Compact Implementations of BLAKE-32 and BLAKE-64 on FPGA

Jean-Luc Beuchat, Eiji Okamoto, and Teppei Yamazaki

Graduate School of Systems and Information Engineering
University of Tsukuba, 1-1-1 Tennodai, Tsukuba, Ibaraki, 305-8573, Japan
jeanluc.beuchat@gmail.com, okamoto@risk.tsukuba.ac.jp, yamazaki@cipher.risk.tsukuba.ac.jp

***Abstract*—We propose compact architectures of the SHA-3 candidates BLAKE-32 and BLAKE-64 for several FPGA families. We harness the intrinsic parallelism of the algorithm to interleave the computation of four instances of the G_i function. This approach allows us to design an Arithmetic and Logic Unit with four pipeline stages, and to achieve high clock frequencies. With careful scheduling, we completely avoid pipeline bubbles. For the time being, the designs presented in this work are the most compact ones for any of the SHA-3 candidates. We show for instance that a fully autonomous implementation of BLAKE-32 on a Xilinx Virtex-5 device requires 56 slices and two memory blocks.**

I. Introduction

In this article we present compact architectures of the SHA-3 candidates BLAKE-32 and BLAKE-64, proposed by Aumasson *et al.* [1], on Field-Programmable Gate Arrays (FPGAs). Such implementations are extremely valuable for constrained environments such as wireless sensor networks or Radio Frequency Identification (RFID) technology, where some security protocols mainly rely on cryptographic hash functions (see for example [2]).

After a short introduction to the BLAKE family of hash functions (Section II), we explain how to implement the required arithmetic operations on several FPGAs (Section III). Then, we harness the intrinsic parallelism to interleave several computations, and design two pipelined Arithmetic and Logic Units (ALUs) (Section IV). We have prototyped our architecture on several Altera and Xilinx FPGAs and discuss our results in Section V.

II. Algorithm Specification

The BLAKE family combines three previously studied components, chosen by Aumasson *et al.* for their complementarity [1]: the iteration mode HAIFA, the internal structure of the hash function LAKE, and a modified version of Bernstein's stream cipher ChaCha as compression function. BLAKE is a family of four hash functions, namely BLAKE-28, BLAKE-32, BLAKE-48, and BLAKE-64 (Table I). In the following, we focus on BLAKE-32 and refer the reader to [1] for more details about BLAKE-28, BLAKE-48, and BLAKE-64. The main differences lie in the length of words and in some constants involved in the algorithm. Once one has a coprocessor for BLAKE-32, writing a VHDL description of another member of the BLAKE family is therefore straightforward.

TABLE I
Properties of the BLAKE family of hash functions (reprinted from [1]). All sizes are given in bits.

Algorithm	Word	Message	Block	Digest	Salt
BLAKE-28	32	$< 2^{64}$	512	224	128
BLAKE-32	32	$< 2^{64}$	512	256	128
BLAKE-48	64	$< 2^{128}$	1024	384	256
BLAKE-64	64	$< 2^{128}$	1024	512	256

BLAKE-32 involves only two arithmetic operations: the addition modulo 2^{32} of two 32-bit unsigned integers (denoted by $\boxplus$) and the bitwise exclusive OR of two 32-bit words (denoted by $\oplus$). The latter is sometimes followed by a rotation of k bits to the right (denoted by $\ggg k$). The compression function of BLAKE-32 produces a new chain value $h' = h'_0, \ldots, h'_7$ from a message block $m = m_0, \ldots, m_{15}$, a chain value $h = h_0, \ldots, h_7$, a salt $s = s_0, \ldots, s_3$, a counter $t = t_0, t_1$, and 16 constants c_i defined in [1, p. 8]. This process consists of three steps. First, a 16-word internal state $v = v_0, \ldots, v_{15}$ is initialized as follows:

$$\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix} \leftarrow \begin{pmatrix} h_0 & h_1 & h_2 & h_3 \\ h_4 & h_5 & h_6 & h_7 \\ s_0 \oplus c_0 & s_1 \oplus c_1 & s_2 \oplus c_2 & s_3 \oplus c_3 \\ t_0 \oplus c_4 & t_0 \oplus c_5 & t_1 \oplus c_6 & t_1 \oplus c_7 \end{pmatrix}.$$

Then, a series of ten rounds is performed. Each of these rounds consists of a transformation of the internal state v based on the G_i function described by Algorithm 1, where σ_r denotes a permutation of $\{0, \ldots, 15\}$ parametrized by the round index r (see Table II). A column step updates the four columns of matrix v as follows: $G_0(v_0, v_4, v_8, v_{12})$, $G_1(v_1, v_5, v_9, v_{13})$, $G_2(v_2, v_6, v_{10}, v_{14})$, and $G_3(v_3, v_7, v_{11}, v_{15})$. Note that each call to G_i updates a distinct column of matrix v. Since we focus on compact implementations of BLAKE-32 in this work, we interleave the computation of G_0, G_1, G_2, and G_3. This approach allows us to design an ALU with four pipeline stages and to achieve high clock frequencies. Then, a diagonal step updates the four diagonals of v: $G_4(v_0, v_5, v_{10}, v_{15})$, $G_5(v_1, v_6, v_{11}, v_{12})$, $G_6(v_2, v_7, v_8, v_{13})$,

Algorithm 1 The G_i function of BLAKE-32.

Input: A function index i and four 32-bit integers a, b, c, and d.

Output: $G_i(a, b, c, d)$.

1. $a \leftarrow a \boxplus b$;
2. $a \leftarrow a \boxplus (m_{\sigma_r(2i)} \oplus c_{\sigma_r(2i+1)})$;
3. $d \leftarrow (d \oplus a) \ggg 16$;
4. $c \leftarrow c \boxplus d$;
5. $b \leftarrow (b \oplus c) \ggg 12$;
6. $a \leftarrow a \boxplus b$;
7. $a \leftarrow a \boxplus (m_{\sigma_r(2i+1)} \oplus c_{\sigma_r(2i)})$;
8. $d \leftarrow (d \oplus a) \ggg 8$;
9. $c \leftarrow c \boxplus d$;
10. $b \leftarrow (b \oplus c) \ggg 7$;

and $G_7(v_3, v_4, v_9, v_{14})$. Here again, each call to G_i modifies a distinct diagonal of the matrix, allowing us to interleave the computation of G_4, G_5, G_6, and G_7.

At the end of the tenth round, a new chain value $h' = h'_0, \ldots, h'_7$ is computed from the internal state v and the previous chain value h (finalization step):

$$\begin{aligned} h'_0 &\leftarrow h_0 \oplus s_0 \oplus v_0 \oplus v_8, & h'_4 &\leftarrow h_4 \oplus s_0 \oplus v_4 \oplus v_{12}, \\ h'_1 &\leftarrow h_1 \oplus s_1 \oplus v_1 \oplus v_9, & h'_5 &\leftarrow h_5 \oplus s_1 \oplus v_5 \oplus v_{13}, \\ h'_2 &\leftarrow h_2 \oplus s_2 \oplus v_2 \oplus v_{10}, & h'_6 &\leftarrow h_6 \oplus s_2 \oplus v_6 \oplus v_{14}, \\ h'_3 &\leftarrow h_3 \oplus s_3 \oplus v_3 \oplus v_{11}, & h'_7 &\leftarrow h_7 \oplus s_3 \oplus v_7 \oplus v_{15}. \end{aligned}$$

In order to guarantee that the length $\ell < 2^{64}$ of a message is a multiple of 512, Aumasson *et al.* suggest the following approach [1]: first, they append a bit 1 followed by a sufficient number of 0 bits such that the length is congruent to 447 modulo 512. Then, they append a bit 1 followed by the 64-bit binary representation of ℓ. The hash can now be computed iteratively (Algorithm 2): the padded message is divided into 16-word blocks $m^{(0)}, \ldots, m^{(N-1)}$ and the chain value $h^{(0)}$ is set to the same initial value as SHA-2 [1, p. 8]. The counter $t^{(i)}$ denotes the number of message bits in $m^{(0)}, \ldots, m^{(i)}$ (*i.e.* excluding padding bits). Note that, if the last block contains only padding bits, then $t^{(N-1)}$ is set to zero. In the following, we assume that our coprocessor is provided with padded messages. A hardware wrapper interface for the SHA-3 candidates comprising communication and padding is described in [3].

Algorithm 2 Iterated hash.

Input: A padded message split into N 16-word blocks and a salt s.

Output: A 256-bit digest.

1. $\left(h_0^{(0)}, \ldots, h_7^{(0)}\right) \leftarrow (\mathrm{IV}_0, \ldots, \mathrm{IV}_7)$;
2. **for** $i \leftarrow 0$ **to** $N - 1$ **do**
3. $\quad h^{(i+1)} \leftarrow$ **compress** $\left(h^{(i)}, m^{(i)}, s, t^{(i)}\right)$;
4. **end for**
5. **return** $h^{(N)}$;

III. FPGA-Specific Issues and their Implications on the Design of BLAKE

Modern FPGAs are mainly designed for digital signal processing applications involving rather small operands (16 to 64 bits). Several FPGA manufacturers (Altera, Xilinx, etc.) chose to include dedicated carry logic enabling the implementation of fast Carry-Ripple Adders (CRA) for such operand sizes.

Let us study the architecture of a Xilinx Spartan-3 device [4]. The slice is the main logic resource for implementing synchronous and combinatorial circuits (one finds the same kind of slices in several other Xilinx FPGAs: Virtex, Virtex-E, Virtex-II, Virtex-II Pro, Virtex-4, etc.). Each slice embeds two 4-input function generators (G-LUT and F-LUT), two storage elements, carry logic (CYMUXG and CYMUXF), arithmetic gates (GAND, FAND, XORG, and XORF), and wide-function multiplexers. Each function generator is implemented by means of a programmable Look-Up Table (LUT).

A Full-Adder (FA) cell computes the sum of a carry-in bit carry_j (coming from a lower bit position) and two bits of same magnitude x_j and y_j. The result is encoded by a sum bit sum_j and a carry-out bit carry_{j+1} such that $2\mathit{carry}_{j+1} + \mathit{sum}_j = x_j + y_j + \mathit{carry}_j$. Let $z_j = x_j \oplus y_j$. Then, we have:

$$\mathit{sum}_j = z_j \oplus \mathit{carry}_j, \tag{1}$$

$$\mathit{carry}_{j+1} = \begin{cases} x_j & \text{if } z_j = 0 \text{ (\textit{i.e.} } x_j = y_j), \\ \mathit{carry}_j & \text{otherwise.} \end{cases} \tag{2}$$

Assume that the F-LUT function generator outputs z_j. Then, the XORF gate computes the sum bit sum_j. The generation of the carry-out bit carry_{j+1} according to Equation (2) involves three multiplexers (CYOF, CYSELF, and CYMUXF). Thanks to the G-LUT function generator, one can implement a second FA cell within the same slice, which thus embeds a 2-bit CRA (Figure 1a). The gates GAND and FAND allows one to build multipliers: one can generate two partial products and compute their sum with a single stage of LUTs.

Since we focus on compact coprocessors for the BLAKE family in this work, we perform a single arithmetic operation at each clock cycle ($\boxplus$ or $\oplus$). A first solution consists in implementing a modular adder and an array of XOR gates, and selecting the operation by means of a multiplexer commanded by a control bit. However, several Xilinx devices (Virtex, Virtex-E, Virtex-II, Virtex-II Pro, Virtex-4, and Spartan-3) offer a much more elegant and compact solution: we can enable or disable carry propagations using a control bit *ctrl* as input to the gates GAND and FAND (Figure 1b). Thus, Equation (2) becomes:

$$\mathit{carry}_{j+1} = \begin{cases} x_j \cdot \mathit{ctrl} & \text{if } z_j = 0 \text{ (\textit{i.e.} } x_j = y_j), \\ \mathit{carry}_j & \text{otherwise.} \end{cases} \tag{3}$$

Assuming that $\mathit{carry}_0 = 0$, we easily check that our operator now behaves as a CRA when $\mathit{ctrl} = 1$ and computes the bitwise exclusive OR of its inputs when $\mathit{ctrl} = 0$ (since $\mathit{ctrl} = \mathit{carry}_j = 0$, the output carry carry_{j+1} is also equal to zero and carry propagations are disabled). Note that the

TABLE II
PERMUTATIONS OF $\{0, \ldots, 15\}$ USED BY THE BLAKE FUNCTIONS (REPRINTED FROM [1]).

σ_0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
σ_1	14	10	4	8	9	15	13	6	1	12	0	2	11	7	5	3
σ_2	11	8	12	0	5	2	15	13	10	14	3	6	7	1	9	4
σ_3	7	9	3	1	13	12	11	14	2	6	5	10	4	0	15	8
σ_4	9	0	5	7	2	4	10	15	14	1	11	12	6	8	3	13
σ_5	2	12	6	10	0	11	8	3	4	13	7	5	15	14	1	9
σ_6	12	5	1	15	14	13	4	10	0	7	6	3	9	2	8	11
σ_7	13	11	7	14	12	1	3	9	5	0	15	4	8	6	2	10
σ_8	6	15	14	9	11	3	0	8	12	2	13	7	1	4	10	5
σ_9	10	2	8	4	7	6	1	5	15	11	9	14	3	12	13	0

functionality described in Equation (3) is that of a dual-field adder [5]. On Spartan-3 FPGAs (and on all other Xilinx FPGAs based on the same slice architecture), it is possible to compute a sum or any function of up to three Boolean variables (Figure 1c).

The latest FPGA families introduced by Xilinx (Virtex-5, Virtex-6, and Spartan-6) are based on 6-input LUTs, each of them having six independent inputs and two independent outputs. It is for instance possible to implement any two 5-input logic functions with shared inputs thanks to this building block (LUT6_2 primitive). Each slice embeds four LUTs and a carry chain that consists of a series of four multiplexers and four XOR gates (CARRY4 primitive). Figure 1d describes how to implement an operator returning either the sum or the bitwise exclusive OR of its two inputs according to a control bit.[1] The carry-out bit $carry_{j+1}$ is determined according to Equation (3), the only difference being that the product $x_j \cdot ctrl$ is now computed within a LUT6_2 primitive. The main drawback of this approach is that design tools are unable to generate such an architecture from a high-level VHDL description of the operator. It is necessary to use specific libraries provided by the FPGA manufacturer and to modify the VHDL code for each device.

Additionally, modern FPGAs feature embedded memory blocks to store relatively large amounts of data. They support several modes (*e.g.* single port, true dual-port, ROM, etc.) and port-width configurations. We refer the reader to the technical literature provided by Altera or Xilinx for further details. In this work, we will take advantage of such memory blocks to implement our register file and store the micro-code of our coprocessors.

IV. TWO COMPACT COPROCESSORS FOR THE BLAKE FAMILY

Our compact coprocessor for BLAKE-32 is based on the observation that the four calls to G_i in a column step or a diagonal step can be computed in parallel. In order to achieve a high clock frequency, we suggest to design an ALU with four pipeline stages and to interleave the computation of four G_i functions. A closer look at Algorithm 1 indicates that each instruction involves the result of the previous one. Thus, our ALU includes a feedback mechanism to bypass the register file of the coprocessor.

[1]The LUT6_2 primitive offers even more flexibility. One can for instance compute a sum or any function of up to four Boolean variables.

A. Arithmetic and Logic Unit

Figure 2a describes our first ALU designed for FPGAs based on 4-input LUTs. It consists of four stages performing the following tasks:

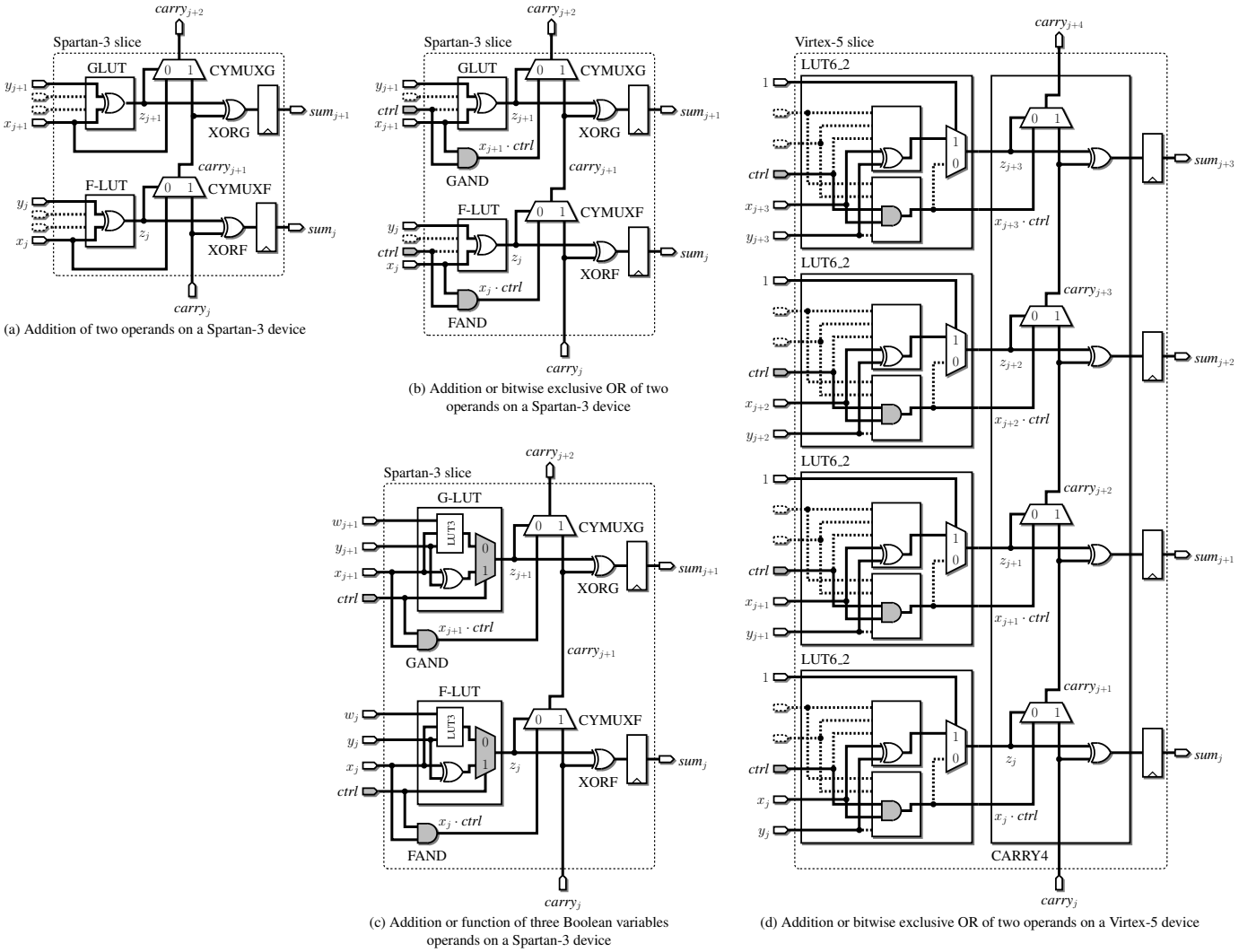
① **Operand selection.** The first operand comes from the register file implemented by means of dual-ported memory. Routing a signal from a memory block to a slice is usually expensive in terms of wire delay and it is recommended to store this signal in a register before performing arithmetic operations. Since a flip-flop is always associated with a 4-input LUT, we can perform some simple pre-processing without increasing the number of slices of the ALU: a control bit $ctrl_0$ selects either a word read from port A or the bitwise exclusive OR of two words read from ports A and B. This allows us to compute $m_{\sigma_r(2i)} \oplus c_{\sigma_r(2i+1)}$ and $m_{\sigma_r(2i+1)} \oplus c_{\sigma_r(2i)}$ for free (Algorithm 1, lines 2 and 7).
As explained above, the second input is almost always the result of a previous operation. However, we have to disable this feedback mechanism during the initialization step: the computation of $v_8 \leftarrow s_0 \oplus c_0$ involves for instance two words stored in the register file. An array of AND gates controlled by $ctrl_1$ allows us to force the second operand to zero in such cases. The critical path is limited to a single LUT and a flip-flop.

② **Addition modulo 2^{32} or bitwise exclusive OR.** This stage consists of the arithmetic operator described in the previous section.

③ **Rotation of 0, 7, 8, or 12 bits to the right.** The two multiplexers commanded by $ctrl_3$ are implemented by means of LUTs. On Xilinx FPGAs, the output of this stage is then selected thanks to a F5MUX primitive.

④ **Rotation of 0 or 16 bits to the right.** The final stage allows us to perform the rotation of 16 bits towards less significant bits requested to update d in Algorithm 1 (line 3). Here again, the critical path is limited to a single LUT and a flip-flop.

Recall that recent FPGAs embed 6-input function generators. We propose here a simple rewriting of the G_i function that allows us to take advantage of these new building blocks.



(a) Addition of two operands on a Spartan-3 device

(b) Addition or bitwise exclusive OR of two operands on a Spartan-3 device

(c) Addition or function of three Boolean variables operands on a Spartan-3 device

(d) Addition or bitwise exclusive OR of two operands on a Virtex-5 device

Fig. 1. Addition and bitwise exclusive OR on Xilinx FPGAs.

It suffices to notice that rotation operations always follow a bitwise exclusive OR and can thus be performed in two steps. We have for instance:

$$(d \oplus a) \ggg 16 = ((d \ggg 7) \oplus (a \ggg 7)) \ggg 9.$$

Algorithm 3 describes an alternative version of the G_i function based on this observation. We obtain a new ALU with three stages (Figure 2b):

① **Operand selection.** We slightly modified the selection of the first operand in order to include the rotation of 7 to the right: the computation of the first operand involves now an array of 5-input LUTs.

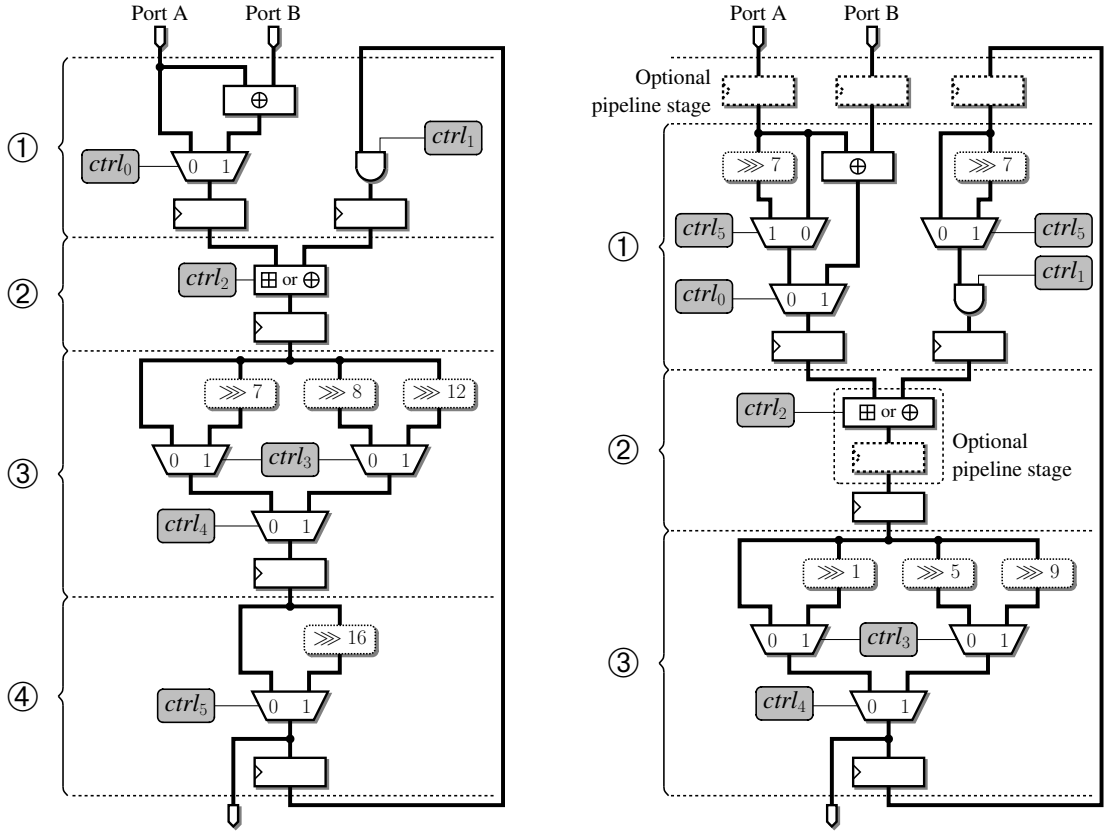
② **Addition modulo 2^{32} or bitwise exclusive OR.** This stage consists again of the arithmetic operator described in the previous section.

③ **Rotation of 0, 1, 5, or 9 bits to the right.** This stage simply consists of a 4-input multiplexer implemented by means of an array of 6-input LUTs.

We have two options for the fourth pipeline stage (Figure 2b). The first one consists in storing the inputs in registers in order to reduce the critical path between the register file and the ALU (note that the embedded memory blocks available in several FPGA families include optional output registers). The second one is to introduce pipeline registers to shorten the worst-case carry path of the modulo 2^{32} adder. We strongly recommend to consider both solutions and to select the most appropriate one according to place-and-route results. According to our place-and-route results on Virtex-5 FPGAs, we obtain the best throughput for BLAKE-32 with the first option, whereas the second one seems to be more appropriate for BLAKE-64.

B. Scheduling

We have to be careful in order to avoid pipeline bubbles between a column step and a diagonal step. Figure 3 describes the state of the ALU depicted in Figure 2a at the end of a column step. It suffices to process the four calls to G_i of the diagonal step in the following order: G_7, G_4, G_5, and G_6.



(a) ALU for FPGAs based on 4-input LUTs

(b) ALU for FPGAs based on 6-input LUTs

Fig. 2. Two arithmetic and logic units for BLAKE-32. (N.B. All control bits $ctrl_j$ belong to $\{0, 1\}$.)

Algorithm 3 The G_i function of BLAKE-32 revisited.

Input: A function index i and four 32-bit integers a, b, c, and d.

Output: $G_i(a, b, c, d)$.

1. $a \leftarrow a \boxplus b$;
2. $a \leftarrow a \boxplus (m_{\sigma_r(2i)} \oplus c_{\sigma_r(2i+1)})$;
3. $d \leftarrow ((d \ggg 7) \oplus (a \ggg 7)) \ggg 9$;
4. $c \leftarrow c \boxplus d$;
5. $b \leftarrow ((b \ggg 7) \oplus (c \ggg 7)) \ggg 5$;
6. $a \leftarrow a \boxplus b$;
7. $a \leftarrow a \boxplus (m_{\sigma_r(2i+1)} \oplus c_{\sigma_r(2i)})$;
8. $d \leftarrow ((d \ggg 7) \oplus (a \ggg 7)) \ggg 1$;
9. $c \leftarrow c \boxplus d$;
10. $b \leftarrow (b \ggg 7) \oplus (c \ggg 7)$;

We check for instance that the ALU outputs the new value of v_4 (last instruction of G_0) at time $\tau + 3$. If we load v_3 from the register file, we can start the computation of G_7 at time $\tau + 4$. We easily check that this scheduling also avoids pipeline bubbles between a diagonal step and a column step. Since each call to G_i involves ten instructions, we need 80 clock cycles to perform a round of BLAKE-32.

The initialization and finalization steps involve 16 and 24 clock cycles, respectively. Furthermore, we need four clock cycles to load v_4, v_5, v_6, and v_7 in the pipeline before the first call to G_0, G_1, G_2, and G_3 (the first operation of G_0 is for instance $v_0 \leftarrow v_0 \boxplus v_4$; recall that we bypass the register file thanks to a feedback mechanism: when we load v_0, we expect the ALU to output v_4). Therefore, we need $16 + 4 + 10 \cdot 80 + 24 = 844$ clock cycles to process a 16-word block. In terms of scheduling, the only difference between BLAKE-32 and BLAKE-64 lies in the number of rounds. The latter involves four additional rounds and requires 1164 clock cycles to process a block.

C. Register File and Control Unit

The register file stores the 16 constants c_i, a message block $m = m_0, \ldots, m_{15}$, the internal state $v = v_0, \ldots, v_{15}$, the chain value $h = h_0, \ldots, h_7$, the salt $s = s_0, \ldots, s_3$, and the counter $t = t_0, t_1$ (Figure 4). When we process several message blocks (iterated hash), we use the same salt s for each call to the compression function. Therefore, the four words $s_0 \oplus c_0$, $s_1 \oplus c_1$, $s_2 \oplus c_2$, and $s_3 \oplus c_3$ involved in the initialization step are constants that can be computed only once and stored in the register file for subsequent calls. Note that no instruction of BLAKE involves at the same time the salt s and the counter t. Therefore, if we store s and t from addresses 64 to 69, we save a control bit: all variables are accessible from port A (7 address bits), but Port B is restricted to the 64 least significant words of the register file (6 address bits).

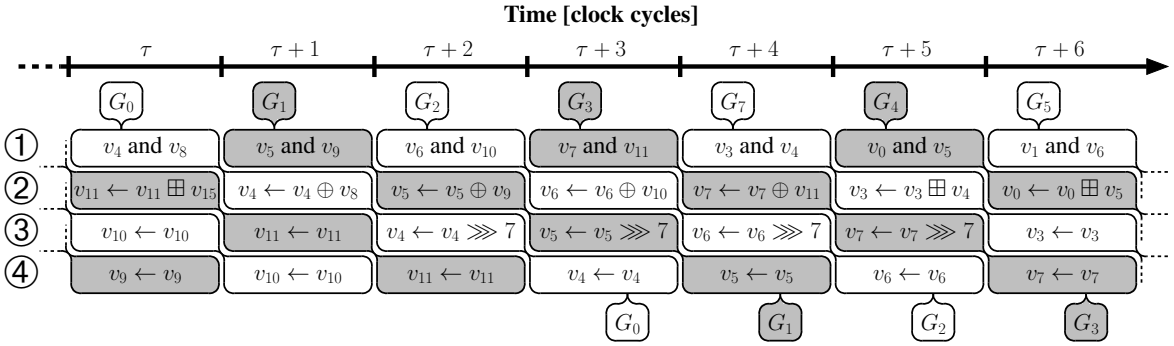


Fig. 3. Avoiding pipeline bubbles between a column step and a diagonal step. The digits ① to ④ refer to the four stages of the ALU depicted in Figure 2a.

The control unit mainly consists of a program counter that addresses an instruction memory implemented by means of a memory block. Our micro-code for BLAKE-32 involves only 14 distinct control words $ctrl_{5:0}$ and it is therefore possible to encode them with 4 bits, thus reducing the size of an instruction to 18 bits at the cost of 6 4-input LUTs. Recall that BLAKE-32 involves 844 instructions[2] and that several FPGAs embed memory blocks whose aspect ratio (*i.e.* width versus depth) is configurable. The 18Kbit blocks available in Spartan-3 or Virtex-4 devices allow one to store 1024 words of 18 bits. Consequently, we can load our micro-code in a single memory block on such FPGAs.

V. Results and Comparisons

We captured our architectures in the VHDL language and prototyped our coprocessors on several Xilinx and Altera FPGAs with average speedgrade (Table III). To the best of our knowledge, the only compact implementations of BLAKE-32 and BLAKE-64 have been proposed by Aumasson *et al.* [1]. Their lightweight architecture consists of an initialization unit, a single G_i unit, and a finalization unit. Since they have to read four elements of the internal state v at each clock cycle, they can not implement the register file by means of dual-ported memory and need 16 registers. Our approach leads to a lower throughput, but our architectures are significantly smaller and improve the area–time trade-off of the compact implementations proposed by Aumasson *et al.* [1].

A few researchers have proposed compact implementations of other SHA-3 candidates. We include in our comparisons the results reported in the SHA-3 Zoo [6], in the hash-forum@nist.gov mailing list, and in the proceedings of the Second SHA-3 Candidate Conference held in late August 2010. Currently, only seven algorithms have been evaluated on FPGA, and it is unfortunately difficult to draw conclusions. Among these algorithms, the BLAKE family offers one of the best area–time trade-offs and leads to the smallest coprocessors on reconfigurable devices.

[2]Note that it is possible to reduce the size of the code by storing the table defining the permutation of $\{0\ldots,15\}$ parametrized by the round index r (Table II) and by generating the addresses of $m_{\sigma_r(2i)}$ and $c_{\sigma_r(2i+1)}$ on the fly. However, this approach would require a more complex control unit. As long as the micro-code fits into a single block of memory, there is no need to try to reduce the number of instructions.

On Xilinx FPGAs, Shabal [7] ranks first in terms of throughput and area–time trade-off. Detrey *et al.* [8] noted that only a small fraction of the internal state of Shabal is used at any step of the algorithm. They exploited this fact and minimized the area of the circuit by taking advantage of the dedicated shift register resources available in the recent Xilinx devices (SRL16 primitive).

Blue Midnight Wish (BMW) [9] involves almost the same arithmetic operations as BLAKE: integer addition and subtraction modulo 2^{32} (or modulo 2^{64}), and bitwise exclusive OR of two 32-bit (or 64-bit) words. On Xilinx FPGAs, BMW benefits from the technique we proposed in Section III in order to enable or disable carry propagations (Figure 1). A second control bit is necessary to select the sign of the operand Y, however this modification is straightforward and has no impact on the circuit area. BMW requires a more sophisticated shifter/rotator and a significantly more complex datapath than BLAKE. Although it is possible to design a low-area coprocessor, the throughput turns out to be disappointing [10].

Several algorithms submitted to the SHA-3 competition are strongly influenced by the Advanced Encryption Standard (AES) [11] (Fugue [12] and Grøstl [13]), or even built around the AES round function itself (ECHO [14] and SHAvite-3 [15]). We have proposed a compact coprocessor based on an 8-bit datapath for ECHO-256 [16]. Even though our architecture does not compete with Shabal or BLAKE in terms of throughput, ECHO has a clear advantage over the other candidates: at the price of a small hardware overhead, it is possible to design a unified architecture for the AES (encryption, decryption, and key expansion for 128-, 192-, and 256-bit keys) and ECHO (224-, 256-, 384-, and 512-bit message digests) [17]. This property is a key asset for embedded systems, and should be taken into account when selecting the new SHA-3 function. Even if a low-area coprocessor is not available yet, Fugue and Grøstl also allow one to combine the hash algorithm and the AES with reasonable overheads [18].

VI. Conclusion

We took advantage of the intrinsic parallelism of the BLAKE family of hash functions to interleave the computation of four instances of the G_i function. Thanks to this approach, we designed an ALU with four pipeline stages and achieved

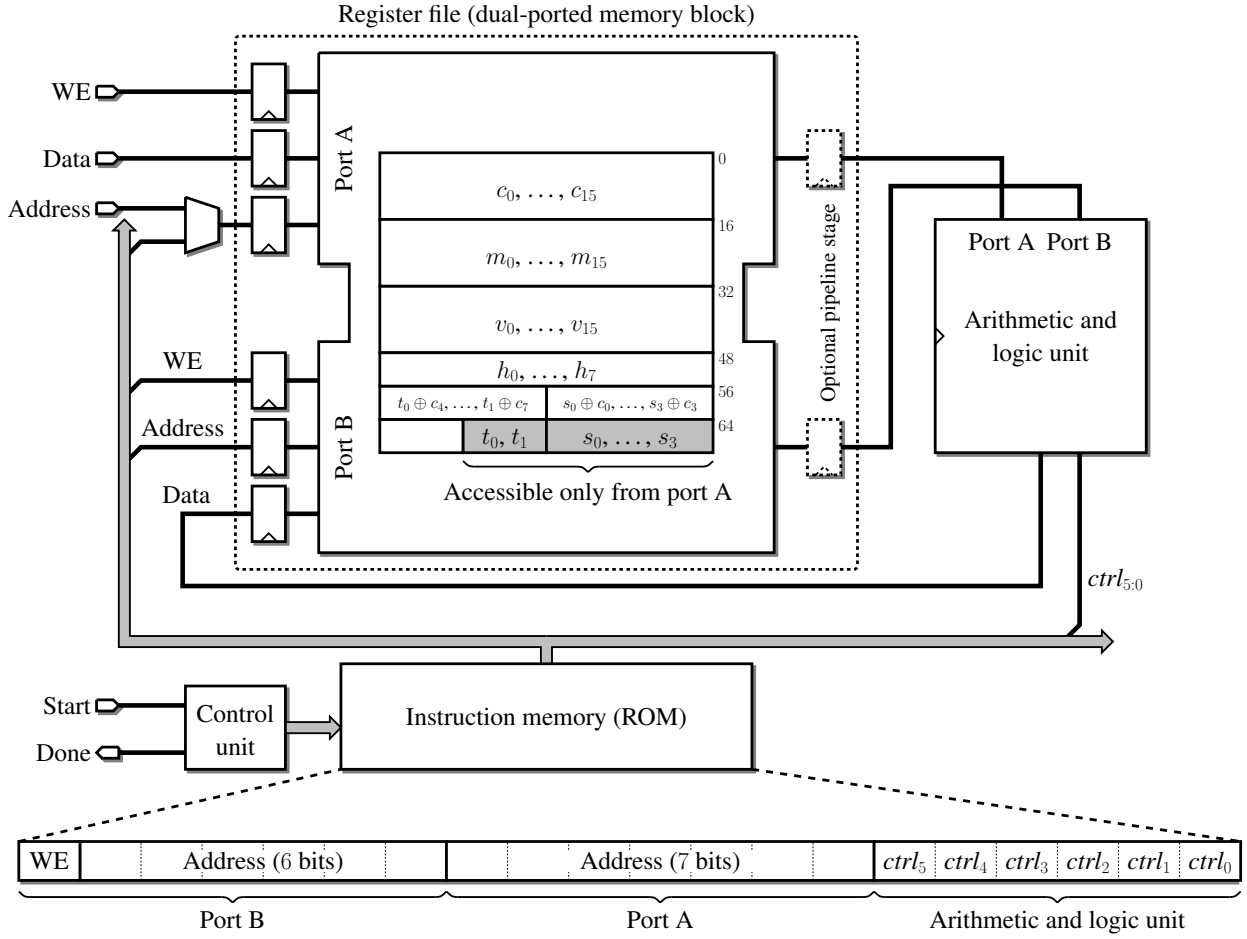


Fig. 4. General architecture of a BLAKE coprocessor.

high clock frequencies. A careful scheduling allowed us to totally avoid pipeline bubbles and memory collisions. We also addressed FPGA-specific issues: we described how to enable or disable dedicated carry logic in Xilinx devices, thus sharing slices between addition and bitwise exclusive OR of two operands. We showed that a rewriting of the G_i function allows us to fully exploit the 6-input LUTs available in the most recent FPGAs. For the time being, our designs are the most compact ones for any of the SHA-3 candidates.

ACKNOWLEDGEMENT

The authors would like to thank Simon Kramer, Jean-Michel Muller, and Francisco Rodríguez-Henríquez for their valuable comments.

REFERENCES

[1] J.-P. Aumasson, L. Henzen, W. Meier, and R. Phan, "SHA-3 proposal BLAKE (version 1.3)," 2009, available at http://www.131002.net/blake.

[2] J. Zhai, C. Park, and G.-N. Wang, "Hash-based RFID security protocol using randomly key-changed identification procedure," in *Computational Science and Its Applications–ICCSA 2006*, ser. Lecture Notes in Computer Science, M. Gavrilova, O. Gervasi, V. Kumar, C. K. Tan, D. Taniar, A. Laganà, Y. Mun, and H. Choo, Eds., no. 3983. Springer, 2006, pp. 296–305.

[3] B. Baldwin, A. Byrne, L. Lu, M. Hamilton, N. Hanley, M. O'Neill, and W. Marnane, "A hardware wrapper for the SHA-3 hash algorithms," 2010, cryptology ePrint Archive, Report 2010/124.

[4] Xilinx, "Spartan-3 FPGA family," Dec. 2009, available at http://www.xilinx.com/support/documentation/data_sheets/ds099.pdf.

[5] E. Savaş, A. Tenca, and Ç.K. Koç, "A scalable and unified multiplier architecture for finite fields GF(p) and GF(2^m)," in *Cryptographic Hardware and Embedded Systems–CHES 2000*, ser. Lecture Notes in Computer Science, Ç.K. Koç and C. Paar, Eds., no. 1965. Springer, 2000, pp. 277–292.

[6] "The SHA-3 zoo," http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo.

[7] E. Bresson, A. Canteaut, B. Chevallier-Mames, C. Clavier, T. Fuhr, A. Gouget, T. Icart, J. Misarsky, M. Naya-Plasencia, P. Paillier, T. Pornin, J. Reinhard, C. Thuillet, and M. Videau, "Shabal, a submission to NIST's cryptographic hash algorithm competition," 2008, available at http://www.shabal.com.

[8] J. Detrey, P. Gaudry, and K. Khalfallah, "A low-area yet performant FPGA implementation of Shabal," 2010, cryptology ePrint Archive, Report 2010/292.

[9] D. Gligoroski, V. Klima, S. Knapskog, M. El-Hadedy, J. Amundsen, and S. Mjølsnes, "Cryptographic hash function BLUE MIDNIGHT WISH," 2009, available at http://people.item.ntnu.no/~danilog/Hash/BMW-SecondRound.

[10] M. El-Hadedy, M. Margala, D. Gligoroski, and S. Knapskog, "Resource-efficient implementation of Blue Midnight Wish-256 hash function on Xilinx FPGA platform," in *The Second SHA-3 Candidate Conference*, Aug. 2010.

[11] J. Daemen and V. Rijmen, *The Design of Rijndael*. Springer, 2002.

[12] S. Halevi, W. Hall, and C. Jutla, "The hash function "Fugue"," 2009, available at http://domino.research.ibm.com/comm/research_projects.nsf/pages/fugue.index.html.

TABLE III
COMPACT IMPLEMENTATIONS OF SHA-3 CANDIDATES.

(a) Xilinx Spartan-3 device

	Algorithm	FPGA	Area [slices]	Memory blocks	Frequency [MHz]	Throughput [Mbps]
This work	BLAKE-32	xc3s50-5	124	2	190	115
This work	BLAKE-64	xc3s200-5	229	3	158	138
Jungk *et al.* [19]	Grøstl-224/256	xc3s5000-5	2486	–	63.2	404
Jungk and Reith [20]	Grøstl-224/256	xc3s200	1276	–	60	192
Jungk and Reith [20]	Grøstl-384/512	xc3s200	2110	–	63	144
Baldwin *et al.* [21]	Shabal	xc3s5000-5	1933	–	89.71	540
Detrey *et al.* [8]	Shabal	xc3s200-5	499	–	100	800

(b) Xilinx Virtex-4 device

	Algorithm	FPGA	Area [slices]	Memory blocks	Frequency [MHz]	Throughput [Mbps]
This work	BLAKE-32	xc4vlx15-11	124	2	357	216
Aumasson *et al.* [1]	BLAKE-32	xc4vlx100	960	–	68	430
This work	BLAKE-64	xc4vlx15-11	230	3	250	219
Aumasson *et al.* [1]	BLAKE-64	xc4vlx100	1856	–	42	381

(c) Xilinx Virtex-5 device

	Algorithm	FPGA	Area [slices]	Memory blocks	Frequency [MHz]	Throughput [Mbps]
This work	BLAKE-32	xc5vlx50-2	56	2	372	225
Aumasson *et al.* [1]	BLAKE-32	xc5vlx110	390	–	91	575
This work	BLAKE-64	xc5vlx50-2	108	3	358	314
Aumasson *et al.* [1]	BLAKE-64	xc5vlx110	939	–	59	533
El-Hadedy *et al.* [10]	BMW-256	xc5vlx110	84	2	116	28
Beuchat *et al.* [16]	ECHO-256	xc5vlx50-2	127	1	352	72
Bertoni *et al.* [22]	Keccak	xc5vlx50-3	448	–	265	52
Baldwin *et al.* [21]	Shabal	xc5vlx220-2	2307	–	222.22	1330
Feron and Francq [23]	Shabal	not specified	596	–	109	1142
Detrey *et al.* [8]	Shabal	xc5vlx30-2	153	–	256	2051

(d) Altera Cyclone III device

	Algorithm	FPGA	Area [LEs]	Memory blocks	Frequency [MHz]	Throughput [Mbps]
This work	BLAKE-32	EP3C5E144A7	285	2	192	116
This work	BLAKE-64	EP3C5F256I7	542	3	140	123
Bertoni *et al.* [22]	Keccak	EP3C5F256C6	1559	–	181	47.8

(e) Altera Stratix III device

	Algorithm	FPGA	Area [ALUTs]	Memory blocks	Frequency [MHz]	Throughput [Mbps]
Namin and Hasan [24]	Skein-256	EP3SL340F1760C3	1385	–	161.42	573.9

[13] P. Gauravaram, L. Knudsen, K. Matusiewicz, F. Mendel, C. Rechberger, M. Schläffer, and S. Thomsen, "Grøstl – a SHA-3 candidate," 2008, available at http://www.groestl.info.

[14] R. Benadjila, O. Billet, H. Gilbert, G. Macario-Rat, T. Peyrin, M. Robshaw, and Y. Seurin, "SHA-3 proposal: ECHO," 2009, available at http://crypto.rd.francetelecom.com/echo.

[15] E. Biham and O. Dunkelman, "The SHAvite-3 hash function (tweaked version)," 2009, available at http://www.cs.technion.ac.il/~orrd/SHAvite-3.

[16] J.-L. Beuchat, E. Okamoto, and T. Yamazaki, "A compact FPGA implementation of the SHA-3 candidate ECHO," 2010, cryptology ePrint Archive, Report 2010/364.

[17] J.-L. Beuchat, "A unified architecture for AES and the SHA-3 candidate ECHO," Aug. 2010, announced on hash-forum@nist.gov.

[18] K. Järvinen, "Sharing resources between AES and the SHA-3 second round candidates Fugue and Grøstl," in *The Second SHA-3 Candidate Conference*, Aug. 2010.

[19] B. Jungk, S. Reith, and J. Apfelbeck, "On optimized FPGA implementations of the SHA-3 candidate Grøstl," 2009, cryptology ePrint Archive, Report 2009/206.

[20] B. Jungk and S. Reith, "On FPGA-based implementations of Grøstl," 2010, cryptology ePrint Archive, Report 2010/260.

[21] B. Baldwin, A. Byrne, M. Hamilton, N. Hanley, R. McEvoy, W. Pan, and W. Marnane, "FPGA implementations of SHA-3 candidates: CubeHash, Grøstl, LANE, Shabal and Spectral Hash," 2009, cryptology ePrint Archive, Report 2009/342.

[22] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Keccak sponge function family main document (version 2.0)," 2009, available at http://keccak.noekeon.org.

[23] R. Feron and J. Francq, "FPGA implementation of Shabal: Our first results," 2010, available at http://www.shabal.com.

[24] A. Namin and M. Hasan, "Hardware implementation of the compression function for selected SHA-3 candidates," Centre for Applied Cryptographic Research, University of Waterloo, Tech. Rep. CACR 2009–28, 2009, available at http://www.vlsi.uwaterloo.ca/~ahasan/web_papers/technical_reports/web_five_SHA_3.pdf.