A rotational distinguisher on Shabal's keyed permutation and its impact on the security proofs

Gilles Van Assche
STMicroelectronics

March 24, 2010

Abstract

In this short note, we apply a rotational distinguisher to the keyed permutation of the SHA-3 candidate Shabal. We then discuss its applicability in the scope of Shabal's mode of operation and its impact on the security proofs.

The SHA-3 candidate Shabal uses its own mode of operation relying on a keyed permutation [3]. The keyed permutation, denoted $\mathcal{P}$, takes as input $M \in \mathbb{Z}_2^{512}$, $A \in \mathbb{Z}_2^{384}$, $B \in \mathbb{Z}_2^{512}$ and $C \in \mathbb{Z}_2^{512}$, and outputs $A' \in \mathbb{Z}_2^{384}$ and $B' \in \mathbb{Z}_2^{512}$. When M and C are fixed, $\mathcal{P}_{M,C}$ is a permutation in the inputs A and B. The inputs M, A, B and C can also be viewed as 16 (or 12 for A) words of 32 bits each. Inside $\mathcal{P}$, the following operations are used: bitwise exclusive or (XOR), bitwise and, cyclic shift on 32 bits (also called rotations and denoted $\ll$), addition modulo 2^{32} and multiplication by 3 and 5 modulo 2^{32}.

Rotational cryptanalysis is similar to differential cryptanalysis. Instead of applying the function under test with pairs of inputs with a given difference (e.g., $(a, a \oplus \Delta)$ for a fixed Δ), the idea is to relate the two members of a pair with a rotation (see [6] and the references therein). In the sequel, we are interested in pairs of input (X, X') such that all the 32-bit words of X are cyclically shifted by one position to the left, i.e., $X'[i] = X[i] \ll 1$, for all i, where $X[i]$ is a 32-bit word of X. To make the notation shorter, one can write $X' = X \ll 1$.

1 Distinguisher on Shabal's keyed permutation $\mathcal{P}$

Most of the operations used by $\mathcal{P}$ preserve the rotation: the bitwise operations and the rotation operation itself. For the additions modulo 2^{32}, conditions on the values of X and Y can be set such that $(X \ll 1) + (Y \ll 1) = (X + Y) \ll 1$. From a statistical point of view, the probability that $(X \ll 1) + (Y \ll 1) = (X + Y) \ll 1$ is about $2^{-1.415}$ when X and Y are drawn uniformly from $\mathbb{Z}_2^{32}$ [6, 5]. For the multiplications by 3 and 5, there are also conditions on the value of the operand such that the rotation is preserved. We have found that:

$$\Pr[3(X \ll 1) \bmod 2^{32} = (3X \bmod 2^{32}) \ll 1] = \frac{2^{32} - 1}{3 \times 2^{32}} \approx \frac{1}{3} \approx 2^{-1.585}, \text{ and}$$
$$\Pr[5(X \ll 1) \bmod 2^{32} = (5X \bmod 2^{32}) \ll 1] = \frac{3 \times 2^{32} - 8}{10 \times 2^{32}} \approx \frac{3}{10} \approx 2^{-1.737},$$

where X is drawn uniformly from $\mathbb{Z}_2^{32}$.

It follows that, with some probability, the output of $\mathcal{P}(M \ll 1, A \ll 1, B \ll 1, C \ll 1)$ is equal to $\mathcal{P}(M, A, B, C) \ll 1$. In $\mathcal{P}$, there are 48 applications of the multiplication by 3, 48 applications of the multiplication by 5 and 36 modular additions. The probability that a rotated pair survives up to the output of $\mathcal{P}$ is thus about

$2^{-(48\times1.585+48\times1.737+36\times1.415)} = 2^{-210}$. With an ideal keyed permutation of the same size, the probability would be $2^{-(384+512)}$.

This is a straightforward application of the rotational cryptanalysis, where the inputs M, A, B and C are chosen arbitrarily. Further analysis can be used to increase the probability of getting a rotated pair at the output. Specific conditions on the words can be written such that the multiplication preserves the rotation. One can use the degrees of freedom in C and in M to satisfy these conditions directly instead of relying on randomly drawn values.

A multiplication by 5 is applied to a word of A directly. When updating a word of A, a word of M is XORed. Hence, we can set the value of M such that the updated word satisfies the conditions to preserve rotation through $\times 5$. Similarly, a word of C is XORed just before multiplying by 3. Hence, it can be used such that the resulting word satisfies the conditions for $\times 3$. This allows us to save 12 multiplications by 3 and 12 by 5, increasing the probability to about $2^{-(36\times1.585+36\times1.737+36\times1.415)} = 2^{-171}$.

Tracking the dependencies between words further to satisfy more conditions can be part of future research and may increase the probability. Using the degrees of freedom in A and B is also possible.

Hence, this shows that one can distinguish $\mathcal{P}$ from an ideal keyed permutation of the same size with about 2^{171} queries. Note that there currently exist distinguishers requiring much less queries, based on different techniques [1, 7, 2].

1.1 A variant with $A = C = 0$ and $B = M$

We note that a variant of the distinguisher can be applied when, at the input of $\mathcal{P}$, the words of A and C are set to zero and the words of B and M are equal. This variant will be used in the sequel.

Here, we consider pairs $(M, M \ll 1)$ and check whether the 512-bit B-part of output, i.e., B' in $(A', B') = \mathcal{P}(M, A, B, C)$, preserves the rotation. Since B' does not depend on the modular additions (and $C = 0$ anyway), we do not need to consider them. Hence, the probability that $\mathcal{P}$ preserves the rotation in B' is about $2^{-(48\times1.585+48\times1.737)} = 2^{-159}$.

2 Applicability to Shabal's mode of operation

Shabal's mode of operation is shown to be indifferentiable from a random oracle (up to a given probability) if the keyed permutation $\mathcal{P}$ is an ideal keyed permutation or not too far from it [3, 4]. The mode of operation is parameterized, among other things, by the initialization vector (IV) and by the number of final rounds. The indifferentiability bound does not depend on these two parameters. Furthermore, Shabal uses a counter on each block but the indifferentiability proofs do not require it. In fact, the theorem in [4] explicitly considers the case where there are no counters and no final rounds.

Hence, we can use a minimal instance of Shabal's mode of operation with IV $A = B = C = 0$, no final rounds and no counter. Note that this differs from the Shabal hash function itself, which uses a specific set of IVs (for different output lengths), has three final rounds and uses block counters.

We can build a distinguisher on a hash function (again, not Shabal itself) that uses Shabal's mode of operation in a minimal way and Shabal's keyed permutation $\mathcal{P}$. Let us build pairs of messages (m, m'), $m, m' \in \mathbb{Z}_2^*$, such that they span only one block and such that M and M' after padding make a rotated pair, i.e., $M' = M \ll 1$. In this instance of the mode of operation, A, B, C are initialized to 0 and M is added wordwise to B, giving $B = M$ at the input of $\mathcal{P}$. After the application of $\mathcal{P}$, the output is extracted from the B-part of the output. Hence, the variant presented in Section 1.1 above can be translated into a distinguisher against this specific instance.

2.1 Discussion

The mode of operation of Shabal was proven to be indifferentiable even if $\mathcal{P}$ differs from an ideal keyed permutation up to a given bias [4]. In the theorem, the keyed permutation can have fixed known relations between its input and output, which always hold. It may be possible that this result can be adapted to a keyed permutation that has relations satisfied only probabilistically but, at this point, the distinguisher of Section 1 falls outside of the scope covered by the proof in [4].

In addition, Section 2 shows a distinguisher on a hash function using $\mathcal{P}$ and a mode of operation proven indifferentiable. This implies that $\mathcal{P}$ is not strong enough to be used with such a mode of operation in a secure way.

The distinguisher presented here cannot be applied on the Shabal hash function for three reasons. First, Shabal has a non-symmetric IV, which makes it harder to preserve the rotation. Second, the addition of a block counter does not preserve the rotation. And third, Shabal has final rounds, which decrease the probability of preserving rotated pairs.

3 Conclusion

We have shown a distinguisher on the keyed permutation of Shabal, applying the rotational cryptanalysis in a fairly straightforward way. We have then applied a variant of this distinguisher to a hash function using Shabal's keyed permutation and an instance of Shabal's mode of operation satisfying the indifferentiability proofs.

Although the distinguisher is not applicable on Shabal at this point, it bypasses Shabal's current security proofs. In conclusion, the security of Shabal relies on features *not* required by these security proofs, namely the non-symmetric initialization vectors, the block counters or the final rounds.

Acknowledgments I would like to thank Anne Canteaut for her constructive comments.

References

[1] Jean-Philippe Aumasson, *On the pseudorandomness of Shabal's keyed permutation*, Available online, 2009.

[2] Jean-Philippe Aumasson, Atefeh Mashatan, and Willi Meier, *More on Shabal's permutation*, OFFICIAL COMMENT, 2009.

[3] Emmanuel Bresson, Anne Canteaut, Benoît Chevallier-Mames, Christophe Clavier, Thomas Fuhr, Aline Gouget, Thomas Icart, Jean-François Misarsky, Marìa Naya-Plasencia, Pascal Paillier, Thomas Pornin, Jean-René Reinhard, Céline Thuillet, and Marion Videau, *Shabal, a submission to NIST's cryptographic hash algorithm competition*, Submission to NIST, 2008.

[4] ———, *Indifferentiability with distinguishers: Why Shabal does not require ideal ciphers*, Cryptology ePrint Archive, Report 2009/199, 2009.

[5] M. Daum, *Cryptanalysis of hash functions of the MD4 family*, PhD thesis, Ruhr-Universität Bochum, 2005.

[6] Dmitry Khovratovich and Ivica Nikolić, *Rotational cryptanalysis of ARX*, Fast Software Encryption 2010, 2010.

[7] Lars R. Knudsen, Krystian Matusiewicz, and Søren S. Thomsen, *Observations on the Shabal keyed permutation*, OFFICIAL COMMENT, 2009.