An Estimator for the ASIC Footprint Area of Lightweight Cryptographic Algorithms

Honorio Martin, Pedro Peris-Lopez, Juan E. Tapiador, and Enrique San Millan

Abstract—In resource-constrained devices such as RFID tags or implantable medical devices, algorithm designers need to make careful choices to ensure that their proposals are sufficiently efficient for the target platform. A common way of expressing such restrictions is in terms of an upper bound for the maximum available footprint area in gate equivalents (GE). For example, RFID tags conforming to standards EPC Class-1 Generation-2 and ISO/IEC 18006-C can devote up to 4K GE to security functions. However, in most cases algorithm designers are not hardware experts, nor they have any quantitative means to find out how much area their designs would occupy in a given technology. In this paper, we attempt to fill this gap by providing an estimate of the upper bound for the footprint area of any algorithm. Our approach takes into account the main components of such algorithms, namely basic arithmetic/logic operations and additional hardware such as registers and multiplexers. We believe that our proposal can help designers in making informed decisions about what kind of algorithmic structures can be afforded for a target environment.

Index Terms—ASIC implementations, Footprint area, RFID, VHDL, Lightweight algorithms.

I. INTRODUCTION

RADIO Frequency Identification (RFID) technology, which uses radio signals for automatic identification, has experienced a notable growth in the last years. An RFID tag responds to a reader request by using the radio channel and including in its answer a value that allows its unequivocal identification. This value is generated by the tag and should be protected to guarantee the privacy of the tag holder. The security of RFID systems is a challenging problem, particularly for low-cost devices such as those covered by the EPC Class-1 Generation-2 [1] and ISO/IEC 18000-6C [2] standards. This is usually achieved by incorporating some cryptographic modules [3], [4], [5] upon which security services can be provided through different protocols (see, e.g., [6], [7], [8]).

A major difficulty in providing RFID tags with security functions comes from the scarcity of computational resources available in such platforms (see, e.g., [9], [10], [11] for recent developments in the design of tiny tags). For example, in a low-cost RFID tag the Gate Equivalents (GE) that can be allocated to security issues have to be in the range between 250 and 4K GE, which restricts affordable solutions to lightweight algorithms only.

Proposals in the area of lightweight cryptography have proliferated over the last years, but most of them do not provide results regarding their implementation. In many cases, arguments in favor of their lightweightness are based on the use of some operations that are generally considered inexpensive. However, this assumption is not always true, and the implementation of some proposals have shown that the area limit of 4K GE is often surpassed. In other cases, the design turns out to be not so lightweight because of factors such as the bit length of the variables, the need for additional memory blocks—which is usually missed in the analysis of resources—, and the overhead imposed by selection and control logic. These and other aspects often make the final gate count much higher than expected.

All in all, providing accurate estimates of the footprint area of an ASIC implementation is a hard task for algorithm designers [13], [14]. More often than not, designers do not have the hardware design skills nor the tools required to implement and analyze their proposals. Furthermore, there is a lack of a standard methodology to provide such an estimation, as the result will vary depending on factors such as the chosen architecture, the manufacturing technology, the possibility of introducing optimizations at various levels, etc. Problems such as this are common in other related areas. For example, designing low-power embedded systems [15], [16] is also a major problem nowadays, and system designers face a situation similar to that described above. Very recently, Ben Atitallah et al. [17] have presented a methodology to provide designers with an estimation of the power consumption of a complete system. Similarly, in this paper we propose a relatively simple estimator for the footprint area occupied by the ASIC implementation of an algorithm. The suggested formula requires the designer to know only a few high-level details about the target implementation, such as the number of registers used to store inputs, outputs and intermediate variables, and some parameters related to the control structures. In principle, our work is motivated by and focussed on lightweight cryptographic algorithms for constrained platforms such as RFID tags or implantable medical devices. Despite this, we believe our approach could be easily extended to non-security designs by incorporating additional factors into our methodology.

The rest of this paper is organized as follows. In Section II we provide an overview of the main basic operations that can be used in lightweight algorithms, and in Section III we show the hardware architectures employed to implement them. Section IV discusses our results synthesizing basic operation blocks using two real manufacturing libraries. Subsequently, in

H. Martin and E. San Millan are with Department of Electronics Technology, Universidad Carlos III de Madrid, 28911 Leganés, Madrid, Spain. E-mail: {hmartin, quique, entrena}@ing.uc3m.es
P. Peris-Lopez and J.E. Tapiador are with the Department of Computer Science, Universidad Carlos III de Madrid, Avda. Universidad 30, 28911 Leganés, Madrid, Spain. e-mail: {pperis, jestevez}@inf.uc3m.es

Atitallah
Section V we present a method to estimate the footprint area of a whole algorithm and discuss our experimental results with a battery of real-world examples. Finally, Section VI concludes the paper and summarizes our main contributions.

II. ELEMENTS IN LIGHTWEIGHT CRYPTOGRAPHY

In this section, we shortly introduce the usual operations found in lightweight cryptographic primitives and protocols. This will serve to motivate our subsequent footprint analysis for individual building blocks.

A. Basic Operations

As in the case of regular security functions, lightweight cryptographic primitives and protocols aim at providing basic constructions to guarantee properties such as the confidentiality, integrity and authenticity of data exchanged in communications. In this case, however, the shortage of resources in the platforms severely limits the sort of processing that can be done. Thus, most proposals attempt to rely only on a few bitwise operations (e.g., XOR, OR, AND, shifts and rotations) and inexpensive arithmetics such as addition modulo $2^m$.

In [18] a short of mapping called triangular functions (T-functions) was introduced. In particular, a T-function is kind of $p \times p$ mapping that does not propagate information (i.e., for each $0 \leq i \leq p$, the $i$-th bit of the output is a function of the current and previous input bits $0, 1, \ldots, i$). Bitwise operations (e.g., NOT, exclusive-OR, OR and AND) and many others found in modern processors (e.g., addition, subtraction and multiplications) are T-functions. Furthermore if T-functions are mixed, the result is also a T-function.

Secure cryptographic primitives and protocols cannot be designed by exclusively using T-functions. A T-function has poor diffusion as it does not propagate information from right to left, and its period is predictable [19]. As a consequence, T-functions are not the only operations that are usually found on lightweight cryptographic algorithms. For instance, in [20], [21] sound arguments are given for mixing triangular and non-triangular functions in order to design more secure ultra-lightweight protocols.

One of the most common non-triangular function used in cryptography is the rotation operation. Rotation can be performed in several ways. For instance, $\text{rot}^x(x, y)$ causes that the bits of $x$ to be circular shifted to the left by a number of positions fixed as it does not propagate information from right to left, and its period is predictable [19]. As a consequence, T-functions are not the only operations that are usually found on lightweight cryptographic algorithms. For instance, in [20], [21] sound arguments are given for mixing triangular and non-triangular functions in order to design more secure ultra-lightweight protocols.

B. Storage and Control

Apart from arithmetic and logical operations, algorithms also require additional hardware resources to store results and to control the execution flow. Such elements are nearly always registers and multiplexers. Registers help to maintain the "state" of the algorithm by storing intermediate and final results, and also by supporting the control functions. Multiplexers are used to select among different inputs according to some condition, and are instrumental in any algorithm that incorporates a minimum flow complexity (i.e., loops, ifs, etc.).

In general, the area occupied by registers and multiplexers is critical, and any good design should find a balance between the amount of basic operations and memory/control logic. It is quite common to find proposals where authors only analyze the complexity of their designs by counting the amount of operations only. While this might be useful to determine the time complexity of the algorithm, ignoring memory and control requirements could be very misleading in terms of the footprint area of the circuit. In fact, in many cases the area required by these elements is much larger than that demanded by the arithmetic and logical components.

III. HARDWARE IMPLEMENTATION OF BASIC OPERATIONS

We next analyze various design elements and their area estimation depending on the complexity of their implementation. For low-complexity blocks, we propose a simple architecture, while for those with higher complexity we study and propose several possible architectures.

A. Elements with Low Complexity Implementation

In this group we include some T-functions such as simple bitwise operations and addition $\mod 2^m$. Registers and multiplexers are also in this category. Each of these elements has a straightforward implementation with very low complexity.

Although it is common to find implementations for 96 bits, as it is a common bit length widely used in low-cost RFID tags (e.g., tags compliant with EPC Gen-2 standard), we study these elements specifically for different number of bits, obtaining a constant $K$ for each basic element. These constants will be subsequently used to obtain area estimations for more complex constructions.

For the above mentioned bitwise operations, we can use a strategy to reduce the area cost with a penalty in throughput. This strategy consists in reducing the bit length of the block and consuming several clock cycles to obtain the final result. For example, in an algorithm that uses an $N$-bit XOR block, it can be reduced to a block of $N/2$ bits but needing two clock cycles to obtain the result. We note that the reduction of a block involves the use of additional multiplexers for the control logic. Thus, we need to find a trade-off between the reduction and the necessary extra logic. Moreover, the drop in throughput has to be taken into consideration, as it should always meet the restrictions imposed by the operational environment. For instance, taking as reference the performance criteria of an RFID system that demands a minimum reading speed of at least 150 tags per second [22], [23], we need to carefully calculate the reduction of the block to fulfill this reading rate requirement. Note, that this reduction strategy can be used with other operations such as adders and the rest of bitwise operations.
For illustration purposes, in Fig. 1(a) we show the scheme of an $N$-bit XOR block. Fig. 1(b) shows the result after halving the XOR block ($N/2$ bits) and introducing additional multiplexers to select inputs and outputs.

**B. Multiplication Operation**

In this section we study the multiplication operation. There are several possible hardware architectures for its implementation, including: 1) a combinational architecture; 2) a shift-and-add architecture; and 3) the Karatsuba-Ofman architecture [24], [25].

1) Classical Combinational Multiplication: The straightforward approach to implement a multiplier consists on the usage of combinational logic only. The operation can be split into partial multiplications and additions to sum the partial results. From the point of view of throughput the solution is the fastest that can be achieved with the penalty of having high cost regarding the size of the circuit. Fig. 2 shows the needed hardware to implement a $4 \times 4$ bit multiplier of unsigned binary operands.

In Fig. 3, we show the internal structure of a basic cell. This cell include a Full Adder (FA) and an AND gate. The AND gate computes the product of each bit of the multiplier $q_j$ with the corresponding bit of the multiplicand $m_j$. The output of this product is one of the inputs to the FA. The remaining operands are the corresponding bit from the previous partial product ($P_{pi}$) and the carry ($c$) generated in the previous stage.

2) Classical Shift and Add Multiplication: We can economize the consumed hardware in the combinational approach by iterating the multiplication of the multiplicand by each bit of the multiplier and storing partial results in a register. Since in each iteration the multiplier is a power of two the partial multiplications can be implemented by shifting left a register, which is very efficient regarding clock cycles consumed. To complete the architecture, as shown in Fig. 4, we need an adder to sum all the partial multiplications and the whole process is under the supervision of the control unit. This approach results very efficient in terms of the consumed hardware but offers a low throughput due to its iterative quality. More precisely, assuming long-bit operands of length $N$, this architecture consumes $N$ clock cycles.

3) Karatsuba-Ofman: Karatsuba Ofman algorithm [24] achieves a trade-off between the chip area and the consumed clock cycles. It is based on diving the problem ($2n$-bit multiplication) into smaller sub-problems ($n$-bit multiplication and several $n$-bit additions and subtractions).

Let assume two integers $X$ and $Y$ of length $2n$, which can be divided into a highest part (i.e., $X_H$ and $Y_H$) and the a lowest part (i.e. $X_L$ and $Y_L$) of length $n$. Then, these integers can be computed by the addition of these two components:
The product of 2n bits operands $X$ and $Y$ can be computed by executing $n$-bit multiplications between the highest and lowest parts of the operands as shown below:

$$X \times Y = (X_H \cdot 2^n + X_L) \times (Y_H \cdot 2^n + Y_L) = 2^{2n}(X_H Y_H) + 2^n(X_H Y_L + X_L Y_H) + X_L Y_L \quad (3)$$

As a final twist, the second element of the above equation can be represented in terms of the first and third element:

$$X_H Y_L + X_L Y_H = (X_H + X_L)(Y_H + Y_L) - X_H Y_H - X_L Y_L \quad (4)$$

Taking into account all the above, Karatsuba-Ofman algorithm computes the multiplication of 2n bits operands by calculating three n-bit multiplications:

$$X \times Y = 2^{2n}(X_H Y_H) + X_L Y_L + 2^n(X_H + X_L)(Y_H + Y_L) - X_H Y_H - X_L Y_L \quad (5)$$

C. Modulo Reduction

This operation is commonly used in modular multiplications or even in rotations like $\text{rot}^n(x, y)$. The hardware needed for its implementation depends on the value of the modulo. Given two positive numbers $P$ (dividend) and $N$ (divisor), $P \mod N$ outputs the remainder of the division of $P$ by $N$. This operation is considered lightweight when $N$ is a multiple of $2^n$ because the division can be executed by shifting to the right. Nevertheless, $N$ may not be a multiple of $2^n$ and for this reason we present an implementation that allows the computation of the modulo for each value $N$.

The modulo operation requires the computation of a division, which is a more complex operation than the multiplication. One straightforward algorithm is the Naive Reduction. This algorithm shifts and substracts the modulus until the remainder is obtained. A subtractor, a comparator and $n$-bit register are the only the hardware needed for its implementation, but it consumes a large amount of clock cycles ($2^n$). Alternatively, if we are wealthy in resources we can use the Non Restoring Reduction (see Fig. 5), which is much more efficient but consumes more hardware. In this case, the modulo is obtained in approximately $n$ steps.

![Fig. 5. Non Restoring Reduction Algorithm](image)

Sometimes, a combination of a multiplication and a modulo reduction can be found in some algorithms. There are special implementations to optimize these combinations, usually involving the Montgomery modular multiplication scheme and different possible architectures [26]. As this kind of operations are often not lightweight, we will not study them in detail in this paper.

IV. AREA RESULTS FOR LOW-COMPLEXITY ELEMENTS

As discussed above, one major goal of this work is to provide an estimation of the area required by a lightweight cryptographic algorithm as a function of some high-level parameters. In these applications, it is crucial to keep in mind that circuits predominantly operate at low frequencies. For instance, many RFID tags function at 100 KHz. (Note that the 100 kHz frequency refers to the clock included in the tag circuit, not to the communication band that is generally in the 860-960 MHz range for EPC C1-G2 tags.) As the clock frequency is fixed, most restrictions in these designs relate to area and power consumption.

In this paper, we report results obtained with two specific manufacturing libraries. A priori, it is unclear to us the extent to which our conclusions generalize to other manufacturing technologies. The results, however, are still useful to compare different algorithms and classify them as lightweight or not. Furthermore, the methodology is general and can be easily extended to other libraries.

A. Experimental Framework

The experimentation has been conducted with two CMOS libraries: Faraday UMC 90 nm [27] and AMI 0.35 $\mu$m [28].
TABLE I
GEs FOR LOW-COMPLEXITY ELEMENTS

<table>
<thead>
<tr>
<th>Lib.</th>
<th>Element</th>
<th>32 bits</th>
<th>64 bits</th>
<th>96 bits</th>
<th>128 bits</th>
<th>$K_{1}$</th>
<th>$K_{2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>UMC 90nm</td>
<td>AND</td>
<td>39.70</td>
<td>79.39</td>
<td>119.08</td>
<td>158.78</td>
<td>$K_{1}=1.24$</td>
<td>$K_{2}=1.24$</td>
</tr>
<tr>
<td></td>
<td>OR</td>
<td>39.70</td>
<td>79.39</td>
<td>119.08</td>
<td>158.78</td>
<td>$K_{1}=1.24$</td>
<td>$K_{2}=1.24$</td>
</tr>
<tr>
<td></td>
<td>XOR</td>
<td>79.39</td>
<td>158.78</td>
<td>238.17</td>
<td>317.56</td>
<td>$K_{1}=2.48$</td>
<td>$K_{2}=2.48$</td>
</tr>
<tr>
<td></td>
<td>ADD</td>
<td>239.66</td>
<td>477.84</td>
<td>716.01</td>
<td>954.19</td>
<td>$K_{1}=4.45$</td>
<td>$K_{2}=4.45$</td>
</tr>
<tr>
<td></td>
<td>Multiplexer</td>
<td>71.00</td>
<td>143.00</td>
<td>214.00</td>
<td>285.81</td>
<td>$K_{mux}=2.23$</td>
<td>$K_{mux}=2.23$</td>
</tr>
<tr>
<td></td>
<td>Register</td>
<td>147.00</td>
<td>287.00</td>
<td>441.00</td>
<td>588.24</td>
<td>$K_{reg}=4.39$</td>
<td>$K_{reg}=4.39$</td>
</tr>
<tr>
<td>AMI 0.35 m</td>
<td>AND</td>
<td>42.66</td>
<td>85.33</td>
<td>127.99</td>
<td>170.64</td>
<td>$K_{1}=1.33$</td>
<td>$K_{2}=1.33$</td>
</tr>
<tr>
<td></td>
<td>OR</td>
<td>53.33</td>
<td>106.65</td>
<td>160.03</td>
<td>213.22</td>
<td>$K_{1}=1.66$</td>
<td>$K_{2}=1.66$</td>
</tr>
<tr>
<td></td>
<td>XOR</td>
<td>74.66</td>
<td>149.34</td>
<td>224.00</td>
<td>298.70</td>
<td>$K_{1}=2.33$</td>
<td>$K_{2}=2.33$</td>
</tr>
<tr>
<td></td>
<td>ADD</td>
<td>203.35</td>
<td>406.00</td>
<td>608.69</td>
<td>811.32</td>
<td>$K_{1}=6.34$</td>
<td>$K_{2}=6.34$</td>
</tr>
<tr>
<td></td>
<td>Multiplexer</td>
<td>85.33</td>
<td>170.66</td>
<td>256.00</td>
<td>341.55</td>
<td>$K_{mux}=2.66$</td>
<td>$K_{mux}=2.66$</td>
</tr>
<tr>
<td></td>
<td>Register</td>
<td>214.33</td>
<td>435.66</td>
<td>651.66</td>
<td>869.00</td>
<td>$K_{reg}=6.77$</td>
<td>$K_{reg}=6.77$</td>
</tr>
</tbody>
</table>

One key reason behind this decision is that these libraries provide comprehensive information about the layout of basic cells. For our purposes, this is essential to obtain a realistic estimate of the area occupied by an algorithm. To synthesize each design we used Synopsys [29], which is one of the most commonly used synthesizers.

The operation frequency is set to 100 KHz. As mentioned before, this is quite a common value for passive RFID tags. Power supply is fixed by the library (1.2 V). As for the synthesis with Synopsys, after experimenting with different configurations we observed that the best results are obtained with the medium effort option in area, delay and power consumption. These options are set for all the experiments.

Finally, the area results are provided using Gate Equivalents (GEs), which is the normalization commonly used for these applications. Using GEs facilitates comparisons among different implementations since the obtained values are independent of the chosen technology. To compute the GE value, the area of the whole circuit is divided by the area of a basic NAND gate. For example, 1 GE for the UMC 90 nm takes 3.16 $\mu$m².

B. Results

Table I summarizes the area results (in GEs) obtained after synthesizing with Synopsys the set of basic elements for UMC 90 nm and AMI 0.35 $\mu$m libraries. In this first analysis, the hardware architecture considered performs all operations (combinational or just registers) in one clock cycle. As shown in Fig. 6, the area occupied by each element increases linearly in the length (in bits) of the variables. The results obtained for the AMI 0.35 $\mu$m library are almost equivalent and follow a similar pattern. This simplifies considerably the analysis of more complex algorithms, as it allows us to associate a constant value, named $K_i$ for element $i$, giving the area per bit for each element.

From these results we can extract some conclusions:

1) The adder occupies significantly more area than bitwise operations. Consequently, if the area of an algorithm needs to be optimized, it is more appropriate to focus on additions rather than concentrating on low complexity elements such as bitwise operations. As all operations are done in one clock cycle, one possibility to optimize the area would be to use an element with lower bit length and carry out the operation in various clock cycles. For example, variables can be split into two parts with half of the bits each and a half-length adder can then be applied over each part. Note, however, that in doing this we need to include additional elements, namely registers to store partial results, multiplexers to choose between different signals, etc.

2) The area cost of registers is also noticeable. Taking into account that we generally can devote just a small area to security subsystems (e.g., up to 4K GEs in most passive RFID tags), and that roughly 50% of it is used for storage, this means that at most five 96-bit registers could be used.

3) As for multiplexers, their cost in terms of area is small. These elements are needed in algorithms with loops (e.g., “for” and “while” iterations) and also when a input/output is selected among different signals.

Overall, it can be concluded that designers will necessarily face some trade-offs among operations and the amount of registers and multiplexers required. As a general rule, bigger building blocks (i.e., using a larger bit length) will require less extra registers/multiplexers, and vice versa.

C. Further Operations: Multiplication and Modulo Reduction

We next explore the area required by two operations that have been extensively used in many cryptographic algorithms: multiplication and reduction modulo $N$. The figures, both the number of GEs and the associated clock cycles required to complete the operation, are shown in Table II for the UMC 90 nm and the AMI 0.35 $\mu$m libraries.

In general terms, multiplication cannot be regarded as a lightweight operation no matter what architecture is chosen, since it demands more than the 4K GEs often required in environments such as RFID systems (96 bits). That being said,
it is worth-noting that some trade-offs also appear here. The combinatorial architecture offers the best performance speedwise, but it demands too much area. Conversely, the Shift-and-Add option is much more efficient in terms of area, but the number of clock cycles required may be prohibitive for many applications. K-O architectures fall somewhere in between of these two alternatives.

Modulo reduction is a special case. As discussed before, it is very lightweight when the bit length $N$ is a power of two, as it can be implemented simply as various right shifts. Otherwise, such as for example for $N = 96$, its area takes around 4K GEs. Thus, our recommendation is to include it only when the resources required by this operation can be reused in other parts of the algorithm.

V. ESTIMATING THE AREA OF LIGHTWEIGHT ALGORITHMS

Estimating the area that an implementation of an algorithm can occupy is quite challenging because it depends on many factors: the architecture(s) chosen by the designer, the specific constraints, the manufacturing library, the basic cells used by the synthesis tool, etc. In this section, we first propose an expression that estimates the total area required by a hardware implementation of an algorithm. Subsequently, we check its validity by comparing its predictions with the actual area obtained with a battery of examples and provide a refinement of our estimator. Note that we have discarded the use of multiplication since this operation consumes resources in excess (>4K GEs) to be categorized as a lightweight operation. Regarding modulo reduction, its usage in a lightweight algorithm is conditioned to be a power of two (i.e. $2^n$); otherwise it demands more than 4K GEs and using it is infeasible. In case of being a power of two, the operation does not consume any extra hardware resources, but requires an upper bound of $n$ clock cycles to compute it.

A. A Linear Estimator

The total area occupied by an algorithm can be roughly divided into two main blocks: datapath and control. The datapath contains the hardware for the different operations required and registers to store inputs, outputs and intermediate results. In many lightweight cryptographic algorithms, the datapath accounts for a significant fraction of the total area, generally around 80% [30] [31].

Our estimate is based on the following rationale. As we previously pointed out, the final footprint depends on the chosen architecture. In turn, opting for one architecture or another depends on the goals and restrictions faced by the designer. For example, in very constrained devices (such as RFID tags or some sensor nodes) minimizing the area is a priority, which heavily influences the decision. Since throughput is often a limiting factor too, one sensible choice is an architecture that optimizes the area without penalizing throughput too much. In general, such a design contains only single block of $N$ bits for each basic operation needed, plus registers to store data and multiplexers to select inputs and outputs.

Based on the previous considerations, we propose a simple linear estimate for the area of the datapath, measured in GE, as a function of the bit length and the number of basic operations, registers and multiplexers:

$$F_{DP} = N \cdot \left[ \sum_{i=1}^{4} A_i \cdot K_i + (B \cdot K_{reg}) + (C + D) \cdot K_{mux} \right]$$ (7)

where:
- $N$ is the bit length of the variables.
- $A_i$ is a parameter dependent on the chosen architecture for the datapath ($i = 1$ for AND, $i = 2$ for OR, $i = 3$ for XOR, and $i = 4$ for ADD). As discussed above, the implementation can range from a fully combinational design to one using smaller operators but requiring more clock cycles. Thus, we measure $A_i$ as the number of $N$-bit operators.
- $K_i$ is the area cost for the $i$-th operation, as shown in Table I.
- $B$ is the number of variables that require storage.
- $K_{reg}$ is the area cost for each register.
- $C$ is the number of multiplexers necessary to select different inputs for the operation blocks. When the block has more than two inputs, $C$ is the number of inputs minus one.
- $D$ is the number of multiplexers necessary to select different inputs for each register. If the algorithm is given in pseudocode, $D$ can be easily estimated as the number of assignments made for each variable.
- $K_{mux}$ is the area cost for the multiplexers.

Obviously, expression (7) only factors in those elements studied in Section IV. However, it can be extended without difficulty to any other blocks that conform to the design rationale given in the paragraph above.

Finally, as the area of datapath and control are in most cases related, we express the total area as:

$$F = (1 + \omega) \cdot F_{DP}$$ (8)
functions using (8), assuming a control overhead ω with 6 inputs. The dataset is well balanced, containing 10 functions with 2 inputs, 10 functions with 4 inputs, and another 10 functions with 6 inputs. Thus, choosing a high value for the number of bits. Each function returns a single final output value denoted Z and uses several input and intermediate variables, represented by X_i and Y_i, respectively. The dataset is well balanced, containing 10 functions with 2 inputs, 10 functions with 4 inputs, and another 10 functions with 6 inputs.

In Fig. 7 we compare the estimated area for all the datasets functions using (8), assuming a control overhead ω = 0.2, versus the actual area given by Synapsis after synthesizing each function. For simplicity, we only show the results obtained for the UMC 90 nm library. As suggested by Tables I and II, the results for the AMI 0.35 µm are completely equivalent, and our experimentation confirms this. The approximation is quite precise, with differences becoming greater when the number of bits N increases. In Fig. 8 we show histograms of the estimation errors for different bit lengths. For N = 32 and 16 bits, errors are bounded by 500 GE and 1K GE respectively. This error increases to 1.5K GE and 2K GEs for N = 96 and 128 bits, respectively. Thus, choosing a high value for the control overhead (20%) in Equation 8 does not minimize errors but guarantees an overestimation of circuit area.

Further investigations reveal that the overestimation does not come from expression (7), but from (8). In other words, the estimate for the datapath area is fairly accurate, but the amount of control logic does not generally increase linearly with the number of bits. For instance, a Finite State Machine (FSM) controlling some parts of an algorithm does not need more states when variables increase their size. That being said, we emphasize that our choosing of (8) may still be valid for constrained designs, where N often varies between 32 and 512, interpreting the result as an upper bound.

C. Adjusting control overheads

As discussed in Section V-A, the datapath and control areas are in most cases related. In the model presented above we made the assumption that the relation is linear, in particular with the control logic being a fraction (1 + ω) of the datapath area. The experimental results discussed above show that this assumption works relatively well for systems of up to 10K GE, particularly with ω = 0.2. The estimation error becomes more significant for bigger systems. This is reasonable, as an increase in the datapath footprint does not necessarily translate into a similar increase of control logic.

Using the dataset of designs described above, we have numerically investigated more precise approximations for the control overhead term used in (8). Two alternatives were explored, both based on the idea that ω varies with some system parameter. In the first one, we assumed that the control overhead depends on the number of bits N, so the total area is actually of the form:

\[ F = \left[ 1 + \omega(N) \right] \cdot F_{DP} \]  

whereas in the second alternative it is assumed that the amount of control logic is a function of the datapath area:

\[ F = \left[ 1 + \omega(F_{DP}) \right] \cdot F_{DP} \]  

The estimation of both functions ω(N) and ω(F_{DP}) was done by couching the problem as a nonnegative least-squares curve fitting one of the form:

\[ \min_{\Omega} \| C \Omega - d \|_2^2 \]  

Fig. 7. Real and estimated footprint area (ω = 0.2).

Fig. 8. Distribution of gate count estimation errors (ω = 0.2)
TABLE III  
NUMERICALLY ESTIMATED CONTROL OVERHEAD FUNCTIONS.

<table>
<thead>
<tr>
<th>$N$</th>
<th>$\omega(N)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>32 bits</td>
<td>0.1518</td>
</tr>
<tr>
<td>64 bits</td>
<td>0.1186</td>
</tr>
<tr>
<td>96 bits</td>
<td>0.1192</td>
</tr>
<tr>
<td>128 bits</td>
<td>0.1103</td>
</tr>
<tr>
<td>$|\text{residual}|_2^2$</td>
<td>3.36E+06</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$F_{DP}$</th>
<th>$\omega(F_{DP})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 2000 GE</td>
<td>0.1906</td>
</tr>
<tr>
<td>2000 - 4000 GE</td>
<td>0.1717</td>
</tr>
<tr>
<td>4000 - 6000 GE</td>
<td>0.1691</td>
</tr>
<tr>
<td>6000 - 8000 GE</td>
<td>0.1271</td>
</tr>
<tr>
<td>8000 - 10000 GE</td>
<td>0.1098</td>
</tr>
<tr>
<td>10000 - 12000 GE</td>
<td>0.0932</td>
</tr>
<tr>
<td>12000 - 14000 GE</td>
<td>0.0774</td>
</tr>
<tr>
<td>$|\text{residual}|_2^2$</td>
<td>1.38E+05</td>
</tr>
</tbody>
</table>

where $\Omega = (\omega_1, \ldots, \omega_k)^T$, with $\omega_i \geq 0$, represents the sought function discretized in $k$ values. Matrix $C$ and vector $d$ contain, respectively, the actual datapath area and total area obtained after synthesis.

We split the dataset of designs into two subsets. The first one, used to estimate the overhead function (training) contains 80 randomly chosen (10 of each bit length) designs out the 120 available. The remaining 40 designs will be subsequently used to test the obtained estimator. Thus, each one of the 80 synthesized functions used for training gives one equation for (11), which are grouped into $k$ bins. In the case of $\omega(N)$, we chose $k = 4$ values (32, 64, 96, and 128 bits), whereas for $\omega(F_{DP})$ we grouped equations into $k = 7$ intervals with a 2K GE difference between each of them.

Using a standard numerical solver, we obtained the $\Omega$-values shown in Table III. Again, these figures correspond to the UMC 90 nm library; those obtained for the AMI 0.35 $\mu$m are very similar. Such overheads represent the best fit, in a least-squares sense, for our experimental dataset. As observed, in both cases the actual overhead is always below the fixed $\omega = 0.2$ value that was used before. Furthermore, it decreases as circuits grow bigger, both in terms of $N$ and in datapath area, which conforms to our previous intuition. For example, in systems with less than 4K GE the overhead accounts for 16%-19% of the datapath area, but it falls down to less than 10% when the datapath is 10K GE or more. This is also observed when the overhead is considered a function of $N$.

Analysis of the squared 2-norm of the residual reveals that the $\omega(F_{DP})$ estimation performs significantly better than $\omega(N)$. Thus, while the former yields a squared residual of 1.38E+05, which roughly translates into an average error of 371 GE per design, the latter is greater by more than an order of magnitude (3.36E+06), meaning an error of around 1833 GE per estimation. This is also reasonable, as it appears to be more sensible that the amount of control logic depends more on the datapath area rather than on the length of registers.

Overall, using functional overheads such as these provide us with a more precise estimation of the total footprint area. For comparison with the plots discussed in previous section, Figs. 9 and 10 show the adjusted estimates for the training and test functions, respectively. Similarly, Fig. 11 shows the error distribution over test functions only. It is clear that the fit is now much more accurate (compare with Fig. 8), even though the new estimation cannot be regarded anymore as an upper bound for the total footprint area.

VI. CONCLUSIONS

In this paper, we have proposed a simple yet accurate procedure to estimate the footprint area of generic lightweight algorithms. We have argued that finding an accurate approximation is extremely hard, since it strongly depends on factors such as the architecture chosen by the designer, the manufacturing technology, the libraries used, the possibility of optimizing the footprint when combining several parts, etc. Despite this, the designer of algorithms for constrained environments (such as, for example, those related to cryptographic functions for RFID tags or sensor nodes) should count on some quantities to drive their choices. One major motivation for this work is to fill this gap by providing algorithm designers with a tool to estimate the cost, in terms of footprint area, of their constructions.
We believe our proposal will help in making some choices at the algorithmic level, even for designers without hardware design skills. Furthermore, it could also be applied to get preliminary comparisons among different proposals (lightweight primitives and more complex constructions such as security protocols) or, at least, to decide if they are simply too costly for certain operational environments.

The work presented in this paper can be extended in a number of ways. One natural direction for future work is the inclusion of other commonly used elements in the $F_{DP}$ estimator, such as for example S-boxes of non-linear filters. Similarly, we expect to test the proposed estimator against well-known lightweight cryptographic primitives and compare the predictions with reported experimental results. Finally, our focus in this work has been exclusively on the footprint area of ASIC implementations. It would be interesting to extend our estimates to include other prominent parameters, primarily throughput and power consumption, as these have also significant influence in design choices. Consider, for example, one the most used RFID standards [1], [2], where a tag must support up to 1500 read attempts per second under ideal conditions, although this rate can be five or ten times smaller (500-150 tags/sec) in real world environments [23]. Therefore, for a tag operating frequency of 100 KHz, the number of clock cycles consumed per reading is upper-bounded by 670 (in fact, 500 clock cycles is an upper bound commonly assumed in previous works [31], [32]). In principle, the methodology discussed in this work can be easily extended to incorporate measures of throughput and power consumption. We expect to tackle this in future work.

REFERENCES


