# Review of ISF proposal 1316/18

March 10, 2018

Secure multi party computation is a fascinating cryptographic protocol allowing a set of parties evaluate a (public) function $f$ on their private inptus, without revieling extra information about their inputs. This should hold even if some of the parties are corrupted, and they collude and attempt to learn extra information from what they have seen (a semi-honest setting). Worse still, the parties may attempt to deviate from the protocol by sending messages to each other (a malicious setting).

Broad feasibility results, stating essentially that all functions can be evaluated securely without any assumptions if a minority of the parties is corrupted, and under reasonable cpryotgraphic assumptions for any adversary (corrupting any number of parties) have been put forward already in the late 80's and early 90's.

However, these results have remained in the realm of theory until some 10 years ago due to relatively high overhead relatively to inseure evaluation of functions, so users have failed to take advantage of the great power of MPC for applications such as performing surveys on private mdeical data agregated from several hospitals (and many more). Unfortuntely, solutions relying on some form of trsuted parties (or just avoiding computation in a setting where inputs should remain private altogether) are typically used instead.

Over the last 10 years or so, a rich body of work has focused on the goal of improving the concrete efficiency of MPC protocols, with the hope of eventually making MPC appealing for practical applications. There is a large gap between MPC in the semi-honest setting and MPC in the malicious setting. While not a realistic assumption, protocols in this setting have been useful as a stepping stone to designing maliciously secure protocols, via ceratin compiling techniques.

The current paper's goal is to narrow the communication and round complexity overhead (both very important measures of complexity) between the malicious setting and the semi-honest setting for 3 or more parties. This is a large and much needed piece of the puzzle of making MPC practically efficient, in light of recent success of achieving the best possible overhead of a multiplicative constant.

This way, efforts to improve complexity can be focused on the easier to tackle semi-honest setting (both for 2 and more parties). Also, an approach of designing a general compiler is preferred over approaches building efficient ad hoc protocols for specific functionalities is preffered since it will allow "regular" programmers, rather then expert cryptographers to design and implement protocols for new tasks as they arise.

In this research proposal, the PI approaches the problem by (further) exploring the seminal technique of *MPC in the head* as a complier from semi-honest to malicious setting. This is a quite innovative approach, as this technique, while broadly used to design MPC protocols, is not broadly considered to be practically efficient. I expect the outputs of this work would independently contribute to the development of this very useful (also in more theoretical work) technique which is of great independent interest.

The proposal is very detailed, and it seems very plausible that the roadmap sketched here will allow to make progress. Furthermore, the concrete goal of achiving constant overhead relatively to semi honest protocols in the multi party setting is the best possible. It is somewhat hard for me to evaluate whether this high bar is likely to be reached by this work, as I am not familiar with all the relevant literature. However, as it appears, the PI has a very detailed plan of how to achieve this goal.

The PI has coauthored several strong preliminary results in this direction, which will serve as a basis for this work, which raises my confidence in the success of the proposed reserach.

She has an impressive body of work on MPC in general, focusing on topics of concretely secure MPC (based on general compilers, in particular MPC in the head, and ad hoc protocols), a seminal

work on fair computation and more. Thus, I think she is highly suitable to perform this research.

I have only a few concrete techniqcal questions to the author, to clarify some points (these are most likely points that I do not understand, rather than real issues in the proposed research).

1. You say the state of the art asymptotic CC overhead over semi-honest protocols in $O(s/log(|C|))$, and you hope to achieve a linear overhead. How likely is it to acheive this ambitious goal? Furthermore, you say that sublinear overhead in $|C|$ could possibly be achieved. This is better then generic semi-honest constructions, as far as I know. Could you please elaborate on this point?

2. You say that one part of your approach is to improve the analysis of MPC in the head . In the relevant section, it seems like the improvement stems from new instantiations of the technique rather then more tight analysis, as I first understood the term here. Am i right ? Also, you say (on page 12) that using [19], which is perfectly correct eliminates the need for watch lists. How does this work? What if more parties then the allowed threshold are corrupted?