On the Computational Asymmetry of the S-boxes Present in Blue Midnight Wish Cryptographic Hash Function

Danilo Gligoroski[1] and Vlastimil Klima[2]

[1] Department of Telematics, Norwegian University of Science and Technology, O.S.Bragstads plass 2B, N-7491 Trondheim, NORWAY
`danilo.gligoroski@item.ntnu.no`
[2] Independent cryptologist - consultant, Czech Republic
`v.klima@volny.cz`

Abstract. Blue Midnight Wish hash function is one of 14 candidate functions that are continuing in the Second Round of the SHA-3 competition. In its design it has several S-boxes (bijective components) that transform 32-bit or 64-bit values. Although they look similar to the S-boxes in SHA-2, they are also different.

It is well known fact that the design principles of SHA-2 family of hash functions are still kept as a classified NSA information. However, in the open literature there have been several attempts to analyze those design principles. In this paper first we give an observation on the properties of SHA-2 S-boxes and then we investigate the same properties in Blue Midnight Wish.

1 Introduction

Cryptographic hash functions are considered as the fundamental building part of the modern cryptography and information security. They are present in numerous protocols and schemes such as digital signatures, commitment schemes, password protection schemes, in algorithms for checking the data integrity, key derivation functions and cryptographic random number generators, authentication schemes and many others.

The most well known family of cryptographic hash functions is the so-called MD4 family to which belong the hash functions: MD4, MD5, SHA-0, SHA-1 and SHA-2.

MD4 and MD5 were designed by Ronald Rivest [1, 2] and SHA family was designed by NSA and adopted by National Institut of Standards and Technology (NIST) as a US federal standard [3, 4]. According to the time plan of the approved use of cryptographic hash functions, the SHA-2 functions are intended to replace SHA-1 in 2010 [4].

Being the most important part of the design of numerous cryptographic algorithms and schemes, cryptographic hash functions of the MD4 family in the last 15–20 years have been scrutinized by numerous cryptographers and we have witnessed several successful attacks and breakthroughs in their cryptanalysis. We can mention the cryptanalysis of den Boer and Bosselaers [5, 6] in 1991 and 1993, Vaudenay [7] in 1995, Dobbertin [8] in 1996 and 1998, Chabaud and Joux [9] in 1998, Biham and Chen [10] in 2004, and Wang et al. [11–14] in 2005. Note that the fastest method for finding MD5 collisions (so called "Tunneling method") was discovered by Klima in 2006 [29] and it is able to generate collisions in several seconds on a standard PC. In short, the most well known cryptographic hash functions such as: MD4, MD5, SHA-0 and SHA-1, have succumbed to those attacks, but so far SHA-2 family remains unbroken.

Since SHA-2 was designed by NSA, the design principles behind its construction are not publicly available. However, several public papers produced by the academic cryptographic community have been devoted to the cryptanalysis of SHA-2 hash functions. Gilbert and Handschuh in 2003 have made an analysis of the SHA-2 family [15]. They proved that there exist XOR-differentials that give a 9-round local collision with probability 2^{-66}. In 2004, Hawkes, Paddon and Rose [16] improved the result and showed existence of addition-differentials of 9-round local collisions with probability of 2^{-39}. Different variants of SHA-256 have been analyzed in 2005 by

Yoshida and Biryukov [17] and by Matusiewicz et al., [18]. In 2006, Mendel et al. [19], found XOR-differentials for 9-round local collisions, also with probability 2^{-39} (recently improved to the value 2^{-38} [20]). In 2008, Nikolič and Biryukov have found collisions in 21 step reduced SHA-256, and their attack was afterwards improved by Indesteege et al., up to 24 steps [22].

Following the developments in the field of cryptographic hash functions, NIST organized two cryptographic hash workshops [23] in 2005 and 2006 respectively. As a result of those workshops, NIST decided to run a 4 year world-wide open hash competition for selection of the new cryptographic hash standard SHA-3 [24]. The requirements for the hash digest size for the new cryptographic hash functions are: 224, 256, 384 and 512 bits - the same as for the current SHA-2 standard. Out of 64 initial submissions, 51 entered the First Round [25], and 14 have been selected for the Second Round of the SHA-3 competition [26].

BLUE MIDNIGHT WISH hash function is the fastest hash function among 14 candidates in the Second Round of the SHA-3 competition [27]. It has several bijective components (S-boxes) that look like the bijective components in SHA-2. In this paper we will describe some of the principles how these components were chosen showing also comparison between the similar bijective components that are present in SHA-2 functions.

The paper is organized as follows: In Section 2 we give some basic observations on the properties of the four S-boxes present in SHA-2 design, in Section 3 we analyze the S-boxes of BLUE MIDNIGHT WISH according to the observed properties of SHA-2 S-boxes, and we end the paper with Conclusions and future work.

2   Observations on some properties of the SHA-2 S-boxes

SHA-2 is actually a family of four hash functions with outputs of 224, 256, 384 and 512 bits, and accordingly, sometimes SHA-2 functions are denoted as SHA-224, SHA-256, SHA-384 and SHA-512. The full description of SHA-2 family can be found in [4].

The main difference between those four functions is that SHA-224 and SHA-256 are defined by operations performed on 32-bit variables, while SHA-384 and SHA-512 are defined by operations performed on 64-bit variables.

We give here the definitions of four S-boxes (or bijective transformations) present in the design of SHA-2 that acts either on 32 or 64 bits, while the rest of the design specifics are not important for this paper.

For SHA-224/256 those four bijective transformations are defined as:

$$
\begin{aligned}
\Sigma_0^{256}(x) &= ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x) \\
\Sigma_1^{256}(x) &= ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x) \\
\sigma_0^{256}(x) &= ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x) \\
\sigma_1^{256}(x) &= ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x)
\end{aligned}
\tag{1}
$$

where $ROTR^n(x)$ means rotation of the 32-bit variable x to the right for n positions and $SHR^n(x)$ means shifting of the 32-bit variable x to the right for n positions.

For SHA-384/512 the four bijective transformations are defined as:

$$
\begin{aligned}
\Sigma_0^{512}(x) &= ROTR^{28}(x) \oplus ROTR^{34}(x) \oplus ROTR^{39}(x) \\
\Sigma_1^{512}(x) &= ROTR^{14}(x) \oplus ROTR^{18}(x) \oplus ROTR^{41}(x) \\
\sigma_0^{512}(x) &= ROTR^1(x) \oplus ROTR^8(x) \oplus SHR^7(x) \\
\sigma_1^{512}(x) &= ROTR^{19}(x) \oplus ROTR^{61}(x) \oplus SHR^6(x)
\end{aligned}
\tag{2}
$$

where $ROTR^n(x)$ means rotation of the 64-bit variable x to the right for n positions and $SHR^n(x)$ means shifting of the 64-bit variable x to the right for n positions.

Previously, an interest to analyze the S-boxes in SHA-2 was described in the work of Matusiewicz et al., [18] where they noted:

- "The substitution boxes Σ_0 and Σ_1 constitute the essential part of the hash function and fulfil two tasks: they add bit diffusion and destroy the ADD-linearity of the function."
- "σ_0 and σ_1 have both the property to increase the Hamming weight of low-weight inputs. This increase is upper bounded by a factor of 3. The average increase of Hamming weight for low-weight inputs is even higher if three rotations are used instead of two rotations and one bit-shift. However, a reason for this bit-shift is given by the next observation."
- "In contrast to all other members of the MD4-family including SHA-1, rotating expanded message words to get new expanded message words is not possible anymore (even in the XOR-linearised case). This is due to the bit-shift being used in σ_0 and σ_1."

In what follows we will give another observation for the used S-boxes in SHA-2. For that purpose let us recall the following simple fact:

Corollary 1. *The relations expressed in equations (1) and (2) can be expressed in a matrix-vector form:*

$$
\begin{aligned}
\Sigma_0^{256}(x) &= \mathbf{\Sigma}_0^{256} \cdot x \\
\Sigma_1^{256}(x) &= \mathbf{\Sigma}_1^{256} \cdot x \\
\sigma_0^{256}(x) &= \mathbf{s}_0^{256} \cdot x \\
\sigma_1^{256}(x) &= \mathbf{s}_1^{256} \cdot x
\end{aligned}
\tag{3}
$$

$$
\begin{aligned}
\Sigma_0^{512}(x) &= \mathbf{\Sigma}_0^{512} \cdot x \\
\Sigma_1^{512}(x) &= \mathbf{\Sigma}_1^{512} \cdot x \\
\sigma_0^{512}(x) &= \mathbf{s}_0^{512} \cdot x \\
\sigma_1^{512}(x) &= \mathbf{s}_1^{512} \cdot x
\end{aligned}
\tag{4}
$$

where $\mathbf{\Sigma}_0^{256}$, $\mathbf{\Sigma}_1^{256}$, $\mathbf{s}_0^{256}$ and $\mathbf{s}_1^{256}$ are 32×32 nonsingular matrices in $GF(2)$, and where $\mathbf{\Sigma}_0^{512}$, $\mathbf{\Sigma}_1^{512}$, $\mathbf{s}_0^{512}$ and $\mathbf{s}_1^{512}$ are 64×64 nonsingular matrices in $GF(2)$ and the vector x is 32 dimensional in equation (3) or is 64 dimensional in equation (4). □

For the properties that we have observed on SHA-2 S-boxes we need the following Lemma:

Lemma 1. *Every nonsingular matrix $\mathbf{S}$ of order $n \times n$ in $GF(2)$, is also nonsingular in the ring $\mathbb{Z}_{2^n}(+, *)$ where the operation "$+$" is addition modulo 2^n and the operation "$*$" is multiplication modulo 2^n.* □

We have used Lemma 1 and interpreted the matrices $\mathbf{\Sigma}_0^{256}$, $\mathbf{\Sigma}_1^{256}$, $\mathbf{s}_0^{256}$ and $\mathbf{s}_1^{256}$ in the ring $\mathbb{Z}_{2^{32}}(+, *)$, counting the number of different elements present in their inverses: $\left(\mathbf{\Sigma}_0^{256}\right)^{-1}$, $\left(\mathbf{\Sigma}_1^{256}\right)^{-1}$, $\left(\mathbf{s}_0^{256}\right)^{-1}$ and $\left(\mathbf{s}_1^{256}\right)^{-1}$.

We did that too for $\left(\mathbf{\Sigma}_0^{512}\right)^{-1}$, $\left(\mathbf{\Sigma}_1^{512}\right)^{-1}$, $\left(\mathbf{s}_0^{512}\right)^{-1}$ and $\left(\mathbf{s}_1^{512}\right)^{-1}$.

Before presenting the results of our analysis of S-boxes used in SHA-2, let us formalize our observations by the following Definition:

Definition 1. *For every nonsingular matrix $\mathbf{S}$ of order $n \times n$ in $GF(2)$, let us denote by $C(\mathbf{S}^{-1})$ the number of different elements present in the inverse matrix $\mathbf{S}^{-1}$ when the inverse is taken in the ring $\mathbb{Z}_{2^n}(+, *)$.*

For example let us take $n = 16$ and let $\mathbf{S}$ be the following matrix:

$$
\mathbf{S} = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0
\end{pmatrix}.
$$

The inverse matrix $\mathbf{S^{-1}}$ in $\mathbb{Z}_{2^{16}}(+, *)$ is the following matrix:

$$\mathbf{S^{-1}} = \begin{pmatrix} 16191 & 60910 & 46261 & 48574 & 12336 & 7710 & 53971 & 50116 & 62452 & 57055 & 19275 & 56284 & 771 & 57826 & 11565 & 15420 \\ 15420 & 16191 & 60910 & 46261 & 48574 & 12336 & 7710 & 53971 & 50116 & 62452 & 57055 & 19275 & 56284 & 771 & 57826 & 11565 \\ 11565 & 15420 & 16191 & 60910 & 46261 & 48574 & 12336 & 7710 & 53971 & 50116 & 62452 & 57055 & 19275 & 56284 & 771 & 57826 \\ 57826 & 11565 & 15420 & 16191 & 60910 & 46261 & 48574 & 12336 & 7710 & 53971 & 50116 & 62452 & 57055 & 19275 & 56284 & 771 \\ 771 & 57826 & 11565 & 15420 & 16191 & 60910 & 46261 & 48574 & 12336 & 7710 & 53971 & 50116 & 62452 & 57055 & 19275 & 56284 \\ 56284 & 771 & 57826 & 11565 & 15420 & 16191 & 60910 & 46261 & 48574 & 12336 & 7710 & 53971 & 50116 & 62452 & 57055 & 19275 \\ 19275 & 56284 & 771 & 57826 & 11565 & 15420 & 16191 & 60910 & 46261 & 48574 & 12336 & 7710 & 53971 & 50116 & 62452 & 57055 \\ 57055 & 19275 & 56284 & 771 & 57826 & 11565 & 15420 & 16191 & 60910 & 46261 & 48574 & 12336 & 7710 & 53971 & 50116 & 62452 \\ 62452 & 57055 & 19275 & 56284 & 771 & 57826 & 11565 & 15420 & 16191 & 60910 & 46261 & 48574 & 12336 & 7710 & 53971 & 50116 \\ 50116 & 62452 & 57055 & 19275 & 56284 & 771 & 57826 & 11565 & 15420 & 16191 & 60910 & 46261 & 48574 & 12336 & 7710 & 53971 \\ 53971 & 50116 & 62452 & 57055 & 19275 & 56284 & 771 & 57826 & 11565 & 15420 & 16191 & 60910 & 46261 & 48574 & 12336 & 7710 \\ 7710 & 53971 & 50116 & 62452 & 57055 & 19275 & 56284 & 771 & 57826 & 11565 & 15420 & 16191 & 60910 & 46261 & 48574 & 12336 \\ 12336 & 7710 & 53971 & 50116 & 62452 & 57055 & 19275 & 56284 & 771 & 57826 & 11565 & 15420 & 16191 & 60910 & 46261 & 48574 \\ 48574 & 12336 & 7710 & 53971 & 50116 & 62452 & 57055 & 19275 & 56284 & 771 & 57826 & 11565 & 15420 & 16191 & 60910 & 46261 \\ 46261 & 48574 & 12336 & 7710 & 53971 & 50116 & 62452 & 57055 & 19275 & 56284 & 771 & 57826 & 11565 & 15420 & 16191 & 60910 \\ 60910 & 46261 & 48574 & 12336 & 7710 & 53971 & 50116 & 62452 & 57055 & 19275 & 56284 & 771 & 57826 & 11565 & 15420 & 16191 \end{pmatrix},$$

so $C(\mathbf{S^{-1}}) = 16$ because the matrix $\mathbf{S^{-1}}$ has these 16 different elements: $\{771, 7710, 11565, 12336, 15420, 16191, 19275, 46261, 48574, 50116, 53971, 56284, 57055, 57826, 60910, 62452\}$.

The measure $C(\mathbf{S^{-1}})$ can be seen as a concept close to the concept of one-wayness of the bijective transformations i.e. close to the concept of the computational asymmetry as defined in [28] and the references there. However, in this moment we do not have a defined strong and precise mathematical connection between our measure $C(\mathbf{S^{-1}})$ and the concept of the computational asymmetry.

By simple application of the Definition 1 we have obtained the following result:

Corollary 2.
  $C\big(\boldsymbol{\Sigma}_0^{256-1}\big) = 32$, $C\big(\boldsymbol{\Sigma}_1^{256-1}\big) = 32$, $C\big(\mathbf{s}_0^{256-1}\big) = 504$ and $C\big(\mathbf{s}_1^{256-1}\big) = 121$.
  $C\big(\boldsymbol{\Sigma}_0^{512-1}\big) = 64$, $C\big(\boldsymbol{\Sigma}_1^{512-1}\big) = 64$, $C\big(\mathbf{s}_0^{512-1}\big) = 116$ and $C\big(\mathbf{s}_1^{512-1}\big) = 2044$. $\qquad\square$

Since S-boxes in SHA-2 are obtained either by only three rotations or by two rotations and one shift to the right, we were interested to see what are the other statistical properties of the whole set of all possible S-boxes that can be obtained either by three rotations or by two rotations and one shift to the right, operating on 32 or 64 bits.

Our findings are presented in the next three Corollaries (the proofs of all of them can be done by simple exhaustive search).

Corollary 3. *If the function* $\boldsymbol{\Sigma} : \{0,1\}^n \to \{0,1\}^n$ *is defined as*

$$\Sigma(x) = ROTR^{r_1}(x) \oplus ROTR^{r_2}(x) \oplus ROTR^{r_3}(x) \equiv (\boldsymbol{\Sigma}) \cdot x \tag{5}$$

where $n = 32$ *or* $n = 64$ *and* $0 \le r_1 < r_2 < r_3 < n$, *then* $Max(C(\boldsymbol{\Sigma}^{-1})) = n$. $\qquad\square$

Corollary 4. *If the function* $\mathbf{s} : \{0,1\}^{32} \to \{0,1\}^{32}$ *is defined as*

$$\sigma(x) = ROTR^{r_1}(x) \oplus ROTR^{r_2}(x) \oplus SHR^{r_3}(x) \equiv \mathbf{s} \cdot x \tag{6}$$

where $0 \le r_1 < r_2 < 32$, $0 \le r_3 < 32$, *then* $Max(C(\mathbf{s}^{-1})) = 523$. $\qquad\square$

Corollary 5. *If the function* $\mathbf{s} : \{0,1\}^{64} \to \{0,1\}^{64}$ *is defined as*

$$\sigma(x) = ROTR^{r_1}(x) \oplus ROTR^{r_2}(x) \oplus SHR^{r_3}(x) = \mathbf{s} \cdot x \tag{7}$$

where $0 \le r_1 < r_2 < 64$, $0 \le r_3 < 64$, *then* $Max(C(\mathbf{s}^{-1})) = 2079$. $\qquad\square$

It is noticeable that NSA designers of SHA-2 have chosen some of the S-boxes to have the maximal possible value, i.e. the values of $C\big(\boldsymbol{\Sigma}_0^{256-1}\big) = 32$, $C\big(\boldsymbol{\Sigma}_1^{256-1}\big) = 32$, $C\big(\boldsymbol{\Sigma}_0^{512-1}\big) = 64$, $C\big(\boldsymbol{\Sigma}_1^{512-1}\big) = 64$. They have also chosen two of the S-boxes with almost maximal values i.e. $C\big(\mathbf{s}_0^{256-1}\big) = 504$ and $C\big(\mathbf{s}_1^{512-1}\big) = 2044$.
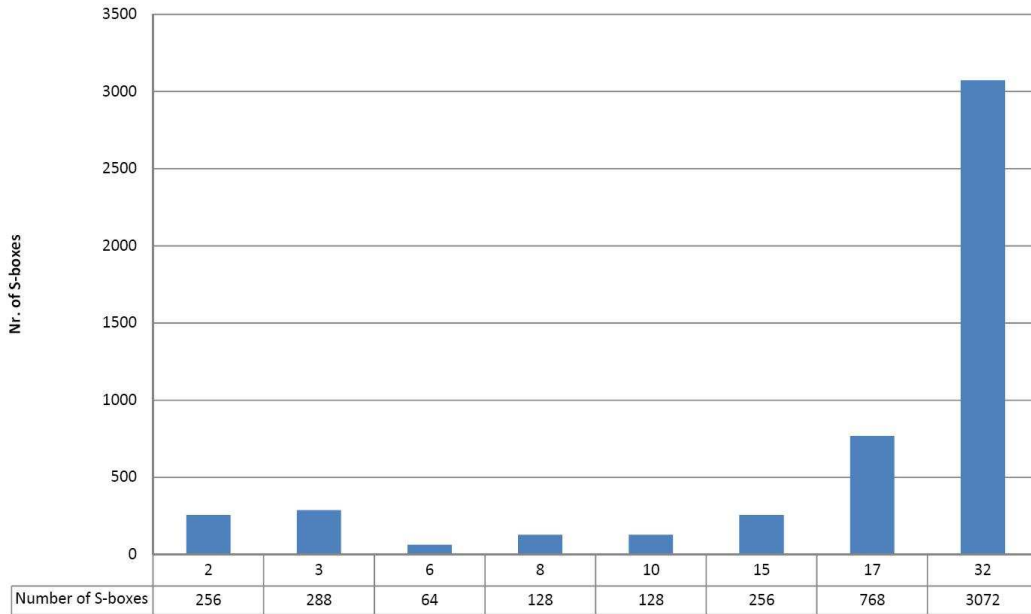
Fig. 1. A distribution of all possible values of $C(\mathbf{\Sigma}^{-1})$ for $n = 32$.

For $n = 32$, the total distribution of $C(\mathbf{\Sigma}^{-1})$ i.e. when $\Sigma(x) = ROTR^{r_1}(x) \oplus ROTR^{r_2}(x) \oplus ROTR^{r_3}(x) \equiv (\mathbf{\Sigma}) \cdot x$ is given on Figure 1. There are in total 4960 S-boxes of type $\mathbf{\Sigma}$ and as we can see, there are just 8 possible values for $C(\mathbf{\Sigma}^{-1})$, forming the set $\{2, 3, 6, 8, 10, 15, 17, 32\}$. The majority of those S-boxes (almost 62%) belongs to the category with 32 different elements in their inverse matrix.

The distribution of $C(\mathbf{s}^{-1})$ i.e. when $\sigma(x) = ROTR^{r_1}(x) \oplus ROTR^{r_2}(x) \oplus SHR^{r_3}(x) \equiv (\mathbf{s}) \cdot x$ is pretty different (and not very appropriate for graphical presentation). There are in total 489 different categories of S-boxes of type $\mathbf{s}$ according to the value of $C(\mathbf{s}^{-1})$, where minimal value is 3 and maximal value is 523.

For $n = 64$, the total distribution of $C(\mathbf{\Sigma}^{-1})$ i.e. when $\Sigma(x) = ROTR^{r_1}(x) \oplus ROTR^{r_2}(x) \oplus ROTR^{r_3}(x) \equiv (\mathbf{\Sigma}) \cdot x$ is given on Figure 2. There are in total 41664 S-boxes of type $\mathbf{\Sigma}$ and as we can see, there are just 11 categories of possible values for $C(\mathbf{\Sigma}^{-1})$, forming the set $\{2, 3, 6, 8, 10, 16, 17, 18, 31, 33, 64\}$. The majority of those S-boxes (almost 69%) belongs to the category with 64 different elements in their inverse matrix.

Similarly, the distribution of $C(\mathbf{s}^{-1})$ i.e. when $\sigma(x) = ROTR^{r_1}(x) \oplus ROTR^{r_2}(x) \oplus SHR^{r_3}(x) \equiv (\mathbf{s}) \cdot x$ is pretty different. There are in total 63923 S-boxes distributed in 2038 categories according to the value of $C(\mathbf{s}^{-1})$, where minimal value is 3 and maximal value is 2079.

So, as a conclusion from this analysis of SHA-2 S-boxes we can say that NSA have chosen majority of the S-boxes (6 out of 8 S-boxes) to have the property that they have maximal or close to maximal value of $C(\mathbf{\Sigma}^{-1})$ or $C(\mathbf{s}^{-1})$. Since the design principles for SHA-2 are still kept classified, we do not know is this observation just a coincidence or there is a stronger mathematical connection.
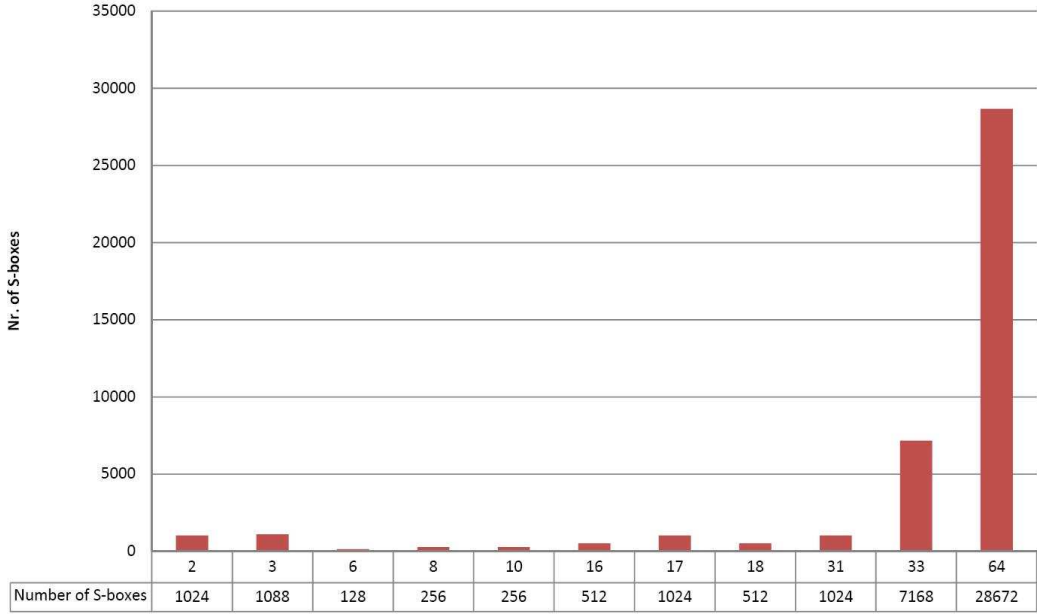
Fig. 2. A distribution of all possible values of $C(\mathbf{\Sigma}^{-1})$ for $n = 64$.

Number of S-boxes	2	3	6	8	10	16	17	18	31	33	64
	1024	1088	128	256	256	512	1024	512	1024	7168	28672

3 Properties of Blue Midnight Wish S-boxes

Blue Midnight Wish hash function has the following bijective components (S-boxes) that are the subject of interest in this paper:

$$BMW224/256 : \begin{cases} s_0(x) = SHR^1(x) \oplus SHL^3(x) \oplus ROTL^4(x) \ \oplus ROTL^{19}(x) \\ s_1(x) = SHR^1(x) \oplus SHL^2(x) \oplus ROTL^8(x) \ \oplus ROTL^{23}(x) \\ s_2(x) = SHR^2(x) \oplus SHL^1(x) \oplus ROTL^{12}(x) \oplus ROTL^{25}(x) \\ s_3(x) = SHR^2(x) \oplus SHL^2(x) \oplus ROTL^{15}(x) \oplus ROTL^{29}(x) \end{cases} \quad (8)$$

$$BMW384/512 : \begin{cases} s_0(x) = SHR^1(x) \oplus SHL^3(x) \oplus ROTL^4(x) \ \oplus ROTL^{37}(x) \\ s_1(x) = SHR^1(x) \oplus SHL^2(x) \oplus ROTL^{13}(x) \oplus ROTL^{43}(x) \\ s_2(x) = SHR^2(x) \oplus SHL^1(x) \oplus ROTL^{19}(x) \oplus ROTL^{53}(x) \\ s_3(x) = SHR^2(x) \oplus SHL^2(x) \oplus ROTL^{28}(x) \oplus ROTL^{59}(x) \end{cases} \quad (9)$$

where $ROTL^n(x)$ means rotation of the variable x to the left for n positions and $SHL^n(x)$ means shifting of the variable x to the left for n positions (variables are 32-bit long for BMW224/256 and they are 64-bit long for BMW384/512).

By simple application of the Definition 1 we can obtain the following result:

Corollary 6.

$$BMW224/256 : \begin{cases} C\left(\mathbf{s_0}^{-1}\right) = 524 \\ C\left(\mathbf{s_1}^{-1}\right) = 528 \\ C\left(\mathbf{s_2}^{-1}\right) = 528 \\ C\left(\mathbf{s_3}^{-1}\right) = 528 \end{cases} \quad (10)$$

$$BMW384/512 : \begin{cases} C\left(\mathbf{s_0}^{-1}\right) = 2080 \\ C\left(\mathbf{s_1}^{-1}\right) = 2080 \\ C\left(\mathbf{s_2}^{-1}\right) = 2080 \\ C\left(\mathbf{s_3}^{-1}\right) = 2080 \end{cases} \quad (11)$$

$\square$

Although S-boxes in Blue Midnight Wish have four operations (compared to the three of SHA-2), it comes as a little surprise that the maximal value of $C(\mathbf{s}^{-1})$ for $n = 32$ and

$n = 64$ for the types of S-boxes defined in BLUE MIDNIGHT WISH is not much bigger than the corresponding maximal values for SHA-2. That is easily checkable fact by a simple exhaustive search of all possible S-boxes of the type defined in BLUE MIDNIGHT WISH.

Corollary 7. *If the function* $\mathbf{s} : \{0,1\}^{32} \to \{0,1\}^{32}$ *is defined as*

$$s(x) = SHR^{r_1}(x) \oplus SHL^{r_2}(x) \oplus ROTL^{r_3}(x) \oplus ROTL^{r_4}(x) \equiv \mathbf{s} \cdot x \tag{12}$$

where $0 \le r_1 < 32$, $0 \le r_2 < 32$, $0 \le r_3 < r_4 < 32$, *then* $Max(C(\mathbf{s}^{-1})) = 528$. $\qquad\square$

Corollary 8. *If the function* $\mathbf{s} : \{0,1\}^{64} \to \{0,1\}^{64}$ *is defined as*

$$s(x) = SHR^{r_1}(x) \oplus SHL^{r_2}(x) \oplus ROTL^{r_3}(x) \oplus ROTL^{r_4}(x) \equiv \mathbf{s} \cdot x \tag{13}$$

where $0 \le r_1 < 64$, $0 \le r_2 < 64$, $0 \le r_3 < r_4 < 64$, *then* $Max(C(\mathbf{s}^{-1})) = 2080$. $\qquad\square$

Corollaries 6, 7 and 8 show that we chose 7 S-boxes with maximal $C(\mathbf{s}^{-1})$ value and one with a value which is very near to the maximum. More precisely, our design criteria were the following:

- Logical functions s_i, $i = 0, \ldots, 3$, are bijections in $\{0,1\}^{32} \to \{0,1\}^{32}$ (resp. in $\{0,1\}^{64} \to \{0,1\}^{64}$) i.e. they are S-boxes.
- They have different pairs of 1-bit, 2-bits or 3-bits shifts to the left and to the right.
- They have different pairs of rotations to the left, in such a way that one rotation is less than $w/2$, $w = 32, 64$, and the other rotation is bigger than $w/2$.
- The values of the rotations that are less than $w/2$ are in the interval of ± 2 (resp. ± 4) around numbers $\{2, 6, 10, 14\}$ (resp. $\{4, 12, 20, 28\}$).
- The values of the rotations that are bigger than $w/2$ are in the interval of ± 2 (resp. ± 4) around numbers $\{18, 22, 26, 30\}$ (resp. $\{36, 42, 50, 58\}$).
- The values $C(\mathbf{s}_i^{-1})$, $i = 0, \ldots, 3$, to be the maximal possible (or very close to the maximal value).

By computer search we have found hundreds of such bijections and from them we have chosen the eight particular functions s_0, s_1, s_2 and s_3 (four for BMW224/256 and four for BMW384/512).

4 Conclusions and Future Work

The design principles of SHA-2 family of hash functions are still kept as a classified NSA information. In the open literature there have been several attempts to analyze those design principles.

In the design of BLUE MIDNIGHT WISH cryptographic hash function as a SHA-3 candidate, several bijective components (S-boxes) have been chosen with properties that are similar to the properties of S-boxes in SHA-2.

The observations presented in this paper probably open more new questions than close some. One obvious thing that have to be done in the next period would be to establish firm mathematical connection between our defined measure $Max(C(\mathbf{s}^{-1}))$ and the theory of computational asymmetry.

References

1. R. Rivest, "The MD4 message-digest algorithm", Request for Comments (RFC) 1320, Internet Activities Board, Internet Privacy Task Force, April 1992.
2. R. Rivest, "The MD5 message-digest algorithm", Request for Comments (RFC) 1321, Internet Activities Board, Internet Privacy Task Force, April 1992.
3. FIPS 180-1, "Secure Hash Standard", Federal Information Processing Standards Publication 180-1, U.S. Department of Commerce/NIST, National Technical Information Service, Springfield, Virginia, April 1995.
4. FIPS 180-2, "Secure Hash Standard", Federal Information Processing Standards Publication 180-2, U.S. Department of Commerce/NIST, National Technical Information Service, Springfield, Virginia, August 2002.
5. B. den Boer, and A. Bosselaers: "An attack on the last two rounds of MD4", CRYPTO 1991, LNCS, 576, pp. 194-203, 1992.
6. B. den Boer, and A. Bosselaers: "Collisions for the compression function of MD5", EUROCRYPT 1993, LNCS 765, pp. 293-304, 1994.
7. S. Vaudenay, "On the need for multipermutations: Cryptanalysis of MD4 and SAFER", Fast Software Encryption - FSE95, LNCS 1008, pp. 286–297, 1995.
8. H. Dobbertin: "Cryptanalysis of MD4", J. Cryptology 11, pp. 253-271, 1998.
9. F. Chabaud and A. Joux, "Differential collisions in SHA-0," Advances in Cryptology, Crypto98, LNCS, vol.1462, pp.56-71, 1998.
10. E. Biham and R. Chen, "Near-collisions of SHA-0," Cryptology ePrint Archive, Report 2004/146, 2004. http://eprint.iacr.org/2004/146
11. X. Wang, X. Lai, D. Feng, H. Chen and X. Yu, "Cryptanalysis of the Hash Functions MD4 and RIPEMD", EUROCRYPT 2005, LNCS 3494, pp. 1–18, 2005.
12. X. Wang and H. Yu , "How to Break MD5 and Other Hash Functions", EUROCRYPT 2005, LNCS 3494, pp. 19–35, 2005.
13. X. Wang, H. Yu, Y. L. Yin "Efficient Collision Search Attacks on SHA-0", CRYPTO 2005, LNCS 3621, pp. 1–16, 2005.
14. X. Wang, Y. L. Yin, H. Yu, "Collision Search Attacks on SHA-1", CRYPTO 2005, LNCS 3621, pp. 17–36, 2005.
15. H. Gilbert and H. Handschuh, "Security analysis of SHA-256 and sisters", Selected Areas in Cryptography'03 (SAC 2003), LNCS 3006, pp. 175–193, 2003.
16. P. Hawkes, M. Paddon and G. G. Rose, "On corrective patterns for the SHA-2 family", Cryptology ePrint Archive, Report 2004/207, 2004.
17. H. Yoshida and A. Biryukov, "Analysis of a SHA-256 variant", Selected Areas in Cryptography'05 (SAC 2005), LNCS 3897, pp. 245–260, 2005.
18. K. Matusiewicz, J. Pieprzyk, N. Pramstaller, C. Rechberger, and V. Rijmen, "Analysis of simplified variants of SHA-256", In Proceedings of WEWoRC 2005, LNI P-74, pages 123134, 2005.
19. F. Mendel, N. Pramstaller, C. Rechberger, and V. Rijmen, "Analysis of step-reduced SHA-256", Fast Software Encryption - FSE06, LNCS 4047, pp. 126-143, 2006.
20. M. Hölbl, C. Rechberger, T. Welzer: "Finding message pairs conforming to simple SHA-256 characteristics: Work in Progress", Western European Workshop on Research in Cryptology - WEWoRC 2007, Bochum, July 4-6, 2007, pp. 21–25, http://www.hgi.rub.de/weworc07/PreliminaryConferenceRecord.pdf
21. I. Nikolič and A. Biryukov, "Collisions for Step-Reduced SHA-256", In Kaisa Nyberg, editor, Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, March 26-28, 2008, LNCS. Springer, 2008.
22. S. Indesteege, F. Mendel, B. Preneel and C. Rechberger, "Collisions and other Non-Random Properties for Step-Reduced SHA-256", Cryptology ePrint Archive, Report 2008/131, 2008, http://eprint.iacr.org/
23. NIST, First Cryptographic Hash Workshop, October 31 - November 1, 2005, Second Cryptographic Hash Workshop, August 24-25, 2006, http://csrc.nist.gov/groups/ST/hash/first_workshop.html, http://csrc.nist.gov/groups/ST/hash/second_workshop.html.
24. NIST Tentative Timeline for the Development of New Hash Functions, http://csrc.nist.gov/groups/ST/hash/timeline.html
25. NIST, SHA-3 First Round Candidates , http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions_rnd1.html
26. NIST, SHA-3 Second Round Candidates , http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/submissions_rnd2.html
27. D. Gligoroski, V. Klima, S. J. Knapskog, M. El-Hadedy, J. Amundsen, and Stig Frode Mjølsnes. Cryptographic Hash Function BLUE MIDNIGHT WISH. Submission to NIST, 2008.
28. J.-C. Birget, "One-way permutations, computational asymmetry and distortion", arXiv:0704.1569v1 [math.GR], 2007, http://arxiv.org/abs/0704.1569v1
29. V. Klima, "Tunnels in Hash Functions: MD5 Collisions Within a Minute", Cryptology ePrint Archive, Report 2006/105, 2006, http://eprint.iacr.org/