| $Function \backslash rounds$                      | 0                                    | 1                     | 2                                 | 3                         | 4                                 | 5   | 6  | 7                          | 8  | 9  | 10  |
|---|--------------------------------------|-----------------------|-----------------------------------|---------------------------|-----------------------------------|---|--|----------------------------|--|--|---|
| rnd_rnd   | 0.01191                              | _                     | _                                 | _                         | _                                 | _   | _  | _                          | _  | _  | _   |
|   |                                      |                       |                                   |                           |                                   |   |  |                            |  |  |   |
| AES   | _                                    | 1.0                   | 1.0                               | 0.175                     | 0.013                             | _   | _  | _                          | _  | _  | _   |
| BLAKE   | 1.0                                  | 0.228                 | 0.011                             | 0.008                     | _                                 | _   | _  | _                          | _  | _  | _   |
| Grain   | _                                    | _                     | 1.0                               | 0.014                     | 0.01                              | _   | _  | _                          | _  | _  | _   |
| Grostl  | _                                    | _                     | 1.0                               | 0.014                     | 0.018                             | 0.008                                       | _  | _                          | _  | _  | _   |
| HC-128  | 0.013                                | 0.01                  | _                                 | _                         | _                                 | _   | _  | _                          | _  | _  | _   |
| JH  | _                                    | _                     | _                                 | _                         | _                                 | _   | 1.0  | 0.008                      | 0.017                                    | _  | _   |
| Keccak  | _                                    | 1.0                   | 1.0                               | 0.013                     | 0.008                             | _   | _  | _                          | _  | _  | _   |
|   |                                      |                       |                                   |                           |                                   |   |  |                            |  |  |   |
| MD6   | _                                    | _                     | _                                 | _                         | _                                 | _   | _  | _                          | 0.993                                    | 0.006                                    | 0.016   |
| MD6<br>Rabbit                                     | -<br>0.011                           | -0.009                | _<br>_                            | _                         | _<br>_                            | _   | _<br>_                                       | _<br>_                     | 0.993                                    | 0.006<br>-                               | 0.016<br>-                                    |
|   |                                      | -<br>0.009<br>0.013   | -<br>-<br>-                       | -<br>-<br>-               | -<br>-<br>-                       | -<br>-<br>-                                 | -<br>-<br>-                                  | -<br>-<br>-                | 0.993<br>-<br>-                          | 0.006<br>-<br>-                          | 0.016<br>-<br>-                               |
| Rabbit  | 0.011                                |                       | -<br>-<br>-                       | -<br>-<br>-               | -<br>-<br>-                       | -<br>-<br>-                                 | _<br>_<br>_<br>_                             | _<br>_<br>_<br>_           | 0.993<br>-<br>-<br>-                     | 0.006<br>-<br>-<br>-                     | 0.016<br>-<br>-<br>-                          |
| Rabbit<br>RC4                                     | 0.011                                |                       | -<br>-<br>-<br>-<br>1.0           | -<br>-<br>-<br>-<br>0.017 | -<br>-<br>-<br>-<br>0.01          | _<br>_<br>_<br>_                            | _<br>_<br>_<br>_                             | _<br>_<br>_<br>_           | 0.993<br>-<br>-<br>-<br>-                | 0.006<br>-<br>-<br>-<br>-                | 0.016<br>-<br>-<br>-<br>-                     |
| Rabbit<br>RC4<br>rnd_rnd                          | 0.011                                | 0.013<br>-            | -<br>-<br>-<br>-<br>1.0           | -<br>-<br>-<br>-<br>0.017 | -<br>-<br>-<br>-<br>0.01<br>0.523 | -<br>-<br>-<br>-<br>0.014                   | -<br>-<br>-<br>-<br>-<br>0.016               | -<br>-<br>-<br>-           | 0.993<br>-<br>-<br>-<br>-<br>-           | 0.006<br>-<br>-<br>-<br>-<br>-           | 0.016<br>-<br>-<br>-<br>-<br>-                |
| Rabbit<br>RC4<br>rnd_rnd<br>Salsa20               | 0.011<br>-<br>0.009<br>-             | 0.013<br>-<br>-       | -<br>-<br>-<br>-<br>1.0           |                           |                                   | -<br>-<br>-<br>-<br>-<br>0.014              | -<br>-<br>-<br>-<br>-<br>0.016               | -<br>-<br>-<br>-<br>-      | 0.993<br>-<br>-<br>-<br>-<br>-           | 0.006<br>-<br>-<br>-<br>-<br>-<br>-      | 0.016<br>-<br>-<br>-<br>-<br>-<br>-           |
| Rabbit<br>RC4<br>rnd_rnd<br>Salsa20<br>SINGLE-DES | 0.011<br>-<br>0.009<br>-<br>-        | 0.013<br>-<br>-       | -<br>-<br>-<br>-<br>1.0<br>-<br>- |                           |                                   | -<br>-<br>-<br>-<br>0.014                   | -<br>-<br>-<br>-<br>0.016<br>-               | -<br>-<br>-<br>-<br>-      | 0.993<br>-<br>-<br>-<br>-<br>-<br>-      | 0.006<br>-<br>-<br>-<br>-<br>-<br>-<br>- | 0.016<br>-<br>-<br>-<br>-<br>-<br>-<br>-      |
| Rabbit RC4 rnd_rnd Salsa20 SINGLE-DES Skein       | 0.011<br>-<br>0.009<br>-<br>-<br>1.0 | -<br>-<br>-<br>-<br>- | _<br>_                            |                           |                                   | -<br>-<br>-<br>-<br>0.014<br>-<br>-<br>0.01 | -<br>-<br>-<br>-<br>0.016<br>-<br>-<br>0.012 | -<br>-<br>-<br>-<br>-<br>- | 0.993<br>-<br>-<br>-<br>-<br>-<br>-<br>- | 0.006<br>-<br>-<br>-<br>-<br>-<br>-<br>- | 0.016<br>-<br>-<br>-<br>-<br>-<br>-<br>-<br>- |

Table 1: Usable testbed results