$probing secure when, given t probes, it is impossible to derive information about the secret values encoded in the masks/shares. One of the main problems addressed in $t-$probing security is *composability*, that is, determining, given two $t-$probing secure gadgets, if their functional composition is still $t-$probing secure. It is common understanding that this depends on the amount of *refreshing*, a procedure that aims to break higher order dependencies and bring back the secret's shares into a uniformly random state, after a series of operations that might have invalidated uniformity [5].

One school of thought, identified as *probing security by optimized composition* [6], exploits inner gadget properties to determine whether their composition is $t-$probing secure. One of them is *strong-non-interference* ($t-$SNI, [7]) which requires that the number of input shares derivable from a certain set of probes depends only on the number of internal positions present in that set (whenever that set's size is less or equal to t). Demonstrating that a gadget is in the first place $t-$SNI might require lengthy proofs or automatic tools [8, 9], but once it has been done, composition can be studied with simpler, although not trivial rules. This kind of scenario is called *optimized* because, in principle, it could lead to gadgets with an overall minimized *refreshing* effort. This is, however, easier said than done as, even recently, some gadgets that were thought to be $t-$probing secure have been shown to be vulnerable to higher order attacks [10]. *Trivial composability* tries, instead, to identify inner gadget properties that could make reasoning about composition even more trivial, in the sense that it suffices for certain gadgets to ensure at least *probe-isolating-non-interference* [6] to be able to compose them.

An additional problem is protecting the gadget from circuit glitches. One way to address this is *threshold implementations* (TI) [11] that ensure that all logic cones of a primitive depend only on a proper subset of the shares. Besides the overall correctness constraints, this means ensuring that, (i) if a gadget's input is fed with shares (computed from the secret) whose distribution is uniform, its outputs must be uniform as well and (ii) each output share can be computed using only a proper subset of the input shares.

The current research trend tries to address $t-$probing security and glitches as a single challenge instead of different, seemingly orthogonal problems. The *robust probing model* is probably the most important conceptual evolution with respect to the original $t-$probing security model [3, 4]. In this attack model, glitches are seen as extended probes that constitute additional observation points of the input values of a given cone of logic. With this model, one can prove that some gadgets are not only $t-$SNI in the conventional sense but can be made robust$-t-$SNI by adding a register layer at the outputs (see e.g., [3]) trading off latency with security. On the side of *trivial composability*, stricter conditions on a gadget, like the t-PINI condition [6, 12], have been identified to ensure robustness in the presence of glitches.

It is currently understood that the minimal input-shares-to-output latency of circuits with optimized composability (e.g., the glitch-robust $t-$SNI multiplication presented in [3]) requires two cycles. In this work, we reduce it to one cycle at the cost of some extra randomness by adopting a different temporal scheme for producing refresh random bits. In fact, we will provide a class of 1-cycle-latency multiplication gadgets that are robust$-t-$SNI. In particular, in Proposition 1, we prove our construction for CMS gadgets to be robust$-t-$SNI, showing, therefore, for arbitrary t, the existence of such gadgets with one cycle latency using (in total) $2 \cdot s^2$ random bits, where $s = t + 1$ is the number of shares. Besides, we show how to lower this bound to $s(s-1)$ and s^2 for the practically most relevant cases $s = 2, 3$ and $s = 4, 5$, respectively, by simply removing some randomness and proving it robust$-t-$SNI with MASKVERIF [13].[1]

The paper is organized as follows: Section 2 summarizes the current state of the art for robust probing security pointing out a few problems with the current approaches. Section 3 presents the main construction proposed in this work, highlighting a few optimized schemes. Section 4 suggests potential applications of the new gadget. Section 5 presents some final comments and indicates some future work.

2 | STATE OF THE ART

Recall that a function f is t-non-interferent ($t-$NI) if, when given a total of o outputs and i internal probes, $o + i \leq t$ implies a dependency on at most $i + o$ input shares. The function f is strongly t-non-interferent ($t-$SNI) if it even implies a dependency on at most i input shares [7]. When considering glitches, probes are *extended* to model information that might be captured with glitches. In particular, they allow the attacker to observe all the inputs of a gadget that connect to a probed output wire, because this is what has been observed in real-world scenarios [14]. When considering such kind of probes, we talk about robust $-$ $t-$probing security instead of conventional $t-$probing security.

In this work, we address the problem of robust$-t-$probing security in the context of optimized composability. Chronologically, the original efforts considered a hybrid of the Ishai–Sahai–Wagner scheme [2] with TI, culminating in the Consolidated Masking Scheme (CMS) [15]. While the results were important in terms of decrease of randomness needed (in CMS with $t + 1$ shares, one needs $(t + 1)^2$ refresh values), it was shown recently that this cannot be extended past $t > 2$ (without even considering robust $t-$probing security [10]). Later proposals for a $t-$probing secure multiplication addressed a reduction in terms of refresh values [16, 17] (with a lower bound identified in [18]) but, after the considerations made in [10], it is not clear how much past $t > 1$ these can be made robust-t-probing secure. Besides, all the proposed gadgets suffer from an increased latency (two cycles) because they need an additional register after the compression stage to be guaranteed robust$-t-$SNI.

Recent efforts put into improving CMS masking without increasing the latency have been proposed [19]. Figure 1 shows a solution for the case for $t = 3, s = 4$ as proposed by the authors in Ref. [19]. Note that the authors elaborate this scheme starting from the first CMS proposed in Ref. [15], changing the order of products $a_i b_j$ and introducing additional random bits q_i to protect the shares; however, as we now show, this gadget is not robust-3-strong-non-interferent (SNI). In fact, consider the three probes marked in green P_1, P_2 and P_3: probes P_2 and P_3 are the only internal probes so all three probes should convey information about up to two shares. P_1 allows us to get $(a_1b_2 + r_0 + r_1, a_1b_0 + r_1 + r_2 + q_0,$ $a_3b_0 + r_2 + r_3 + q_1, a_3b_2 + r_3 + r_4)$, whereas the two internal probes P_2 and P_3 allow us to get (a_2b_3, r_0, r_{15}) and (a_1b_0, r_1, r_2, q_0), respectively. In principle, the information on the secrets derived from P_1 (e.g., a_1b_2) is covered by at least two random bits (e.g., a_1b_2 is covered with r_0 and r_1); however, it is possible to unmask a_1b_2 from P_1 adding r_0 and r_1 recovered from P_2 and P_3, respectively. Then, three shares of b are exposed (b_2 from P_1, b_3 from P_2 and b_0 from P_3) with only two internal probes.

3 | A PROVABLY ROBUST-t-SNI, 1-CYCLE-LATENCY CMS-LIKE SCHEME

The problem with the scheme in Figure 1 is that internal extended probes give access to each random bit used in the refresh layer (yellow section). To overcome this leak, one can sum and save into a register these pairs of random bits so as to avoid that a single probe (such as e.g., P_3) has access to both intermediate products and individual refresh random bits. Note that, from the point of view of the input-to-output latency, the gadget is still one cycle as this sum could be pre-computed before receiving the shares a

[1] See https://github.com/vzaccaria/maskverif.docker for the MASKVERIF scripts for reproducing the results.

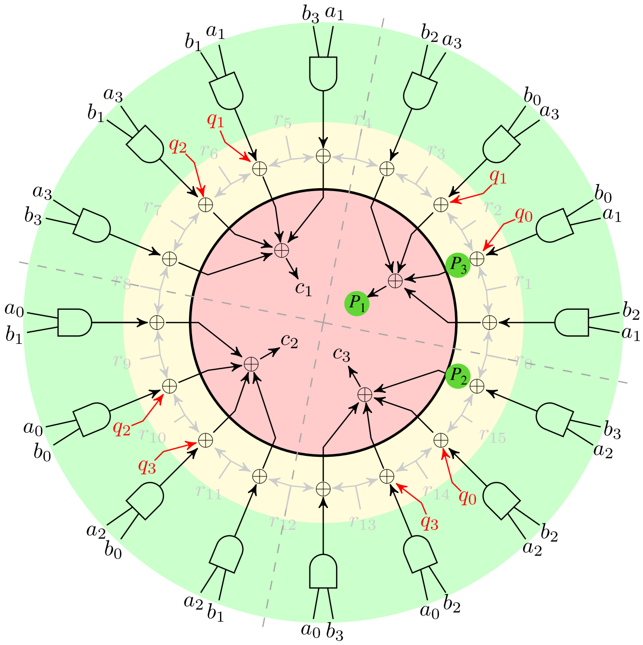

FIGURE 1 1-cycle latency Consolidated Masking Scheme derived gadget proposed in [19]. Green discs represent the three extended probes that make it not robust-3-strong-non-interferent. The black thick line indicates the register layer. The expressions to compute the outputs are those in Equation (1) except that the values in red brackets are not sampled in an additional register, that is, only those values in the black brackets are sampled

and b. For the above gadget, we would have the following expressions:

$$\begin{aligned} c_0 = & [a_1 b_2 + [r_0 + r_1]] + [a_1 b_0 + [r_1 + r_2] + q_0] + \\ & + [a_3 b_0 + [r_2 + r_3] + q_1] + [a_3 b_2 + [r_3 + r_4]] \\ c_1 = & [a_1 b_3 + [r_4 + r_5]] + [a_1 b_1 + [r_5 + r_6] + q_1] + \\ & + [a_3 b_1 + [r_6 + r_7] + q_2] + [a_3 b_3 + [r_7 + r_8]] \\ c_2 = & [a_0 b_1 + [r_8 + r_9]] + [a_0 b_0 + [r_9 + r_{10}] + q_2] + \\ & + [a_2 b_0 + [r_{10} + r_{11}] + q_3] + [a_2 b_1 + [r_{11} + r_{12}]] \\ c_3 = & [a_0 b_3 + [r_{12} + r_{13}]] + [a_0 b_2 + [r_{13} + r_{14}] + q_3] + \\ & + [a_2 b_2 + [r_{14} + r_{15}] + q_0] + [a_2 b_3 + [r_{15} + r_0]] \end{aligned} \tag{1}$$

where square brackets indicate registered values (see Table 1), with additional red colour when they refer to the registered sum of refresh random bits; one can verify with MASKVERIF [13] that the above gadget is in fact robust-3-SNI. Note that Equation (1) describes the scheme in Figure 1 with some added registers (red brackets). This strategy is not entirely new as it has been used, to the best of our knowledge, only recently [6] in the field of *trivial composability*. However, we will show that also optimized composability might benefit from such strategy, as it is possible to generalize this idea to derive a sufficient condition for a gadget being 1-cycle robust$-t-$SNI, whose general cone structure is shown in Figure 2.

TABLE 1 Meaning of some mathematical symbols employed in the text

Symbol	Meaning
$[\cdot]$	Value saved into a register
$:=$	Mathematical definition
$\lvert \cdot \rvert$	Set cardinality
$\langle v_i \vert i \in I \rangle$	Vector space generated by the vectors $(v_i)_{i \in I}$
$x = y \bmod V$	x equals y modulo the subspace V, i.e.:
	$x = y + v$ for some $v \in V$

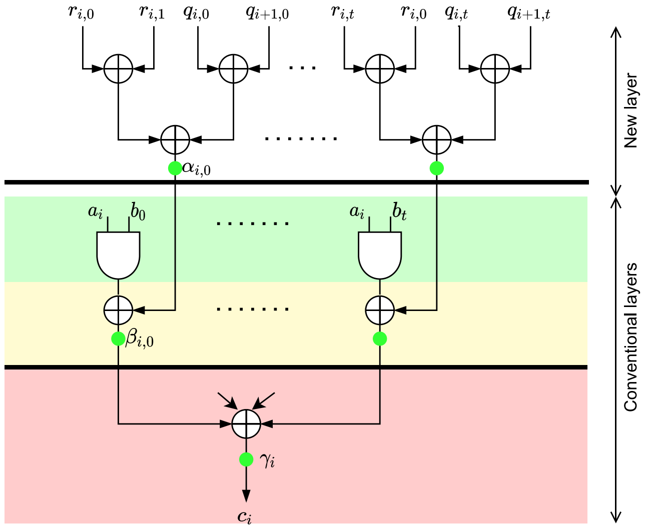

FIGURE 2 A cone of the proposed robust $-t-$ SNI CMS structure that has still 1-cycle latency. Green discs represent the possible probes used in Proposition 1. The black thick lines indicate register layers

Note that the shares a_i and b_j are organized as in the original CMS scheme [15], and the random bits are summed up and registered before using them in the refresh layer.

Proposition 1 *Given $2s^2$ independent random bits $(q_{ij})_{0 \leq i,j \leq t}$ and $(r_{ij})_{0 \leq i,j \leq t}$ the following AND-gadget is* robust$-t-$SNI:

$$c_i := \sum_{0 \leq j \leq t} [a_i \cdot b_j + [r_{i,j} + r_{i,j+1} + q_{i,j} + q_{i+1,j}]] \tag{2}$$

where $r_{is} := r_{i0}, q_{si} := q_{0i}$ for $0 \leq i \leq t$ and $s := t + 1$.

Proof. For the meaning of mathematical symbols, see Table 1. Setting $o_{i,j} := a_i \cdot b_j + s_{i,j}$ with $s_{i,j} := r_{i,j} + r_{i,j+1} + q_{i,j} + q_{i+1,j}$ for $0 \leq i,j \leq t$, the extended output probes are $\gamma_i := \{o_{i,j} \vert 0 \leq j \leq t\}$ for $0 \leq i \leq t$, and the maximal extended inner probes are $\alpha_{i,j} := \{r_{i,j}, r_{i,j+1}, q_{i,j}, q_{i+1,j}\}$ and $\beta_{i,j} := \{a_i \cdot b_j, s_{i,j}\}$ for $0 \leq i,j \leq t$.

An attacker gets to pick at most t extended probes, let us say a set Γ of output probes of type γ_j, a set A of inner probes of type $\alpha_{i,j}$ and a set B of inner probes of type $\beta_{i,j}$, s.t. $|\Gamma| + |\mathrm{A}| + |\mathrm{B}| \leq t$.

Setting $I := \{i \mid \alpha_{i,j} \in \mathrm{A} \text{ or } \beta_{i,j} \in \mathrm{B}\}$ and $J := \{j \mid \alpha_{i,j} \in \mathrm{A} \text{ or } \beta_{i,j} \in \mathrm{B}\}$, we claim that the attacker can simulate all those probes knowing just the inputs a_i for $i \in I$ and b_j for $j \in J$, where clearly $|I| \leq |\mathrm{A}| + |\mathrm{B}|$ and $|J| \leq |\mathrm{A}| + |\mathrm{B}|$ ($|\mathrm{A}| + |\mathrm{B}|$ is the number of the chosen inner probes). All the information derivable from the extended probes Γ, A and B can be expressed using elements of $\langle \Gamma, \mathrm{A}, \mathrm{B} \rangle$, which can be seen as sums of standard probes derived from the extended ones. As the image of the uniform distribution under a linear map is the uniform distribution on its image, an element of $\langle \Gamma, \mathrm{A}, \mathrm{B} \rangle$ has a uniform distribution and is independent of all inputs a_i and b_j unless it is already contained in $\langle a_i \cdot b_j \mid 0 \leq i, j \leq t \rangle$. Hence, the above claim can be expressed as follows:

$$\langle \Gamma, \mathrm{A}, \mathrm{B} \rangle \cap \langle a_i \cdot b_j \mid 0 \leq i, j \leq t \rangle \subseteq \langle a_i \cdot b_j \mid i \in I, j \in J \rangle.$$

All standard probes are linear combinations of the linearly independent values $a_i \cdot b_j$, $r_{i,j}$ and $q_{i,j}$ for $0 \leq i, j \leq t$, that is, elements of the vector space $\langle a_i \cdot b_j, r_{i,j}, q_{i,j} \mid 0 \leq i, j \leq t \rangle$. Applying to the probes the modulo operation w.r.t. the vector subspace $\langle a_i \cdot b_j, r_{i,j} \mid 0 \leq i, j \leq t \rangle$, the probes have values $q_{i,j}$, respectively. $q_{i,j} + q_{i+1,j}$; for each j, the values $q_{i,j} + q_{i+1,j}$ span a t-dimensional subspace of the $(t+1)$-dimensional space generated by the $q_{i,j}$ with $0 \leq i \leq t$, so $\sum_{0 \leq i \leq t} (q_{i,j} + q_{i+1,j}) = 0$ is the only non-trivial linear dependency of the values $q_{i,j} + q_{i+1,j}$ for fixed j. Then, for any j, with $R := \langle a_i \cdot b_j, r_{i,j} \mid 0 \leq i, j \leq t \rangle$

$$\sum_{i \in I} s_{i,j} = 0 \bmod R \;\Rightarrow\; I = \emptyset \text{ or } I = \{0, \ldots, t\}. \tag{3}$$

Analogously, applying to the probes the modulo operation w.r.t. the vector space $Q := \langle a_i \cdot b_j, q_{i,j} \mid 0 \leq i, j \leq t \rangle$, for fixed j, the only non-trivial linear dependency of the values $r_{i,j} + r_{i,j+1}$ is $\sum_{0 \leq j \leq t} (r_{i,j} + r_{i,j+1}) = 0$. Then, for any i,

$$\sum_{j \in J} s_{i,j} = 0 \bmod Q \;\Rightarrow\; J = \emptyset \text{ or } J = \{0, \ldots, t\}. \tag{4}$$

Now take $\sigma \in \langle \Gamma, \mathrm{A}, \mathrm{B} \rangle \cap \langle a_i \cdot b_j \mid 0 \leq i, j \leq t \rangle$. We have to show $\sigma \in \langle a_i \cdot b_j \mid i \in I, j \in J \rangle$. If σ involves a summand containing the term $a_i \cdot b_j$, this term stems either from the inner probe $\beta_{i,j} \in \mathrm{B}$—implying $i \in I$ and $j \in J$ (confirming our claim)—or from the summand $o_{i,j} \in \gamma_i \in \Gamma$. As $o_{i,j} = s_{i,j} \bmod \langle a_i \cdot b_j \mid 0 \leq i, j \leq t \rangle$, assuming $\beta_{i,j} \notin \mathrm{B}$ implies, using Equation (3), that σ involves either (a) $t+1$ terms $s_{i',j}$ (with $0 \leq i' \leq t$) obtainable from $t+1$ standard probes or (b) a summand $q_{i',j}$ for some $0 \leq i' \leq t$. The latter case (b) implies that $\alpha_{i',j}$ or $\alpha_{i'-1,j}$ is probed, and hence $j \in J$ (confirming our claim). The former case (a) requires at least t more probes (as no extended probe involves terms $s_{i,j}$ for more than one i) contradicting the original assumption that $|\Gamma| + |\mathrm{A}| + |\mathrm{B}| \leq t$.

Analogously, given the implication of Equation (4), σ involves either (a) $t+1$ terms $si';j$ (with $0 \leq j' \leq t$) obtainable from $t+1$ standard probes or (b) a summand $r_{i,j'}$ for some $0 \leq j' \leq t$. The latter case (b) implies that $\alpha_{i,j'}$ or $\alpha_{i,j'-1}$ is probed, and hence $i \in I$ (confirming our claim). For the former case (a), by just probing γ_i, an attacker can get all the terms $s_{i,j'}$. However, we previously showed that for each term $s_{i,j'}$ contained in a summand of σ is necessarily $j' \in J$, implying $J = \{0, \ldots, t\}$. This contradicts that the attacker can choose at most t probes because for each inner probe at most one element is added to J. □

The placement of the products $a_i \cdot b_j$ in the output cones c_i as well as the presence of randomness in Equation (2) is essential to guarantee that the proposed construction is robust $-t-$ SNI. Indeed, a different placement can break (robust) strong non-interference for s big enough. In fact, assume that an attacker chooses n extended output probes $\gamma_1, \ldots, \gamma_n$ placed on adjacent cones, and $4(n-1)$ inner probes $\alpha_{1,i}, \alpha_{i,1}, \alpha_{n,i}, \alpha_{i,n}$ for $1 \leq i \leq n$. The probes $\gamma_1, \ldots, \gamma_n$ give access to all values $o_{i,j}$ for $1 \leq i, j \leq n$, whose sum is

$$\begin{aligned} &\sum_{1 \leq i,j \leq n} a_i \cdot b_j + \sum_{1 \leq i,j \leq n} (r_{i,j} + r_{i,j+1}) + \sum_{1 \leq i,j \leq n} \left(q_{i,j} + q_{i+1,j} \right) \\ &= \sum_{1 \leq i,j \leq n} a_i \cdot b_j + \sum_{1 \leq i \leq n} (r_{i,1} + r_{i,n+1}) + \sum_{1 \leq j \leq n} \left(q_{1,j} + q_{n+1,j} \right). \end{aligned}$$

The inner probes allow us to derive $r_{i,1} \in \alpha_{i,1}$, $r_{i,n+1} \in \alpha_{i,n}$, $q_{1,i} \in \alpha_{1,i}$ and $q_{n+1,i} \in \alpha_{n,i}$, effectively exposing the first summand $\sum_{1 \leq i,j \leq n} a_i \cdot b_j$ of the equation above; thus, $4(n-1) + n$ probes allow us to derive n^2 different products $a_i \cdot b_j$. The arrangement of the $a_i \cdot b_j$ in Equation (2) is such that even knowing these n^2 products do not break strong non-interference as the attacker only obtains n different shares a_i and b_j $(1 \leq i, j \leq n)$. But already for $s = 12$ and $n = 3$, a different placement of the products $a_i \cdot b_j$ can expose more than $4(n-1)$ shares of either secret, making it not robust strong-interferent.

3.1 | Saving randomness for $t \leq 4$

For $t \leq 4$, the scheme presented in Proposition 1 can be simplified by removing the random bits $r_{i,j}$ without compromising security. This decreases the number of involved random bits from $2 \cdot s^2$ to s^2 (see Figure 3 for this construction). In particular, as one can verify with MASKVERIF, robust$-t-$probing security can be ensured with just the $q_{i,j}$:

$$c_i = \sum_{0 \leq j \leq t} \left[a_i b_j + [q_{i,j} + q_{i+1,j}] \right] \tag{5}$$

for $0 \leq i, j \leq t$, $t \leq 4$. However, for $t \geq 5$, this particular scheme breaks because, with a specific choice of three external probes on adjacent c_i and two internal probes, an attacker is able to recover three shares of a. For example, if the attacker places

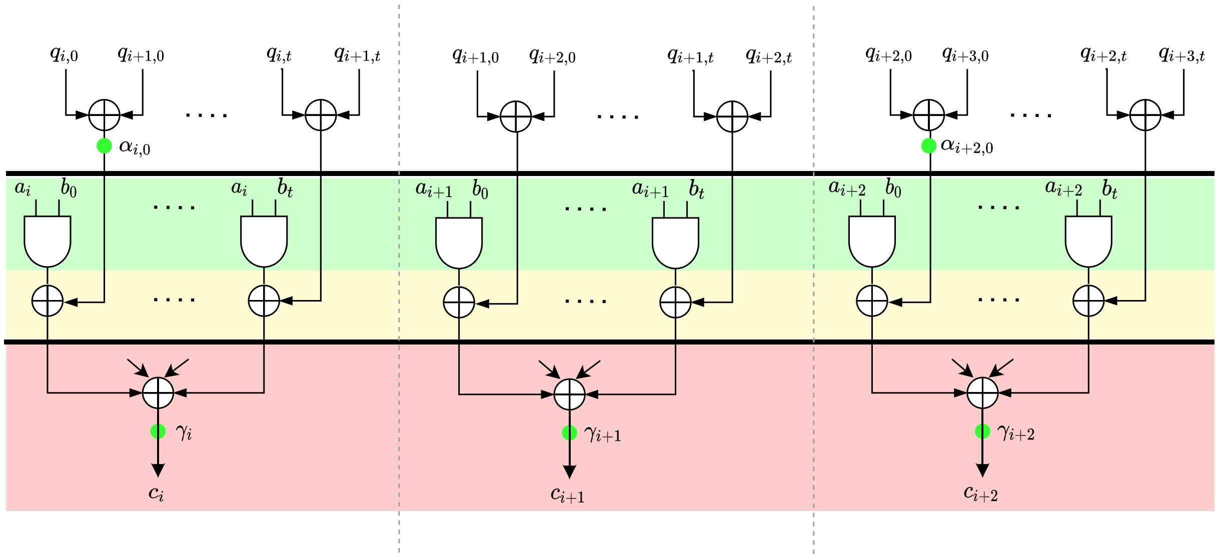

FIGURE 3 The optimized construction that is valid for any $t < 5$ but fails for $t \geq 5$. Green discs represent the probes used to mount the attack

five probes (see Figure 3's green dots) on $\gamma_i, \gamma_{i+1}, \gamma_{i+2}, \alpha_{i,0}$ and $\alpha_{i+2,0}$ then they are able to derive three shares of a, with only two internal probes. This attack is possible for any $t \geq 5$.

For $t \leq 2$, one can additionally remove the random bits $q_{i,i}$, deriving for $t = 1$ the following scheme with only two random bits instead of $s^2 = 4$:

$$\begin{aligned} c_0 &= [a_0 b_0 + q_{1,0}] + [a_0 b_1 + q_{0,1}] \\ c_1 &= [a_1 b_0 + q_{1,0}] + [a_1 b_1 + q_{0,1}] \end{aligned} \tag{6}$$

Similarly, for $t = 2$, one obtains the following construction with only six random bits instead of $s^2 = 9$:

$$\begin{aligned} c_0 &= [a_0 b_0 + q_{1,0}] + [a_0 b_1 + q_{0,1}] + [a_0 b_2 + [q_{0,2} + q_{1,2}]] \\ c_1 &= [a_1 b_0 + [q_{1,0} + q_{2,0}]] + [a_1 b_1 + q_{2,1}] + [a_1 b_2 + q_{1,2}] \\ c_2 &= [a_2 b_0 + q_{2,0}] + [a_2 b_1 + [q_{2,1} + q_{0,1}]] + [a_2 b_2 + q_{0,2}] \end{aligned} \tag{7}$$

Both schemes are robust−t−SNI (for $t = 1$ and $t = 2$ respectively), as one can verify with MASKVERIF.

4 | APPLICATIONS

Our proposed structure allows us to obtain an input-share-to-output-share latency of one cycle while still being robust−t −SNI, at the expense of increased randomness. A t−SNI gadget could be made robust−t−SNI with reasonable latency by replacing all t−SNI ANDs with our proposed gadget, all t−NI ANDs with DOM ANDs, and all t−SNI refresh gadgets with the robust−t−SNI refresh gadgets from Ref. [6]. Indeed, compared to the DOM [20] and the HPC2 [6] gadgets, which both need $s(s-1)/2$ random bits, our gadgets require 2× randomness for $s = 2, 3$, about 2.5× for $s = 4, 5$ and more than 4× for $s > 5$. However, our solution requires only 1-cycle latency instead of at least two cycles of latency that characterizes the current DOM and HPC2; it is thus clearly a matter of trade off between latency and randomness. Another application could be to lower the latency of an HPC2-based construction by 'kickstarting' the S-boxes: after 1, 2, 3 rsp. 4 cycles, one can obtain with HPC2 gadget values of algebraic degrees 1, 2, 3 rsp. 5 in the input bits due to their asymmetric latency of 1 rsp. 2 in their inputs. Replacing just all HPC2 gadgets in the first layer with our gadget can save one cycle latency, as the achievable algebraic degrees are then 2, 3, 5 rsp. 8. This can be done, for example, for the optimized PRESENT S-box of fig. 6b of [6] to regain the better latency of the DOM-based construction. If additionally all S-box inputs that are added to the PRESENT S-Box outputs are refreshed before with a robust mask refresh, the resulting circuit becomes robust probing secure for, we believe, a moderate increase in area.

5 | CONCLUSIONS

In this work, we have derived a new robust−t−SNI construction for multiplying two secrets in a robust strongly non-interferent way. The novel construction has 1-cycle input-to-output latency and, for low security degrees t, the randomness complexity is comparable with conventional, 2-cycle-latency approaches. As a future work, we plan to study the use of the proposed gadget in the S-boxes of known cryptographic algorithms as well as the randomness requirements for higher t. In particular, preliminary work shows that a scheme that involves 42 randoms for $t = 5$ is possible, but we believe this not to be the lowest bound achievable.

ACKNOWLEDGEMENT

None.

CONFLICT OF INTEREST

None.

PERMISSION TO REPRODUCE MATERIALS FROM OTHER SOURCES

None.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are openly available in https://github.com/vzaccaria/maskverif.docker.

ORCID

Maria Chiara Molteni https://orcid.org/0000-0003-2901-2972

Vittorio Zaccaria https://orcid.org/0000-0001-5685-9795

REFERENCES

1. Chari, S., et al.: Towards sound approaches to counteract power-analysis attacks. In: Wiener, M. (ed.) Advances in Cryptology — CRYPTO '99. Lecture Notes in Computer Science, pp. 398–412. Springer, Berlin (1999)
2. Ishai, Y., Sahai, A., Wagner, D.: Private circuits: securing hardware against probing attacks. In: Boneh, D. (ed.) Advances in Cryptology — CRYPTO 2003. Lecture Notes in Computer Science, pp. 463–481. Springer, Berlin (2003)
3. Faust, S., et al.: Composable masking schemes in the presence of physical defaults: the robust probing model. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(3), 89–120 (2018)
4. Meyer, L.D., Bilgin, B., Reparaz, O.: Consolidating security notions in hardware masking. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2019(3), 119–147 (2019)
5. Coron, J.S.: Higher order masking of look-up tables. In: Nguyen, P.Q., Oswald, E. (eds.) Advances in Cryptology — EUROCRYPT 2014. Lecture Notes in Computer Science, pp. 441–458. Springer, Berlin (2014)
6. Cassiers, G., et al.: Hardware private circuits: from trivial composition to full verification. IEEE Trans. Comput. (2020). https://doi.org/10.1109/TC.2020.3022979
7. Barthe, G., et al.: Strong non-interference and type-directed higher-order masking. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. CCS '16, pp. 116–129. ACM, New York (2016)
8. Bloem, R., et al.: Formal verification of masked hardware implementations in the presence of glitches. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology — EUROCRYPT 2018. Lecture Notes in Computer Science, pp. 321–353. Springer International Publishing (2018)
9. Belaïd, S., Goudarzi, D., Rivain, M.: Tight private circuits: achieving probing security with the least refreshing. In: Peyrin, T., Galbraith, S., (eds.) ASIACRYPT (2). vol. 11273 of Lecture Notes in Computer Science, pp. 343–372. Springer, Switzerland (2018)
10. Moos, T., et al.: Glitch-resistant masking revisited: or why proofs in the robust probing model are needed. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2019(2), 256–292 (2019)
11. Nikova, S., Rijmen, V., Schläffer, M.: Secure hardware implementation of nonlinear functions in the presence of glitches. J. Cryptol. 24(2), 292–321 (2011)
12. Cassiers, G., Standaert, F.X.: Trivially and efficiently composing masked gadgets with probe isolating non-interference. IEEE Trans. Inf. Forensics Secur. 15, 2542–2555 (2020)
13. Barthe, G., et al.: maskVerif: automated verification of higher-order masking in presence of physical defaults. In: Sako, K., Schneider, S., Ryan, P.Y.A. (eds.) ESORICS (1). vol. 11735 of Lecture Notes in Computer Science, pp. 300–318. Springer, Switzerland (2019)
14. Bertoni, G., Martinoli, M., Molteni, M.C.: A methodology for the characterisation of leakages in combinatorial logic. J. Hardw. Syst. Secur. 1(3), 269–281 (2017)
15. Reparaz, O., et al.: Consolidating masking schemes. In: Gennaro, R., Robshaw, M. (eds.) Advances in Cryptology — CRYPTO 2015, vol. 9215, pp. 764–783. Springer, Berlin (2015)
16. Gross, H., Mangard, S., Korak, T.: An efficient side-channel protected aes implementation with arbitrary protection order. In: Handschuh, H. (ed.) Topics in Cryptology – CT-RSA 2017. Lecture Notes in Computer Science, pp. 95–112. Springer International Publishing, Switzerland (2017)
17. Gross, H., Mangard, S.: A unified masking approach. J. Cryptogr. Eng. 8(2), 109–124 (2018)
18. Belaïd, S., et al.: Randomness complexity of private circuits for multiplication. In: FischlinJean, M., Coron, J.S., (eds.) EUROCRYPT (2). vol. 9666 of Lecture Notes in Computer Science, pp. 616–648. Springer, Switzerland (2016)
19. Molteni, M.C., Zaccaria, V.: On the spectral features of robust probing security. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2020, 24–48 (2020)
20. Groß, H., Mangard, S., Korak, T.: Domain-oriented masking: compact masked hardware implementations with arbitrary protection order. In: Bilgin, B., Nikova, S., Rijmen, V. (eds.) Proceedings of the ACM Workshop on Theory of Implementation Security, TIS@CCS 2016, p. 3. ACM, Vienna, October 2016

How to cite this article: Molteni, M.C., Pulkus, J., Zaccaria, V.: On robust strong-non-interferent low-latency multiplications. IET Inf. Secur. 1–6 (2021). https://doi.org/10.1049/ise2.12048