B Appendix - Equivalent number of NAND gates

Equivalent number of 2-input NAND gates, represents a measure of area for ASIC designs. It is equal to the total area of each design (including the I/O registers) divided by the area of a 2-input NAND gate of low driving strength from the library. Table 11 lists the equivalent number of 2-input NAND gates for our ASIC implementations.

Hash	Equivalent Number of 2-Input NAND Gates
BMW	164 K
Luffa	122 K
Skein	369 K
Skein-1c	21 K
Shabal	20 K
Blake	53 K
SHA-2	368 K
SHA-2-1c	13 K

Table 11. Equivalent number of 2-input NAND gates for ASIC implementation summary of the different compression functions