School of Electrical, Electronic & Computer Engineering

RTL Implementations of GF(2) and GF(4) Arithmetic Components

A.Rafiev, J.P.Murphy, A.Yakovlev

Technical Report Series

NCL-EECE-MSD-TR-2008-139

December 2008

Contact:

ashur.rafiev@ncl.ac.uk

j.p.murphy@ncl.ac.uk

alex.yakovlev@ncl.ac.uk

Supported by EPSRC grant GR/F016786/1

NCL-EECE-MSD-TR-2008-139

School of Electrical, Electronic & Computer Engineering,
Merz Court,
Newcastle University,
Newcastle upon Tyne, NE1 7RU, UK

`http://async.org.uk/`

RTL Implementations of GF(2) and GF(4) Arithmetic Components

A.Rafiev, J.P.Murphy, A.Yakovlev

December 2008

Abstract

Logic design for security application requires the use of specific encoding and higher radix elements thus implying an additional level of abstraction – a component level which is subsequently mapped into a gate level netlist. Implementation of particular components can be made in different ways, however RTL-based design of the multi-valued logic components is of more practical interest as it better integrates to the conventional EDA flow.

This report presents possible implementations of Galois Field arithmetic components using typical library cells and the estimation of their physical characteristics for AMS C35 (0.35μm) library. The proposed component design is suggested to be used in further research of multi-valued logic synthesis for security applications, particularly in mixed radix Reed-Muller expansions.

1 Introduction

The approach presented in this article is related with the research of optimisation techniques for cryptographic logic synthesis where the key qualities are power, area and security metrics. Security is considered in the scope of side-channel attacks, e.g. differential power analysis [10]. Data independent (balanced) switching of wires improves the resistance of the circuit against differential power analysis attacks [4, 11] and can be achieved using switching-balanced data encoding, e.g. m-of-n.

M-of-n codes are an encoding scheme in which data is represented using n wires and where m of them are set to an active level (usually high). A protocol separating data using dummy symbols (spacers) is called a *spacer protocol*. Circuits based on m-of-n codes, typically 1-of-4 or 1-of-2 (dual-rail), over the years have been used in a number of areas of electronics, in particular clockless circuits and networks-on-chip [2].

M-of-n codes other than dual-rail imply multi-valued logic (MVL) synthesis. Unfortunately the conventional EDA flow considers neither MVL synthesis nor encoding of data signals, hence it is not directly applicable for the security aware design. From this point of view the use of enhanced synthesis techniques is definitely more desirable, in particular the use of logic synthesis based on Galois field arithmetic which is natural for cryptography.

Galois field denoted as GF(p) is an algebraic structure consisting of a set of p elements and operations of addition and multiplication. Our work covers binary and quaternary Galois fields, namely GF(2) and GF(4). In GF(2) the operation of addition refers to the binary XOR operation, and the operation of

+	0	1	A	B
0	0	1	A	B
1	1	0	B	A
A	A	B	0	1
B	B	A	1	0

×	0	1	A	B
0	0	0	0	0
1	0	1	A	B
A	0	A	B	1
B	0	B	1	A

Figure 1: Addition and multiplication over GF(4)

multiplication refers to the binary AND. Denoting elements of GF(4) as 0, 1, A, and B, addition and multiplication over GF(4) can be defined as shown in Figure 1. Extended description and properties of Galois fields can be found in [3].

One of the known methods to synthesise MVL combinational circuits is based on higher radix Reed-Muller expansions. Computation of the quaternary Reed-Muller expansions over Galois fields of radix 4 has a long research history [5, 6, 7, 8, 9, 12]. These expansions are popular due to the efficiency of their hardware implementations and testability. These expansions have a form of the sum of products in Galois field arithmetic.

A computation algorithm gives the expansion in a form of mathematical equation. For mapping the RM expansions into the hardware the first task is to decompose the expressions into the operations of multiplication ($x \cdot y$), addition ($x + y$), multiplication by a constant (cx), and addition of a constant ($x + c$) over GF(2) or GF(4), where x, y are 2-valued or 4-valued variables; c is a constant value. Each of these operations corresponds to an arithmetic component. A component level of abstraction is the representation of the circuit using components as basic elements.

The efficient mapping from the component level of abstraction into a gate level netlist becomes a significant problem since concrete gate level implementations of Galois field arithmetic components in different radices, encodings and trade-offs between balancing and power costs have different merits and demerits as discussed in Section 2. For example, efficient for data transfer multi-valued signals may introduce considerable overhead in the corresponding logic implementation. The target of this work is to develop security-aware implementations of the Galois field arithmetic components and estimate their physical characteristics. This will allow the different synthesis methods to be compared in terms of physical efficiency of the generated circuits.

This report is organised as follows. Section 2 presents implementations of GF(2) and GF(4) components describing the underlying methodology. Section 3 analyses and compares physical characteristics of the proposed components. The last section concludes the work.

2 Component implementation

Arithmetic components for GF(2) and GF(4) can be implemented in different ways with respect to the selected encoding for binary and quaternary signals. Single-rail is a typical binary representation of signals. However, the focus of the paper is switching balanced codes, in particular 1-of-2 (dual-rail) and 1-of-4. Dual-rail encodes binary values using 2 wires: 0 is encoded as 01, 1 as 10. 00 is a spacer value. Quaternary values can be encoded as shown in Table 1.

Since the primary attribute of m-of-n codes is a balanced switching, the components should also display this feature. Ideally, for cryptographic applications, the form and size of power signature of the

Table 1: Encoded quaternary values

value	single-rail	dual-rail	1-of-4
0	00	01 01	0001
1	01	01 10	0010
A	10	10 01	0100
B	11	10 10	1000
spacer (NULL)	–	00 00	0000

component should be symmetric with respect to switching from a spacer to any data and vise versa. Usually this is made by introducing additional dummy-logic paths. However for real life examples an ideal symmetry is impossible, but the components can be "fully balanced" with respect to the technology capabilities.

Generic approaches for m-of-n codes over Galois fields are patented in [15]. In this report we concentrate on using RTL design flow, thus the described implementations are built using typical RTL cells.

2.1 GF(2)

Single-rail encoded GF(2) addition is simply an XOR gate and GF(2) multiplication is an AND gate. Hence their dual-rail implementations are known from the research of the dual-rail encoded binary logic [14, 13]. However these components are described in details within this section in order to provide simple examples of power-balancing for security applications.

According to [13], dual-rail AND and XOR gate have the mathematical representation shown in (1) and (2).

$$\begin{aligned} q_0 &= x_0 + y_0 \\ q_1 &= x_1 y_1 \end{aligned} \tag{1}$$

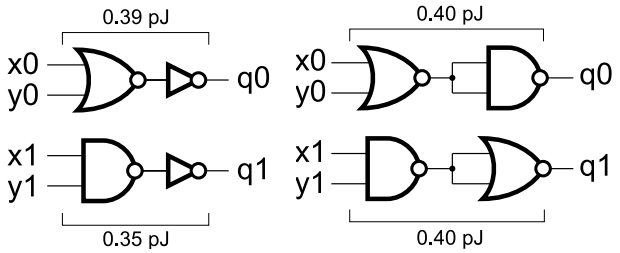
$$\begin{aligned} q_0 &= x_0 y_0 + x_1 y_1 \\ q_1 &= x_0 y_1 + x_1 y_0 \end{aligned} \tag{2}$$

where $\{q_0, q_1\}$ are wires of dual-rail encoded output, $\{x_0, x_1\}$ and $\{y_0, y_1\}$ are wires of dual-rail encoded operands x and y.

As most of the runtime libraries are based on the negative logic, these equations should be decomposed into NANDs and NORs. Mapping of the equation (1) into negative logic cells is shown in Figure 2(a). Switching the input $[x, y]$ from the spacer value to $[0,0]$, $[0,1]$ and $[1,0]$ causes NOR gate to fire. Switching from the spacer to $[1,1]$ fires NAND gate. NAND and NOR gates have different switching energy values thus the component balancing is not good in this case. Note that the switching energy values shown in the pictures in this section are taken from the library specification as discussed in the Section 3.

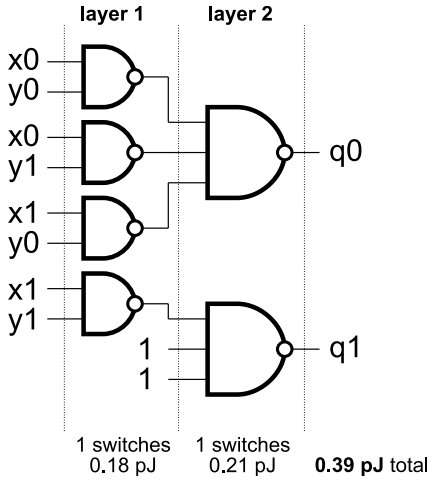
Figure 2(b) illustrates another suggestion for balancing based on replacing the inverters with a NAND and a NOR so the component form a symmetric structure with equalised switching energy. However the difference in gate delays introduces certain data dependency in the power signature of the component.

In order to balance it better we have to put additional logic paths making the structure of the component symmetric with respect to gates and input signals switching activity. The following equation is



(a) relaxed balancing

(b) relaxed balancing with equalised energy comsumption



(c) fully balanced

Figure 2: Dual-rail encoded GF(2) multiplication

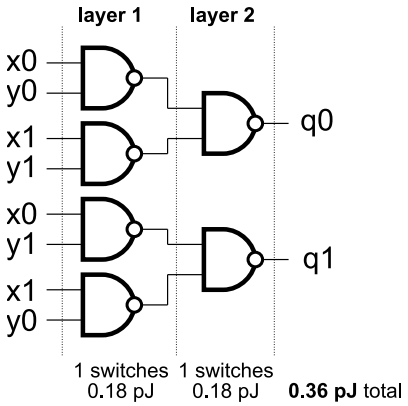


Figure 3: Dual-rail encoded GF(2) addition

derived from (1), and its gate level implementation is shown in Figure 2(c).

$$\begin{aligned} q_0 &= x_0y_0 + x_0y_1 + x_1y_0 = \overline{\overline{x_0y_0} \cdot \overline{x_0y_1} \cdot \overline{x_1y_0}} \\ q_1 &= x_1y_1 = \overline{\overline{x_1y_1} \cdot 1 \cdot 1} \end{aligned}$$

In the spacer state all inputs are set to low thus all outputs of 2-input NAND gates in the first layer are set to high precharging NAND gates in the second layer. Arrival of any data signal ($[0,0]$, $[0,1]$, $[1,0]$, or $[1,1]$) causes exactly one gate from the first layer to fire. This will produce only one 0 signal to the second layer switching one of the 3-input NANDs. Addition of constant inputs to certain gates guarantees that all gates in each layer are equal.

Although there are certain unavoidable aspects of the technology such as transistor level asymmetry which introduce little disbalance even to this design, an implementation is acceptable if it fits the requirements of the security standard [1]. For the same reason the structure shown in Figure 2(a) might also be sufficient since the difference in switching energy is not large. This implies the approach of "relaxed" balancing when the security is slightly compromised for significant power and area gains.

The equation for addition (2) implies switching balancing by construction. NAND gate implementation of this component is shown in Figure 3. However in [13] dual-rail XOR gate is implemented using complex gates. The reason is that the internal wires within the component are supposed to have equal capacitance in order to support overall power balancing in the component. This requirement introduces additional complexity for place and route task in scope of the design flow. Moreover, the use of complex gates is not always applicable. For example, GF(4) components presented in the next section imply complex gates of up to 14 inputs which definitely cannot be build using CMOS technology due to the transistor stack size constraints.

2.2 GF(4)

According to Figure 1 the operations of addition and multiplication over GF(4) are defined as shown in equations (3) and (4).

$$\begin{aligned} q_0 &= x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3 \\ q_1 &= x_0y_1 + x_1y_0 + x_2y_3 + x_3y_2 \\ q_2 &= x_0y_2 + x_1y_3 + x_2y_0 + x_3y_1 \\ q_3 &= x_0y_3 + x_1y_2 + x_2y_1 + x_3y_0 \end{aligned} \tag{3}$$

$$\begin{aligned} q_0 &= x_0 + y_0 \\ q_1 &= x_1y_1 + x_2y_3 + x_3y_2 \\ q_2 &= x_1y_2 + x_2y_1 + x_3y_3 \\ q_3 &= x_1y_3 + x_2y_2 + x_3y_1 \end{aligned} \tag{4}$$

An addition component has switching-balanced structure and can be used as it is. It's negative logic decomposition and switching analysis are shown in Figure 4.

As it can be seen from (4), the evaluation of q_0 differs from other signals thus the direct decomposition shown in Figure 5 is not properly balanced. Moreover, it is significant that the number of entries of each input signal in the set of equations determines the fanout of the corresponding intercomponent wire

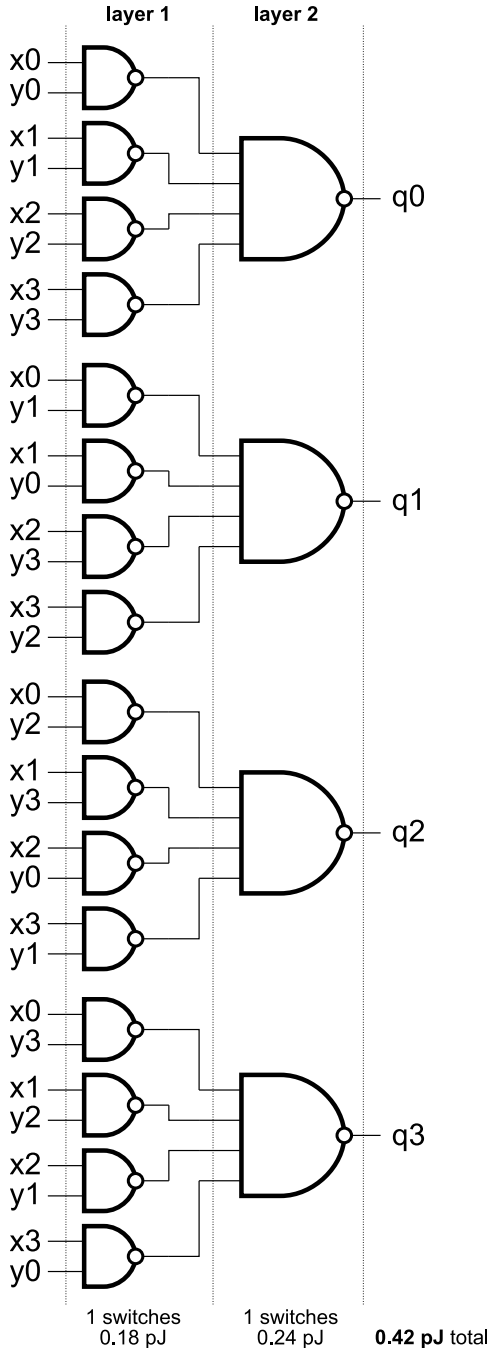


Figure 4: 1-of-4 encoded GF(4) addition

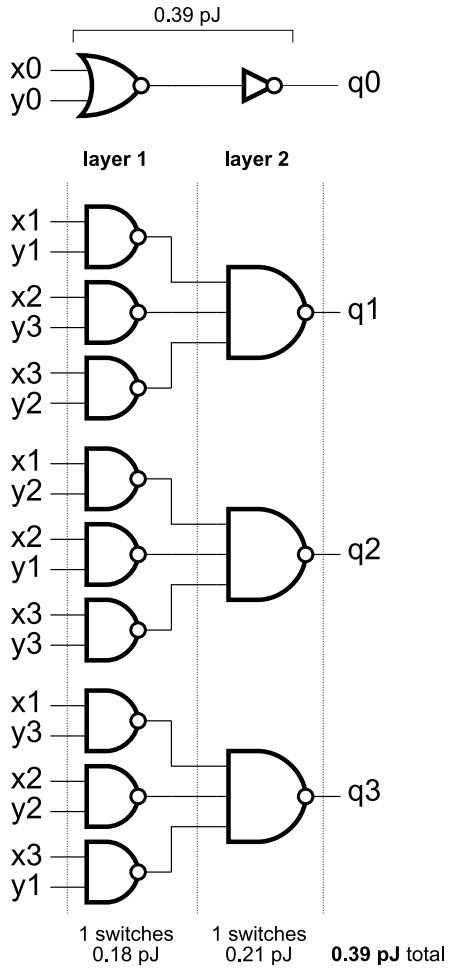


Figure 5: 1-of-4 encoded GF(4) multiplication, relaxed balancing

and directly affects its capacitance. A power-balanced 1-of-4 signal line is considered as a set of four physically equal wires. Therefore, in order to match security requirements, the number of argument entries should also be equalised:

$$\begin{aligned} q_0 &= x_0y_0 + x_0y_1 + x_0y_2 + x_0y_3 + x_1y_0 + x_2y_0 + x_3y_0 \\ q_1 &= x_1y_1 + x_2y_3 + x_3y_2 \\ q_2 &= x_1y_2 + x_2y_1 + x_3y_3 \\ q_3 &= x_1y_3 + x_2y_2 + x_3y_1 \end{aligned}$$

Fully balanced decomposition derived from this equation is shown in Figure 6.

3 Analysis

As it was mentioned in Section 1, the report is aiming at developing methods for security applied MVL synthesis. The underlying research necessitates the ability to estimate physical characterictics of the

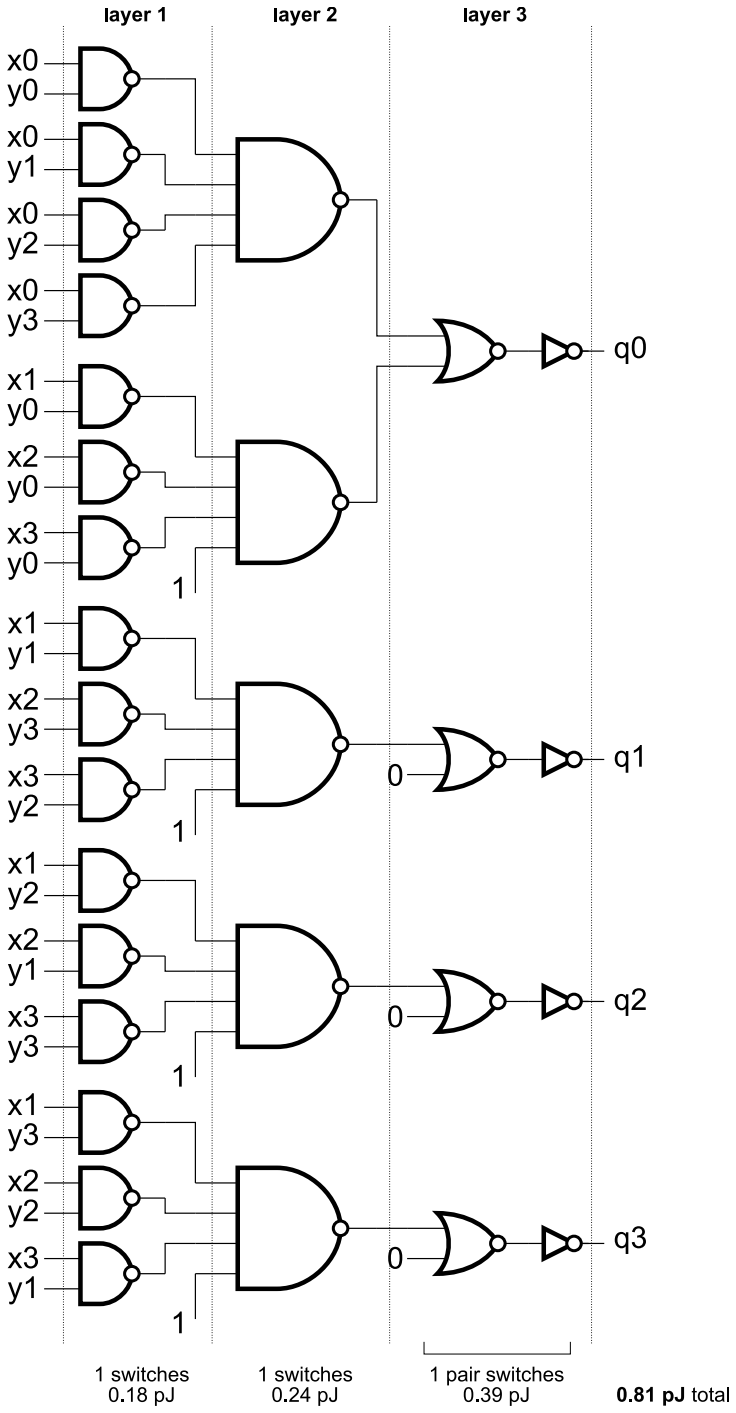


Figure 6: 1-of-4 encoded GF(4) multiplication, fully balanced

Table 2: AMS C35 0.35μm physical characteristics for the selection of library items

item	description	sw. energy, pJ	area, μm
INV0	inverter	0.17	36
NAND20	2-input NAND gate	0.18	55
NAND30	3-input NAND gate	0.21	73
NAND40	4-input NAND gate	0.24	91
NOR20	2-input NOR gate	0.22	55

Table 3: Switching energy and area for GF components

parameter	GF(2)			GF(4)		
	dual-rail			1-of-4		
	$+$	$\times$*	$\times$	$+$	$\times$*	$\times$
max sw. en., pJ	0.36	0.39	0.39	0.42	0.39	0.81
area, μm^2	330	182	366	1244	805	1699

* relaxed balancing

generated circuits in order to compare the efficiency of the proposed synthesis techniques. The precise physical simulation is available only after the placement and routing have been made which form a rather complex task. At the current state of the research it is inappropriate to produce fully designed circuits in order to analyse their parameters. We intend to use more generic evaluation using statistical information based on numeric values from RTL documentation.

Since different library specifications use different approaches to specify physical parameters, our analysis method constrains the comparison to the same library. In our examples we used AMS C35 (0.35μm). This library was chosen due to the availability of documented physical characteristics of the library cells. Some of the values are displayed in Table 2.

Energy and area estimations of the proposed components are shown in Table 3. The calculation of switching energy values is based on the analysis of component structures displayed in Figures 2, 3, 4, 5, and 6. Total switching energy is a sum of switching energies for each layer in a component circuit. Total area of a component is a sum of area values for all gates in its circuit.

4 Conclusions

Implementations of Galois Field arithmetic components based on RTL cells are proposed and analysed. The estimation of their physical characteristics can be used to compare the synthesis techniques for quaternary and mixed radix logic. The components themselves are developed to be used in the design flow for security based circuits.

A further development of Galois Field components suggest the following works. The implementations can be made using other run-time libraries, where 90nm technology is of the greatest interest. The possibility to compare different implementations and technologies is also highly important, and it requires precise physical simulation. Hence a few benchmarks should be fully designed and tested with respect to the conventional EDA flow.

References

[1] Federal information processing standards FIPS 140-3 (draft). National Institute of Standards and Technology.

[2] W.J. Bainbridge, W.B. Toms, D.A. Edwards, and S.B. Furber. Delay-insensitive, point-to-point interconnect using m-of-n codes. In *Proc. of ASYNC'03*, 2003.

[3] T. C. Bartee and D. I. Schneider. *Computation with Finite Fields*, volume 6 of *Inform. Contr.* June 1963.

[4] A. Bystrov, D. Sokolov, A. Yakovlev, and A. Koelmans. Balancing power signature in secure systems. In *Proc. 14th UK Asynchronous Forum*, 2003.

[5] B.J. Falkowski and S. Rahardja. Efficient computation of quaternary fixed polarity Reed-Muller expansions. *Computers and Digital Techniques, IEE Proc.*, 142:345–352, 1995.

[6] Bogdan J. Falkowski and Cicilia C. Lozano. Quaternary fixed-polarity Reed-Muller expansion computation through operations on disjoint cubes and its comparison with other methods. *Computers & Electrical Engineering*, 31:112–131, 2005.

[7] D.H. Green. Reed-Muller expansions with fixed and mixed polarities over GF(4). In *IEE Proc., Part E*, volume 137, 1990.

[8] Dragan Jankovic and Radomir S. Stankovic. Efficient calculation of fixed-polarity polynomial expressions for multiple-valued logic functions. In *Proc. of ISMVL '02*, page 76. IEEE Comp. Soc., 2002.

[9] Dragan Jankovic, Radomir S. Stankovic, and Claudio Moraga. Optimization of GF(4) expressions using the extended dual polarity property. In *Proc. of ISMVL '03*, page 50. IEEE Comp. Soc., 2003.

[10] P. Kocher, J. Jaffe, and B. Jun. Introduction to differential power analysis and related attacks, 1998.

[11] S. Moore, R. Anderson, P. Cunningham, R. Mullins, and G. Taylor. Improving smart card security using self-timed circuits. *Proc. of Asynchronous Circuits and Systems*, pages 211–218, 2002.

[12] S. Rahardja and B.J. Falkowski. Efficient algorithm to calculate Reed-Muller expansions over GF(4). *Circuits, Devices and Systems, IEE Proc.*, 148:289–295, 2001.

[13] D. Sokolov. *Automated synthesis of asynchronous circuits using direct mapping for control and data paths*. PhD thesis, University of Newcastle upon Tyne, 2006.

[14] Danil Sokolov, Julian Murphy, Alexander Bystrov, and Alex Yakovlev. Design and analysis of dual-rail circuits for security applications. *IEEE Trans. Comput.*, 54(4):449–460, 2005.

[15] UK Patent No. 0719455.8. Cryptographic processing and processors. Newcastle University.