Comprehensive Comparison of Hardware Performance of Fourteen Round 2 SHA-3 Candidates with 512-bit Outputs Using Field Programmable Gate Arrays[1]

Kris Gaj, Ekawat Homsirikamol, and Marcin Rogawski

ECE Department, George Mason University

{kgaj, ehomsiri, mrogawsk}@gmu.edu

Abstract. In this paper, we extend our evaluation of the hardware performance of 14 Round 2 SHA-3 candidates, accepted for the presentation at CHES 2010, to the case of high security variants, with 512 bit outputs. A straightforward method for predicting the performance of 512-bit variants, based on the results for 256-bit versions of investigated hash functions is presented, and confirmed experimentally. The VHDL codes for 512-bit variants of all 14 SHA-3 Round 2 candidates and the old standard SHA-2 have been developed and thoroughly verified. These codes have been then used to evaluate the relative performance of all aforementioned algorithms using seven modern families of Field Programmable Gate Arrays (FPGAs) from two major vendors, Xilinx and Altera. The results point to very significant differences among all evaluated algorithms in terms of both throughput and area. Only two candidates, Keccak and CubeHash, outperform SHA-512 in terms of the primary optimization target used in this study, throughput to area ratio.

1. Introduction

Both the current NIST cryptographic hash function standard, FIPS 180-3 [1] (commonly referred as SHA-2) as well as the call for a new standard, SHA-3 [2], assume that each hash function family includes variants with at least the following four output sizes: 224, 256, 384, and 512-bits. These variants should have a security equivalent to Triple DES, AES-128, AES-192, and AES-256, respectively.

Although 256-bit versions of cryptographic hash functions seem to provide adequate security for majority of current applications and common use scenarios, there exist already several recommendations suggesting the use of more secure hash function variants, with the outputs of 384 and 512 bits. For example, if a hash function is used as a part of a digital signature used to authenticate a life will, which is required to remain valid for tens of years from now, a 512-bit variant of a hash function seems to be a prudent choice.

Several recent recommendations clearly specify the need for such high-security variants [3]. Examples include

- Federal documents requiring protection well beyond the year 2030, according to the 2007 NIST recommendation [4],
- Top Secret Documents according to the NSA Suite B Cryptography Fact Sheet [5],
- Level 8 of protection according to the recent ECRYPT II Recommendations [6].

Clearly, candidates for the new SHA-3 standard, which is likely to remain in effect well beyond the year 2030, should be evaluated from the point of view of performance of their most secure variant.

Since replacing a 256-variant of a hash function with a 512-bit variant increases the resistance against the best known (birthday-paradox) attack from 2^{128} to 2^{256} (i.e., by a factor of $2^{128} \approx 3.4\ 10^{38}$), one might expect that a significant performance penalty will be incurred for such a tremendous increase in security.

[1] This work was partially supported through the NIST/ARRA grant no. 60NANB10D004.

Contrary to that, it has been observed that the 512-bit variant of the current standard, SHA-2 (known as SHA-512), is actually about 33% faster then even the 160-bit variant (SHA-1), when implemented in hardware using Xilinx Virtex FPGAs [7]. The only penalty incurred concerns the area (by a factor of about two), and not the speed of the implementation [7].

The explanation of this phenomena is quite simple - in hardware all bits of a message block are processed in parallel, so increasing the size of a message block from 512 bits to 1024 bits has a positive influence on speed, which is counteracted only by more complex operations in the critical path of the circuit (namely six 64-bit additions vs. four 32-bit additions), and thus a smaller clock frequency.

The same property clearly does not apply to traditional software implementations, where doubling message block size typically at least doubles the amount of clock cycles required for processing of this block.

In this paper, we will investigate whether the increase in the speed of a more secure hash function variant, first observed in the case of SHA-1 and SHA-2 functions, applies also to new SHA-3 candidates. We will also explore the imposed area penalty (if any), and the change in the throughput to area ratio when switching from a 256-bit variant to a 512-bit variant of a hash function.

Finally, we will also explore the relative performance of the 512-bit variants of all SHA-3 candidates in terms of the throughput, area, and throughput to area ratio.

2. Previous work

At the time of writing, relatively few hardware implementations of the 512-bit variants of SHA-3 candidates have been reported in the literature. Major results concerning FPGA implementations targeting high speed are summarized in [8, 9]. These results have been obtained using different FPGA families and different and not always clear optimization targets. The designers differ with experience and skills. Additionally, no common interface has been applied, and some of the designs are not fully autonomous but rather implement core functionality only [9].

The comparison of 256-bit variants of all candidates is somewhat more explored, with two groups reporting a full set of FPGA results [10, 11], two groups reporting ASIC results [12, 13], and several other groups reporting results for a subset of all candidates [14-20].

3. Design Methodology

Our design and evaluation methodologies follow exactly the approach outlined in our earlier CHES 2010 paper [11] on comparison of SHA-3 candidate variants with 256-bit outputs.

Our study is comprehensive as it covers all 14 SHA-3 candidates, and presents results for seven major families of FPGAs from two major vendors: Xilinx and Altera. The results for 512-bit variants of all candidates are compared with the results for 256-bit variants, implemented using the same language, tools, design methodology, and coding style, and reported earlier by our team in [11].

The fairness of our comparison is assured by using

- *firm optimization target*, the throughput to area ratio, that clearly guides the entire development process from the choice of a high-level architecture, through the implementation of basic operations, to the choice of low-level tool options;
- the *same library of basic operations* that are used in more than one SHA-3 candidate (such as AES SubBytes, Binary Galois Field multiplications by small constants (x02..x07), two-operand and multi-operand addition, etc. (see Table 2 in [11])

- *identical input/output interface*, proposed earlier by our group [11, 21], and applied consistently to all 256-bit and 512-bit variants of all compared algorithms;
- the *same assumptions and simplifications*, such as no padding in hardware, and no support for special modes of operation, such as tree hashing or MAC.
- the *same tools, options of tools*, and *identical optimization effort* in case of each of the evaluated hash functions;
- a *small team of designers* with similar skills, who closely collaborate with each other, and review each other's codes.

The results are then normalized by dividing them by equivalent results for the current SHA-2 standard (variant with equivalent security). Normalized results are then averaged for all investigated FPGA families.

All VHDL codes have been thoroughly verified using a universal testbench [22], capable of testing an arbitrary hash function core that follows interface described in [11, 21]. A special padding script was developed in Perl in order to pad messages included in the Known Answer Test (KAT) files distributed as a part of each candidate's submission package.

For synthesis and implementation, we have used tools developed by FPGA vendors themselves:
- for Xilinx: Xilinx ISE Design Suite v. 11.1, including Xilinx XST,
- for Altera: Quartus II v. 9.1 Subscription Edition Software.

The generation of a large number of results was facilitated by an open source benchmarking environment, called ATHENa (Automated Tool for Hardware EvaluatioN), developed at George Mason University [22].

4. Performance Measures

The three most important performance measures we use to characterize our hardware implementations of hash functions are: Throughput, Area, and Throughput to Area Ratio. Below we characterize each of these measures one by one.

4.1. Throughput

The Throughput is understood as the throughput for long messages, and does not take into account the time taken for reading the very first block of the message, initialization, finalization, and writing the hash value to the output memory. To be exact, we define Throughput using the following formula:

$$Thr = \frac{Block\_size}{T \bullet (Htime(N+1) - HTime(N))} \quad (1)$$

where *Block_size* is a message block size, characteristic for each hash function (as defined in the function specification, and shown in Table 2), *HTime*(*N*) is a total number of clock cycles necessary to hash an N-block message, *T* is a clock period, different and characteristic for each hardware implementation of a specific hash function.

All our designs follow the same interface, described in detail in [11, 21]. This interface has the following two variable parameters:

- w = the width of the input data bus, *din*, and the output data bus, *dout*. These buses are independent of each other, and both have the width w.
- $r_{IO} = Freq_{IO\_CLK}/Freq_{CLK}$, i.e., the ratio of the clock frequency for the fast I/O clock (used only for the fast communication with the surrounding circuits, typically Input and Output FIFOs), and

the clock frequency for the main clock used for data processing. If only one clock is used for both functions, $r_{IO}=1$.

The general formula for the time necessary to hash N blocks of the message can be written in the following form:

$$HTime(N) = c_{INIT} + c_{IN}/r_{IO} + c_{BLOCK} \cdot N + c_{FINAL} + c_{OUT}/r_{IO} \quad (2)$$

In this formula:

- c_{INIT} is the number of clock cycles necessary to establish communication with the source of data (typically, Input FIFO) and read the length of the message (in our formulas we assume that the length of the message is smaller than 2^w).
- c_{IN} is the number of clock cycles required to read the very first block of the message. $c_{IN} = Block\_size/w$.
- c_{BLOCK} is the number of clock cycles required to process one block of the message.
- c_{FINAL} is the number of clock cycles required for the finalization. We assume that only one finalization is required per entire message (if the finalization needs to be repeated for every block of the message, its number of clock cycles is included in c_{BLOCK}).
- c_{OUT} is the number of clock cycles required to write hash value to the destination circuit (typically Output FIFO). $c_{OUT}=output\_size/w$.

Table 1. The I/O Data Bus Width (in bits), Hash Function Execution Time (in clock cycles), and Throughput (in Mbits/s) for the 256-bit and 512-bit variants of all SHA-3 candidates and the current standard, SHA-2. T denotes the clock period in µs. Values different between 256-bit and 512-bit variants are shown in bold.

	256-bit variants			512-bit variants		
	I/O Bus Width	**Hash Time [cycles]**	**Throughput [Mbit/s]**	**I/O Bus Width**	**Hash Time [cycles]**	**Throughput [Mbit/s]**
BLAKE	64	1+8+10·N+4	512/(10·T)	64	1+**16/2**+14·N+**8/2**	**1024**/(**14**·T)
BMW	64	1+8/8+N+1	512/T	64	1+**16/16**+N+**8/16**	**1024**/T
CubeHash	64	1+4+16·N+160+4	256/(16·T)	64	1+4+16·N+160+**8**	256/(16·T)
ECHO	64	2+24+25·N+4	1536/(25·T)	64	2+**16**+**31**·N+**8**	**1024**/(**31**·T)
Fugue	32	1+2·N+18+8	32/(2·T)	32	1+**4**·N+**21+16**	32/(**4**·T)
Groestl	64	1+8+21·N+4	512/(21·T)	64	1+**16/2**+29·N+**8/2**	**1024**/(**29**·T)
Hamsi	32	2+1+3·(N-1)+6+8	32/(3·T)	**64**	2+1+6·(N-1)+6+8	**64**/(**6**·T)
JH	64	2+8+36·N+4	512/(36·T)	64	2+8+36·N+**8**	512/(36·T)
Keccak	64	1+16+24·N+4	1088/(24·T)	64	1+16+24·N+**8**	**576**/(24·T)
Luffa	64	2+4+8·N+8+4	256/(8·T)	64	2+4+8·N+8+**8**	256/(8·T)
Shabal	64	2+8+1+49·N+ 3·49+4	512/(49·T)	64	2+8+1+49·N+ 3·49+**8**	512/(49·T)
SHAvite-3	64	2+8+37·N+4	512/(37·T)	64	2+16+**57**·N+**8**	**1024**/(**57**·T)
SIMD	64	2+8+8+9·N+4	512/(9·T)	64	2+16+9+9·N+**8**	**1024**/(9·T)
Skein	64	1+4+9·N+4	256/(9·T)	64	1+8+9·N+**8**	**512**/(9·T)
SHA-2	32	1+1+65·N+8	512/(65·T)	**64**	1+1+81·N+8	**1024**/(**81**·T)

The ratio of the I/O clock frequency to the main clock frequency is selected in such a way that the following condition, given by Eq. (3) holds:

$$c_{IN}/r_{IO} \leq c_{BLOCK}. \quad (3)$$

This condition assures that any next message block (i.e. any block other than the very first block) can be read in parallel with processing of the previous block.

In Table 2, we summarize the formulas for the Hash Function Execution Time and the Throughput for all investigated algorithms. All formulas for the Hash Time, *HTime(N)*, are written in agreement with Eq. (2). If c_{FINAL}=0 for the given algorithm, this term is omitted in the equation.

The I/O bus width, *w*, was selected to be equal to 64 for majority of algorithms in order to limit the pin requirements of the hash modules. The only exceptions are Fugue-256, Hamsi-256, and Fugue-512, for which we choose *w*=32, because they all have block size equal to 32 bits, and thus cannot be sped up by using a wider I/O data bus. Similarly, SHA-256 can start processing data after receiving just one 32-bit word, and cannot be easily sped-up by using a wider input data bus. The fast I/O clock is required only in BMW-256 ($r_{IO}=8$), BLAKE-512 and Groestl-512 ($r_{IO}=2$), and BMW-512 ($r_{IO}=16$).

4.2. Area

In general the resource utilization in FPGAs, is a vector, with coordinates specific to the given FPGA family. For example,

$$Resource\ Utilization_{\text{Spartan3}} = (\#CLB\ slices, \#BRAMs, \#MULs) \quad (4)$$

$$Resource\ Utilization_{\text{Cyclone III}} = (\#LE, \#memory\_bits, \#MULs). \quad (5)$$

Taking into account that vectors cannot be easily compared to each other, we have decided to opt out of using any dedicated resources in the hash function implementations used for our comparison. Thus, all coordinates of our vectors, other than the first one have been forced (by choosing appropriate options of the synthesis and implementation tools) to be zero. This way, our resource utilization (further referred to as *Area*) is characterized using a single number, specific to the given family of FPGAs, namely the number of CLB slices (*#CLB_slices*) for Xilinx FPGAs, the number of Logic Elements (*#LE*) for Cyclone II and Cyclone III, and the number of Adaptive Look-Up Tables (#ALUTs) in Stratix II and Stratix III.

We believe that majority of SHA-3 candidates will be most naturally implemented without the use of dedicated logic resources. The capability of using such resources should be treated as a measure of the algorithm flexibility, and may be investigated in our future publications.

5. Relative Performance of the 512 and 256-bit Variants of the SHA-3 Candidates

In Table 2, we summarize major parameters of the 512 and 256-bit variants of the SHA-3 candidates and SHA-2.

The ratio of the area of the 512-bit variant to the 256-bit variant depends primarily on the datapath width. In all our hardware architectures, due to the optimization for the maximum throughput to area ratio, the datapath width is equal to the state size. As a result, the area ratio can be approximated very roughly as the state size ratio, as shown in Eq. (6) below:

$$\frac{Area(512)}{Area(256)} \approx \frac{Datapath\_width(512)}{Datapath\_width(256)} = \frac{State\_size(512)}{State\_size(256)} \quad (6)$$

Table 2. Major parameters of the 256-bit and 512-bit variants of all SHA-3 candidates and the current standard, SHA-2. Values different between 256-bit and 512-bit variants are shown in bold. The first approximations of the predicted area ratio (512 vs. 256-bit variant) and the predicted throughput ratio (512 vs. 256-bit variant) are given in the last two columns.

	256-bit variant				512-bit variant				Predicted Area Ratio (based on Eq. (6))	Predicted Thr Ratio (based on Eq. (8))
	State size	Block size	Round no	Word size	State size	Block size	Round no	Word size		
BLAKE	**512**	**512**	**10**	32	**1024**	**1024**	**14**	**64**	**2**	**1.43**
BMW	**512**	**512**	**16**	32	**1024**	**1024**	**16**	**64**	**2**	**2**
CubeHash	1024	256	16	32	1024	256	16	32	1	1
ECHO	2048	**1536**	**8**	32	2048	**1024**	**10**	32	1	**0.53**
Fugue	**960**	32	**2**	32	**1152**	32	**4**	32	**1.2**	**0.5**
Groestl	**512**	**512**	**10**	64	**1024**	**1024**	**14**	64	**2**	**1.43**
Hamsi	**512**	**32**	**3**	32	**1024**	**64**	**6**	32	**2**	**1**
JH	1024	512	36	64	1024	512	36	64	1	1
Keccak	1600	**1088**	24	64	1600	**576**	24	64	1	**0.53**
Luffa	**768**	256	8	32	**1280**	256	8	32	**1.67**	**1**
Shabal	1408	512	48	32	1408	512	48	32	1	1
SHAvite-3	**512**	**512**	**36**	32	**1024**	**1024**	**56**	32	**2**	**1.29**
SIMD	**512**	**512**	36	32	**1024**	**1024**	36	32	**2**	**2**
Skein	**256**	**256**	72	64	**512**	**512**	72	64	**2**	**2**
SHA-2	**256**	**512**	64	**32**	**512**	**1024**	**80**	**64**	**2**	**1.60**

The additional factors that affect this ratio include:

- *message block size*, which determines the size of the input shift register
- *output size*, which determines the size of the output shift register
- *logic of the main round*, which may be more complex in the case of a 512-bit variant of a function
- logic required for *initialization and finalization*, which may not follow the datapath width
- size of the *control unit*, which is likely to remain constant between two variants, but typically contributes only small percentage to the total circuit area.

All these factors cause that the Eq. (6) is only the first approximation, and the actual results may vary and may be dependent on a particular FPGA family.

The throughput of each variant is given by

$$Thr(k) = \frac{Block\_size(k)}{c \bullet Round\_no(k) \bullet T(k, Word\_size(k))} \tag{7}$$

where

- k denotes output size, 256 or 512 bits;
- c is a number of main rounds executed in a single clock cycle (possibly a fraction). In our implementations, this number is constant and independent of the function variant.
- $T(k, Word\_size(k))$ is a minimum clock period, which is a function of the logic included in the main round, and in particular of the word size.

In majority of considered algorithms, with the exception of BLAKE, BMW, and SHA-2, the word size remains the same between the two variants. Additionally, the logic of the main round remains either the

same, or at least have the similar critical path. As a result, the following first order approximation, given in Eq. (8), can be used to estimate the throughput ratio:

$$\frac{Thr(512)}{Thr(256)} \approx \frac{\frac{Bloc\_size(512)}{Block\_size(256)}}{\frac{Round\_no(512)}{Round\_no(256)}} = \frac{Block\_size\_ratio}{Round\_no\_ratio} \tag{8}$$

For BLAKE, BMW, and SHA-2, the ratio is expected to be smaller because of the increase in the word size from 32 bits to 64-bits, and the influence of this change on the delay of the multi-operand additions, which appear in the critical paths of these algorithms. At the same time, this effect is expected to be significantly smaller than 2, because of

- the properties of the fast carry chain adders embedded in Xilinx and Altera FPGAs (the delay of these adders as a function of the number of bits, n, is given by $d(n) = a \cdot n + b$, with the relatively large b and small a); and
- the fact that the multi-operand adder constitutes only a fraction of the critical path.

The first rough approximations of the area ratio (based on Eq. (6)) and the throughput ratio (based on Eq. (8)) are given in the last two columns of Table 2. Based on these approximations, we can divide 15 investigated algorithms into the following 6 major groups:

- Group 1: area and throughput are not affected by the change of the output size: *CubeHash*, *JH*, *Shabal*.
- Group 2: area and throughput both double: *BMW*, *SIMD*, *Skein*.
- Group 3: area and throughput both increase, but area increases more: *BLAKE*, *Groestl*, *SHAvite-3*, and *SHA-2*.
- Group 4: area stays the same and throughput decreases: *ECHO*, *Keccak*.
- Group 5: throughput stays the same and area increases: *Hamsi*, *Luffa*.
- Group 6: area increases and throughput decreases: *Fugue*.

Table 3. Major performance measures of SHA-3 candidates (512-bit and 256-bit variants) when implemented in Xilinx Virtex 5 FPGAs

	Max Clk Freq [MHz]			Throughput [Mbit/s]			Area [CLB slices]			Throughput/Area		
	512	**256**	**ratio**	**512**	**256**	**ratio**	**512**	**256**	**ratio**	**512**	**256**	**ratio**
BLAKE	27.14	31.80	0.85	1985.02	1628.16	1.22	5429	2078	2.61	0.37	0.78	0.47
BMW	N/A	13.31	N/A	N/A	6814.72	N/A	N/A	5647	N/A	N/A	1.21	N/A
CubeHash	141.70	137.00	1.03	2267.25	2192.00	1.03	775	699	1.11	2.93	3.14	0.93
ECHO	130.58	156.60	0.83	4313.42	9621.50	0.45	6987	5986	1.17	0.62	1.61	0.38
Fugue	106.62	109.19	0.98	852.97	1747.10	0.49	1097	912	1.20	0.78	1.92	0.41
Groestl	161.34	189.72	0.85	5697.04	4625.48	1.23	4294	2390	1.80	1.33	1.94	0.69
Hamsi	128.40	152.70	0.84	1369.63	1628.80	0.84	2508	1011	2.48	0.55	1.61	0.34
JH	213.77	282.20	0.76	3040.24	4013.51	0.76	1569	1275	1.23	1.94	3.15	0.62
Keccak	157.18	165.07	0.95	3772.39	7483.22	0.50	1417	1414	1.00	2.66	5.29	0.50
Luffa	111.43	124.30	0.90	3565.86	3977.60	0.90	3122	1641	1.90	1.14	2.42	0.47
Shabal	156.30	151.33	1.03	1633.17	1581.24	1.03	1355	1261	1.07	1.21	1.25	0.96
SHAvite-3	163.08	139.00	1.17	2929.70	1923.46	1.52	2632	1199	2.20	1.11	1.60	0.69
SIMD	27.99	29.59	0.95	3184.07	1683.34	1.89	16996	7671	2.22	0.19	0.22	0.85
Skein	27.20	31.70	0.86	1547.32	901.69	1.72	2120	1476	1.44	0.73	0.61	1.19
SHA-2	150.20	153.60	0.98	1898.76	1209.90	1.57	813	429	1.90	2.34	2.82	0.83

Table 4. Major performance measures of SHA-3 candidates (512-bit and 256-bit variants) when implemented in Altera Stratix III FPGAs

	Max Clk Freq [MHz]			Throughput [Mbit/s]			Area [ALUTs]			Throughput/Area		
	512	**256**	**ratio**	**512**	**256**	**ratio**	**512**	**256**	**ratio**	**512**	**256**	**ratio**
BLAKE	39.07	51.63	0.76	2857.69	2643.46	1.08	10927	5780	1.89	0.26	0.46	0.57
BMW	8.26	16.45	0.50	8458.24	8422.40	1.00	47575	12632	3.77	0.18	0.67	0.27
CubeHash	203.17	228.00	0.89	3250.72	3648.00	0.89	1931	1934	1.00	1.68	1.89	0.89
ECHO	163.26	164.20	0.99	5392.85	10088.45	0.53	22069	21689	1.02	0.24	0.47	0.53
Fugue	204.33	204.67	1.00	1634.64	3274.72	0.50	2760	2541	1.09	0.59	1.29	0.46
Groestl	302.30	298.24	1.01	10674.32	7271.38	1.47	9777	4929	1.98	1.09	1.48	0.74
Hamsi	164.61	244.14	0.67	1755.84	2604.16	0.67	6589	2265	2.91	0.27	1.15	0.23
JH	339.44	346.40	0.98	4827.59	4926.58	0.98	3608	3117	1.16	1.34	1.58	0.85
Keccak	295.68	296.30	1.00	7096.32	13432.27	0.53	3930	4458	0.88	1.81	3.01	0.60
Luffa	214.32	265.04	0.81	6858.24	8481.28	0.81	7758	3395	2.29	0.88	2.50	0.35
Shabal	219.73	210.75	1.04	2295.95	2202.12	1.04	3413	3382	1.01	0.67	0.65	1.03
SHAvite-3	192.53	255.00	0.76	3458.78	3528.65	0.98	5732	2497	2.30	0.60	1.41	0.43
SIMD	40.89	45.74	0.89	4652.37	2602.10	1.79	50093	23310	2.15	0.09	0.11	0.83
Skein	50.91	49.30	1.03	2896.21	1402.31	2.07	6396	3622	1.77	0.45	0.39	1.17
SHA-2	234.80	199.80	1.18	2968.34	1573.81	1.89	1620	978	1.66	1.83	1.61	1.14

Table 5. Ratio of the respective performance measures (Throughput (Thr), Area, Throughput to Area Ratio (Thr/Area)) for a 512-bit variant vs. 256-bit variant, averaged (using geometric mean) over all 7 FPGA families (Overall), 3 Xilinx families, and 4 Altera Families.

	Overall 512 vs. 256 variant			Xilinx Families 512 vs. 256 variant			Altera Families 512 vs. 256 variant		
	Thr	**Area**	**Thr/Area**	**Thr**	**Area**	**Thr/Area**	**Thr**	**Area**	**Thr/Area**
BLAKE	1.11	2.00	0.56	1.23	2.23	0.55	1.06	1.89	0.56
BMW	1.00	3.77	0.27	N/A	N/A	N/A	1.00	3.77	0.27
CubeHash	1.01	1.07	0.95	1.05	1.10	0.95	0.98	1.04	0.94
ECHO	0.48	1.09	0.45	0.48	1.14	0.43	0.49	1.04	0.47
Fugue	0.50	1.17	0.42	0.49	1.18	0.42	0.50	1.17	0.43
Groestl	1.29	1.95	0.66	1.18	1.91	0.62	1.38	1.98	0.69
Hamsi	0.61	2.63	0.23	0.75	2.41	0.31	0.52	2.82	0.18
JH	0.98	1.08	0.90	0.94	1.06	0.88	1.01	1.09	0.92
Keccak	0.52	0.91	0.57	0.53	0.95	0.56	0.52	0.88	0.59
Luffa	0.88	2.25	0.39	1.06	2.11	0.50	0.77	2.36	0.33
Shabal	1.07	1.01	1.06	1.12	1.07	1.05	1.03	0.96	1.07
SHAvite-3	1.18	2.35	0.50	1.38	2.49	0.55	1.05	2.25	0.47
SIMD	1.78	2.23	0.80	1.80	2.30	0.78	1.77	2.15	0.82
Skein	1.93	1.62	1.19	1.85	1.54	1.20	2.07	1.76	1.18
SHA-2	1.65	1.72	0.96	1.58	1.45	1.12	1.67	1.75	0.95

From the point of view of the throughput to area ratio, Groups 1 and 2 are the best, followed by Groups 3, 4, and 5, and ending with the Group 6, with the worst trend. Among the Groups 1 and 2, belonging to the Group 2 is less desirable, especially for the algorithms that already take significant area for a 256-bit variant, such as BMW and SIMD.

In Tables 3 and 4, we report the actual performance measures of the 512-bit and the 256-bit variants of all investigated algorithms, for the case of Xilinx Virtex 5 and Altera Stratix III, respectively.

In Table 5, we report ratios of all three major performance measures (Throughput, Area, and Throughput to Area Ratio) for a 512-bit variant vs. a 256-bit variant, averaged (using geometric mean) over

- all seven FPGA families,
- three Xilinx families (Spartan 3, Virtex 4 and Virtex 5), and
- four Altera families (Cyclone II and III, Stratix II and III).

Based on this table, there seems to be a pretty good agreement between the values of respected ratios for Xilinx and Altera families, with the largest discrepancies (over 25%) seen in case of the Throughput and Area of Luffa, and the Area of SHA-2.

The comparison of the rough approximations for the ratios of Throughputs and Areas based on Equations (6) and (8) (see the last two columns of Table 2) with the actual values of these ratios averaged over seven families of FPGAs (see Table 5, Overall, Thr and Area columns) reveals a very good agreement between our predictions and experimental results. The only algorithms, for which the ratios are substantially different are listed below together with the short explanation:

BMW: the area ratio seems to be substantially larger than expected (3.77 vs. 2). This effect is most likely caused be the routing congestion, which also prevented this circuit from being fully placed and routed for six out of seven investigated FPGAs families, other than Stratix III. The additional reason for a very large area might have been the replacement of a tree of carry propagate adders (used in BMW-256) by a tree of carry save adders, which appeared to be necessary to facilitate routing.

Hamsi: the area ratio is larger than expected (2.63 vs. 2) and the throughput ratio smaller than expected (0.61 vs. 1). Both effects seem to be caused by our implementation of the message expansion unit, which is based on look-up tables. The total size of the look-up tables for the 512-bit variant is four times bigger than for the 256-bit variant (1 Mbit vs. 256 kbit). Additionally, all table look-ups in the 256-bit version can be performed in parallel, while in the 512-bit variant, two groups of the table look-ups need to be performed sequentially, one by one, because of the data dependency.

Keccak: the area ratio is smaller than predicted (0.91 vs. 1). This effect is caused by the smaller value of the block size for the 512-bit variant of the algorithm (576 bits vs. 1088 bits). This value affects only the size of the input shift register, and has no influence on the size of the datapath. It should be noted that the size of the output shift register increases in the 512-bit variant (512-bits vs. 256-bits) but this increase is smaller than the decrease in the size of the input register.

Luffa: the area ratio is larger than predicted (2.25 vs. 1.67), and the throughput ratio smaller than predicted (0.88 vs. 1). This effect can be explained by the more complex computations performed in the 512-bit variant of Luffa during the Message Injection phase. In particular, the GF(2^8) constants used as inputs in Galois Field multiplications, change from small values of {1, 2, 3, 4} to the larger values including {01, 02, 04, 08, 10, 0A, 0F}.

6. Results

In Table 6, the maximum clock frequencies are listed for each pair: hash algorithm – FPGA family. These frequencies can be used together with the formulas provided in Table 1, in order to compute the exact execution times of each algorithm (depending on the number of message blocks, N) and the values of the throughputs for long messages. The clock period (in microseconds), T, is a direct inverse of the clock frequency, f, in MHz. Thus, in the formulas from Table 1, we can replace directly $1/T$ by f, and we will obtain the Throughput in Mbits/s.

Table 6. Clock frequencies of all SHA-3 candidates (512-bit variants) and SHA-512 expressed in MHz (post placing and routing)

Candidate	Spartan 3	Virtex 4	Virtex 5	Cyclone II	Cyclone III	Stratix II	Stratix III
BLAKE	N/A	25.024	27.139	17.22	21.14	31.01	39.07
BMW	N/A	N/A	N/A	N/A	N/A	N/A	8.26
CubeHash	81.967	138.217	141.703	116.27	128.63	150.6	203.17
ECHO	52.787	114.233	130.582	N/A	79.67	107.54	163.26
Fugue	56.664	84.488	106.621	83.54	98	142.61	204.33
Groestl	66.181	120.671	161.342	153.78	179.02	208.38	302.3
Hamsi	57.61	128.833	128.403	61.96	77.65	99.54	164.61
JH	105.787	194.175	213.767	173.55	196.31	264.46	339.44
Keccak	80.386	135.63	157.183	149.61	171.88	196.66	295.68
Luffa	57.359	110.132	111.433	80.05	117.26	155.93	214.32
Shabal	53.882	131.01	156.299	117.45	125.85	165.45	219.73
SHAvite-3	67.6	118.666	163.079	79.51	93.91	142.17	192.53
SIMD	N/A	24.01	27.985	N/A	N/A	29.63	40.89
Skein	16.531	32.227	27.199	N/A	N/A	38.19	50.91
SHA-512	85.616	153.965	150.195	93.41	119.39	167.25	234.8

Table 7. Results for the reference implementation of SHA-512 (architecture with rescheduling [])

	Spartan 3	Virtex 4	Virtex 5	Cyclone II	Cyclone III	Stratix II	Stratix III
Max. Clk Freq. [MHz]	85.62	153.97	150.20	93.41	119.39	167.25	234.80
Throughput [Mbit/s]	1082.36	1946.42	1898.76	1180.89	1509.33	2114.37	2968.34
Area	1531	1488	813	3633	4137	1623	1620
Throughput to Area Ratio	0.71	1.31	2.34	0.33	0.36	1.30	1.83

For several algorithms, implementing (placing & routing) the 512-bit variant was not possible for low cost FPGA families, such as Spartan 3 from Xilinx and Cyclone II and Cyclone III from Altera. These cases are denoted by "N/A" in Table 6 and in subsequent Tables 8-10. BMW-512 is a special case in the sense that we have been able to properly route the circuit for only one out of seven investigated FPGA families, namely for Stratix III. For all remaining families, routing was not possible, despite the fact that the tested FPGA devices contained more than sufficient number of logic resources. This is certainly one of the major drawbacks of BMW, which is also relatively inflexible in terms of trading speed for area.

In Table 7, we summarize the absolute results obtained for our implementation of the current standard SHA-512. The results are repeated for all seven FPGA families used in our study. As hardware architecture, we have selected the architecture by Chaves et al., presented at CHES 2006 [23]. This architecture has been specifically optimized for the maximum throughput to area ratio [23, 24] and is considered one of the best known SHA-2 architectures of this type.

In the following analysis, the absolute values of the three major performance measures: throughput, area, and the throughput to area ratio, for the 512-bit variants of all SHA-3 candidates, have been normalized by dividing them by the corresponding values for the reference implementation of SHA-512. The corresponding ratios, referred to as normalized throughput, normalized area, and normalized throughput to area ratios are summarized in Tables 8, 9, and 10. In all these tables, the Overall column represents the geometric mean of all normalized results, averaged over all seven investigated FPGA

families. The candidate algorithms are ranked based on the value of this Overall metric, representing the performance for a wide range of different FPGA families.

In Table 8, the normalized throughputs are reported. Only four candidates, Groestl, BMW, Keccak, and Luffa outperform SHA-512 by a factor larger then two. The additional 6 candidates have a normalized throughput in the range from 1 to 2. Four candidates, Skein, Shabal, Hamsi, and Fugue, are slower than SHA-512, with Fugue, slower by more than a factor of two.

In Table 9, the normalized areas are reported. Based on this table, all SHA-3 candidates, in their 512-bit variants, are larger than SHA-512. The spread of results is much larger than in the case of the throughput, with the smallest SHA-3 candidate, CubeHash, almost the same size as SHA-512, and the largest two, BMW and SIMD, lagging behind by a factor of almost 30. The leading group, including Cubehash, Fugue, Shabal, Keccak, and JH covers the range from 1.1 to 2.2, and includes only one candidate, Keccak, who excells also in terms of speed.

Table 8. Throughput of all SHA-3 candidates (512-bit variants) normalized to the throughput of SHA-512

Candidate	Spartan 3	Virtex 4	Virtex 5	Cyclone II	Cyclone III	Stratix II	Stratix III	Overall
Groestl	2.16	2.19	3.00	4.60	4.19	3.48	3.60	3.20
BMW	N/A	N/A	N/A	N/A	N/A	N/A	2.85	2.85
Keccak	1.78	1.67	1.99	3.04	2.73	2.23	2.39	2.22
Luffa	1.70	1.81	1.88	2.17	2.49	2.36	2.31	2.08
ECHO	1.61	1.94	2.27	0.00	1.74	1.68	1.82	1.83
JH	1.39	1.42	1.60	2.09	1.85	1.78	1.63	1.66
SIMD	N/A	1.40	1.68	N/A	N/A	1.59	1.57	1.56
CubeHash	1.21	1.14	1.19	1.58	1.36	1.14	1.10	1.24
SHAvite-3	1.12	1.10	1.54	1.21	1.12	1.21	1.17	1.20
BLAKE	N/A	0.94	1.05	1.07	1.02	1.07	0.96	1.02
Skein	0.87	0.94	0.81	N/A	N/A	1.03	0.98	0.92
Shabal	0.52	0.70	0.86	1.04	0.87	0.82	0.77	0.78
Hamsi	0.57	0.71	0.72	0.56	0.55	0.50	0.59	0.59
Fugue	0.42	0.35	0.45	0.57	0.52	0.54	0.55	0.48

Table 9. Area (utilization of programmable logic blocks) of all SHA-3 candidates (512-bit variants) normalized to the area of SHA-512

Candidate	Spartan 3	Virtex 4	Virtex 5	Cyclone II	Cyclone III	Stratix II	Stratix III	Overall
CubeHash	1.30	1.32	0.95	0.99	0.88	1.19	1.19	1.11
Fugue	2.03	2.15	1.35	2.00	1.75	1.82	1.70	1.81
Shabal	2.04	2.37	1.67	1.66	1.47	2.10	2.11	1.89
Keccak	2.03	2.27	1.74	1.46	1.30	2.45	2.43	1.90
JH	2.65	2.77	1.93	2.12	1.87	2.23	2.23	2.23
Hamsi	2.97	3.06	3.08	2.45	2.08	4.14	4.07	3.04
Skein	3.39	3.64	2.61	N/A	N/A	3.95	3.95	3.47
Luffa	4.32	4.38	3.84	3.25	2.83	4.83	4.79	3.97
SHAvite-3	6.49	6.58	3.24	5.74	5.05	3.46	3.54	4.68
BLAKE	N/A	7.77	6.68	4.81	4.22	6.82	6.75	6.04
Groestl	12.82	13.03	5.28	9.55	8.35	6.04	6.04	8.23
ECHO	18.25	18.76	8.59	0.00	17.40	13.48	13.62	14.53
SIMD	N/A	28.65	20.91	N/A	N/A	31.57	30.92	27.65
BMW	N/A	N/A	N/A	N/A	N/A	N/A	29.37	29.37

Table 10. Throughput to Area Ratio of all SHA-3 candidates normalized to the throughput to area ratio of SHA-512

Candidate	Spartan 3	Virtex 4	Virtex 5	Cyclone II	Cyclone III	Stratix II	Stratix III	Overall
Keccak	0.88	0.74	1.14	2.09	2.11	0.91	0.99	1.16
CubeHash	0.94	0.86	1.25	1.59	1.55	0.96	0.92	1.12
JH	0.52	0.51	0.83	0.98	0.99	0.80	0.73	0.74
Luffa	0.39	0.41	0.49	0.67	0.88	0.49	0.48	0.52
Shabal	0.25	0.30	0.52	0.62	0.59	0.39	0.37	0.41
Groestl	0.17	0.17	0.57	0.48	0.50	0.58	0.60	0.39
Skein	0.26	0.26	0.31	N/A	N/A	0.26	0.25	0.27
Fugue	0.21	0.16	0.33	0.28	0.30	0.30	0.32	0.26
SHAvite-3	0.17	0.17	0.48	0.21	0.22	0.35	0.33	0.26
Hamsi	0.19	0.23	0.23	0.23	0.26	0.12	0.15	0.20
BLAKE	N/A	0.12	0.16	0.22	0.24	0.16	0.14	0.17
ECHO	0.09	0.10	0.26	0.00	0.10	0.12	0.13	0.13
BMW	N/A	N/A	N/A	N/A	N/A	N/A	0.10	0.10
SIMD	N/A	0.05	0.08	N/A	N/A	0.05	0.05	0.06

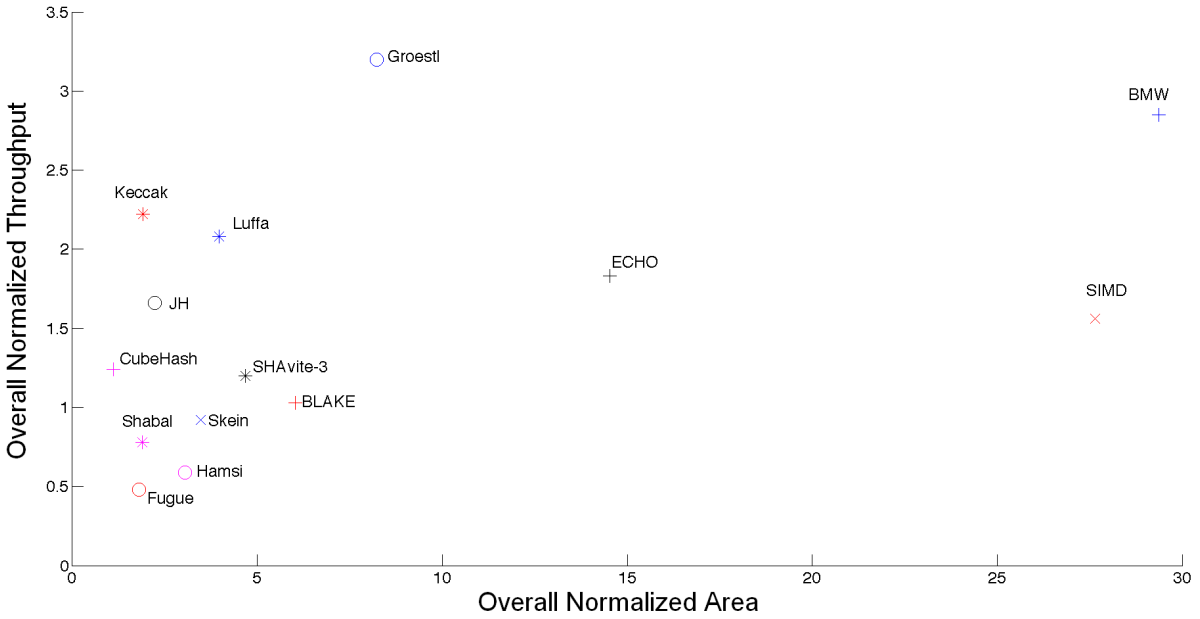

Fig. 1. Relative performance of all Round 2 SHA-3 Candidates (512-bit variants) in terms of the overall normalized throughput and the overall normalized area (with SHA-512 used as a reference point).

In Table 10, the throughput to area ratio is reported. This table is the best considered together with Fig. 1, which presents a two dimensional diagram, with Normalized Area on the X-axis and Normalized Throughput on the Y-axis. Only two algorithms, Keccak and CubeHash, outperform SHA-512 in terms of the throughput to area ratio. Out of them Keccak is almost twice as fast, but CubeHash is about 70% smaller. ECHO, SIMD, and BMW are more than 8 times worse than Keccak in terms of the throughput to area ratio, and more than 7 times bigger. The implementations of these algorithms are not likely to scale to the same performance region as implementations of majority of other candidates, even if significantly trading speed for reduced area. BLAKE and Hamsi also lag behind in terms of the throughput to area ratio by a factor of 5 and 6, respectively, compared to Keccak.

7. Conclusions

Our evaluation methodology, applied to 512-bit variants of all 14 Round 2 SHA-3 candidates, has demonstrated large differences among competing candidates. The ratio of the best result to the worst result was equal to about 7 in terms of the throughput (Groestl vs. Fugue), about 27 in terms of area (CubeHash vs. BMW), and about 19 in terms of our primary optimization target, the throughput to area ratio (Keccak vs. SIMD). Only two candidates, Keccak and CubeHash, have demonstrated the throughput to area ratio better than the current standard SHA-512. Out of these three algorithms, Keccak have also demonstrated very high throughputs, while CubeHash outperformed other candidates in terms of minimum area. Almost all candidates, except Fugue, Hamsi, Shabal, and Skein, outperform SHA-512 in terms of the throughput, but at the same time none of them, except CubeHash, matches SHA-512 in terms of the area.

Future work will include the development of different architectures of SHA-3 candidates, representing various trade-offs between speed and area. The uniform padding units will be added to each SHA core, and their cost estimated. In terms of FPGA families, our study will be extended to the most recent families of FPGAs from two major vendors, namely Spartan 6 and Virtex 6 from Xilinx, and Cyclone IV, Stratix IV, and Arria II from Altera. We will also investigate the influence of synthesis tools from different vendors (e.g., Synplify Pro from Synopsys). The evaluation may be also extended to the cases of hardware architectures optimized for the minimum area (cost) and minimum power consumption. Each algorithm will be also evaluated in terms of its suitability for implementation using dedicated FPGA resources, such embedded memories, dedicated multipliers, and DSP units. Finally, an extension of our methodology to the standard-cell ASIC technology will be investigated.

References

[1] FIPS 180-3, Secure Hash Standard (SHS), October 2008, available at http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html

[2] NIST's SHA-3 Contest: http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

[3] BlueCrypt, Cryptographic Key Length Recommendation, available at http://www.keylength.com/

[4] Recommendation for Key Management, Special Publication 800-57 Part 1, NIST, 03/2007, available at http://csrc.nist.gov/groups/ST/toolkit/key_management.html

[5] Fact Sheet Suite B Cryptography, NSA, 03/2010, available at http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

[6] Yearly Report on Algorithms and Keysizes (2009), D.SPA.7 Rev. 1.0, ICT-2007-216676 ECRYPT II, 07/2009, available at http://www.ecrypt.eu.org/documents/D.SPA.7.pdf

[7] T. Grembowski, R. Lien, K. Gaj, N. Nguyen, P. Bellows, J. Flidr, T. Lehman, B. Schott, "Comparative Analysis of the Hardware Implementations of Hash Functions SHA-1 and SHA-512," LNCS 2433, Information Security, Eds. G. I. Davida, Y. Frankel, 5th International Conference, ISC 2002, Sao Paulo, Brazil, Sep./Oct. 2002, pp. 75-89.

[8] SHA-3 Zoo : http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo

[9] SHA-3 Hardware Implementations: http://ehash.iaik.tugraz.at/wiki/SHA-3_Hardware_Implementations
[10] K. Kobayashi, et al., "Evaluation of hardware performance for the SHA-3 candidates using SASEBO-GII. Cryptology ePrint Archive, Report 2010/010, 2010. http://eprint.iacr.org/.
[11] K. Gaj, E. Homsirikamol, and M. Rogawski, "Fair and Comprehensive Methodology for Comparing Hardware Performance of Fourteen Round Two SHA-3 Candidates using FPGAs," Proc. Cryptographic Hardware and Embedded Systems workshop, CHES 2010, Santa Barbara, Aug. 2010 (in print).
[12] S. Tillich, et al. "High-speed hardware implementations of Blake, Blue Midnight Wish, Cubehash, ECHO, Fugue, Grøstl, Hamsi, JH, Keccak, Luffa, Shabal, Shavite-3, SIMD, and Skein. Cryptology ePrint Archive, Report 2009/510, 2009. http://eprint.iacr.org/.
[13] L. Henzen, P. Gendotti, P. Guillet, E. Pargaetzi, M. Zoller and F.K. Gurkaynak, "Developing a Hardware Evaluation Method for SHA-3 Candidates," Proc. Cryptographic Hardware and Embedded Systems workshop, CHES 2010, Santa Barbara, Aug. 2010 (in print).
[14] B. Baldwin, et al., "FPGA implementations of SHA-3-3 candidates: Cubehash, Grøstl, Lane, Shabal and Spectral Hash. Cryptology, ePrint Archive, Report 2009/342, 2009. http://eprint.iacr.org/.
[15] I. Verbauwhede and M. Kneevic, "Hardware evaluation of the Luffa hash family. COSIC Publication, Online, 2009. http://www.cosic.esat.kuleuven.be/publications/article-1282.pdf.
[16] J. Apfelbeck, B. Jungk, S. Reith, "On optimized FPGA implementations of the SHA-3 candidate Grøstl. Cryptology ePrint Archive, Report 2009/206, 2009. http://eprint.iacr.org/.
[17] Joachim Strombergson, "Implementation of the Keccak hash function in FPGA devices," Online, 2008. http://www.strombergson.com/files/.
[18] M. Bernet, et al., "Hardware implementations of the SHA-3 candidates Shabal and Cubehash," Circuits and Systems, pp. 515-518, 2009. 52nd IEEE International Midwest Symposium.
[19] M. Long, "Implementing Skein hash function on Xilinx Virtex-5 FPGA platform. Online, 2010. http://www.skein-hash.info/sites/default/files/.
[20] A.H. Namin and M.A. Hasan. Hardware implementation of the compression function for selected SHA-3 candidates. In CACR 2009-28, page 29, July 2009.
[21] "Hardware Interface of a Secure Hash Algorithm (SHA)," by CERG Team, George Mason University, 2010, available at http://cryptography.gmu.edu/athena/index.php?id=interfaces
[22] "ATHENa Project Website," http://cryptography.gmu.edu/athena/.
[23] R. Chaves, G. Kuzmanov, L. Sousa and S.Vassiliadis, "Improving SHA-2 hardware implementations, In Workshop on Cryptographic Hardware and Embedded Systems, CHES 2006.
[24] R. Chaves, G. Kuzmanov, L. Sousa, and S. Vassiliadis, "Cost efficient SHA hardware accelerators," in IEEE Transactions on Very Large Scale Integration Systems, Aug 2008, pp. 999–1008.