Detailed Response to Reviewers

Md. Refazul Islam Refat, Md. Mosaddek Khan*, Euna Islam, Md. Mamum-or-Rashid

---

Thanks a lot for pointing out some deficient parts of the paper that needs further revision.

1. Fundamental

Cache misses are handle by a complete transfer of cache line or block and typically size of cache line is 64 Bytes. Therefore, a whole 64 Bytes block of data will be transferred even in the need of 4 Bytes of data. To be more specific, there is no way of inspecting exactly which Bytes were needed in the last CPU cycle due to memory protection. So if Block size equals to 64 Bytes, a cache miss will transfer 16 entries from the lookup table since each entry is of 32 bits. But RAT table entries were much smaller in size (just 1 Byte) and each miss will transfer as much as 64 entries from it. So knowledge of displacement from RAT table will not help much as any of those 64 entries can be the right one, and furthermore, knowledge of displacement from lookup table will not help at all since it is completely randomized.

In this revision, we've managed to fit the whole RAT into an 8 Byte data structure at the expense of slight performance degradation. In future development section, we mentioned if it is possible make an instruction for the inverse mapping operation, this compromise of performance can be alleviated to a great extent.

2. Abridgement

Pages 2-6 served to visualize preliminary ideas but in this revision we tried to concise them as much as possible.

3. Performance Analysis

Performance analysis was presented in a rather abstract way (in terms of number of lookup operations, conditional XOR operations, required memory etc.) because execution of a particular operation varies greatly among different types of processors and we didn't intend to cover them in our last submission. In this revision, we presented a real time encryption timing analysis.

4. AES-NI

Intel AES-NI seems to abstract one round of operation of AES in one single instruction, but those might not be suitable for RISC processors. Our proposal is targeted for general class of processors.

5. Integrity of AES

The outcome is exactly the same. The way of accessing memory is modified, not the core algorithm. The integrity of AES is maintained and the results will definitely match the published test vectors.

Email addresses: refazul.refat@gmail.com (Md. Refazul Islam Refat), mosaddek@cse.univdhaka.edu (Md. Mosaddek Khan*), euna.islam@gmail.com (Euna Islam), mamun@cse.univdhaka.edu (Md. Mamum-or-Rashid)