Bug Fix in the SHAvite-3 Submission Package

Eli Biham[1,⋆] and Orr Dunkelman[2,3]

[1] Computer Science Department, Technion
Haifa 32000, Israel
biham@cs.technion.ac.il
[2] École Normale Supérieure
Département d'Informatique,
CNRS, INRIA
[3] Faculty of Mathematics and Computer Science
Weizmann Institute of Science
P.O. Box 26
Rehovot 76100, Israel
orr.dunkelman@weizmann.ac.il

Abstract. This document lists the different changes in the the SHAvite-3 submission package, following our bug fix.

Due to the bug fix, we had to change the IVs and test vectors for SHAvite-3_{512}. The algorithm's performance was measured again, and it has not changed. We also fixed two small typos in the documentation which may have confused readers and implementors.

The changes in the documentation were kept as minimal as possible, and we report all of them in this document.

1 Bug Fix Changes

Due to a small bug in the software of SHAvite-3_{512}, all 128-bit words were rotated to the wrong side. As this bug affected the reference implementation as well, the suggested MIV_{512}, and all derived chaining values related to it, were incorrectly calculated.

Location	Original Text	New Text
Sect. 4: Specifications of SHAvite-3		
Pp. 16, section 4.2.4	$MIV_{512} = C_{512}(0,0,0,0) =$ 9A762FED...BE4076EE$_x$	$MIV_{512} = C_{512}(0,0,0,0) =$ F0C11673...F1320A9F$_x$
Pp. 17, Table 3	IV_{384} was changed from CEB54AC9 ...0AD83828$_x$	To 71F48510...2C3E9F25$_x$
Pp. 17, Table 3	IV_{512} was changed from D5652B63 ...0AD83828$_x$	To 71F48510 ...21E11499$_x$
Pp. 39–41	All test vectors changed	with a new set of test vectors

2 Typo Fixes

Two typos were fixed. The first concerns which message words are XORed with the counter, and the second concerns the algorithm. In both cases, the reference code has not changed, and the meaning of the algorithm has not changed as well.

⋆ The first author was supported in part by the Israel MOD Research and Technology Unit.

Location	Original Text	New Text
Sect. 4: Specifications of SHAvite-3		
Pp. 10, third para.	and $rk[17]^{\star}$, $rk[53]$, $rk[90]$, and $rk[127]^{\star}$, are XORed with $cnt[1]$.	and $rk[17]^{\star}$, $rk[57]$, $rk[86]$, and $rk[127]^{\star}$, are XORed with $cnt[1]$.
Pp. 11, Step 1	Steps 1(d) and 1(h) were swapped.	There was no change in the actual steps.