A Document describing all modifications made on the Blue Midnight Wish cryptographic hash function before entering the Second Round of SHA-3 hash competition

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. In this document we elaborate changes to the original Blue Midnight Wish, as it will enter the Second Round of SHA-3 competition. Generally, we can say that there are two technical changes (or typo corrections) and two minor tweaks in the design. The first technical change is in correcting a typo in the initial double pipe value $H^{(0)}$ for the 224 and 384 versions, and the second technical change is in correcting a typo in the order of the use of two logical functions s_4 and s_5. The tweaks in the design consist of tweaks in functions f_0 and f_1 and an additional (final) use of the compression function.
For us as designers of Blue Midnight Wish it is very important that the tweaks do not introduce any new building blocks which would need new analysis. The chosen tweaks are quite simple. They use the same building blocks which were used in the original Blue Midnight Wish hash function. Only the inputs of the building blocks are changed in a fully transparent manner. The goals of the proposed tweaks are also simple and transparent. For instance the first tweak adds the old double pipe to the result of the function f_0 and to the "key" of the function f_1. This strongly decouples the original input $M \oplus H$ into two independently acting variables M and H. The second tweak is an additional (final) invocation of the compression function. It also uses the old building block and it is a pivotal security countermeasure against many types of preimage, near, pseudo and other types of attacks. At first glance it may seem that by this additional final invocation of the compression function we have over-designed Blue Midnight Wish. However having in mind the excellent speed performance of both non-tweaked and tweaked function we can say that this additional final invocation of the compression function brings additional rise in our confidence of the strength and quality of Blue Midnight Wish with only a minor efficiency penalty.
In fact, the introduced tweaks do not affect the speed of the hash computation on messages longer than 1000 bytes, but it becomes visible on hashing extremely short or short messages, as would be expected. On the other hand, for the optimized versions of the tweaked Blue Midnight Wish we have documented higher operating speed than the speed reported in the documentation for the non-tweaked function.

1 Methodology

We will elaborate all changes by the following methodology:

1. We will give the non-tweaked (or non-changed) part in the old submission,
2. We will give the new tweaked (or changed) part,
3. We will give a rationale for the tweak (technical change).

2 Technical change Nr. 1

The original submission of Blue Midnight Wish for the 224-bit digest size had the initial double pipe $H^{(0)}$ given in Table 1.

Note the value $H_{13}^{(0)} =$ `0x24353637`! The value should be $H_{13}^{(0)} =$ `0x34353637`, so the corrected $H^{(0)}$ for BMW224 now is given in Table 2.

$H_0^{(0)} =$ 0x00010203	$H_1^{(0)} =$ 0x04050607
$H_2^{(0)} =$ 0x08090A0B	$H_3^{(0)} =$ 0x0C0D0E0F
$H_4^{(0)} =$ 0x10111213	$H_5^{(0)} =$ 0x14151617
$H_6^{(0)} =$ 0x18191A1B	$H_7^{(0)} =$ 0x1C1D1E1F
$H_8^{(0)} =$ 0x20212223	$H_9^{(0)} =$ 0x24252627
$H_{10}^{(0)} =$ 0x28292A2B	$H_{11}^{(0)} =$ 0x2C2D2E2F
$H_{12}^{(0)} =$ 0x30313233	$H_{13}^{(0)} =$ 0x24353637
$H_{14}^{(0)} =$ 0x38393A3B	$H_{15}^{(0)} =$ 0x3C3D3E3F

Table 1. Initial double pipe $H^{(0)}$ for old BMW224

$H_0^{(0)} =$ 0x00010203	$H_1^{(0)} =$ 0x04050607
$H_2^{(0)} =$ 0x08090A0B	$H_3^{(0)} =$ 0x0C0D0E0F
$H_4^{(0)} =$ 0x10111213	$H_5^{(0)} =$ 0x14151617
$H_6^{(0)} =$ 0x18191A1B	$H_7^{(0)} =$ 0x1C1D1E1F
$H_8^{(0)} =$ 0x20212223	$H_9^{(0)} =$ 0x24252627
$H_{10}^{(0)} =$ 0x28292A2B	$H_{11}^{(0)} =$ 0x2C2D2E2F
$H_{12}^{(0)} =$ 0x30313233	$H_{13}^{(0)} =$ 0x34353637
$H_{14}^{(0)} =$ 0x38393A3B	$H_{15}^{(0)} =$ 0x3C3D3E3F

Table 2. Initial double pipe $H^{(0)}$ for tweaked BMW224

$H_0^{(0)} =$ 0x0001020304050607	$H_1^{(0)} =$ 0x08090A0B0C0D0E0F
$H_2^{(0)} =$ 0x1011121314151617	$H_3^{(0)} =$ 0x18191A1B1C1D1E1F
$H_4^{(0)} =$ 0x2021222324252627	$H_5^{(0)} =$ 0x28292A2B2C2D2E2F
$H_6^{(0)} =$ 0x3031323324353637	$H_7^{(0)} =$ 0x38393A3B3C3D3E3F
$H_8^{(0)} =$ 0x4041424344454647	$H_9^{(0)} =$ 0x48494A4B4C4D4E4F
$H_{10}^{(0)} =$ 0x5051525354555657	$H_{11}^{(0)} =$ 0x58595A5B5C5D5E5F
$H_{12}^{(0)} =$ 0x6061626364656667	$H_{13}^{(0)} =$ 0x68696A6B6C6D6E6F
$H_{14}^{(0)} =$ 0x7071727374757677	$H_{15}^{(0)} =$ 0x78797A7B7C7D7E7F

Table 3. Initial double pipe $H^{(0)}$ for old BMW384

The original submission of Blue Midnight Wish for the 384-bit digest size had the initial double pipe $H^{(0)}$ given in Table 3.

Note the value $H_6^{(0)} =$ 0x3031323324353637! The value should be $H_6^{(0)} =$ 0x3031323334353637, so the corrected $H^{(0)}$ for BMW384 now is given in Table 4.

$H_0^{(0)} =$ 0x0001020304050607	$H_1^{(0)} =$ 0x08090A0B0C0D0E0F
$H_2^{(0)} =$ 0x1011121314151617	$H_3^{(0)} =$ 0x18191A1B1C1D1E1F
$H_4^{(0)} =$ 0x2021222324252627	$H_5^{(0)} =$ 0x28292A2B2C2D2E2F
$H_6^{(0)} =$ 0x3031323334353637	$H_7^{(0)} =$ 0x38393A3B3C3D3E3F
$H_8^{(0)} =$ 0x4041424344454647	$H_9^{(0)} =$ 0x48494A4B4C4D4E4F
$H_{10}^{(0)} =$ 0x5051525354555657	$H_{11}^{(0)} =$ 0x58595A5B5C5D5E5F
$H_{12}^{(0)} =$ 0x6061626364656667	$H_{13}^{(0)} =$ 0x68696A6B6C6D6E6F
$H_{14}^{(0)} =$ 0x7071727374757677	$H_{15}^{(0)} =$ 0x78797A7B7C7D7E7F

Table 4. Initial double pipe $H^{(0)}$ for tweaked BMW384

3 Tweak Nr. 1

The tweak Nr. 1 was performed to make infeasible finding free-start near collisions and finding pseudo-preimages and pseudo-collisions as hard as finding real preimages and real collisions. To achieve that we tweaked both f_0 and f_1 functions.

3.1 Tweak in f_0

The old f_0 had the following form:

$f_0 : \{0,1\}^{2m} \rightarrow \{0,1\}^m$

Input: Message block $M^{(i)} = (M_0^{(i)}, M_1^{(i)}, \ldots, M_{15}^{(i)})$, and the previous double pipe $H^{(i-1)} = (H_0^{(i-1)}, H_1^{(i-1)}, \ldots, H_{15}^{(i-1)})$.
Output: First part of the quadruple pipe $Q_a^{(i)} = (Q_0^{(i)}, Q_1^{(i)}, \ldots, Q_{15}^{(i)})$.

1. Bijective transform of $M^{(i)} \oplus H^{(i-1)}$:

$$
\begin{aligned}
W_0^{(i)} &= (M_5^{(i)} \oplus H_5^{(i-1)}) - (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)}) + (M_{14}^{(i)} \oplus H_{14}^{(i-1)}) \\
W_1^{(i)} &= (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_8^{(i)} \oplus H_8^{(i-1)}) + (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) + (M_{14}^{(i)} \oplus H_{14}^{(i-1)}) - (M_{15}^{(i)} \oplus H_{15}^{(i-1)}) \\
W_2^{(i)} &= (M_0^{(i)} \oplus H_0^{(i-1)}) + (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_9^{(i)} \oplus H_9^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) + (M_{15}^{(i)} \oplus H_{15}^{(i-1)}) \\
W_3^{(i)} &= (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_1^{(i)} \oplus H_1^{(i-1)}) + (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)}) \\
W_4^{(i)} &= (M_1^{(i)} \oplus H_1^{(i-1)}) + (M_2^{(i)} \oplus H_2^{(i-1)}) + (M_9^{(i)} \oplus H_9^{(i-1)}) - (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) - (M_{14}^{(i)} \oplus H_{14}^{(i-1)}) \\
W_5^{(i)} &= (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_2^{(i)} \oplus H_2^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) + (M_{15}^{(i)} \oplus H_{15}^{(i-1)}) \\
W_6^{(i)} &= (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)}) \\
W_7^{(i)} &= (M_1^{(i)} \oplus H_1^{(i-1)}) - (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) - (M_{14}^{(i)} \oplus H_{14}^{(i-1)}) \\
W_8^{(i)} &= (M_2^{(i)} \oplus H_2^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) - (M_6^{(i)} \oplus H_6^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)}) - (M_{15}^{(i)} \oplus H_{15}^{(i-1)}) \\
W_9^{(i)} &= (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_3^{(i)} \oplus H_3^{(i-1)}) + (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{14}^{(i)} \oplus H_{14}^{(i-1)}) \\
W_{10}^{(i)} &= (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_1^{(i)} \oplus H_1^{(i-1)}) - (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{15}^{(i)} \oplus H_{15}^{(i-1)}) \\
W_{11}^{(i)} &= (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_2^{(i)} \oplus H_2^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) + (M_9^{(i)} \oplus H_9^{(i-1)}) \\
W_{12}^{(i)} &= (M_1^{(i)} \oplus H_1^{(i-1)}) + (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_9^{(i)} \oplus H_9^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) \\
W_{13}^{(i)} &= (M_2^{(i)} \oplus H_2^{(i-1)}) + (M_4^{(i)} \oplus H_4^{(i-1)}) + (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) + (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) \\
W_{14}^{(i)} &= (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) + (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) \\
W_{15}^{(i)} &= (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) - (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_9^{(i)} \oplus H_9^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)})
\end{aligned}
$$

2. Further bijective transform of $W_j^{(i)}, j = 0, \ldots, 15$:

$$
\begin{aligned}
&Q_0^{(i)} = s_0(W_0^{(i)}); Q_1^{(i)} = s_1(W_1^{(i)}); Q_2^{(i)} = s_2(W_2^{(i)}); Q_3^{(i)} = s_3(W_3^{(i)}); \\
&Q_4^{(i)} = s_4(W_4^{(i)}); Q_5^{(i)} = s_0(W_5^{(i)}); Q_6^{(i)} = s_1(W_6^{(i)}); Q_7^{(i)} = s_2(W_7^{(i)}); \\
&Q_8^{(i)} = s_3(W_8^{(i)}); Q_9^{(i)} = s_4(W_9^{(i)}); Q_{10}^{(i)} = s_0(W_{10}^{(i)}); Q_{11}^{(i)} = s_1(W_{11}^{(i)}); \\
&Q_{12}^{(i)} = s_2(W_{12}^{(i)}); Q_{13}^{(i)} = s_3(W_{13}^{(i)}); Q_{14}^{(i)} = s_4(W_{14}^{(i)}); Q_{15}^{(i)} = s_0(W_{15}^{(i)});
\end{aligned}
$$

Table 5. Definition of the function f_0 in the old Blue Midnight Wish

The tweak in f_0 is done in the Step 2:

$f_0 : \{0,1\}^{2m} \to \{0,1\}^m$

Input: Message block $M^{(i)} = (M_0^{(i)}, M_1^{(i)}, \ldots, M_{15}^{(i)})$, and the previous double pipe $H^{(i-1)} = (H_0^{(i-1)}, H_1^{(i-1)}, \ldots, H_{15}^{(i-1)})$.
Output: First part of the quadruple pipe $Q_a^{(i)} = (Q_0^{(i)}, Q_1^{(i)}, \ldots, Q_{15}^{(i)})$.

1. Bijective transform of $M^{(i)} \oplus H^{(i-1)}$:

$$
\begin{aligned}
W_0^{(i)} &= (M_5^{(i)} \oplus H_5^{(i-1)}) - (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)}) + (M_{14}^{(i)} \oplus H_{14}^{(i-1)})\\
W_1^{(i)} &= (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_8^{(i)} \oplus H_8^{(i-1)}) + (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) + (M_{14}^{(i)} \oplus H_{14}^{(i-1)}) - (M_{15}^{(i)} \oplus H_{15}^{(i-1)})\\
W_2^{(i)} &= (M_0^{(i)} \oplus H_0^{(i-1)}) + (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_9^{(i)} \oplus H_9^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) + (M_{15}^{(i)} \oplus H_{15}^{(i-1)})\\
W_3^{(i)} &= (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_1^{(i)} \oplus H_1^{(i-1)}) + (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)})\\
W_4^{(i)} &= (M_1^{(i)} \oplus H_1^{(i-1)}) + (M_2^{(i)} \oplus H_2^{(i-1)}) + (M_9^{(i)} \oplus H_9^{(i-1)}) - (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) - (M_{14}^{(i)} \oplus H_{14}^{(i-1)})\\
W_5^{(i)} &= (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_2^{(i)} \oplus H_2^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) + (M_{15}^{(i)} \oplus H_{15}^{(i-1)})\\
W_6^{(i)} &= (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)})\\
W_7^{(i)} &= (M_1^{(i)} \oplus H_1^{(i-1)}) - (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) - (M_{14}^{(i)} \oplus H_{14}^{(i-1)})\\
W_8^{(i)} &= (M_2^{(i)} \oplus H_2^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) - (M_6^{(i)} \oplus H_6^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)}) - (M_{15}^{(i)} \oplus H_{15}^{(i-1)})\\
W_9^{(i)} &= (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_3^{(i)} \oplus H_3^{(i-1)}) + (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{14}^{(i)} \oplus H_{14}^{(i-1)})\\
W_{10}^{(i)} &= (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_1^{(i)} \oplus H_1^{(i-1)}) - (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{15}^{(i)} \oplus H_{15}^{(i-1)})\\
W_{11}^{(i)} &= (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_2^{(i)} \oplus H_2^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) + (M_9^{(i)} \oplus H_9^{(i-1)})\\
W_{12}^{(i)} &= (M_1^{(i)} \oplus H_1^{(i-1)}) + (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_9^{(i)} \oplus H_9^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)})\\
W_{13}^{(i)} &= (M_2^{(i)} \oplus H_2^{(i-1)}) + (M_4^{(i)} \oplus H_4^{(i-1)}) + (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) + (M_{11}^{(i)} \oplus H_{11}^{(i-1)})\\
W_{14}^{(i)} &= (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) + (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)})\\
W_{15}^{(i)} &= (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) - (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_9^{(i)} \oplus H_9^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)})
\end{aligned}
$$

2. Further bijective transform of $W_j^{(i)}, j = 0, \ldots, 15$:

$$
\begin{aligned}
&Q_0^{(i)} = s_0(W_0^{(i)}) + H_1^{(i-1)};\ Q_1^{(i)} = s_1(W_1^{(i)}) + H_2^{(i-1)};\ Q_2^{(i)} = s_2(W_2^{(i)}) + H_3^{(i-1)};\ Q_3^{(i)} = s_3(W_3^{(i)}) + H_4^{(i-1)};\\
&Q_4^{(i)} = s_4(W_4^{(i)}) + H_5^{(i-1)};\ Q_5^{(i)} = s_0(W_5^{(i)}) + H_6^{(i-1)};\ Q_6^{(i)} = s_1(W_6^{(i)}) + H_7^{(i-1)};\ Q_7^{(i)} = s_2(W_7^{(i)}) + H_8^{(i-1)};\\
&Q_8^{(i)} = s_3(W_8^{(i)}) + H_9^{(i-1)};\ Q_9^{(i)} = s_4(W_9^{(i)}) + H_{10}^{(i-1)};\ Q_{10}^{(i)} = s_0(W_{10}^{(i)}) + H_{11}^{(i-1)};\ Q_{11}^{(i)} = s_1(W_{11}^{(i)}) + H_{12}^{(i-1)};\\
&Q_{12}^{(i)} = s_2(W_{12}^{(i)}) + H_{13}^{(i-1)};\ Q_{13}^{(i)} = s_3(W_{13}^{(i)}) + H_{14}^{(i-1)};\ Q_{14}^{(i)} = s_4(W_{14}^{(i)}) + H_{15}^{(i-1)};\ Q_{15}^{(i)} = s_0(W_{15}^{(i)}) + H_0^{(i-1)};
\end{aligned}
$$

Table 6. Definition of the function f_0 of the tweaked Blue Midnight Wish

If we denote the Step 1 of f_0 as a transformation $\mathbf{A}_1 : \{0,1\}^{(16\times 2)w} \to \{0,1\}^{16w}$ and the Step 2 as a transformation $\mathbf{A}_2 : \{0,1\}^{(16\times 2)w} \to \{0,1\}^{16w}$, (where w is 32 or 64) then we can describe the function f_0 as

$$f_0(M_i, H_{i-1}) \equiv \mathbf{A}_2(\mathbf{A}_1 \cdot (M_i \oplus H_{i-1})) + ROTL^1(H_{i-1}),$$

where we denote by $ROTL^1(H_{i-1}) = (H_1^{(i-1)}, H_2^{(i-1)}, \ldots, H_{15}^{(i-1)}, H_0^{(i-1)})$ the rotation by one position to the left of the vector $(H_0^{(i-1)}, H_1^{(i-1)}, \ldots, H_{15}^{(i-1)})$. The reason why we put this additional term $ROTL^1(H_{i-1})$ (see that it is not present in the Round 1 version of Blue Midnight Wish) is that we installed two actions of a decoupling the M_i and H_{i-1} in order to prevent pseudo-attacks that can use the fact that $M_i \oplus H_{i-1} = 0$ iff $M_i = H_{i-1}$. This is the first such decoupling, and the second one is installed in the expansion function f_1.

3.2 Tweak in f_1

The old function f_1 had the following description:

$f_1 : \{0,1\}^{(16\times 2)w} \rightarrow \{0,1\}^{16w}$
Input: Message block $M^{(i)} = (M_0^{(i)}, M_1^{(i)}, \ldots, M_{15}^{(i)})$, and the first part of quadruple pipe $Q_a^{(i)} = (Q_0^{(i)}, Q_1^{(i)}, \ldots, Q_{15}^{(i)})$. **Output:** Second part of the quadruple pipe $Q_b^{(i)} = (Q_{16}^{(i)}, Q_{17}^{(i)}, \ldots, Q_{31}^{(i)})$.
1. Double pipe expansion according to the tunable parameters $ExpandRounds_1$ and $ExpandRounds_2$. **1.1** For $ii = 0$ to $ExpandRounds_1 - 1$ $Q_{ii+16}^{(i)} = expand_1(ii + 16)$ **1.2** For $ii = ExpandRounds_1$ to $ExpandRounds_1 + ExpandRounds_2 - 1$ $Q_{ii+16}^{(i)} = expand_2(ii + 16)$

Table 7. Definition of the old function f_1

The tweaked function f_1 has the following description:

$f_1 : \{0,1\}^{(16\times 3)w} \rightarrow \{0,1\}^{16w}$
Input: Message block $M^{(i)} = (M_0^{(i)}, M_1^{(i)}, \ldots, M_{15}^{(i)})$, the previous double pipe $H^{(i-1)} = (H_0^{(i-1)}, H_1^{(i-1)}, \ldots, H_{15}^{(i-1)})$ and the first part of the quadruple pipe $Q_a^{(i)} = (Q_0^{(i)}, Q_1^{(i)}, \ldots, Q_{15}^{(i)})$. **Output:** Second part of the quadruple pipe $Q_b^{(i)} = (Q_{16}^{(i)}, Q_{17}^{(i)}, \ldots, Q_{31}^{(i)})$.
1. Double pipe expansion according to the tunable parameters $ExpandRounds_1$ and $ExpandRounds_2$. **1.1** For $ii = 0$ to $ExpandRounds_1 - 1$ $Q_{ii+16}^{(i)} = expand_1(ii + 16)$ **1.2** For $ii = ExpandRounds_1$ to $ExpandRounds_1 + ExpandRounds_2 - 1$ $Q_{ii+16}^{(i)} = expand_2(ii + 16)$

Table 8. Definition of the tweaked function f_1 of Blue Midnight Wish

So in the tweaked f_1 we are also using the values of the previous double pipe $H^{(i-1)}$ which was not used in the old version od Blue Midnight Wish.

We will describe how concretely we are using the values $H^{(i-1)}$ in the tweaked version by the following comparison.

The description of logical functions used in old Blue Midnight Wish was the following:

BMW224/BMW256	BMW384/BMW512
$s_0(x) = SHR^1(x) \oplus SHL^3(x) \oplus ROTL^4(x) \oplus ROTL^{19}(x)$ $s_1(x) = SHR^1(x) \oplus SHL^2(x) \oplus ROTL^8(x) \oplus ROTL^{23}(x)$ $s_2(x) = SHR^2(x) \oplus SHL^1(x) \oplus ROTL^{12}(x) \oplus ROTL^{25}(x)$ $s_3(x) = SHR^2(x) \oplus SHL^2(x) \oplus ROTL^{15}(x) \oplus ROTL^{29}(x)$ $s_4(x) = SHR^1(x) \oplus x$ $s_5(x) = SHR^2(x) \oplus x$ $r_1(x) = ROTL^3(x)$ $r_2(x) = ROTL^7(x)$ $r_3(x) = ROTL^{13}(x)$ $r_4(x) = ROTL^{16}(x)$ $r_5(x) = ROTL^{19}(x)$ $r_6(x) = ROTL^{23}(x)$ $r_7(x) = ROTL^{27}(x)$ $AddElement(j) = M_j^{(i)} + M_{j+3}^{(i)} - M_{j+10}^{(i)} + K_{j+16}$	$s_0(x) = SHR^1(x) \oplus SHL^3(x) \oplus ROTL^4(x) \oplus ROTL^{37}(x)$ $s_1(x) = SHR^1(x) \oplus SHL^2(x) \oplus ROTL^{13}(x) \oplus ROTL^{43}(x)$ $s_2(x) = SHR^2(x) \oplus SHL^1(x) \oplus ROTL^{19}(x) \oplus ROTL^{53}(x)$ $s_3(x) = SHR^2(x) \oplus SHL^2(x) \oplus ROTL^{28}(x) \oplus ROTL^{59}(x)$ $s_4(x) = SHR^1(x) \oplus x$ $s_5(x) = SHR^2(x) \oplus x$ $r_1(x) = ROTL^5(x)$ $r_2(x) = ROTL^{11}(x)$ $r_3(x) = ROTL^{27}(x)$ $r_4(x) = ROTL^{32}(x)$ $r_5(x) = ROTL^{37}(x)$ $r_6(x) = ROTL^{43}(x)$ $r_7(x) = ROTL^{53}(x)$ $AddElement(j) = M_j^{(i)} + M_{j+3}^{(i)} - M_{j+10}^{(i)} + K_{j+16}$
$expand_1(j) = s_1(Q_{j-16}^{(i)}) + s_2(Q_{j-15}^{(i)}) + s_3(Q_{j-14}^{(i)}) + s_0(Q_{j-13}^{(i)})$ $+ s_1(Q_{j-12}^{(i)}) + s_2(Q_{j-11}^{(i)}) + s_3(Q_{j-10}^{(i)}) + s_0(Q_{j-9}^{(i)})$ $+ s_1(Q_{j-8}^{(i)}) + s_2(Q_{j-7}^{(i)}) + s_3(Q_{j-6}^{(i)}) + s_0(Q_{j-5}^{(i)})$ $+ s_1(Q_{j-4}^{(i)}) + s_2(Q_{j-3}^{(i)}) + s_3(Q_{j-2}^{(i)}) + s_0(Q_{j-1}^{(i)})$ $+ AddElement(j-16)$	$expand_1(j) = s_1(Q_{j-16}^{(i)}) + s_2(Q_{j-15}^{(i)}) + s_3(Q_{j-14}^{(i)}) + s_0(Q_{j-13}^{(i)})$ $+ s_1(Q_{j-12}^{(i)}) + s_2(Q_{j-11}^{(i)}) + s_3(Q_{j-10}^{(i)}) + s_0(Q_{j-9}^{(i)})$ $+ s_1(Q_{j-8}^{(i)}) + s_2(Q_{j-7}^{(i)}) + s_3(Q_{j-6}^{(i)}) + s_0(Q_{j-5}^{(i)})$ $+ s_1(Q_{j-4}^{(i)}) + s_2(Q_{j-3}^{(i)}) + s_3(Q_{j-2}^{(i)}) + s_0(Q_{j-1}^{(i)})$ $+ AddElement(j-16)$
$expand_2(j) = Q_{j-16}^{(i)} + r_1(Q_{j-15}^{(i)}) + Q_{j-14}^{(i)} + r_2(Q_{j-13}^{(i)})$ $+ Q_{j-12}^{(i)} + r_3(Q_{j-11}^{(i)}) + Q_{j-10}^{(i)} + r_4(Q_{j-9}^{(i)})$ $+ Q_{j-8}^{(i)} + r_5(Q_{j-7}^{(i)}) + Q_{j-6}^{(i)} + r_6(Q_{j-5}^{(i)})$ $+ Q_{j-4}^{(i)} + r_7(Q_{j-3}^{(i)}) + s_5(Q_{j-2}^{(i)}) + s_4(Q_{j-1}^{(i)})$ $+ AddElement(j-16)$	$expand_2(j) = Q_{j-16}^{(i)} + r_1(Q_{j-15}^{(i)}) + Q_{j-14}^{(i)} + r_2(Q_{j-13}^{(i)})$ $+ Q_{j-12}^{(i)} + r_3(Q_{j-11}^{(i)}) + Q_{j-10}^{(i)} + r_4(Q_{j-9}^{(i)})$ $+ Q_{j-8}^{(i)} + r_5(Q_{j-7}^{(i)}) + Q_{j-6}^{(i)} + r_6(Q_{j-5}^{(i)})$ $+ Q_{j-4}^{(i)} + r_7(Q_{j-3}^{(i)}) + s_5(Q_{j-2}^{(i)}) + s_4(Q_{j-1}^{(i)})$ $+ AddElement(j-16)$

Table 9. Logic functions used in old Blue Midnight Wish. Note that for the function $AddElement(j)$ index expressions involving the variable j for M are computed modulo 16.

The new description of the used logical functions is the following:

BMW224/BMW256	BMW384/BMW512
$s_0(x) = SHR^1(x) \oplus SHL^3(x) \oplus ROTL^4(x) \oplus ROTL^{19}(x)$ $s_1(x) = SHR^1(x) \oplus SHL^2(x) \oplus ROTL^8(x) \oplus ROTL^{23}(x)$ $s_2(x) = SHR^2(x) \oplus SHL^1(x) \oplus ROTL^{12}(x) \oplus ROTL^{25}(x)$ $s_3(x) = SHR^2(x) \oplus SHL^2(x) \oplus ROTL^{15}(x) \oplus ROTL^{29}(x)$ $s_4(x) = SHR^1(x) \oplus x$ $s_5(x) = SHR^2(x) \oplus x$ $r_1(x) = ROTL^3(x)$ $r_2(x) = ROTL^7(x)$ $r_3(x) = ROTL^{13}(x)$ $r_4(x) = ROTL^{16}(x)$ $r_5(x) = ROTL^{19}(x)$ $r_6(x) = ROTL^{23}(x)$ $r_7(x) = ROTL^{27}(x)$ $AddElement(j) = \Big(ROTL^{(j+1)}(M_j^{(i)}) + ROTL^{(j+4)}(M_{j+3}^{(i)})$ $- ROTL^{(j+11)}(M_{j+10}^{(i)}) + K_{j+16}\Big) \oplus H_{j+7}^{(i)}$	$s_0(x) = SHR^1(x) \oplus SHL^3(x) \oplus ROTL^4(x) \oplus ROTL^{37}(x)$ $s_1(x) = SHR^1(x) \oplus SHL^2(x) \oplus ROTL^{13}(x) \oplus ROTL^{43}(x)$ $s_2(x) = SHR^2(x) \oplus SHL^1(x) \oplus ROTL^{19}(x) \oplus ROTL^{53}(x)$ $s_3(x) = SHR^2(x) \oplus SHL^2(x) \oplus ROTL^{28}(x) \oplus ROTL^{59}(x)$ $s_4(x) = SHR^1(x) \oplus x$ $s_5(x) = SHR^2(x) \oplus x$ $r_1(x) = ROTL^5(x)$ $r_2(x) = ROTL^{11}(x)$ $r_3(x) = ROTL^{27}(x)$ $r_4(x) = ROTL^{32}(x)$ $r_5(x) = ROTL^{37}(x)$ $r_6(x) = ROTL^{43}(x)$ $r_7(x) = ROTL^{53}(x)$ $AddElement(j) = \Big(ROTL^{(j+1)}(M_j^{(i)}) + ROTL^{(j+4)}(M_{j+3}^{(i)})$ $- ROTL^{(j+11)}(M_{j+10}^{(i)}) + K_{j+16}\Big) \oplus H_{j+7}^{(i)}$
$expand_1(j) = s_1(Q_{j-16}^{(i)}) + s_2(Q_{j-15}^{(i)}) + s_3(Q_{j-14}^{(i)}) + s_0(Q_{j-13}^{(i)})$ $+ s_1(Q_{j-12}^{(i)}) + s_2(Q_{j-11}^{(i)}) + s_3(Q_{j-10}^{(i)}) + s_0(Q_{j-9}^{(i)})$ $+ s_1(Q_{j-8}^{(i)}) + s_2(Q_{j-7}^{(i)}) + s_3(Q_{j-6}^{(i)}) + s_0(Q_{j-5}^{(i)})$ $+ s_1(Q_{j-4}^{(i)}) + s_2(Q_{j-3}^{(i)}) + s_3(Q_{j-2}^{(i)}) + s_0(Q_{j-1}^{(i)})$ $+ AddElement(j-16)$	$expand_1(j) = s_1(Q_{j-16}^{(i)}) + s_2(Q_{j-15}^{(i)}) + s_3(Q_{j-14}^{(i)}) + s_0(Q_{j-13}^{(i)})$ $+ s_1(Q_{j-12}^{(i)}) + s_2(Q_{j-11}^{(i)}) + s_3(Q_{j-10}^{(i)}) + s_0(Q_{j-9}^{(i)})$ $+ s_1(Q_{j-8}^{(i)}) + s_2(Q_{j-7}^{(i)}) + s_3(Q_{j-6}^{(i)}) + s_0(Q_{j-5}^{(i)})$ $+ s_1(Q_{j-4}^{(i)}) + s_2(Q_{j-3}^{(i)}) + s_3(Q_{j-2}^{(i)}) + s_0(Q_{j-1}^{(i)})$ $+ AddElement(j-16)$
$expand_2(j) = Q_{j-16}^{(i)} + r_1(Q_{j-15}^{(i)}) + Q_{j-14}^{(i)} + r_2(Q_{j-13}^{(i)})$ $+ Q_{j-12}^{(i)} + r_3(Q_{j-11}^{(i)}) + Q_{j-10}^{(i)} + r_4(Q_{j-9}^{(i)})$ $+ Q_{j-8}^{(i)} + r_5(Q_{j-7}^{(i)}) + Q_{j-6}^{(i)} + r_6(Q_{j-5}^{(i)})$ $+ Q_{j-4}^{(i)} + r_7(Q_{j-3}^{(i)}) + s_4(Q_{j-2}^{(i)}) + s_5(Q_{j-1}^{(i)})$ $+ AddElement(j-16)$	$expand_2(j) = Q_{j-16}^{(i)} + r_1(Q_{j-15}^{(i)}) + Q_{j-14}^{(i)} + r_2(Q_{j-13}^{(i)})$ $+ Q_{j-12}^{(i)} + r_3(Q_{j-11}^{(i)}) + Q_{j-10}^{(i)} + r_4(Q_{j-9}^{(i)})$ $+ Q_{j-8}^{(i)} + r_5(Q_{j-7}^{(i)}) + Q_{j-6}^{(i)} + r_6(Q_{j-5}^{(i)})$ $+ Q_{j-4}^{(i)} + r_7(Q_{j-3}^{(i)}) + s_4(Q_{j-2}^{(i)}) + s_5(Q_{j-1}^{(i)})$ $+ AddElement(j-16)$

Table 10. Logic functions used in tweaked Blue Midnight Wish. Note that for the function $AddElement(j)$ index expressions involving the variable j for left rotations, M and H are computed modulo 16.

By comparing old and new list of logical functions used in f_1 the difference is in the definition of the element $AddElement()$. The old term was giving a chance an attacker to make changes in the most significant bits of the message and due to the operations of addition, those changes were canceling each other up to the last variable Q_{31}, thus giving free-start near collisions in the compression function. The new (tweaked) expression for $AddElement(j)$ rotates the values of the message $M^{(i)}$, and additionally operates with the vector $ROTL^7(H_{i-1}) = (H_7^{(i-1)}, H_8^{(i-1)}, \ldots, H_5^{(i-1)}, H_6^{(i-1)})$ which is a rotation by seven position to the left of the vector $(H_0^{(i-1)}, H_1^{(i-1)}, \ldots, H_{15}^{(i-1)})$. This is our second introduction of expressions that decouples the input values of the message $M^{(i)}$ and the chaining double pipe $H^{(i-1)}$ with the particular values from $M^{(i)}$ and $H^{(i-1)}$ that are repeatedly used in the Blue Midnight Wish expressions.

4 A technical typo correction in f_1

We have corrected another technical typo that was present in the previous version of Blue Midnight Wish.

Namely, in the old f_1 we had the following order of using the logical functions s_4 and s_5 in the expression

$$expand_2(j) = \ldots + s_5(Q_{j-2}^{(i)}) + s_4(Q_{j-1}^{(i)}) + \ldots$$

The proper order of using s_4 and s_5 should be as it is done in the new tweaked version:

$$expand_2(j) = \ldots + s_4(Q_{j-2}^{(i)}) + s_5(Q_{j-1}^{(i)}) + \ldots$$

5 Tweak Nr. 2

The second tweak consist of an additional (final) use of the compression function.

The generic description of the old Blue Midnight Wish had the following structure:

Algorithm: Blue Midnight Wish
Input: Message M of length l bits, and the message digest size n. **Output:** A message digest $Hash$, that is long n bits.

1. Preprocessing
(a) Pad the message M.
(b) Parse the padded message into N, m-bit message blocks, $M^{(1)}$, $M^{(2)}$, $\ldots$, $M^{(N)}$.
(c) Set the initial value of the double pipe $H^{(0)}$.
2. Hash computation
For $i = 1$ to N
{
$Q_a^{(i)} = f_0(M^{(i)}, H^{(i-1)})$;
$Q_b^{(i)} = f_1(M^{(i)}, Q_a^{(i)})$;
$H^{(i)} = f_2(M^{(i)}, Q_a^{(i)}, Q_b^{(i)})$;
}
3. $Hash$ =Take_n_Least_Significant_Bits($H^{(N)}$).

Table 11. A generic description of the Blue Midnight Wish hash algorithm

Together with the tweak introduced in f_0 and f_1 the generic description of the tweaked Blue Midnight Wish has the following structure:

Algorithm: Blue Midnight Wish
Input: Message M of length l bits, and the message digest size n. **Output:** A message digest $Hash$, that is n bits long.

1. Preprocessing
(a) Pad the message M.
(b) Parse the padded message into N, m-bit message blocks, $M^{(1)}$, $M^{(2)}$, $\ldots$, $M^{(N)}$.
(c) Set the initial value of the double pipe $H^{(0)}$.
2. Hash computation
For $i = 1$ to N
{
$Q_a^{(i)} = f_0(M^{(i)}, H^{(i-1)})$;
$Q_b^{(i)} = f_1(M^{(i)}, H^{(i-1)}, Q_a^{(i)})$;
$H^{(i)} = f_2(M^{(i)}, Q_a^{(i)}, Q_b^{(i)})$;
}
3. Finalization
$Q_a^{final} = f_0(H^{(N)}, CONST^{final})$;
$Q_b^{final} = f_1(H^{(N)}, CONST^{final}, Q_a^{final})$;
$H^{final} = f_2(H^{(N)}, Q_a^{final}, Q_b^{final})$;
4. $Hash$ =Take_n_Least_Significant_Bits(H^{final}).

Table 12. A generic description of the Blue Midnight Wish hash algorithm

As it is shown in Table 12, in the final invocation of the compression function we have changed the role of the chaining double pipe and the message. Since there is no more message to be digested, the role that the message data was performing in the previous invocations of the compression function is now given to the last obtained double pipe $H^{(N)}$. In such a case the role of the chaining double pipe is fixed to a constant that we denote as: $CONST^{final}$.

We have chosen 16 components of the vector $CONST^{final} = (CONST_0^{final}, \ldots, CONST_{15}^{final})$ to be

- $CONST_j^{final} = \texttt{0xaaaaaaa0} + j, \quad j = 0, 1, \ldots, 15$ for BMW224 and BMW256.
- $CONST_j^{final} = \texttt{0xaaaaaaaaaaaaaaa0} + j, \quad j = 0, 1, \ldots, 15$ for BMW384 and BMW512.

By fixing the $CONST^{final}$ we are removing this variable from the attacker's repository, in his attempt to find pseudo collisions and pseudo-preimages. Additionally the final invocation of the compression function is a measure for any attack that can find near collisions or near-pseudo-collisions or near preimages or near-pseudo-preimages of the compression function of Blue Midnight Wish.

Acknowledgement

We would like to thank Søren S. Thomsen, the member of Grøstl team, for his analysis and his discovery of near and pseudo attacks on the initial Blue Midnight Wish submission and to Niels Ferguson, the member of Skein team, for his remark (send to us privately in his analysis of Edon-R) about the cryptographic value of having additional final invocation of the compression function.