

Corrections in the document “AURORA: A Cryptographic Hash Algorithm Family (October 31, 2008)”

Submitters:

Sony Corporation¹ and Nagoya University²

Algorithm Designers:

Tetsu Iwata², Kyoji Shibutani¹, Taizo Shirai¹, Shiho Moriai¹, Toru Akishita¹

January 9, 2009

position	reason	changes
p.12, 2.1 Notation, symbols for AURORA-224M/256M	typo	$ME_y^x \rightarrow MS_y^x$ (four positions in total)
ditto	misword	Message Expansion \rightarrow Message Scheduling
p.23, Fig. 2.7, p.31, Fig. 2.9, and p.32, Fig. 2.10	typo	$ME_y^x \rightarrow MS_y^x$ (two positions in each figure)
p.56, 3.2 Domain Extension	clarification	Add “(a similar method was proposed by Nandi [37])” just after the second sentence.
p.61, 3.4.2 F-function	typo	$ME_y^x \rightarrow MS_y^x$ (two times)
p.69-71 4.2.2 Security Proofs of DMMD Transform	typo	an arbitrarily order \rightarrow an arbitrary order (four positions in total)
p.105, Table 5.8	typo	CF call \rightarrow 1 CF call