Tweaking SIMD

Gaëtan Leurent, Pierre-Alain Fouque, Charles Bouillaguet

École Normale Supérieure – Département d'Informatique,
45 rue d'Ulm, 75230 Paris Cedex 05, France
{Gaetan.Leurent,Pierre-Alain.France,Charles.Bouillaguet}@ens.fr

Abstract. The version 1.1 of SIMD has been tweaked to deal with some unwanted properties of the Feistel structure. This documents details the changes and how the new values were selected.

1 Description of the Tweak

The tweak consists in two parts: changing the permutation $p^{(i)}$, and changing the rotations $r^{(i)}$ and $s^{(i)}$.

1.1 The Permutations

SIMD-256 The old permutations were:

$$p^{(i)}(x) = \begin{cases} x+1 \pmod 4 & \text{if } i \text{ is even} \\ x+2 \pmod 4 & \text{if } i \text{ is odd} \end{cases}$$

The new permutations are:

	j	0	1	2	3
$p^{(0)}(j) = j \oplus 1$	$p^{(0)}(j)$	1	0	3	2
$p^{(1)}(j) = j \oplus 2$	$p^{(1)}(j)$	2	3	0	1
$p^{(2)}(j) = j \oplus 3$	$p^{(2)}(j)$	3	2	1	0

where $p^{(i)} = p^{(i \bmod 3)}$. Note that the number of permutations has been changed from 2 to 3.

SIMD-512 The old permutations were:

$$p^{(0)}(x) = \begin{cases} x+1 \pmod 8 & \text{if } x = 0 \pmod 2 \\ x-1 \pmod 8 & \text{otherwise} \end{cases}$$

$$p^{(1)}(x) = \begin{cases} x+2 \pmod 8 & \text{if } x = 0 \pmod 4 \text{ or } x = 1 \pmod 4 \\ x-2 \pmod 8 & \text{otherwise} \end{cases}$$

$$p^{(2)}(x) = 7 - x \pmod 8$$

$$p^{(3)}(x) = x + 4 \pmod 8$$

The new permutations are:

	j	0	1	2	3	4	5	6	7
$p^{(0)}(j) = j \oplus 1$	$p^{(0)}(j)$	1	0	3	2	5	4	7	6
$p^{(1)}(j) = j \oplus 6$	$p^{(1)}(j)$	6	7	4	5	2	3	0	1
$p^{(2)}(j) = j \oplus 2$	$p^{(2)}(j)$	2	3	0	1	6	7	4	5
$p^{(3)}(j) = j \oplus 3$	$p^{(3)}(j)$	3	2	1	0	7	6	5	4
$p^{(4)}(j) = j \oplus 5$	$p^{(4)}(j)$	5	4	7	6	1	0	3	2
$p^{(5)}(j) = j \oplus 7$	$p^{(5)}(j)$	7	6	5	4	3	2	1	0
$p^{(6)}(j) = j \oplus 4$	$p^{(6)}(j)$	4	5	6	7	0	1	2	3

where $p^{(i)} = p^{(i \bmod 7)}$. Note that the number of permutations has been changed from 4 to 7.

1.2 The Rotations

The old rotations were:

Round	π_0	π_1	π_2	π_3
0	3	20	14	27
1	26	4	23	11
2	19	28	7	22
3	15	5	29	9

The new rotations are:

Round	π_0	π_1	π_2	π_3
0	3	23	17	27
1	28	19	22	7
2	29	9	15	5
3	4	13	10	25

2 Motivation

A differential trail with probability 2^{-507} has been found in the Feistel structure of SIMD-512 1.0 by Nad and Mendel [1]. This path does not introduce any difference in the message, and goes from some difference Δ_{in} in the chaining value to some other difference Δ_{out}. This can be used to mount a distinguisher on the compression function of SIMD-512 with complexity 2^{427} using some message modification techniques. We do not believe this to be a threat on the full hash function, because free-start attack on the compression function can hardly be transferred into attack on the full function when the chaining variable is wide (which is the case in all versions of SIMD). However, when studying this attack, we found some bad properties of the Feistel structure in SIMD, and we decided to tweak SIMD so as to avoid those properties.

2.1 The Composition of Four Permutations Gives the Identity

The main unwanted property in the design of SIMD is the fact that in SIMD-512, the composition of the four permutations gives the identity: $p^{(3)} \circ p^{(2)} \circ p^{(1)} \circ p^{(0)} = id$.

Let us assume that all the Boolean function are absorbing (ie. is a single input is active, the output will not be active). This is possible for all the Boolean functions in

SIMD, and happens with probability 1/2 for each active input bit. Then when a single difference is introduced in the state, it propagates according to Path 1:

- At step 4, the difference in $A_i^{(3)}$ is diffused to $A_j^{(4)}$.
- At step 5, the difference in $A_j^{(4)}$ is diffused to $A_k^{(5)}$.
- At step 6, the difference in $A_k^{(5)}$ is diffused to $A_l^{(6)}$.
- At step 7, the difference in $A_l^{(6)}$ is diffused to $A_i^{(7)}$. However, $A_i^{(7)}$ is already active because of $D_i^{(6)}$. Therefore, only 4 registers per round will be active in the remaining of the Feistel structure.

This allows to build good differential paths in the compression function of SIMD-512.

Differential Path 1 Diffusion when all Boolean functions are absorbing, and $p^{(3)}p^{(2)}p^{(1)}p^{(0)} = id$. This happened in SIMD-512

Step	Feistel i				Feistel j				Feistel k				Feistel l			
0	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-
2	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-
3	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4	-	x	-	-	x	-	-	-	-	-	-	-	-	-	-	-
5	-	-	x	-	-	x	-	-	x	-	-	-	-	-	-	-
6	-	-	-	x	-	-	x	-	-	x	-	-	x	-	-	-
7	x	-	-	-	-	-	-	x	-	-	x	-	-	x	-	-
8	-	x	-	-	x	-	-	-	-	-	-	x	-	-	x	-
9	-	-	x	-	-	x	-	-	x	-	-	-	-	-	-	x
10	-	-	-	x	-	-	x	-	-	x	-	-	x	-	-	-

$$
\begin{aligned}
j &= p^{(0)}(i) \\
k &= p^{(1)}(j) = p^{(1)}p^{(0)}(i) \\
l &= p^{(2)}(k) = p^{(2)}p^{(1)}p^{(0)}(i) \\
p^{(3)}(l) &= p^{(3)}p^{(2)}p^{(1)}p^{(0)}(i) = i
\end{aligned}
$$

2.2 Exploiting the Periodicity

In the intial version of SIMD, we use 4 permutations (resp. 2 in SIMD-256). Since the Feistel has 4 registers, we can build paths with periodicity 4, and the same permutation will always be used in the same position. This allows to build some good truncated differential paths, see Path 2 and Path 3.

Differential Path 2 when the permutations are repeated with period four.

Step	Feistel i				Feistel j			
0	-	x	-	-	-	-	-	x
1	-	-	x	-	x	-	-	-
2	-	-	-	x	-	x	-	-
3	x	-	-	-	-	-	x	-
4	-	x	-	-	-	-	-	x
5	-	-	x	-	x	-	-	-
6	-	-	-	x	-	x	-	-
7	x	-	-	-	-	-	x	-

$$j = p^{(0)}(i)$$
$$p^{(2)}(j) = p^{(2)}p^{(0)}(i) = i$$

Differential Path 3 when the permutations are repeated with period four.

Step	Feistel i				Feistel j			
0	-	x	-	-	-	x	-	-
1	-	-	x	-	-	-	x	-
2	-	-	-	x	-	-	-	x
3	x	-	-	-	x	-	-	-
4	-	x	-	-	-	x	-	-
5	-	-	x	-	-	-	x	-
6	-	-	-	x	-	-	-	x
7	x	-	-	-	x	-	-	-

$$j = p^{(0)}(i)$$
$$i = p^{(0)}(j)$$

Differential Path 4 when the permutations are repeated with period three.

Step	Feistel i				Feistel j			
0	-	x	-	-	-	x	-	-
1	-	-	x	-	-	-	x	-
2	x	-	-	x	x	-	-	x
3	-	x	-	-	-	x	-	-
4	-	-	x	-	-	-	x	-
5	x	-	-	x	x	-	-	x
6	-	x	-	-	-	x	-	-

$$j = p^{(0)}(i)$$
$$i = p^{(0)}(j)$$

3 Choice of the New Permutations

To improve the design of SIMD, we used the following criterion for the choice of the permutations:

1. The permutations should achieve full diffusion after 3 rounds (resp. 2 for SIMD-256);
2. Use an odd number of permutations (see Section 2.2);
3. The composition of any two permutations should not have fixed points.
4. The composition of 4 successive permutations should not give the identity (see Section 2.1);

If possible we try to use more than 4 permutations to avoid paths like Path 4.

For SIMD-256, we selected the only set of permutation that can fulfill conditions 1, 2, and 3.

For SIMD-512, we decided to use the set of all permutations of the form $j \mapsto j \oplus \alpha$ because it gives seven permutations that fulfill conditions 1, 2, and 3. We implemented a search for optimal truncated differential paths to select a good combination.

4 Choice of the New Rotations

The rotations should be chosen so that it is not possible to create a small loop in a differential path, *i.e.* the various way a given active bit can propagate should not cancel each other.

In SIMD 1.0 the rotations had been chosen so that in each round, sums and differences of rotations do not cancel or give special values (like 1 or 16). The rotation are chosen so that the 16 values used in the four rounds are all different.

However, we did not consider the case of loops at a round boundary. For the tweaked version, we added a constraint that all the possible propagation of a given bit after three rounds should be in different bit positions. Then we selected the candidate that minimized the number of even rotations, and multiples of bigger powers of 2.

References

1. Nad, T., Mendel, F. Private communication (August 2009)