AMD tag overhead in a MPC outsourcing environment

Christian Bobach, 20104256

December 13, 2016

Abstract

Contents

1 Intorduction

In this paper I will be investigating the overhed of introducing the proposal for how to outsource computation in a muliparty computation environment from the paper [JNO16].

2 Experiment

3 Conclution

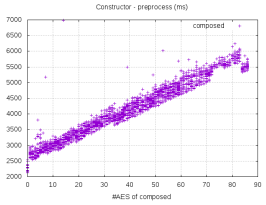
4 Continiued work

References

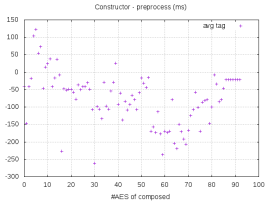
[JNO16] Thomas P. Jakobsen, Jesper Buus Nielsen, and Claudio Orlandi. A framework for outsourcing of secure computation. Cryptology ePrint Archive, Report 2016/037, 2016. `http://eprint.iacr.org/2016/037`.

A Data

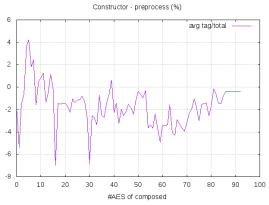
A.1 Preprocess



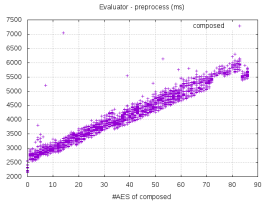
(a)



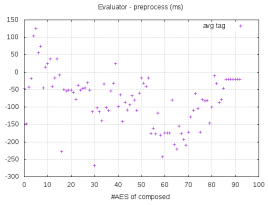
(b)



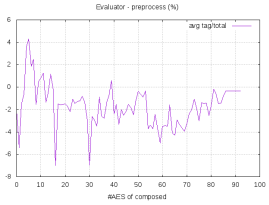
(c)



(d)

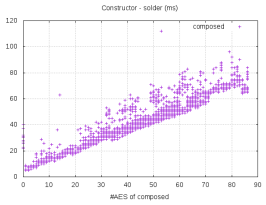


(e)

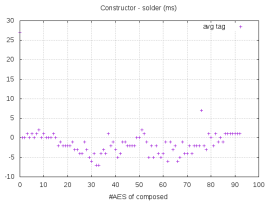


(f)

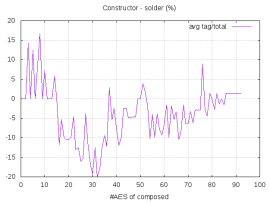
A.2 Solder



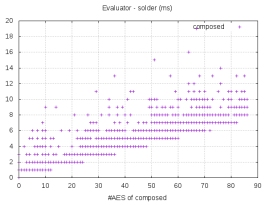
(a)



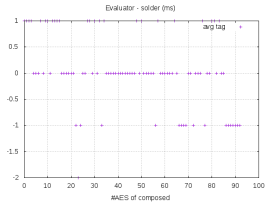
(b)



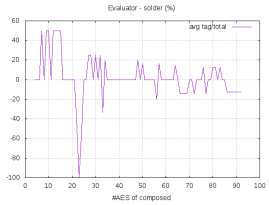
(c)



(d)

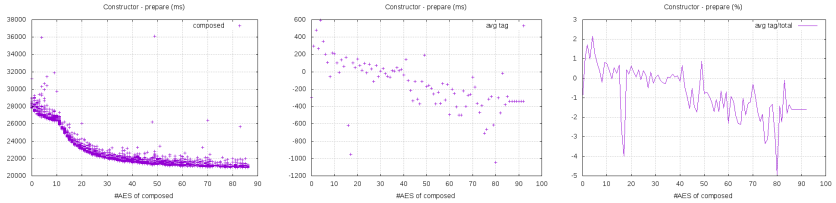


(e)

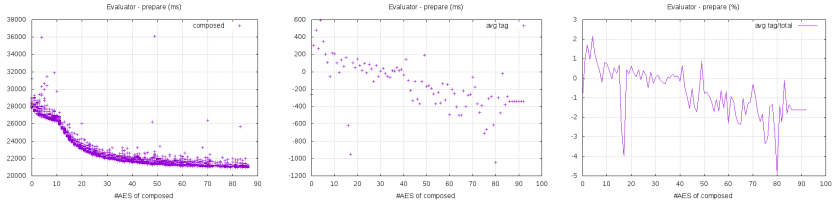


(f)

A.3 Prepare

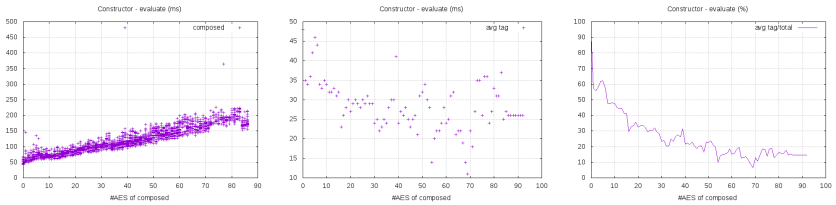


(a) (b) (c)

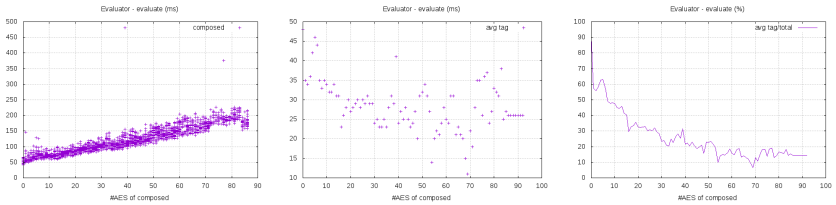


(d) (e) (f)

A.4 Evaluate

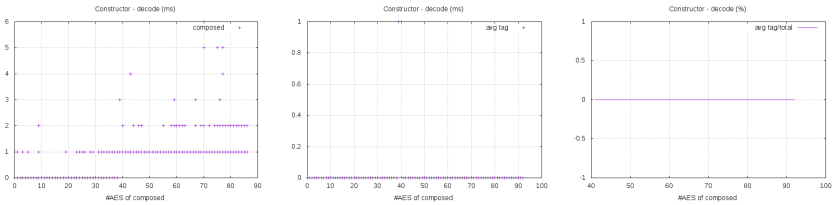


(a) (b) (c)

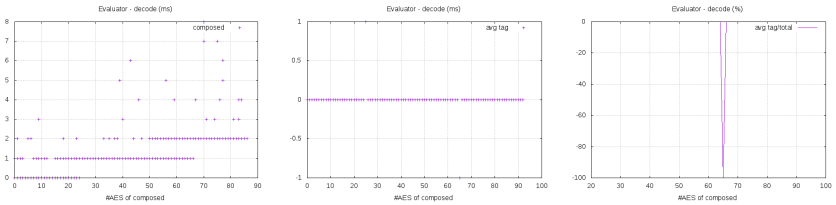


(d) (e) (f)

A.5 Decode


Constructor - decode (ms)
composed
#AES of composed
Constructor - decode (ms)
avg tag
#AES of composed
Constructor - decode (%)
avg tag/total
#AES of composed

(a) (b) (c)


Evaluator - decode (ms)
composed
#AES of composed
Evaluator - decode (ms)
avg tag
#AES of composed
Evaluator - decode (%)
avg tag/total
#AES of composed

(d) (e) (f)