

Symmetric, hash-based encryption

by Salko Korac
40517266@live.napier.ac.uk

Applied cryptography coursework
MSc Advanced Security & Digital Forensics

Abstract

Established symmetric encryption methods use fixed key lengths.
This practical coursework aims flexibility and security
by supporting anything from any length as key input.

Coursework Advisor:
Coursework submitted:
Last revision:

Prof. Bill Buchanan, Edinburgh Napier University, UK
May 14, 2021
May 14, 2021

Introduction

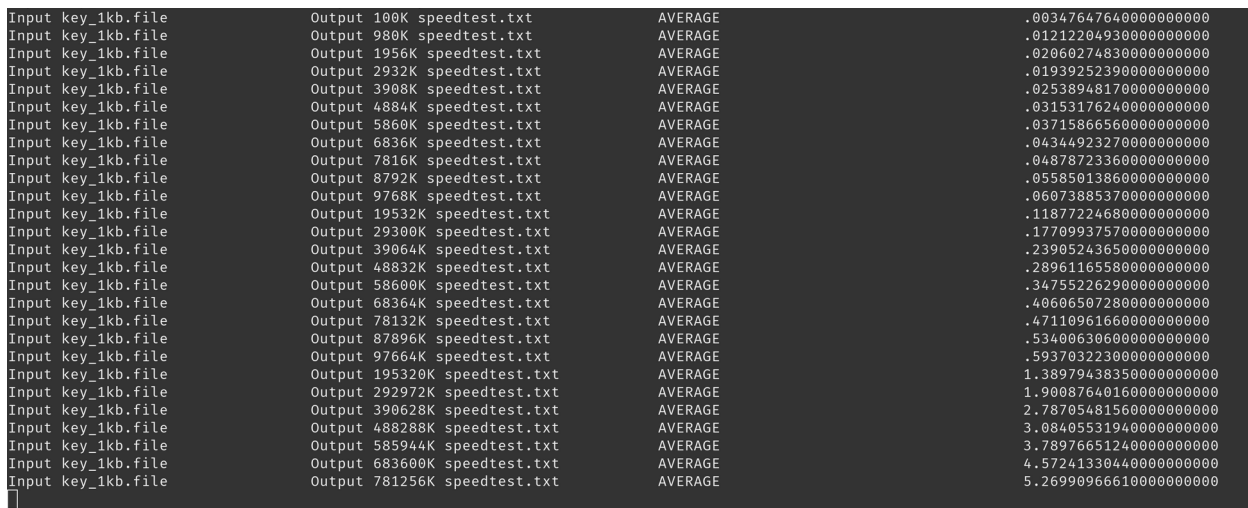
The hash functions Blake3, KangarooTwelve (“K12”) and Shake support outputs of arbitrary length. This coursework will evaluate this hash functions as Key Derivation Function (KDF) and Extendable Output Function (XOF). In regards to the predecessor Blake2, only the fork Blake2X supports outputs of arbitrary length; a rust implementation was not found. Therefore the Blake2 family was not considered in this coursework. To ensure comparability, all tests were performed with the respective rust crates “b3sum”, “k12sum” and “rash” in single-core mode.

Blake3 is well-promising in terms of speed and supports multi-threaded processing on multi-core CPUs. Shake and KangarooTwelve were derived from Keccak. Keccak won the NIST contest for the next generation hash function in 2012 (i.e. now known as SHA-3).

Speed and security of the hash functions are the two main criteria. The best balanced performer in both criteria will be used for a proof of concept. The speed was measured in two dimensions (i.e. input size and output size), while the security was evaluated by a literature review.

Speed of hash functions

The tested input sizes were 1 KB to 10 GB. The tested output sizes were 32 bytes to 1 GB, dumped as HEX. The measurement was done on three different platforms: notebook with Intel i7 x64 and SSD, Android mobile with ARMv8 and eMMC, as well as a dedicated cloud server with Xeon x64 and HDD. The system setup is visible in appendix a. As shown in figure 1, each hash operation was repeated 10 times and the average time was calculated to avoid unwanted breakouts during the measurement. The shell script used for the speed test is attached in appendix e. The raw results are attached in appendix b, c and d.



Input	Output	AVERAGE
key_1kb.file	100K speedtest.txt	.00347647640000000000
key_1kb.file	980K speedtest.txt	.01212204930000000000
key_1kb.file	1956K speedtest.txt	.02060274830000000000
key_1kb.file	2932K speedtest.txt	.01939252390000000000
key_1kb.file	3908K speedtest.txt	.02538948170000000000
key_1kb.file	4884K speedtest.txt	.03153176240000000000
key_1kb.file	5860K speedtest.txt	.03715866560000000000
key_1kb.file	6836K speedtest.txt	.04344923270000000000
key_1kb.file	7816K speedtest.txt	.04878723360000000000
key_1kb.file	8792K speedtest.txt	.05585013860000000000
key_1kb.file	9768K speedtest.txt	.06073885370000000000
key_1kb.file	19532K speedtest.txt	.11877224680000000000
key_1kb.file	29300K speedtest.txt	.17709937570000000000
key_1kb.file	39064K speedtest.txt	.23905243650000000000
key_1kb.file	48832K speedtest.txt	.28961165580000000000
key_1kb.file	58600K speedtest.txt	.34755226290000000000
key_1kb.file	68364K speedtest.txt	.40606507280000000000
key_1kb.file	78132K speedtest.txt	.47110961660000000000
key_1kb.file	87896K speedtest.txt	.53400630600000000000
key_1kb.file	97664K speedtest.txt	.59370322300000000000
key_1kb.file	195320K speedtest.txt	1.38979438350000000000
key_1kb.file	292972K speedtest.txt	1.90087640160000000000
key_1kb.file	390628K speedtest.txt	2.78705481560000000000
key_1kb.file	488288K speedtest.txt	3.08405531940000000000
key_1kb.file	585944K speedtest.txt	3.78976651240000000000
key_1kb.file	683600K speedtest.txt	4.57241330440000000000
key_1kb.file	781256K speedtest.txt	5.26990966610000000000

Figure 1: execution of the speed test.

For Blake3, the measurement showed: On system 1 (x64, i7) and system 3 (x64, XEON) the input size did not influence the hash speed so much. For example, on system 1, Blake3 needed 0.00813 seconds to hash a 1KB file to 32 bytes. And for 10GB, Blake3 needed only 1.47779 seconds. Exceptionally outstanding is system 2 (ARMv8). The afore-mentioned speed results are not valid here. The Samsung Galaxy Tab S5e needed 0.03526 seconds to hash a 1 KB file. But for 10 GB, the system needed 35.86665 seconds. Full details can be seen in appendix b.

For K12, the measurement showed: The results were very similar to Blake3. K12 was in many cases faster than Blake3, when input files were small (i.e. < 5 MB) or output was bigger (> 200 MB < 1 GB). But when it came to very large input files, K12 fall slightly behind Blake3. For example, to hash a 10 GB file to 32 bytes, K12 needed 4.59177 seconds. Blake3 needed for same task 1.47779 seconds. The difference of approx. 3.11398 seconds is also visible when expanding the hash to 1 GB. To hash same file to 1 GB output, K12 needed 9.78375 seconds where Blake3 needed 6.20759 seconds. The reason for that is mainly due to higher number of rounds compared to Blake3, while the sponge functions of K12 and Blake were pretty similarly fast.

For Shake, the speed was the slowest as can be seen in table 1. For example, hashing a 10 GB file to 32 bytes took 33.37358 seconds on system 1, where Blake3 needed 1.47779 seconds as afore-mentioned. In conclusion, the speed was assessed as impractical for hash-based encryption, and therefore it was not considered any-more. In general, Shake is a excellent hash function, which provides very good security and has it’s legitimate use cases (e.g. password hashing).

Hash function on system 1	Speed @ 1 KB input, 32 bytes output	Speed @ 1 GB input, 32 bytes output	Speed @ 10 GB input, 32 bytes output
Blake3	0.00813	0.11541	1.47779
K12	0.00275	0.48192	4.59177
Shake	0.01096	3.5393	33.37358

Table 1: hashing of different input files to 32 bytes on system 1 (in seconds)

Hash function on system 1	Speed @ 10 MB input, 1 KB output	Speed @ 10 MB input, 100 MB output	Speed @ 10 MB input, 1 GB output
Blake3	0.00474	0.54758	5.67466
K12	0.00597	0.57576	6.18107
Shake	0.03583	2.53898	25.63152

Table 2: hashing of a 10 MB file to different output sizes on system 1 (in seconds)

Hash function on system 1	Speed @ 10 GB input, 1 GB output
Blake3	6.20759
K12	9.78375
Shake	58.78856

Table 3: hashing of large input and to large output on system 1 (in seconds)

The winner?

The speed test proofed that hash functions are in general fast enough to be used in a hash-based stream cipher. It is hard to nominate an winner. Blake3 was unbeatable when large files have to be hashed. In case of smaller inputs and larger outputs, in many cases, K12 is a better choice. For mobile applications, K12 has significant advantages, as it performed best at smaller inputs. For storage based encryption, Blake3 is a better choice. This coursework prefers Blake3 for implementation, as it provides a well-balanced speed in all situations.

Critical appraisal for executed speed tests

Please read the chapter “Conclusions”.

Why hash concatenation was not considered?

Why established hash functions (e.g. SHA-512) were not considered?

We will assume following: A file of 100 MB needs to be encrypted. Assuming that the processing is done with the raw bit stream, 156.250 SHA-512 operations are needed. If the key is a 10 MB file, 0.027s are needed for one SHA-512 operation on system 1 (i.e. x64 arch). To expand this to 100 MB size, approx. 70.31 minutes would be needed. Even if the performance can be improved slightly by some tweaks, this range is way beyond the required speed. Therefore the idea of SHA-512 chained outputs was not followed up. For the afore-mentioned task, Blake3 needed 0.54758 seconds instead of 70.31 minutes.

Security Review

KangarooTwelve has 12 rounds, which is seen as a sufficient safety margin [1]. However, some derivatives like “MarsupilamiFourteen” use 14 rounds to increase the complexity of the attack. The original Keccak algorithm uses 24 rounds, thus it is more secure, but also slower. For Keccak, a collision attack was possible only up to 6 rounds [2, 3]. Therefore the security margin is still sufficient.

Blake3 has 7 rounds, which is the major reason for the unbeatable speed. The predecessor Blake2b uses 12 rounds and Blake2s 10 rounds [4]. While the Blake hash family is seen as still secure, there are proofs that the complexity of Boomerang attacks was lowered to 2^{184} [5]. Blake3 targets 128-bit security against (second-) preimage, differentiability or collision attacks [6]. The reduction to 7 rounds is justified based on long term efforts in cryptanalysis for Blake (version 1) and Blake2 [6]. In conclusion, the authors are of the opinion that a hash function can also be secure with a lower number rounds and benefit from speed. To enhance the security, the Blake3 compression function was improved compared to the predecessor Blake2 (e.g. finalization returns 16 words instead of 8).

Cube attacks on Blake were researched and not followed-up any more due to expected failure [7]. For Blake2, theoretical attacks on the 2.5 rounds on a reduced version were possible [8]. During the competition for SHA-3, NIST assessed that Blake and Keccak “have very large security margins” [9]. However, this applies to the predecessor versions and it is not ensured that this assessment applies to Blake3 and KangarooTwelve as well. Relevant documented attacks for Blake3 were not found.

In conclusion, Blake3 was chosen for implementation. First of all, there were no relevant proofs of security weaknesses found for Blake3 and its predecessors; there was no indicator found that Blake3 is broken or insecure for the goal of this coursework. This coursework continues under the assumption that Blake3 is secure and the speed remains as the major selection criteria. Anyway, if any doubt on the security occur in future, it is easily possible to replace Blake3 by another hash function or to increase the iterations or the rounds. In conclusion, Blake3 is very fast especially for big files. The rust implementation of Blake3 supports multi-core CPUs, which can enhance more speed.

For all hash functions it is necessary that the input and output is selected long enough to ensure the security. For KangarooTwelve, it is recommended to choose the output at least at 128-bit to ensure 128-bit (second-) preimage security; for 128-bit collision security output should be at least 256-bits [2].

Concept of symmetric, hash-based encryption

As displayed in figure 2, Alice and Bob use a hash box (“h-Box”) to derive a key for the message. The h-Box takes anything as input, but at least one long-term secret (e.g. a picture or any other digital good), a true random salt to avoid dictionary or rainbow attacks and the time to avoid replay-attacks. More custom inputs are possible (i.e. X_i).

The hash result will be expanded to the length of the plain text. A XOR operation will take the plaintext P_i and the expanded hash result H_i as input. The hash function acts like a trapdoor function, where the creation of a hash H_i is easy, but the reverse function is impossible and finding a collision is a hard problem.

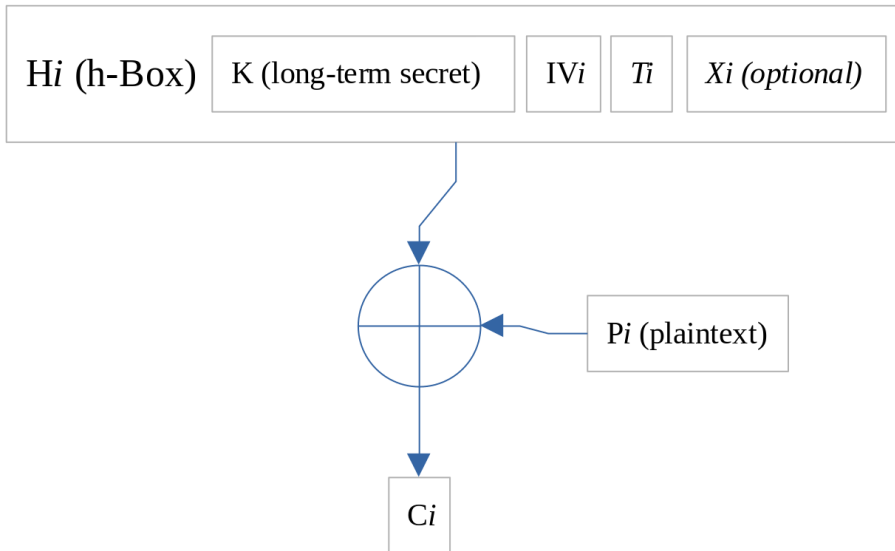


Figure 2: overview of the encryption and decryption process

For decryption, the process is the same as encryption, which is defined as:

$$\begin{aligned} C_i &= P_i \oplus H_i(K, IV_i, T_i, X_i) \\ P_i &= C_i \oplus H_i(K, IV_i, T_i, X_i) \\ \text{where } \text{len}(H_i) &= \text{len}(P_i) = \text{len}(C_i) \end{aligned}$$

Implementation of SHE proof of concept

This coursework aims a basic implementation in a proof of concept quality. An implementation was evaluated in different languages (e.g. C-, rust- or python-based) but withdrawn at an early stage because of disappointing speed achievements. It turned out that the most effective way is to use the Blake3 rust crate “b3sum”. For the proof of concept, the h-Box function was implemented only for a single long-term secret; the initialisation vector IV_i , the time T_i and X_i were not considered in the proof of concept. The shell script can be found in appendix f.

SHE.sh asks for the key file, the plaintext file and the desired output name. In a first step, the script derives a key out of the given key file. This steps includes also to find out the size of the plaintext file to stretch the key respectively. Finally, the script performs a file-based XOR encryption. The `xorfiles` tool was compiled from github.com/sciguy16/xorfiles.

```
./SHE.sh

Enter your key file: new21Scollectionhome.jpg
Enter your input file: plain_10MB.txt
Enter your output file: plain_10MB.txt.enc
===== STEP 1: derive key

real    0m0.026s
user    0m0.026s
sys     0m0.009s
===== STEP 2: XOR the two files together

real    0m0.113s
user    0m0.092s
sys     0m0.020s
===== STEP 3: en-/decryption finished. Cleaned up. See output.
```

If the file `plain_10MB.txt.enc` is decrypted, the decrypted file and the original file are equal according to sha256sum:

```
e5b844cc57f57094ea4585e235f36c78c1cd222262bb89d53c94dcb4d6b3e55d  plain_10MB.txt.dec
e5b844cc57f57094ea4585e235f36c78c1cd222262bb89d53c94dcb4d6b3e55d  plain_10MB.txt
```

In the afore-mentioned example, `new21Scollectionhome.jpg` is a picture of 500kb and the plaintext file `plain_10MB.txt` was created out of `/dev/null`.

Excerpt of the derived key, converted from RAW to HEX:

```
43dd24a6aeef6610dd77b09fad04da47333a9c5cde055291b342eac41df
e39c57d8c98688b7f78a362ebb06011ffb36b800071ff5837d4989e27664
3015f049b996838f1975c6ba8aeea63384d8107303061c41b1d060898b09
7e2c93b62669a8f337cacc9e1462525f8789f6d678843f4aa8063af65eec
0a36dca6b59ad5bdeff7361c728f36f39b5820f0c506dea499e2f3067c86
846d475eb59a23afcb793a931d5e307b8a2ef7b06b8234b9214439bda0e2
91969692c55dd69fc09253d73bec2dd0cc1e5a2874a6c3f73f6b30a6f9fb
530b1ec33640f0baea0db781b2d99f7bde4d8a9298048b0b3e8a4cde926c
9575dac135b868ebeb386f3cbe05d1dc56f59985ab510c21e076b5fc6bb
9818e97bebf9c9f16c0cae0f773051a1cc19c48b2b65157731f62c3a97801
118ce9349aabb270b27e8b4094f597e3c05d89019d37cf6a2a397786e02
e332a62dd3bc705d95ce120c4dff177b706236bc0bd723458387dfd2f9d2
f759d15038fe27a015f1ee03c30c1aec1f4658e6758d577e3d900a63d2bc
db49f18fe6d1aedf153c75140a36cb1e5fea5b87744b9a767c5a9b0002ee
acd2a7b3062060887074df634d4c01e335e45d939439da877561640f0251
.....
```

Evaluation

As shown in table 4, the time was reduced significantly when dumping the hash output in raw format instead of as HEX.

Output of 500.000.000 byte length	Speed in s
In RAW (500 MB)	0.467
As HEX (1 GB)	4.070

Table 4: speed – Dumping in hex vs. dumping in raw format.

In general, the speed results were well-promising. But, the selected XOR file operation took the most time as shown in table 5.

SHE encryption in s with 1 MB key	10 MB file	100 MB file	1 GB file
h-Box operation*	0.027	0.161	1.457
XOR Encryption (i.e. file based)	0.113	1.099	11.113
Total	0.14	1.26	12.57

* including XOF function and writing temporary file to disk

Table 5: sample encryption speed

The ultimate goal is to reach AES encryption speed levels. The AES encryption result for same files is visible in table 6. The SHE.sh script took up to 6.6 times longer than AES, which is mainly due to the inefficient XOR operation and writing data temporary to disk. Considering the “quick-and-dirty” proof of concept implementation and a relatively big key size of 1MB, this is a respectful result. It is very interesting what speed can be achieved after implementation of a state-of-the-art XOR-function. This task is a good follow-up work.

AES encryption in s	10 MB file	100 MB file	1 GB file
128-CBC	0.033	0.205	1.889

Table 6: AES encryption speed (i.e. 128-CBC mode)

Conclusions

Definition of follow-up work

The course work represents a practical experiment. Further work is necessary:

- Detailed analysis of the speed results, especially calculation of throughput (i.e. efficiency).
- State-of-the-art code implementation, especially implementation of a fast XOR function.
- After state-of-the-art code implementation, benchmark against AES.
- Research if hash-based encryption can be used in or to enhance public key cryptography.

Advantages of hash-based encryption

1. **New Use-Cases:** hash-based encryption enables many new use cases; the user can fill h-Box arbitrarily, which increases the attacking complexity as well. But, finally, the security is always restricted by the security of the hash function. Possible uses cases are e.g.:
 1. Encryption depending on where you are: The system environment (e.g. the kernel) can be included in the h-Box. In consequence, once encrypted, decryption requires to be inside the same pre-defined environment / machine.
 2. Encryption with things you own and things you know: The h-Box can be filled with everything you own (e.g. pictures, movies, hash of usb-sticks) as well as your individual secrets.
 3. Additional protection against reading attempts: Audit logs can be used to enforce control of encryption and decryption. For example, the audit log of a HSM can be part of the h-Box. The rotating audit log of YubiHSM 2 supports 62 entries. The first 60 entries could be put into the h-Box. In consequence, the audit log rotates and information needed for decryption gets lost in case of multiple unwanted reading attempts.
2. **Easy:** Hash based encryption is easy to implement and it is very flexible.
3. **Future proof:** Because of it's flexibility, hash based encryption can be used on long-term, with no need to adapt the implementation itself.
4. **Efficiency:** The h-Box input size can be increased without loosing efficiency significantly. For example: On System 1, hashing a 10 MB file to 1MB output took 0.0175 seconds, while hashing a 100 MB file to same length took only 0.01817 seconds.
5. **Interchangeable:** If the security of the hash function is broken, it can be replaced easily.

Critical appraisal for the coursework and speed tests

The coursework was started at an unexperienced status regarding hash speed and security. Therefore the strategy was to spend most of the time to evaluate the security and perform speed tests at large extent, without restriction of the test scope. Main goal was to learn more about the hash functions and to leave the door open for any result. It was very challenging to measure all constellations and isolate the influencing factors to reduce noise. It was necessary to adapt the test procedure several times, including manual re-tests. Finally a lot of data was collected, which potential was not utilized fully for the coursework because no more time left. Only few findings and statements were possible. The data has to be analyzed in detail afterwards (e.g. throughput).

At the beginning of the coursework, each hash operation was executed only one time. This approach had a high risk of noise. To reduce noise, it was necessary to execute each hash operation 10 times to calculate the average time. In consequence, approx. 2 days of time were lost.

Furthermore, after screening the results on system 3 (i.e. XEON with HDD), it was recognized that the first hash operation took always significantly longer time. The first operation hashed a given file to 32 bytes. The second operation hashed the same file again to 500 bytes, but took only a fraction of the previous one. For example, b3sum hashed a 10 GB file to 32 byte in 14.59 seconds. Directly after this, the same file was hashed to 500 bytes in 1.80 seconds; the second operation took 12.79 seconds less. This behavior was very strange at the first look. O'CONNOR from the Blake3-Team was asked to support the root cause analysis; see issue 172 on github.com/BLAKE3-team/BLAKE3. After several manual retests and going through an elimination process, the reason for that behavior is mainly identified in the reading and caching process of Hard Disk Drives (HDDs). All hash operations of a loop pointed to the same input file. The system continued than with cached data if the next operation points to the same file (-name). This large difference (i.e. 12.79 seconds in case of 10 GB input) was only observed when HDDs were in use. If SSDs were in use, the difference was in most of all cases in a range between 10-200 milliseconds. In consequence, all system 3 tests for 32 bytes output were repeated to ensure comparability and overcome the HDD caching and reading issue. Retrospectively, it would had been a better approach, to name all input files differently, although they are equal (e.g. as "key_10GB.file.A", "key_10GB.-file.B", etc.). By this, tests would include the reading speed of the disk as well. However, this was not necessary for the coursework. The coursework aimed to compare the hash functions under same conditions. This was reached successfully and noise level was reduced.

Finally, it was evaluated to write the output to `/dev/null` instead to disk. After manual retests it was identified that this is not relevant to solve the afore-mentioned problem and was therefore not implemented.

In conclusion, the speed results were useful and adequate for the scope of the coursework. However, in future work, more attention should be put on a clear definition of measurement goals and strategy to avoid unnecessary operations and noise *before* test execution. With a better testing goal definition several re-tests could have been avoided.

But, one is always wiser after the work.

Bibliography

- 1 J-P. Aumasson, “Too Much Crypto”, 2019. [Online]. Available: <https://eprint.iacr.org/2019/1492.pdf>
- 2 G. Bertoni, J. Aemen, M. Peeters, G. V. Assche, R. V. Keer and B. Viguier, “KangarooTwelve: fast hashing based on Keccak-p”, 2016. [Online]. Available: <https://eprint.iacr.org/2016/770.pdf>
- 3 J. Guo, G. Liao, G. Liu, M. Liu, K. Qiao, L. Song, “Practical Collision Attacks against Round-Reduced SHA-3*”, 2019. [Online]. Available: <https://eprint.iacr.org/2019/147.pdf>
- 4 M-J. Saarinen and J-P. Aumasson, “The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)”, November 2015. [Online]. Available: <https://tools.ietf.org/html/rfc7693>
- 5 Y. Hao, “The Boomerang Attacks on BLAKE and BLAKE2”, 2014. [Online]. Available: <https://eprint.iacr.org/2014/1012.pdf>
- 6 J. O’Connor, J-P Aumasson, S. Neves, Z. Wilcox-O’Hearn, “BLAKE3 one function, fast everywhere”. [Online]. Available: <https://github.com/BLAKE3-team/BLAKE3-specs/blob/master/blake3.pdf>
- 7 J. Lathrop, “Cube attacks on cryptographic hash functions”, 2009. [Online]. Available: <https://scholarworks.rit.edu/cgi/viewcontent.cgi?article=1653&context=theses>
- 8 “BLAKE2 – fast secure hashing”, <https://www.blake2.net>
- 9 S-j. Chang, R. Perlner, W. E. Burr, M. S. Turan, J. M. Kelsey, S. Paul, L. E. Bassham, “Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition”, 2012. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf>

List of Appendix

- a. Test system and platform configuration
- b. Complete speed results for Blake3
- c. Complete speed results for KangarooTwelve
- d. Complete speed results for Shake
- e. speedtest-blake3.sh: Sample shell script
- f. SHE.sh: encryption and decryption script as proof of concept

Appendix a) Test system and platform configuration

System 1 — x64 architecture - High-end Notebook — HP Zbook x360 G5

CPU	Intel Core i7-8750H; 6 cores @ Max. 4100 MHz
GPU	NVIDIA QUADRO P1000 mobile, GP107GLM
RAM	64 GB (2x32 GB) @ Configured Memory Speed: 2667 MT/s, SODIMM
OS	POP!_OS 20.10 (Ubuntu based)
Storage	1TB SSD

System 2 — ARMv8 architecture - Android Tablet Samsung Tab S5e LTE 64GB

CPU	Kryo 360; 8 cores @ 2x2000 MHz & 6x1700 MHz
GPU	Adreno 615
RAM	4 GB
OS	Android
Storage	64GB eMMC

System 3 — x64 architecture - XEON dedicated server

CPU	Intel Xeon E31230; 4 cores @ Max. 3200 MHz
GPU	none
RAM	4 GB
OS	Ubuntu 20.04
Storage	2TB HDD

Appendix b) Complete speed results for Blake3

General hint: each hash pair was repeated 10 times and the average time was calculated.

On system 1 - x64*

input \ output	1KB	1MB	2MB	3MB	4MB	5MB	6MB	7MB	8MB	9MB	10MB	20MB	30MB	40MB	50MB	60MB	70MB	80MB	90MB	100MB	200MB	300MB	400MB	500MB	600MB	700MB	800MB	900MB	1GB	2GB	3GB	4GB	5GB	6GB	7GB	8GB	9GB	10GB
std (32b)	0.00813	0.01303	0.01258	0.01141	0.01296	0.01141	0.01139	0.01193	0.01256	0.01168	0.01171	0.01434	0.02079	0.02144	0.01961	0.01944	0.02172	0.02744	0.02406	0.02831	0.03747	0.04621	0.06284	0.07567	0.08106	0.08933	0.10443	0.13688	0.11541	0.253	0.37762	0.55147	0.59982	0.73545	0.84696	0.9698	1.10497	1.47779
1kb	0.00621	0.00205	0.00181	0.00181	0.00184	0.00222	0.00205	0.00242	0.00262	0.00392	0.00474	0.0072	0.00738	0.00613	0.00657	0.00747	0.0099	0.00957	0.01119	0.01227	0.02003	0.031	0.03969	0.04419	0.05588	0.06062	0.06976	0.09603	0.09122	0.16844	0.26415	0.35215	0.41634	0.50284	0.57941	0.66684	0.75491	0.86516
10kb	0.00279	0.00217	0.00277	0.00214	0.00196	0.00226	0.00213	0.00928	0.00918	0.0094	0.00964	0.00512	0.00697	0.00574	0.00639	0.0099	0.01306	0.01083	0.02855	0.01161	0.02005	0.02828	0.03487	0.04683	0.04988	0.05975	0.06673	0.08099	0.08013	0.17246	0.25317	0.36665	0.41832	0.50552	0.56982	0.66204	0.75102	0.85619
100kb	0.00348	0.00292	0.01054	0.01061	0.00258	0.00322	0.00271	0.00875	0.00688	0.0112	0.01161	0.00868	0.00742	0.00591	0.00795	0.01201	0.01191	0.0116	0.03402	0.01211	0.02063	0.0292	0.03312	0.04371	0.05773	0.06408	0.06878	0.07581	0.08976	0.17136	0.25496	0.36443	0.40765	0.50585	0.58611	0.66494	0.74905	0.8488
1MB	0.01212	0.00974	0.01959	0.01189	0.00793	0.02186	0.0078	0.01547	0.01363	0.01494	0.01758	0.01166	0.0123	0.01153	0.01273	0.01407	0.01827	0.01755	0.02689	0.01817	0.02775	0.03605	0.04131	0.04654	0.05621	0.06633	0.08074	0.12375	0.09641	0.18345	0.26383	0.37721	0.42897	0.51093	0.59198	0.67545	0.75416	0.87444
2MB	0.0206	0.01749	0.01724	0.01546	0.0135	0.01795	0.01576	0.01633	0.01793	0.0176	0.01714	0.01858	0.02178	0.02197	0.02118	0.02204	0.02281	0.02321	0.02495	0.02835	0.03531	0.04994	0.04874	0.052	0.06197	0.07897	0.08571	0.0927	0.1051	0.1777	0.27488	0.3793	0.41901	0.50716	0.58862	0.66439	0.74932	0.94975
3MB	0.01939	0.0251	0.02296	0.02141	0.01873	0.01904	0.02052	0.02023	0.02162	0.01921	0.02011	0.0285	0.02577	0.02585	0.0263	0.02578	0.02855	0.02908	0.03115	0.0347	0.04124	0.04785	0.06143	0.06832	0.06768	0.08027	0.09687	0.09898	0.10747	0.19367	0.27097	0.36903	0.42892	0.51347	0.59385	0.69063	0.76213	0.99431
4MB	0.02539	0.03223	0.03417	0.02444	0.02446	0.02438	0.02456	0.02476	0.03155	0.02463	0.02858	0.03227	0.03171	0.03644	0.02915	0.03486	0.03736	0.04343	0.03919	0.04127	0.04485	0.05653	0.06257	0.07092	0.08494	0.09654	0.09596	0.11038	0.11124	0.20754	0.27682	0.38629	0.44612	0.52176	0.59849	0.69006	0.76525	0.9473
5MB	0.03153	0.04006	0.03839	0.03002	0.03083	0.03011	0.03022	0.03336	0.03573	0.03317	0.03118	0.04262	0.03604	0.03697	0.03917	0.04027	0.0423	0.03964	0.04241	0.04633	0.05194	0.06004	0.07056	0.07869	0.09016	0.10414	0.11017	0.13542	0.12474	0.19826	0.28697	0.37114	0.44325	0.52198	0.61483	0.69081	0.76901	0.96773
6MB	0.03716	0.04606	0.04584	0.03544	0.03535	0.03558	0.03564	0.03593	0.03789	0.0359	0.03588	0.04526	0.04113	0.04515	0.04502	0.04504	0.05148	0.04651	0.04704	0.04839	0.05413	0.06507	0.0663	0.08505	0.09403	0.09827	0.11018	0.11388	0.12914	0.20567	0.29477	0.40457	0.44849	0.52505	0.6162	0.69715	0.77594	0.9593
7MB	0.04345	0.05108	0.05604	0.04091	0.04093	0.04387	0.04122	0.04521	0.04672	0.04123	0.0414	0.05259	0.04986	0.04824	0.04517	0.04964	0.0549	0.05405	0.05167	0.05578	0.06059	0.06801	0.07633	0.08417	0.0922	0.10417	0.11428	0.11729	0.13156	0.21061	0.29123	0.4016	0.45153	0.53655	0.62627	0.70492	0.77727	1.00196
8MB	0.04879	0.066	0.06209	0.04654	0.04647	0.04649	0.04652	0.05004	0.05209	0.04656	0.04848	0.05578	0.04924	0.05098	0.05654	0.05595	0.05794	0.05368	0.05791	0.06003	0.06825	0.07565	0.08114	0.08927	0.09531	0.10537	0.11762	0.13777	0.13273	0.22747	0.3007	0.41644	0.46441	0.55233	0.62779	0.71252	0.78202	0.99397
9MB	0.05585	0.07901	0.0663	0.05215	0.05239	0.05242	0.05241	0.0539	0.0585	0.05249	0.05252	0.06218	0.05564	0.06091	0.05899	0.06149	0.06639	0.06893	0.06622	0.06595	0.07585	0.083	0.08677	0.09609	0.10414	0.11499	0.12213	0.15485	0.1369	0.223	0.30649	0.421	0.47187	0.60953	0.62783	0.71285	0.79163	1.04185
10MB	0.06074	0.08423	0.07293	0.05773	0.05741	0.05742	0.05742	0.0643	0.06283	0.05916	0.05834	0.07	0.06487	0.06391	0.06784	0.06751	0.06937	0.06745	0.07507	0.06891	0.08054	0.08512	0.09285	0.10099	0.10707	0.12212	0.13133	0.13546	0.14478	0.22822	0.32053	0.40718	0.46835	0.57336	0.63866	0.73358	0.81217	1.00794
20MB	0.11877	0.15277	0.11566	0.11113	0.11034	0.11061	0.11096	0.12052	0.11941	0.11138	0.11116	0.13361	0.1135	0.1162	0.12205	0.11765	0.11875	0.11767	0.12325	0.12506	0.12986	0.13951	0.14731	0.1522	0.16259	0.16891	0.17699	0.1859	0.19425	0.28228	0.36033	0.50559	0.52873	0.65709	0.69608	0.76511	0.84568	1.05828
30MB	0.1771	0.22776	0.17988	0.16481	0.16473	0.16441	0.16375	0.1666	0.17738	0.16447	0.16515	0.17647	0.17482	0.16862	0.16728	0.16967	0.17085	0.17057	0.17413	0.17487	0.18302	0.1915	0.19686	0.20616	0.2116	0.22389	0.28611	0.28	0.24888	0.33041	0.41474	0.49695	0.58941	0.72533	0.74944	0.827	0.9051	1.09798
40MB	0.23905	0.29893	0.26352	0.21933	0.21783	0.21852	0.21719	0.22234	0.2249	0.21721	0.21961	0.25726	0.22131	0.21985	0.21959	0.22089	0.22268	0.22493	0.22733	0.22703	0.23658	0.24149	0.25221	0.2605	0.27124	0.28295	0.29994	0.29613	0.3015	0.39481	0.46953	0.56388	0.63516	0.73974	0.80093	0.88518	0.96694	1.17318
50MB	0.28961	0.3623	0.30738	0.27245	0.27074	0.27152	0.27138	0.2706	0.30965	0.27222	0.27238	0.36502	0.27493	0.27389	0.27591	0.27528	0.27684	0.27547	0.28739	0.28001	0.29318	0.29805	0.30593	0.3137	0.32463	0.33597	0.41656	0.39482	0.37009	0.43775	0.51983	0.65919	0.68862	0.81428	0.86551	0.9554	1.05296	1.21275
60MB	0.34755	0.49954	0.39784	0.38286	0.33064	0.32767	0.33059	0.32621	0.39371	0.32783	0.32704	0.44376	0.33843	0.33715	0.32592	0.33097	0.3306	0.3322	0.38511	0.33386	0.34243	0.34739	0.35896	0.36818	0.38337	0.39517	0.45453	0.40848	0.42692	0.49129	0.59122	0.67534	0.76134	0.84577	0.93186	1.02365	1.13492	1.27289
70MB	0.40607	0.55551	0.45461	0.38127	0.37977	0.37974	0.37758	0.38027	0.47181	0.38643	0.38323	0.44062	0.388	0.38395	0.38232	0.38813	0.38774	0.38434	0.39365	0.39264	0.39986	0.40267	0.41195	0.422	0.43352	0.44197	0.48137	0.52144	0.47659	0.54406	0.6407	0.78909	0.826	0.93369	0.98625	1.08981	1.16015	1.34361
80MB	0.47111	0.62948	0.50742	0.44014	0.44495	0.43105	0.43983	0.43396	0.51922	0.43074	0.43512	0.53305	0.43748	0.43609	0.43302	0.43327	0.43942	0.43677	0.44802	0.44517	0.45271	0.45548	0.47007	0.48208	0.48645	0.50162	0.58125	0.55151	0.52829	0.59761	0.69513	0.81557	0.87932	0.98734	1.04481	1.14173	1.23865	1.36764
90MB	0.53401	0.66983	0.56805	0.49383	0.48628	0.48941	0.49185	0.49869	0.59181	0.49017	0.49342	0.69392	0.49612	0.48999	0.49254	0.49075	0.49382	0.49346	0.4986	0.49454	0.4979	0.51995	0.52256	0.52265	0.54471	0.55665	0.63644	0.58638	0.58842	0.664	0.74885	0.89168	0.92441	1.04125	1.08998	1.19776	1.2825	1.4345
100MB	0.5937	0.86658	0.63403	0.55005	0.55277	0.54907	0.54114	0.55007	0.75711	0.54726	0.54758	0.66286	0.56436	0.54701	0.54347	0.54528	0.55816	0.54195	0.55949	0.5544	0.56206	0.5679	0.57751	0.58241	0.59248	0.61261	0.71114	0.68251	0.64779	0.71135	0.79955	0.92629	0.98996	1.09748	1.14301	1.24791	1.34244	1.51188
200MB	1.38979	1.84632	1.27845	1.09812	1.08287	1.09597	1.07827	1.09253	1.39246	1.08145	1.10125	1.23249	1.10214	1.10478	1.08905	1.07383	1.10409	1.07686	1.12216	1.09154	1.08383	1.09252	1.11688	1.13199	1.13652	1.15614	1.35056	1.25619	1.18249	1.2615	1.35109	1.48663	1.51416	1.67021	1.69243	1.81303	1.92137	2.10943
300MB	1.90088	2.27407	1.90592	1.64252	1.73142	1.61975	1.62427	1.63428	1.83979	1.64529	1.6157	1.92468	1.64715	1.64413	1.61556	1.61071	1.643	1.61571	1.63439	1.62061	1.63512	1.62971	1.6349	1.65254	1.67805	1.67136	2.03397	1.83984	1.72524	1.79854	1.9062	2.10329	2.0929	2.25296	2.19842	2.27946	2.40016	2.63498
400MB	2.78705	2.93376	2.57268	2.20783	2.43264	2.17963	2.16534	2.1726	2.25827	2.18204	2.18884	2.48503	2.18964	2.																								

* on system 3 - XEON*																																						
output	input																																					
	1KB	1MB	2MB	3MB	4MB	5MB	6MB	7MB	8MB	9MB	10MB	20MB	30MB	40MB	50MB	60MB	70MB	80MB	90MB	100MB	200MB	300MB	400MB	500MB	600MB	700MB	800MB	900MB	1GB	2GB	3GB	4GB	5GB	6GB	7GB	8GB	9GB	10GB
std (32b)	0.00046	0.00053	0.00058	0.00059	0.00066	0.00068	0.02246	0.00068	0.00062	0.00085	0.00087	0.0009	0.0011	0.0012	0.00215	0.00162	0.00188	0.00241	0.00211	0.00249	0.00591	0.00624	0.00822	0.0101	0.01222	0.01469	0.01589	0.01871	0.01974	0.03914	0.05792	0.07661	0.09693	0.11531	0.13512	0.15931	0.1775	0.19711
1kb	0.00237	0.00184	0.00355	0.0032	0.00345	0.00357	0.00405	0.00414	0.00475	0.00454	0.00498	0.00661	0.00844	0.00997	0.01558	0.01357	0.01543	0.01705	0.01945	0.02213	0.03841	0.05623	0.07453	0.09188	0.10998	0.12776	0.14629	0.16508	0.18248	0.36245	0.5406	0.71906	0.90143	1.08205	1.25973	1.44126	1.61999	1.80659
10kb	0.00309	0.00219	0.00369	0.0039	0.00402	0.00416	0.00431	0.00445	0.00466	0.00435	0.00496	0.00659	0.00833	0.0101	0.01186	0.01373	0.01543	0.01735	0.01945	0.02144	0.03846	0.05625	0.07425	0.09192	0.11053	0.12826	0.14629	0.16522	0.18263	0.36228	0.54056	0.71861	0.90132	1.08031	1.25958	1.44115	1.62081	1.80284
100kb	0.00473	0.00379	0.00525	0.0051	0.00491	0.00545	0.00501	0.00532	0.00593	0.00619	0.00618	0.00754	0.00944	0.01102	0.01316	0.01453	0.01714	0.01814	0.02031	0.02246	0.03929	0.05697	0.07503	0.09261	0.11076	0.12869	0.14795	0.16693	0.18415	0.36288	0.54106	0.719	0.90243	1.08118	1.26787	1.44246	1.62019	1.80513
1MB	0.01645	0.01476	0.01623	0.01524	0.01545	0.0157	0.01664	0.01873	0.01676	0.01593	0.01598	0.01786	0.01918	0.02212	0.02287	0.02391	0.02559	0.02658	0.0286	0.03008	0.0483	0.0651	0.08305	0.10119	0.12017	0.13689	0.15701	0.17471	0.19097	0.37051	0.54837	0.72663	0.91024	1.0879	1.26712	1.44988	1.62882	1.81123
2MB	0.02466	0.02529	0.02507	0.02699	0.02527	0.02545	0.02663	0.03025	0.02633	0.02655	0.02599	0.02813	0.02897	0.03056	0.0322	0.03348	0.03551	0.03793	0.03788	0.0399	0.05823	0.07445	0.09251	0.11042	0.12806	0.14578	0.16418	0.18387	0.20053	0.37981	0.56049	0.73866	0.92255	1.10449	1.27792	1.46261	1.63951	1.82791
3MB	0.03323	0.03444	0.03628	0.03421	0.03418	0.0353	0.03832	0.03431	0.03469	0.03458	0.03964	0.04253	0.03861	0.04069	0.04096	0.04246	0.04394	0.04778	0.0474	0.05065	0.06759	0.08353	0.10294	0.12283	0.1387	0.15827	0.17364	0.19609	0.21176	0.38893	0.57135	0.75145	0.93162	1.10794	1.29218	1.48079	1.64731	1.82862
4MB	0.04282	0.0424	0.04216	0.04322	0.04316	0.04271	0.04428	0.04278	0.04396	0.04354	0.04382	0.04675	0.06089	0.05942	0.06249	0.06277	0.06568	0.06642	0.069	0.07411	0.08804	0.09937	0.11345	0.13419	0.15122	0.17407	0.18254	0.21499	0.22682	0.4	0.5908	0.75822	0.94159	1.12636	1.30383	1.48168	1.67149	1.84406
5MB	0.07434	0.07447	0.07518	0.07332	0.07414	0.07471	0.07502	0.07967	0.08254	0.08243	0.0832	0.08475	0.07164	0.075	0.07168	0.07456	0.07791	0.0785	0.08163	0.08352	0.09681	0.1116	0.13135	0.1492	0.17901	0.18731	0.19855	0.23718	0.24129	0.4185	0.60328	0.78798	0.96479	1.14263	1.31904	1.49647	1.68452	1.86055
6MB	0.08828	0.08691	0.08755	0.08535	0.08827	0.08765	0.09267	0.096	0.10128	0.10055	0.09928	0.11341	0.08986	0.09463	0.08715	0.08784	0.08858	0.08852	0.08917	0.09405	0.10768	0.12967	0.14771	0.16426	0.18224	0.19916	0.21124	0.25762	0.24851	0.4355	0.62077	0.81016	0.97588	1.16047	1.34313	1.51866	1.7031	1.86865
7MB	0.10083	0.10329	0.09877	0.09817	0.09845	0.10614	0.10944	0.1083	0.11072	0.11404	0.12006	0.12036	0.09163	0.09282	0.10438	0.1031	0.10488	0.10287	0.10328	0.10481	0.12284	0.14376	0.16308	0.18002	0.20674	0.21897	0.23568	0.27559	0.26509	0.4399	0.63642	0.81488	0.99508	1.17488	1.3553	1.53408	1.71075	1.89563
8MB	0.11068	0.10776	0.10362	0.10346	0.10173	0.10957	0.11784	0.11948	0.11953	0.12437	0.13355	0.13754	0.10315	0.10529	0.11156	0.10785	0.1108	0.11565	0.11583	0.12678	0.13938	0.15707	0.17478	0.19664	0.21685	0.24103	0.23545	0.2892	0.27776	0.45569	0.63993	0.82733	1.02152	1.18867	1.36288	1.55119	1.73195	1.909
9MB	0.1111	0.10868	0.12339	0.11375	0.11627	0.11003	0.1232	0.12551	0.12826	0.12952	0.13106	0.14701	0.11478	0.11819	0.11749	0.1241	0.12572	0.13103	0.13173	0.13351	0.15699	0.17027	0.19113	0.20708	0.23645	0.25346	0.26513	0.30919	0.29185	0.4691	0.65951	0.82709	1.02932	1.20361	1.37683	1.57655	1.75234	1.91394
10MB	0.11912	0.11669	0.12195	0.12169	0.12095	0.11684	0.13433	0.12913	0.14338	0.13894	0.14812	0.15447	0.12216	0.12751	0.13102	0.13592	0.13503	0.14353	0.14681	0.14481	0.16722	0.18485	0.20463	0.2247	0.24593	0.27483	0.27046	0.32798	0.29946	0.47761	0.67069	0.84926	1.04773	1.21788	1.38065	1.5665	1.7542	1.94056
20MB	0.24393	0.25155	0.2582	0.24954	0.25996	0.25445	0.26662	0.26837	0.2931	0.30154	0.30211	0.31514	0.26339	0.25926	0.26372	0.26402	0.26194	0.27893	0.27604	0.28253	0.3013	0.32934	0.3532	0.37731	0.41258	0.42303	0.45439	0.49281	0.42279	0.60561	0.81734	0.97231	1.17316	1.3485	1.52813	1.70922	1.88799	2.07496
30MB	0.38792	0.39347	0.40255	0.38835	0.39213	0.40839	0.40536	0.4126	0.44525	0.44076	0.44772	0.49537	0.37204	0.38971	0.38869	0.39238	0.40385	0.40445	0.40921	0.42224	0.45016	0.47081	0.48474	0.53269	0.55353	0.59911	0.61928	0.68224	0.54732	0.73503	0.91395	1.0865	1.305	1.45753	1.6589	1.84741	2.05188	2.2266
40MB	0.5079	0.51777	0.52883	0.53405	0.51693	0.54583	0.55458	0.56336	0.61587	0.62662	0.64341	0.68075	0.5036	0.51932	0.52464	0.52694	0.5247	0.53282	0.53534	0.54876	0.57678	0.6051	0.62964	0.67133	0.70124	0.75736	0.80127	0.85555	0.67606	0.89625	1.0542	1.23179	1.43118	1.60341	1.78694	1.9941	2.14704	2.37772
50MB	0.64795	0.65421	0.66922	0.67184	0.67503	0.7151	0.7176	0.72844	0.76222	0.79295	0.82415	0.85017	0.62196	0.63448	0.64409	0.63881	0.66405	0.67782	0.6908	0.69518	0.73501	0.75959	0.78161	0.82343	0.86874	0.925	0.98403	1.05379	0.79631	1.00172	1.19963	1.37345	1.58106	1.74375	1.94137	2.13892	2.31631	2.51623
60MB	0.77882	0.8075	0.81107	0.81174	0.82007	0.8084	0.87196	0.86803	0.91557	0.94286	0.96957	1.02797	0.73474	0.77565	0.77267	0.77379	0.78467	0.80487	0.81785	0.829	0.86277	0.90256	0.92562	0.98752	1.02393	1.08565	1.16796	1.23275	0.92876	1.13296	1.33449	1.49015	1.68846	1.88155	2.07925	2.26193	2.44476	2.6715
70MB	0.90992	0.93688	0.92981	0.94971	0.97242	0.97857	1.00132	1.03719	1.06552	1.1132	1.14184	1.22477	0.89636	0.91125	0.92269	0.90806	0.91741	0.92316	0.9525	0.94667	1.00761	1.04072	1.06312	1.12475	1.18964	1.27994	1.32082	1.44001	1.0764	1.2502	1.45523	1.64229	1.81511	2.02796	2.21815	2.40535	2.60592	2.80151
80MB	1.05761	1.06783	1.0506	1.11578	1.08754	1.0991	1.14897	1.1825	1.23673	1.26977	1.30816	1.39684	0.99315	1.02451	1.03857	1.03953	1.05409	1.079	1.0885	1.10419	1.15529	1.181	1.22772	1.31	1.34121	1.4311	1.52496	1.61594	1.18804	1.36134	1.56496	1.75323	1.95109	2.15974	2.35765	2.55201	2.74876	2.93933
90MB	1.16608	1.21951	1.2481	1.19645	1.24557	1.28566	1.32872	1.31201	1.42829	1.42518	1.52916	1.59891	1.12254	1.14512	1.18675	1.16857	1.19387	1.22822	1.242	1.27829	1.30359	1.33698	1.38351	1.45442	1.50239	1.59738	1.6971	1.80978	1.30195	1.52102	1.72847	1.87906	2.06349	2.28294	2.46856	2.67602	2.88285	3.09897
100MB	1.33152	1.36031	1.34746	1.38578	1.39778	1.41988	1.46674	1.51023	1.58653	1.58538	1.67851	1.77456	1.29041	1.27689	1.26998	1.30651	1.32683	1.35572	1.33984	1.37701	1.43242	1.50945	1.54268	1.6049	1.67257	1.74155	1.86691	1.98464	1.4406	1.66262	1.81343	2.03067	2.23143	2.43022	2.58623	2.80374	3.01699	3.24158
200MB	2.64846	2.65427	2.72765	2.76556	2.80377	2.81448	2.8938	2.95219	3.07792	3.14429	3.34087	3.53681	2.55529	2.57284	2.53972	2.59227	2.53873	2.68085	2.74081	2.76264	2.79575	2.9205	2.95578	3.11417	3.09907	3.39052	3.60925	3.79648	2.63968	2.85229	3.14859	3.33413	3.54685	3.65594	3.94068	4.18131	4.41533	4.66506
300MB	3.79809	4.02465	4.10814	4.12554	4.07844	4.2054	4.33037	4.44883	4.65322	4.75227	4.88085	5.39692	3.61217	3.78311	3.89102	3.90055	3.94576	3.94234	4.08887	4.12909	4.1434	4.18624	4.38667	4.58988	4.63863	4.99025	5.16203	5.41739	3.94858	4.10805	4.31466	4.59881	4.77789	5.07402	5.30595	5.52923	5.76826	6.10285
400MB	5.27921	5.33675	5.43407	5.52961	5.65431	5.68931	5.5054	5.95021	6.22751	6.32301	6.68611	7.13607	5.08583	5.15	5.22366	5.01173	5.27892	5.37387	5.24912	5.46067	5.66057	5.70255	5.69621	6.1266														

Appendix c - Complete speed results for KangarooTwelve

General hint: each hash pair was repeated 10 times and the average time was calculated.

On system 1 - x64*

input \ output	1KB	1MB	2MB	3MB	4MB	5MB	6MB	7MB	8MB	9MB	10MB	20MB	30MB	40MB	50MB	60MB	70MB	80MB	90MB	100MB	200MB	300MB	400MB	500MB	600MB	700MB	800MB	900MB	1GB	2GB	3GB	4GB	5GB	6GB	7GB	8GB	9GB	10GB
std (32b)	0.00275	0.01094	0.01161	0.01217	0.01278	0.01325	0.01344	0.01705	0.01586	0.01531	0.01584	0.02479	0.0289	0.05595	0.04521	0.04091	0.04743	0.05181	0.05577	0.06154	0.10928	0.15544	0.20332	0.25215	0.347	0.36462	0.38873	0.43442	0.48192	0.95387	1.42076	1.89617	2.38066	2.82973	3.30378	3.76273	4.29606	4.59177
1kb	0.00104	0.00147	0.002	0.00264	0.00287	0.00342	0.00397	0.00435	0.00486	0.00529	0.00597	0.01807	0.01552	0.03216	0.03536	0.0304	0.03647	0.04418	0.04414	0.04964	0.09587	0.13963	0.18771	0.23385	0.34324	0.32338	0.36853	0.41569	0.4585	0.90616	1.36361	1.82037	2.28249	2.72706	3.16716	3.61148	4.1595	4.59945
10kb	0.00095	0.00138	0.00189	0.00238	0.00283	0.00334	0.00385	0.00447	0.00487	0.0053	0.00595	0.0121	0.01561	0.02444	0.03269	0.03067	0.03826	0.04411	0.04404	0.05	0.0954	0.14074	0.18665	0.2372	0.29863	0.32735	0.37119	0.41402	0.45923	0.91481	1.36928	1.82593	2.27754	2.71461	3.16515	3.61119	4.16459	4.60576
100kb	0.00139	0.00191	0.00235	0.00288	0.00341	0.00388	0.00437	0.00475	0.00524	0.00574	0.00648	0.01147	0.01668	0.02159	0.03583	0.03129	0.03716	0.04046	0.04456	0.05007	0.09589	0.14079	0.1866	0.23785	0.28334	0.32659	0.36929	0.4148	0.46344	0.91722	1.37509	1.82528	2.27031	2.71541	3.19367	3.62776	4.1326	4.60849
1MB	0.00637	0.00694	0.00732	0.00776	0.0085	0.00877	0.00918	0.00964	0.0102	0.01066	0.01135	0.01655	0.02152	0.03277	0.03843	0.03619	0.04247	0.04566	0.04925	0.05498	0.10115	0.1462	0.19151	0.24378	0.28986	0.32713	0.37947	0.42025	0.46374	0.92091	1.37224	1.81309	2.29484	2.72306	3.2048	3.6317	4.16884	4.61519
2MB	0.01185	0.01244	0.0128	0.01335	0.01379	0.01433	0.01489	0.01547	0.01569	0.01598	0.01693	0.02195	0.02683	0.04897	0.04516	0.04145	0.05093	0.051	0.05521	0.06043	0.10736	0.151	0.19718	0.24702	0.29413	0.33565	0.38285	0.42483	0.47136	0.91954	1.37352	1.82349	2.29657	2.72962	3.17108	3.68372	4.12932	4.63499
3MB	0.01707	0.0178	0.01811	0.01856	0.019	0.0195	0.02029	0.02083	0.021	0.02166	0.02224	0.02813	0.03371	0.05522	0.05242	0.04699	0.06046	0.05651	0.05985	0.06557	0.11145	0.1569	0.20233	0.25354	0.30738	0.33873	0.38698	0.43138	0.47511	0.92701	1.37247	1.83433	2.29906	2.72365	3.17849	3.62018	4.13908	4.67336
4MB	0.02244	0.02327	0.02331	0.02431	0.0246	0.02521	0.02559	0.02617	0.02638	0.02669	0.02773	0.03797	0.0454	0.08356	0.05795	0.05219	0.06023	0.06207	0.06529	0.07065	0.11704	0.16201	0.20736	0.2541	0.32587	0.34805	0.39522	0.43644	0.4792	0.93679	1.37798	1.83084	2.3193	2.7492	3.19255	3.63223	4.15982	4.74411
5MB	0.0279	0.02894	0.02889	0.02964	0.03027	0.0307	0.03148	0.03159	0.03209	0.03221	0.03336	0.05334	0.05093	0.08449	0.06477	0.05739	0.08581	0.06736	0.07074	0.0767	0.12304	0.1673	0.21365	0.26058	0.31243	0.35617	0.39827	0.44048	0.48348	0.93612	1.39956	1.83914	2.31982	2.77274	3.1863	3.64547	4.15925	4.75106
6MB	0.03409	0.03401	0.03398	0.03524	0.03598	0.03622	0.03647	0.03696	0.03779	0.03738	0.03851	0.04939	0.04923	0.07904	0.07362	0.06244	0.07997	0.07311	0.07613	0.08196	0.1289	0.17312	0.21808	0.26627	0.31917	0.35877	0.40017	0.44715	0.48996	0.93926	1.40247	1.84243	2.30724	2.73187	3.18579	3.64173	4.16977	4.79644
7MB	0.03914	0.03963	0.03951	0.04053	0.04071	0.04138	0.04196	0.04222	0.04265	0.04276	0.04389	0.05005	0.05456	0.0719	0.08578	0.06864	0.08608	0.07804	0.08104	0.08696	0.13394	0.1783	0.22539	0.27131	0.32225	0.36635	0.41052	0.45105	0.49629	0.95009	1.39874	1.86331	2.29479	2.75387	3.25127	3.65256	4.20872	4.69421
8MB	0.04451	0.04508	0.0448	0.04641	0.04635	0.04681	0.04758	0.04759	0.04858	0.04849	0.04932	0.05978	0.06268	0.0823	0.12484	0.07472	0.08065	0.08279	0.08608	0.09236	0.13854	0.18325	0.22983	0.27711	0.32995	0.37454	0.41189	0.45561	0.50353	0.95748	1.42035	1.88686	2.30248	2.74432	3.29831	3.67822	4.19574	4.69214
9MB	0.05064	0.05099	0.05081	0.05274	0.05235	0.05284	0.0534	0.05389	0.05402	0.05397	0.05529	0.07101	0.0696	0.08453	0.11527	0.0799	0.08727	0.08863	0.09367	0.09779	0.14364	0.18843	0.23628	0.28504	0.33879	0.38376	0.42169	0.46543	0.50537	0.96784	1.40581	1.85942	2.30519	2.7536	3.25824	3.68823	4.21072	4.71985
10MB	0.05589	0.05596	0.05643	0.07945	0.05798	0.05801	0.05864	0.0586	0.05915	0.05902	0.06034	0.08744	0.0713	0.08597	0.11519	0.08489	0.09158	0.09375	0.09802	0.1028	0.15041	0.1938	0.24156	0.29111	0.34169	0.38474	0.42221	0.46889	0.51591	0.96915	1.41612	1.86683	2.32013	2.7663	3.25887	3.66856	4.22707	4.72917
20MB	0.10917	0.11031	0.10953	0.11103	0.11229	0.11146	0.11264	0.11285	0.1123	0.11185	0.116	0.16339	0.133	0.15751	0.17254	0.13793	0.15932	0.14693	0.15101	0.15574	0.20112	0.24521	0.29712	0.3473	0.39276	0.43866	0.47118	0.521	0.56775	1.01385	1.46756	1.90939	2.37788	2.82392	3.28315	3.73223	4.27181	4.72753
30MB	0.16268	0.16804	0.16091	0.17201	0.1651	0.16565	0.16602	0.16604	0.16582	0.16481	0.16878	0.20179	0.21641	0.27346	0.23296	0.19227	0.19596	0.20074	0.20412	0.20901	0.25535	0.2995	0.35324	0.40686	0.45076	0.48975	0.52679	0.5765	0.62042	1.07879	1.52902	1.9669	2.41868	2.89719	3.32076	3.77334	4.34382	4.77553
40MB	0.21591	0.21815	0.2142	0.23686	0.21783	0.21873	0.21917	0.22236	0.21958	0.21806	0.22483	0.27608	0.25373	0.29973	0.29697	0.24897	0.24859	0.25493	0.25603	0.26197	0.32307	0.35478	0.40686	0.48847	0.50746	0.53857	0.5809	0.62714	0.67399	1.13635	1.5787	2.0209	2.48049	2.94463	3.39934	3.81724	4.38383	4.83514
50MB	0.26714	0.26997	0.26803	0.29041	0.27469	0.27216	0.27408	0.27622	0.27277	0.27044	0.2796	0.4336	0.34547	0.35829	0.36914	0.30835	0.31434	0.32576	0.3093	0.31951	0.366	0.40961	0.45541	0.53188	0.55133	0.58816	0.63621	0.68024	0.72558	1.19113	1.6349	2.09441	2.52814	2.97466	3.42201	3.86157	4.43368	4.8968
60MB	0.32856	0.32661	0.32264	0.34959	0.33713	0.32601	0.32928	0.33251	0.32762	0.32697	0.33057	0.44437	0.37598	0.53548	0.36329	0.40734	0.36625	0.36976	0.36311	0.37145	0.41555	0.46175	0.51055	0.56307	0.61608	0.64779	0.68822	0.73386	0.77699	1.23002	1.69328	2.15047	2.57847	3.05574	3.48402	3.93874	4.46741	4.94662
70MB	0.39032	0.37784	0.37593	0.40949	0.40003	0.38787	0.38266	0.39334	0.38789	0.38072	0.38621	0.51086	0.41746	0.49591	0.50021	0.44184	0.42412	0.42657	0.42272	0.4276	0.47522	0.51672	0.56323	0.6112	0.67317	0.69105	0.74577	0.78515	0.82852	1.29988	1.73634	2.17888	2.6331	3.14881	3.56703	3.98671	4.47141	4.97232
80MB	0.46223	0.43507	0.43356	0.4573	0.46994	0.44335	0.4476	0.45	0.44158	0.43503	0.445	0.52059	0.49101	0.51664	0.55729	0.50165	0.47442	0.4996	0.47746	0.47804	0.52864	0.57115	0.6157	0.68402	0.73782	0.75018	0.80197	0.8412	0.88261	1.35491	1.78736	2.24575	2.69141	3.14314	3.61025	4.0428	4.59649	5.08424
90MB	0.50622	0.49196	0.49206	0.5066	0.49752	0.49775	0.4927	0.50417	0.50536	0.48896	0.49499	0.57213	0.5478	0.5424	0.54936	0.68379	0.52403	0.55036	0.5354	0.52886	0.58023	0.63963	0.67615	0.73052	0.77239	0.80106	0.85291	0.89688	0.93329	1.3902	1.85282	2.28418	2.74565	3.21767	3.65989	4.09288	4.65448	5.09843
100MB	0.54845	0.54941	0.5407	0.54613	0.56008	0.56562	0.56018	0.54913	0.55682	0.54632	0.57576	0.6083	0.60114	0.65131	0.59631	0.66259	0.57037	0.58903	0.58867	0.59139	0.63516	0.67894	0.72469	0.79859	0.82596	0.85555	0.90353	0.95539	0.98388	1.44766	1.89923	2.32234	2.79685	3.26374	3.71597	4.14055	4.71675	5.19547
200MB	1.09607	1.10698	1.07904	1.15569	1.09801	1.09951	1.11917	1.09966	1.11794	1.11019	1.12472	1.28007	1.14494	1.56544	1.23779	1.23574	1.14413	1.1219	1.11542	1.12929	1.19335	1.21387	1.29114	1.35045	1.40119	1.3885	1.43876	1.48846	1.53696	1.98855	2.39426	2.8768	3.35133	3.77088	4.20927	4.67561	5.16385	5.71954
300MB	1.64232	1.62407	1.61014	1.71581	1.6977	1.62681	1.66966	1.63064	1.64374	1.61723	1.65478	1.94412	1.93342	2.25882	1.89505	1.86194	1.68088	1.67219	1.69378	1.68003	1.73468	1.76876	1.83983	1.8422	1.95571	1.93948	1.98945	2.04291	2.05599	2.43795	2.92383	3.41681	3.86366	4.2986	4.75826	5.21026	5.67871	6.24885
400MB	2.21909	2.16445	2.15662	2.20642	2.16266	2.18525	2.19348	2.19271	2.20613	2.1704	2.19631	2.41404	2.27066	2.94813	2.30059	2.28746	2.38268	2.20089	2.17749	2.19593	2.22499	2.22206	2.															

	0.00175	0.00382	0.00557	0.00854	0.00861	0.01154	0.01192	0.01448	0.01585	0.017	0.01891	0.02987	0.04079	0.05144	0.06088	0.07533	0.08438	0.09605	0.10492	0.12276	0.2297	0.34148	0.45435	0.5717	0.6819	0.79684	0.90447	1.01665	1.12833	2.26068	3.39485	4.52479	5.6423	6.7846	7.89613	9.03392	10.17991	11.27339
1kb	0.0048	0.00477	0.00564	0.00746	0.00845	0.01221	0.01364	0.01281	0.016	0.01793	0.02012	0.03056	0.041	0.05244	0.06208	0.07528	0.08436	0.09592	0.10609	0.1192	0.23077	0.34275	0.45802	0.56894	0.68185	0.79274	0.90462	1.01632	1.12942	2.25819	3.39701	4.51083	5.63894	6.76793	7.89237	9.03144	10.18018	11.28143
100kb	0.00273	0.0043	0.00638	0.00864	0.00922	0.01194	0.01247	0.01581	0.01539	0.01841	0.01899	0.03071	0.04097	0.05344	0.06297	0.07554	0.0855	0.09699	0.10824	0.12094	0.23026	0.34321	0.45577	0.57157	0.68225	0.79274	0.90946	1.01947	1.13437	2.2609	3.39359	4.50518	5.64281	6.76779	7.8918	9.04262	10.16203	11.29133
1MB	0.01511	0.01674	0.01856	0.02035	0.01924	0.02069	0.02421	0.02268	0.02532	0.02774	0.02674	0.03783	0.04994	0.05991	0.07155	0.08313	0.09348	0.10408	0.11524	0.12685	0.23945	0.35089	0.46373	0.57562	0.69103	0.80482	0.91583	1.0267	1.13799	2.26623	3.40487	4.51589	5.64938	6.81162	7.89728	9.03836	10.17496	11.29515
2MB	0.02586	0.02596	0.02808	0.02861	0.02963	0.03122	0.03269	0.03418	0.03591	0.03549	0.03701	0.04789	0.05916	0.0696	0.0805	0.09231	0.10254	0.11359	0.12505	0.13976	0.24687	0.3588	0.47422	0.58486	0.69964	0.81371	0.92489	1.03761	1.1462	2.27656	3.40927	4.53588	5.66884	6.80788	7.90498	9.0512	10.17928	11.30178
3MB	0.03391	0.03693	0.04146	0.03514	0.04131	0.0413	0.04415	0.04068	0.04291	0.04543	0.04771	0.05886	0.06759	0.08296	0.09397	0.10829	0.1211	0.12883	0.13965	0.15533	0.26902	0.37541	0.48866	0.59523	0.70982	0.83351	0.95111	1.06309	1.17027	2.28838	3.44192	4.541	5.67867	6.79558	7.94719	9.05564	10.21067	11.30279
4MB	0.04376	0.04419	0.04513	0.04699	0.06058	0.05052	0.05092	0.05325	0.05216	0.05466	0.055	0.06707	0.07848	0.09707	0.1137	0.12312	0.13624	0.1462	0.16066	0.17821	0.28697	0.38958	0.50348	0.60592	0.7189	0.84968	0.95923	1.07356	1.1937	2.29784	3.46852	4.55435	5.70416	6.81121	7.95777	9.08571	10.23357	11.33196
5MB	0.07862	0.08481	0.08704	0.08917	0.09773	0.08	0.07956	0.08145	0.08806	0.07827	0.08713	0.08948	0.09712	0.11276	0.12575	0.1388	0.14961	0.16577	0.17714	0.19548	0.31158	0.40349	0.51311	0.64509	0.73764	0.87094	0.97959	1.08661	1.20278	2.36098	3.47813	4.57889	5.71971	6.84741	7.9764	9.10663	10.24991	11.35027
6MB	0.09679	0.09859	0.09978	0.10504	0.11071	0.08956	0.08825	0.09306	0.09236	0.09365	0.08966	0.0936	0.09879	0.1302	0.1411	0.15588	0.16725	0.18195	0.20564	0.21288	0.33033	0.41708	0.52922	0.65745	0.75544	0.88835	1.00085	1.10328	1.22055	2.37101	3.49643	4.61652	5.73162	6.86087	8.00467	9.12019	10.26343	11.38946
7MB	0.10814	0.10907	0.11818	0.11016	0.12967	0.10012	0.09452	0.10132	0.09953	0.10272	0.10299	0.09801	0.11296	0.14369	0.15807	0.16964	0.19713	0.19674	0.21356	0.23609	0.35532	0.42756	0.5427	0.67165	0.77925	0.89791	1.0139	1.11502	1.24146	2.37843	3.51083	4.62424	5.74953	6.91535	8.0296	9.15958	10.28509	11.39528
8MB	0.11391	0.12264	0.12212	0.12869	0.1503	0.11033	0.10774	0.10937	0.11022	0.11077	0.11049	0.11346	0.1266	0.16048	0.17515	0.18955	0.22926	0.21696	0.2309	0.25378	0.37002	0.44514	0.55817	0.69291	0.79326	0.91203	1.03037	1.14135	1.25099	2.40094	3.53364	4.63151	5.76547	6.91587	8.01946	9.19755	10.33741	11.3946
9MB	0.12361	0.13333	0.13749	0.13878	0.14389	0.11617	0.1118	0.1146	0.11282	0.11622	0.11356	0.13055	0.1449	0.17446	0.19086	0.201	0.24035	0.22758	0.24783	0.27091	0.39051	0.45468	0.56897	0.7035	0.80711	0.92751	1.05039	1.15276	1.26389	2.41144	3.53544	4.64322	5.7784	6.93198	8.05886	9.19534	10.32726	11.40796
10MB	0.15432	0.14604	0.14543	0.16078	0.16944	0.12741	0.1329	0.12794	0.12231	0.12806	0.1333	0.1435	0.15291	0.19181	0.20173	0.215	0.2916	0.24673	0.26416	0.28837	0.40875	0.46981	0.58211	0.7079	0.82947	0.9452	1.05764	1.18259	1.29331	2.42654	3.56645	4.67431	5.79515	6.95857	8.05689	9.19343	10.34201	11.42318
20MB	0.28586	0.29934	0.31043	0.32872	0.3486	0.25945	0.26434	0.28428	0.27485	0.28074	0.27697	0.30647	0.31956	0.33388	0.35261	0.3734	0.50271	0.42074	0.44319	0.47422	0.60676	0.61349	0.75239	0.85555	0.97671	1.08229	1.2019	1.3139	1.43743	2.54799	3.69838	4.81664	5.95456	7.08873	8.23855	9.3759	10.52609	11.57274
30MB	0.44265	0.4664	0.5	0.52343	0.5548	0.40949	0.3938	0.4144	0.41057	0.41523	0.42197	0.44269	0.44422	0.48035	0.5117	0.52048	0.60406	0.58078	0.6158	0.64858	0.8058	0.74547	0.86841	0.97676	1.08513	1.22076	1.33999	1.45212	1.57667	2.68687	3.84623	4.96997	6.11862	7.26907	8.38921	9.53652	10.69627	11.72459
40MB	0.61412	0.64369	0.67387	0.7173	0.75046	0.55175	0.53516	0.54989	0.55252	0.57451	0.58664	0.60281	0.5991	0.62833	0.66522	0.68184	0.72444	0.72602	0.78299	0.85148	1.01383	0.89299	0.99939	1.12078	1.23507	1.35889	1.48604	1.58835	1.71564	2.85438	3.98715	5.11369	6.27522	7.41743	8.55368	9.7081	10.89897	11.89591
50MB	0.77281	0.81869	0.85323	0.94592	0.9499	0.67909	0.68719	0.70229	0.6993	0.7176	0.72886	0.71323	0.76649	0.77253	0.80564	0.82382	0.86615	0.90489	0.97795	1.02907	1.23136	1.02843	1.15566	1.25446	1.37101	1.47297	1.64528	1.72072	1.84421	2.99824	4.14337	5.27251	6.43673	7.57006	8.71757	9.87916	11.06967	12.01151
60MB	0.94055	1.01169	1.04721	1.10078	1.13378	0.82705	0.82324	0.81749	0.82598	0.83693	0.86767	0.89144	0.90419	0.91491	0.96256	0.9897	1.04739	1.08395	1.14901	1.21075	1.42782	1.14859	1.26627	1.38899	1.52654	1.63732	1.76924	1.88418	2.00853	3.15617	4.30743	5.41117	6.59205	7.74716	8.89618	10.0507	11.26231	12.17425
70MB	1.10281	1.17741	1.1918	1.25291	1.33367	0.96749	0.94914	0.96607	0.98245	1.00531	1.02758	1.03443	1.04965	1.08292	1.12247	1.18569	1.2322	1.24812	1.34276	1.38658	1.61886	1.28494	1.40505	1.54458	1.67337	1.8125	1.93104	2.00621	2.14632	3.28662	4.46835	5.59631	6.75522	7.85204	9.07666	10.259	11.45072	12.33597
80MB	1.26464	1.33153	1.3885	1.47525	1.53242	1.09129	1.0931	1.12344	1.12271	1.14217	1.1631	1.16818	1.17623	1.25608	1.29146	1.32129	1.37985	1.43995	1.49475	1.57586	1.66521	1.42362	1.52011	1.68437	1.78221	1.94066	2.04728	2.17196	2.29505	3.44343	4.60496	5.75139	6.92128	8.0846	9.21836	10.42518	11.64475	12.47701
90MB	1.42919	1.51442	1.57785	1.66496	1.74346	1.24711	1.23963	1.25788	1.26833	1.25714	1.28909	1.3393	1.35822	1.39952	1.43361	1.46057	1.54407	1.58708	1.61727	1.77363	1.45085	1.54714	1.68914	1.81638	1.94166	2.06962	2.20671	2.31831	2.41574	3.59096	4.74485	5.91917	7.04388	8.22643	9.41318	10.54849	11.80652	12.6367
100MB	1.62444	1.65003	1.74396	1.82996	1.89717	1.37824	1.3796	1.36114	1.38433	1.41483	1.4655	1.47769	1.45726	1.50596	1.52831	1.5761	1.7073	1.75738	1.89779	2.00302	1.54749	1.72452	1.79787	1.92076	2.07226	2.19973	2.31576	2.46541	2.51879	3.73975	4.87297	6.00438	7.21054	8.38633	9.57426	10.59579	11.95249	12.78333
200MB	3.19654	3.2946	3.49275	3.67377	3.95931	2.69385	2.66897	2.72657	2.76803	2.79303	2.87666	2.9365	2.95131	2.92977	3.0884	3.16972	3.22026	3.40247	3.52727	3.67854	2.8935	2.96794	3.15039	3.21378	3.45566	3.61179	3.75868	3.91816	4.03208	5.23132	6.37427	7.54004	8.73196	9.85337	11.00346	12.42652	13.7568	14.23393
300MB	4.82173	4.84813	5.25005	5.44473	5.84584	3.95405	3.88387	4.1258	4.09529	4.19261	4.2872	4.39272	4.34385	4.3491	4.60951	4.5616	4.80137	5.01081	5.33673	5.64405	4.11628	4.37397	4.37736	4.66356	4.62832	5.01892	5.1099	5.31956	5.34443	6.53299	7.88509	9.09016	10.278	11.45272	12.93567	14.22013	15.66496	15.82151
400MB	6.44973	6.65742	6.81682	7.18801	6.28286	5.44032	5.41991	5.36536	5.34273	5.45203	5.51108	5.68001	5.72911	6.07477	5.98134	6.13852	6.61772	6.39763	7.20188	7.06923	5.5662	5.62594	5.74634	6.02401	5.96747	6.43083	6.62048	6.79041	6.76809	8.22433	9.41403	10.70255	11.58656	13.27762	14.63644	16.01322	17.62193	17.04613
500MB	8.08826	8.28146	8.69608	9.22383	6.47586	6.8288	6.77949	6.66931	6.71119	6.94504	6.99265	7.09225	7.20436	7.19281	7.18809	7.71479	8.23007	8.31636	8.7939	9.33995	6.80184	6.94579	6.93663	7.24888	7.58527	7.74858	7.31747	8.22686	8.55096	9.51785	10.96547	11.70323	13.50977	14.79029	16.25695	18.07552	19.14896	18.57794
600MB	8.90059	8.96565	10.44335	10.91939	7.96896	8.11306	8.15485	8.07962	8.1873	7.98554	8.60013	8.54231	8.86066	8.80403	8.43845																							

Appendix d) Complete speed results for Shake

General hint: each hash pair was repeated 10 times and the average time was calculated.

On System 1 - x64*

input \ output	1KB	1MB	2MB	3MB	4MB	5MB	6MB	7MB	8MB	9MB	10MB	20MB	30MB	40MB	50MB	60MB	70MB	80MB	90MB	100MB	200MB	300MB	400MB	500MB	600MB	700MB	800MB	900MB	1GB	2GB	3GB	4GB	5GB	6GB	7GB	8GB	9GB	10GB
std (32b)	0.01096	0.01508	0.01715	0.02166	0.02493	0.02807	0.03183	0.03543	0.03866	0.04229	0.04724	0.08074	0.11657	0.15398	0.18594	0.21885	0.25448	0.29236	0.33495	0.37384	0.72322	1.06942	1.44833	1.78949	2.16598	2.59965	2.92154	3.1553	3.5393	6.98853	10.53037	13.95613	17.34732	20.98099	24.56752	28.25945	31.78718	33.37358
1kb	0.00096	0.00446	0.00778	0.01119	0.01464	0.01839	0.02148	0.02482	0.02823	0.03152	0.03583	0.0682	0.10233	0.13813	0.16971	0.20157	0.23819	0.26848	0.31209	0.34937	0.686	1.00839	1.37358	1.67679	2.06061	2.68249	2.78677	2.97842	3.30973	6.3065	9.93918	13.20076	16.50519	19.86196	23.30453	26.50947	31.81704	33.25745
10kb	0.00112	0.0046	0.00791	0.0113	0.01521	0.01818	0.02167	0.02499	0.02865	0.0319	0.03595	0.06912	0.10335	0.13961	0.16865	0.20495	0.2382	0.26927	0.30759	0.35153	0.68262	1.00499	1.33588	1.66526	2.06079	2.95317	2.90656	2.97611	3.30335	6.60401	9.90116	13.18766	16.51921	20.02554	23.47698	26.57443	31.8852	33.34657
100kb	0.00335	0.00681	0.01024	0.01356	0.01702	0.02034	0.02391	0.02736	0.03086	0.03443	0.0382	0.07384	0.10535	0.14128	0.17123	0.20697	0.23817	0.27123	0.31084	0.3479	0.68335	1.01533	1.34111	1.68228	2.0515	2.80409	2.70769	2.97375	3.3156	6.61763	9.89776	13.23631	16.57887	20.28925	23.42602	26.65553	32.00359	33.34913
1MB	0.02649	0.02939	0.0328	0.03657	0.03949	0.04284	0.04663	0.0503	0.05385	0.05618	0.06023	0.09403	0.12749	0.16551	0.19573	0.22728	0.26039	0.29294	0.33635	0.37018	0.70318	1.04459	1.35742	1.69857	2.05651	2.99161	2.75447	2.99426	3.32579	6.6244	9.98875	13.2292	16.4999	20.12739	24.0165	27.08658	30.42282	33.44964
2MB	0.05126	0.05409	0.05744	0.06057	0.06496	0.06786	0.07247	0.07577	0.07834	0.0814	0.08491	0.11801	0.15371	0.19207	0.21791	0.25164	0.2859	0.32114	0.35889	0.39632	0.74134	1.0664	1.38764	1.71192	2.08474	2.53449	2.7316	3.02099	3.36878	6.66728	9.96539	13.27531	16.56341	19.99327	24.08931	27.09007	30.80182	33.34004
3MB	0.07619	0.07973	0.08161	0.08625	0.08911	0.09247	0.09527	0.10028	0.10547	0.10561	0.11362	0.14348	0.17847	0.21062	0.23752	0.27191	0.3122	0.35018	0.38047	0.42063	0.76754	1.10633	1.41151	1.73902	2.13746	2.75285	2.73106	3.0558	3.39044	6.67938	10.06479	13.27805	16.61272	20.01189	23.32323	26.9715	30.70368	33.23898
4MB	0.10588	0.10376	0.10635	0.11685	0.1158	0.11937	0.1239	0.12716	0.12983	0.13277	0.13707	0.16961	0.20155	0.23799	0.27105	0.29954	0.33554	0.37205	0.4087	0.45818	0.79393	1.13347	1.43622	1.77298	2.09947	3.12703	2.80176	3.07391	3.4114	6.76328	10.02856	13.3796	16.77018	19.91929	23.36005	26.96484	31.34574	33.46603
5MB	0.13017	0.12805	0.13098	0.13479	0.13946	0.14237	0.1507	0.15189	0.15812	0.1547	0.16049	0.19579	0.22761	0.25841	0.29562	0.32362	0.36342	0.39927	0.43987	0.48497	0.82051	1.13121	1.46432	1.7886	2.14204	3.21537	2.81508	3.10868	3.43655	6.74789	10.11207	13.38024	16.63627	20.00729	23.2662	26.71677	31.97089	33.48448
6MB	0.15945	0.15306	0.15546	0.16247	0.16358	0.16625	0.17663	0.17826	0.17965	0.18772	0.19243	0.22281	0.2508	0.29122	0.31559	0.35052	0.39026	0.41986	0.45238	0.51228	0.84747	1.15612	1.49495	1.87472	2.17382	3.18472	2.79387	3.13189	3.47219	6.75956	10.06912	13.4614	16.77055	20.25719	23.27007	26.95718	31.31901	33.52154
7MB	0.18434	0.18474	0.17967	0.18643	0.19051	0.19712	0.20386	0.20315	0.20323	0.20931	0.21844	0.25047	0.28653	0.3254	0.3435	0.38329	0.41534	0.44394	0.48411	0.54443	0.86386	1.17658	1.51392	1.83779	2.16926	3.22658	2.82074	3.15705	3.50311	6.77976	10.08873	13.4043	16.70436	20.0974	23.35356	26.99003	32.24516	33.6436
8MB	0.21077	0.20796	0.20421	0.20964	0.22532	0.21669	0.23504	0.22961	0.22842	0.22911	0.24104	0.27279	0.30927	0.33351	0.37332	0.40609	0.44179	0.47869	0.51764	0.56199	0.87282	1.20385	1.5744	1.86922	2.19175	2.99945	2.86603	3.18085	3.50445	6.81312	10.08952	13.42592	16.76128	20.21773	23.51189	27.11565	32.0303	33.50402
9MB	0.23693	0.23111	0.23191	0.24111	0.24752	0.24687	0.25457	0.25575	0.25075	0.25689	0.25872	0.29579	0.3261	0.37101	0.39087	0.43408	0.4648	0.49962	0.54096	0.57725	0.90349	1.25698	1.56254	1.89019	2.21996	3.11385	2.88105	3.19945	3.56513	6.84269	10.12269	13.44378	16.71412	20.16229	23.36285	27.53505	33.98256	33.49983
10MB	0.26216	0.25518	0.26433	0.26859	0.27184	0.27299	0.28393	0.27873	0.28525	0.28108	0.28867	0.32072	0.34841	0.39079	0.4256	0.45916	0.49307	0.53462	0.56676	0.59976	0.93075	1.25821	1.60251	1.93367	2.26067	2.93132	2.90668	3.22446	3.55145	6.90032	10.25943	13.47224	16.83753	20.29815	23.50238	27.8644	34.64115	33.45755
20MB	0.51264	0.49949	0.49537	0.52148	0.53317	0.51057	0.5353	0.53853	0.53332	0.53172	0.52749	0.56617	0.59872	0.63278	0.67551	0.69945	0.74903	0.77947	0.81383	0.84228	1.19261	1.50191	1.91024	2.22061	2.62145	3.19127	3.17192	3.4796	3.81121	7.10804	10.53294	13.73388	17.04551	20.47711	23.66388	26.97053	37.15154	33.62762
30MB	0.74835	0.7575	0.7469	0.7812	0.79417	0.75942	0.78508	0.78452	0.79837	0.79625	0.82625	0.80802	0.84307	0.94657	0.95839	0.9543	0.98447	1.02646	1.06343	1.09121	1.46052	1.79983	2.25446	2.41616	2.77626	3.92197	3.39007	3.5564	4.05403	7.38602	10.68278	13.99686	17.25504	20.6361	27.17969	35.03238	34.07465	
40MB	0.99674	1.02727	1.02878	1.02982	1.05894	1.02876	1.02598	1.00793	1.03367	1.06072	1.03175	1.05254	1.09661	1.16709	1.20829	1.20705	1.24256	1.27757	1.33662	1.35029	1.73788	2.03587	2.38261	2.67201	3.0562	4.19688	3.65896	4.00223	4.37326	7.62265	10.97437	14.29647	17.46679	20.97892	24.18776	27.43176	35.41145	34.19593
50MB	1.25323	1.24829	1.26576	1.3047	1.30492	1.25463	1.28737	1.25282	1.28903	1.29246	1.31541	1.30302	1.41773	1.37868	1.47331	1.43183	1.49068	1.54388	1.57483	1.62698	1.97463	2.29102	2.62197	2.91106	3.31589	4.55991	3.89997	4.24589	4.57873	7.84578	11.23941	14.50031	17.78915	21.37188	24.64458	27.80098	36.3629	34.41771
60MB	1.52895	1.50216	1.49383	1.56172	1.57754	1.5074	1.50968	1.54853	1.55923	1.52588	1.54464	1.57905	1.67169	1.66317	1.74689	1.7118	1.7609	1.82103	1.86492	1.86739	2.2009	2.53571	2.88405	3.17334	3.56091	5.05854	4.14425	4.48183	4.80866	8.07656	11.53019	14.81543	17.9831	21.4476	24.74764	27.99986	35.83159	34.64847
70MB	1.76496	1.74864	1.74967	1.80723	1.79311	1.74996	1.78425	1.80913	1.79556	1.74945	1.81386	1.84752	1.87566	2.02648	1.98412	1.92996	2.00147	2.07783	2.06031	2.08953	2.48498	2.77091	3.18586	3.40964	3.9282	4.50259	4.38637	4.771	5.03992	8.33422	11.76634	15.49955	18.44455	21.53081	24.88874	28.38384	35.06974	34.89444
80MB	2.0175	2.03559	1.99391	2.05784	2.02823	1.99535	2.02444	2.04113	2.04047	2.09492	2.04047	2.11557	2.13627	2.34824	2.17872	2.20452	2.28111	2.3381	2.33941	2.35495	2.71943	2.97505	3.39015	3.67297	4.1961	4.42364	4.63578	5.00064	5.33746	8.57833	11.90026	15.25467	18.51333	21.79514	26.42965	28.54496	31.72284	35.31928
90MB	2.29935	2.30008	2.24953	2.27653	2.28296	2.26004	2.3644	2.33851	2.33265	2.31986	2.30884	2.36925	2.45259	2.41746	2.43428	2.51712	2.45067	2.60905	2.58893	2.64281	2.971	3.28019	3.6421	3.94625	4.64082	4.87281	4.88126	5.17981	5.55044	8.86823	12.2568	15.49821	18.83535	22.01879	26.26357	28.76826	32.06599	35.45791
100MB	2.54161	2.48687	2.53338	2.51195	2.55859	2.50347	2.56473	2.55214	2.5517	2.59572	2.53898	2.67647	2.68759	2.7004	2.6615	2.78042	2.71667	2.8795	2.82881	2.91399	3.2347	3.5218	3.92572	4.4002	5.00045	5.78804	5.16381	5.44697	5.80737	9.08287	12.36593	15.47917	18.95513	22.29949	26.02622	29.25001	32.67259	35.76721
200MB	4.96579	5.02167	5.03612	5.02606	5.17655	5.06924	5.10958	5.16952	5.04129	5.19286	5.06767	5.19063	5.1226	5.15239	5.20578	5.24137	5.29107	5.4838	5.35726	5.62075	5.68989	6.06845	6.48976	6.78454	7.58975	10.2681	7.63511	7.9378	8.38868	11.58544	14.97422	18.2958	21.57063	24.67332	28.52188	31.56731	34.92079	38.0881
300MB	7.60431	7.50835	7.57985	7.59896	7.62172	7.60347	7.58514	7.70006	7.65348	7.73825	7.51747	7.70138	7.64587	7.69506	8.05209	7.74867	7.76349	7.94109	7.90019	8.00715	8.1775	8.53137	8.84324	9.16805	11.43766	11.776	10.17361	10.48345	10.85909	14.06284	17.34814	20.59041	24.02498	27.21707	31.02054	34.45989	37.60	

input		output																																				
output	1KB	1MB	2MB	3MB	4MB	5MB	6MB	7MB	8MB	9MB	10MB	20MB	30MB	40MB	50MB	60MB	70MB	80MB	90MB	100MB	200MB	300MB	400MB	500MB	600MB	700MB	800MB	900MB	1GB	2GB	3GB	4GB	5GB	6GB	7GB	8GB	9GB	10GB
std (32b)	0.0167	0.02366	0.02966	0.03417	0.0336	0.04528	0.04897	0.05148	0.05875	0.06682	0.0675	0.11698	0.1609	0.2092	0.25984	0.30544	0.35401	0.40427	0.45002	0.5084	0.98217	1.46117	1.94775	2.42783	2.92112	3.39775	3.88186	4.44818	4.84364	9.68641	15.07164	19.3428	25.13938	29.28891	35.03782	40.80949	45.32501	49.87626
1kb	0.00414	0.00962	0.01589	0.02279	0.021	0.031	0.03555	0.041	0.04424	0.04817	0.05479	0.09814	0.14373	0.19074	0.23779	0.28253	0.33167	0.37567	0.42424	0.4798	0.93759	1.39955	1.86177	2.33397	2.7956	3.25028	3.71657	4.19539	4.64546	9.33777	13.92755	18.55734	23.37747	27.84688	32.85771	37.12928	41.79694	46.41248
10kb	0.00145	0.01044	0.01651	0.02176	0.02207	0.02951	0.03456	0.03965	0.04458	0.04832	0.05459	0.10056	0.14444	0.1913	0.23695	0.28269	0.3313	0.37599	0.42218	0.48214	0.93259	1.39664	1.85977	2.32268	2.78925	3.28608	3.75842	4.19696	4.64592	9.28172	13.93024	18.55476	23.21077	27.83382	32.50061	37.16456	41.84123	46.4204
100kb	0.00482	0.01501	0.01988	0.02438	0.03139	0.03473	0.03657	0.04143	0.04825	0.05112	0.05746	0.10234	0.14648	0.19402	0.24247	0.28679	0.33387	0.38149	0.43023	0.48328	0.94222	1.40014	1.88899	2.32659	2.80659	3.25327	3.71874	4.18424	4.64832	9.28462	13.99924	18.58347	23.34604	27.84122	32.609	37.2638	42.22196	46.41287
1MB	0.03779	0.051	0.05232	0.05536	0.06573	0.06541	0.06981	0.07467	0.07954	0.08338	0.0887	0.13438	0.18312	0.22696	0.27187	0.31998	0.36559	0.41332	0.45949	0.51937	0.96822	1.43464	1.89637	2.35809	2.82699	3.28498	3.75514	4.21607	4.68045	9.31096	13.95421	18.7151	23.24704	27.92148	32.53286	37.14362	41.80017	47.23488
2MB	0.0768	0.08332	0.08955	0.09153	0.1041	0.10209	0.1079	0.11154	0.11431	0.11793	0.12342	0.18113	0.21848	0.26678	0.31399	0.3537	0.40488	0.44848	0.49542	0.56711	1.01575	1.47207	1.9433	2.42924	2.8645	3.33591	3.81316	4.25361	4.72061	9.35224	13.99802	18.6314	23.51669	28.1113	32.93241	37.5531	41.83744	46.47985
3MB	0.11939	0.12022	0.12372	0.1312	0.13056	0.13928	0.1389	0.14355	0.14944	0.15317	0.16695	0.21476	0.26542	0.30701	0.35238	0.40604	0.4453	0.48939	0.5414	0.6023	1.07256	1.52267	1.98126	2.45722	2.91202	3.41386	3.84613	4.37906	4.7794	9.40747	14.10166	18.68082	23.3344	28.01243	32.98406	37.22895	41.89279	46.53296
4MB	0.1681	0.15546	0.1589	0.16607	0.17232	0.18156	0.17801	0.18729	0.19045	0.19287	0.19721	0.26544	0.31374	0.34393	0.39401	0.44315	0.48574	0.53276	0.58755	0.65627	1.09618	1.57079	2.05521	2.49758	2.96826	3.48497	3.9277	4.368	4.82467	9.45142	14.09785	18.84106	23.38169	28.22864	32.66047	37.29411	42.30382	46.57021
5MB	0.21305	0.2078	0.20549	0.21093	0.21249	0.2215	0.22217	0.22841	0.256	0.23699	0.24337	0.28419	0.33649	0.38659	0.43624	0.47561	0.5253	0.58483	0.63176	0.7058	1.1477	1.60806	2.10289	2.56581	2.99896	3.48691	3.93492	4.39097	4.86677	9.50746	14.13804	18.76033	23.57543	28.10129	32.70887	37.33939	42.3744	46.60639
6MB	0.25716	0.24028	0.24708	0.27376	0.25185	0.26064	0.26796	0.26465	0.27745	0.2804	0.28221	0.32269	0.39668	0.43259	0.48675	0.53096	0.57961	0.61442	0.68249	0.74608	1.20733	1.63988	2.10886	2.58632	3.05121	3.54381	3.9982	4.49339	4.94438	9.65372	14.18634	18.80331	23.55121	28.1053	32.75212	37.38965	41.99714	46.65458
7MB	0.29924	0.2812	0.30125	0.3043	0.30378	0.31626	0.31819	0.3124	0.31849	0.32434	0.32376	0.37651	0.43932	0.4704	0.52381	0.56703	0.62598	0.64672	0.72196	0.79621	1.20554	1.67762	2.15951	2.63812	3.08208	3.56631	4.04638	4.49879	5.05823	9.64508	14.24641	19.18742	23.49593	28.53373	32.77872	37.42052	42.27619	46.72164
8MB	0.33385	0.32592	0.34082	0.34552	0.35041	0.33932	0.34419	0.36555	0.36067	0.37303	0.392	0.40085	0.47701	0.48968	0.58621	0.62358	0.66996	0.70805	0.75794	0.82004	1.25806	1.73782	2.20142	2.71026	3.12742	3.60955	4.07498	4.53221	5.0588	9.61841	14.28352	19.08498	24.00991	28.57015	32.82531	37.82827	42.23387	47.06857
9MB	0.86475	0.38183	0.41236	0.40692	0.42854	0.38471	0.39126	0.40223	0.41976	0.42334	0.41487	0.48864	0.53045	0.53099	0.61657	0.66273	0.69924	0.74106	0.78599	0.88117	1.30499	1.78917	2.27305	2.7046	3.17777	3.65874	4.09192	4.5967	5.07577	9.73308	14.41533	18.93862	23.58816	28.23545	32.87749	37.53305	42.39627	46.75801
10MB	0.41762	0.41658	0.43296	0.43933	0.44501	0.47255	0.43325	0.45437	0.44556	0.49099	0.49807	0.5293	0.56606	0.60556	0.65913	0.71903	0.7459	0.80523	0.84075	0.91879	1.36899	1.81234	2.29435	2.76644	3.24859	3.6952	4.15183	4.63599	5.11374	9.73019	14.37828	18.96512	23.82945	28.28093	32.91112	37.6209	42.15093	46.88329
20MB	0.8915	0.89628	0.88805	0.96096	0.94911	0.84764	0.86689	0.88183	0.90521	0.90203	0.92416	0.98562	1.06088	1.01381	1.06011	1.12183	1.14402	1.22549	1.23571	1.30352	1.78045	2.26401	2.72373	3.23896	3.65399	4.1068	4.57974	5.10024	5.53466	10.20983	14.84031	19.46869	24.04613	28.78258	33.39788	38.25753	42.60435	47.45575
30MB	1.80026	1.34386	1.3904	1.41124	1.40926	1.26646	1.24191	1.278	1.33742	1.37084	1.36348	1.43481	1.54198	1.37429	1.46401	1.53901	1.52694	1.63594	1.69422	1.74118	2.1956	2.67254	3.19587	3.64139	4.06032	4.53626	5.007	5.46671	6.02126	10.66996	15.31474	19.82019	24.46889	29.12459	33.88804	38.94909	43.08309	47.72431
40MB	2.19852	1.77412	1.76	1.84315	1.94154	1.68429	1.68493	1.7352	1.7597	1.75342	1.80287	1.8689	1.99239	1.8154	1.87726	1.87952	1.97089	1.97807	2.13467	2.12526	2.6044	3.0783	3.52017	4.02872	4.4481	4.97369	5.47145	5.90852	6.38896	11.09009	15.7591	20.27862	24.8587	29.62685	34.24895	38.95455	43.56384	48.19124
50MB	2.47752	2.15054	2.1989	2.33856	2.30626	2.04334	2.03698	2.20285	2.17947	2.20556	2.22092	2.32577	2.48306	2.20979	2.31928	2.33723	2.33798	2.50369	2.43857	2.58511	3.01244	3.53052	3.9927	4.41708	4.88433	5.38998	5.85948	6.34418	6.87043	11.48652	16.23677	20.57659	25.27048	30.00794	35.16909	39.27012	44.01052	48.96684
60MB	3.4375	2.56142	2.65783	2.67937	2.80432	2.50989	2.55847	2.51216	2.5984	2.59014	2.71173	2.85983	2.87175	2.59997	2.65837	2.74961	2.71709	2.85236	2.8804	2.9416	3.48253	3.98832	4.35377	4.86072	5.31257	5.78238	6.36973	6.87082	7.2991	11.92616	16.67315	20.93988	26.09818	30.43261	35.06825	39.9809	44.34729	49.25419
70MB	3.91381	3.06989	3.14834	3.13218	3.25251	2.94841	2.89649	3.0553	3.10411	3.1045	3.07202	3.34529	3.39023	2.9451	3.07786	3.16387	3.21004	3.17344	3.27032	3.40918	3.7787	4.4633	4.85645	5.27923	5.74722	6.38777	6.67421	7.30014	7.79734	12.43278	17.20356	21.47765	26.18563	30.82608	35.47537	40.35267	45.12276	49.71797
80MB	3.91228	3.6059	3.59887	3.6193	3.75295	3.25749	3.26878	3.41178	3.45577	3.55364	3.66651	3.60479	3.81813	3.46071	3.41302	3.52654	3.5444	3.64456	3.737	3.90013	4.26336	4.80664	5.11147	5.71959	6.13397	6.75194	7.21276	7.56412	8.29632	12.91831	17.77077	21.79608	26.63195	31.40295	35.99236	40.55253	45.83084	50.02397
90MB	5.0747	3.91372	4.00143	4.07193	4.13235	3.67468	3.81751	3.77893	3.91755	3.98313	3.92268	4.12315	4.168	3.81009	3.85064	3.91211	4.09259	4.05579	4.11432	4.19245	4.69088	5.09846	5.69171	6.09634	6.65726	7.14123	7.61674	8.06254	8.57919	13.45684	18.13129	22.42304	27.1034	31.62071	36.35612	40.93871	45.73606	50.41121
100MB	5.46352	4.45108	4.434	4.47539	4.63611	4.16664	4.03832	4.32041	4.48234	4.42905	4.49859	4.55243	4.72014	4.19827	4.45634	4.39368	4.36911	4.45627	4.54183	4.5844	5.13513	5.42981	5.93703	6.61715	7.13597	7.52451	8.08145	8.43078	9.2267	13.78192	18.48301	22.65029	27.62376	32.12786	36.94145	41.45209	46.13128	50.97256
200MB	9.32734	8.6426	8.71042	8.9126	9.45911	8.47695	8.04639	8.58261	8.83725	8.75721	8.91946	9.50327	9.2202	8.19629	8.24893	8.23389	8.39249	8.57797	8.90114	9.03393	9.23019	9.79423	10.10875	10.81068	11.47801	11.72854	12.31452	12.70866	13.46623	18.56625	23.02831	26.65671	31.77027	36.20359	41.33502	46.27461	50.41702	55.42115
300MB	13.73353	13.22489	13.40084	13.90026	14.24366	12.24125	12.3182	12.73867	12.67742	13.44689	13.13483	13.42356	14.4114	12.41163	12.425	12.44302	12.28614	12.72577	12.82691	13.1326	13.30872	13.95026	14.34922	14.7493	15.21692	16.07477	16.99544	16.93418	17.75492	22.96825	27.79988	31.2006	35.65579	41.02884	45.87418	50.0276	55.45449	60.01122
400MB	18.14982																																					

Appendix e) speedtest-blake3.sh: Sample shell script

```
#!/bin/bash

declare -a input=("key_1kb.file" "key_1MB.file" "key_2MB.file" "key_3MB.file" "key_4MB.file" "key_5MB.file"
"key_6MB.file" "key_7MB.file" "key_8MB.file" "key_9MB.file" "key_10MB.file" "key_20MB.file" "key_30MB.file"
"key_40MB.file" "key_50MB.file" "key_60MB.file" "key_70MB.file" "key_80MB.file" "key_90MB.file"
"key_100MB.file" "key_200MB.file" "key_300MB.file" "key_400MB.file" "key_500MB.file" "key_600MB.file"
"key_700MB.file" "key_800MB.file" "key_900MB.file" "key_1GB.file" "key_2GB.file" "key_3GB.file" "key_4GB.file"
"key_5GB.file" "key_6GB.file" "key_7GB.file" "key_8GB.file" "key_9GB.file" "key_10GB.file" )

declare -a output=("32" "500" "5000" "50000" "500000" "1000000" "1500000" "2000000" "2500000" "3000000"
"3500000" "4000000" "4500000" "5000000" "10000000" "15000000" "20000000" "25000000" "30000000" "35000000"
"40000000" "45000000" "50000000" "100000000" "150000000" "200000000" "250000000" "300000000" "350000000"
"400000000" "450000000" "500000000")

for i in "${input[@]}"
do
key_file=$i
#echo File $key_file

        for o in "${output[@]}"
        do
                output_size=$o

                counter=1
                start_time="$(date -u +%s.%N)"
                #echo STARTTIME $start_time

                while [ $counter -lt 11 ];
                do

                        b3sum $key_file -l $output_size > speedtest.txt
                        #ls -lh speedtest.txt
                        #rm speedtest.txt
                        #echo "$(date -u +%s.%N)"
                        counter=$((counter+1))

                done

                end_time="$(date -u +%s.%N)"
                elapsed="$(bc <<<"$end_time-$start_time")"
                average="$(bc -l <<<"$elapsed/10")"
                #echo ENDTIME $end_time
                #echo ELAPSED $elapsed

                echo -e Input $key_file "\t\t" Output "$(ls -s
speedtest.txt --block-size=K)" "\t\t" "AVERAGE"\t\t ""\t\t
t " $average

        done

        echo ""
        echo ""

done
```

Appendix f) SHE.sh: encryption and decryption script as proof of concept

```
read -p "Enter your key file: " key
read -p "Enter your input file: " plaintext
read -p "Enter your output file: " output

# find out the size of the plaintext file in bytes
plain_size=$(stat --format="%s" $plaintext)

# h-BOX: derive the key as long as the plaintext file
echo "===== STEP 1: derive key"
time b3sum $key -l $plain_size --raw --no-names > derivedkey.txt
derived_key_size=$(stat --format="%s" derivedkey.txt)

echo "===== STEP 2: XOR the two files together"
time ./xorfiles derivedkey.txt $plaintext > $output
rm derivedkey.txt
echo "===== STEP 3: en-/decryption finished. Cleaned up. See output."
```