CAREER panel summary and reviews

First submission

CAREER: Pushing the Practicality of Secure Multiparty Computation

Panel recommendation: Competitive

Individual ratings: Very Good/Good | Excellent | Very Good | Very Good/Good

Panel summary

Summary of proposed research activity

The proposal lays out an agenda on building secure multiparty computation (MPC) protocols. Applied MPC has seen a lot of excitement lately, given its potential to improve privacy of various applications and the continuing efficiency improvements. The work lays out a few thrusts, including general compilers for malicious security, integrating MPC with protocols for random access memory (ORAMs), sharper concrete security analyses, and exploration of applications in specific domains including law and medicine.

Intellectual merit

The panel felt that the proposal targets an interesting and timely area, and were uniformly excited about the proposal's included domain-specific applications and collaborations. Opening up applications for these techniques would indeed be ground breaking. In terms of weaknesses, there were concerns that the proposed work would be relatively incremental in terms of algorithmic improvements. It was unclear how much of the technical directions involved combining mostly existing tooling that the community has already developed, compared to newly produced techniques. The concrete security discussion struck some reviewers as somewhat shallow and under-developed.

Broader impacts

The panel was excited about the broader impacts this work could have on practical use cases of MPC. The focus on societally impactful applications, such as healthcare and sexual harassment, were particularly compelling. The proposed development of, and more importantly support for, an open source library would help amplify potential impact. The education plan seemed somewhat standard, but sound.

CAREER-specific criteria

The education and research plans are well integrated, and the open-source library development will make for curricular opportunities that would otherwise not be available. While the overall vision and proposed activities are representative of a very good CAREER proposal, the proposal lacked evidence that the technical directions themselves would lead to significant performance improvements.

Suggestions for improvement

The proposal could be improved by focusing more on factoring out the new technical directions of the work from the (admittedly large amount of) existing work in this space. Some reviewers felt the proposal could be improved by including conceptual nuggets capturing the new insights that will drive significant improvements in practicality of these systems. Some reviewers expressed skepticism regarding the fundamental overheads the ORAM-based approaches will incur, and the proposal could be improved by addressing this issue explicitly. The broader impacts were though to be quite good, but the proposal could be improved by connecting in more detail the challenges expected in the application domains with the technical work.

Summary statement

The panel was excited about the topic area and the potential for the work to be transformative in terms of opening up new application areas for MPC. The main concerns surround the technical directions and whether they have the potential for driving large improvements in practical efficiency. The recommendation of the panel is that the proposal is Competitive.

The summary was read by/to the panel and the panel concurred that the summary accurately reflects the panel discussion.

PANEL RECOMMENDATION: Competitve

Review 1

Multiple Rating: (Very Good/Good)

Intellectual merit

This proposal considers a number of directions in the development of protocols for efficient MPC, focusing in particular on three topics: (1) A general compiler to achieve malicious security, (2) MPC protocols in the RAM model, and (3) concrete security of MPC protocols.

The PI made an impressive volume of contributions to the area of applied MPC, and he is therefore best-positioned to carry out the research. In particular, much of the research proposed builds on top of recent results of the PI, and it is therefore highly likely to succeed in some form.

Still, it is not clear the proposed research is as transformative as we wish it to be in a CAREER proposal - the proposed directions are either very safe, or, at the complete other end, somewhat vague, and do not provide a compelling vision on research in this domain. This proposal has substantial potential, but may benefit from a further iteration to highlight some high-order bits the PI aims to set in the course of the next five years.

For example, RT1 is centered around a new approach to compile an MPC protocol with semi-honest security into one with malicious security. However, the compiler itself is already given in its entirety in the proposal, and the stated goals are to prove its security and improve its efficiency. With respect to the first goal, it is uncommon for the security proof to present any challenges, and no evidence is given to the contrary. For the second goal, the improvements are only superficially discussed, without highlighting the main challenges -- there is also no particular discussion of the computational efficiency of the compiler, which could potentially be an issue when using LPN. Similarly, for RT2, it is hard to get an impression work is not incremental - as an example, the first proposed direction combines the fact that (1) RAM-based MPC relies on GMW, (2) the PI has an improved implementation of the GWM paradigm, and (3) The combination of the two, with a better-engineered ORAM circuit may give a better protocol.

In contrast, RT3 is particularly exciting, however it also lacks details and connections with related works -- one goal is to obtain tighter correlation robustness in the standard model, but there is substantial work on this topic which is not cited (e.g., from symmetric cryptography, tight reductions in public-key cryptography, etc). Also, concrete security in the context of simulation-based notions has a long history in the context of indifferentiability - this is also not mentioned.

The collaborations with industry and with research on law are also exciting and appreciated, but here too, the proposal fails to highlight how this is going to be beneficial to the research agenda. For the legal use case, it would have been interesting to address how the usage of the proposed platform is compatible with NDAs, and whether existing settlement practices need to be modified accordingly to allow for this platform to function properly. (Much of this is likely new legal territory.) There is also a plant to submit a proposal to NIST's competition for threshold cryptography, but insufficient details are provided.

The departmental letter indicates strong support for the research activities by the PI. The available mentoring opportunities include in particular interaction with two senior faculty members, who are (respectively) a theory and a systems researcher.

Broader impacts

The educational component of this proposal is in line with the expectations for an assistant professor, and includes a graduate course connecting systems and cryptography, and an undergraduate research seminar.

In addition to collaborations with industry, the broader impacts also include the publication of an open source library for MPC, as well as the potential of adopting a system to detect repeated sexual assault defenders from settlements. The former is clearly very valuable. The latter, as discussed above, may require further discussion in order to address its actual feasibility (as opposed to being purely of academic/research interest). No actual mechanism to discuss success is described.

The PI is well-qualified to carry out the proposed activities, and the departmental letter indicates support.

Summary statement

The proposal covers several potential advances on secure multi-party computation. However, some of the proposed research feels rather incremental, and it is hard to isolate high-order bits this research aims to set. There is also a clear plan to collaborate with industry, but the way in which synergies can be exploited for the proposed research plan is not clearly addressed.

The broader impacts include an integrated educational component, as well as an open source MPC library. The proposal also considers a potential application of MPC to identify repeated sexual assault offenders across confidential settlements.

Review 2

Rating: Excellent

Summary

The proposal is on secure multiparty computation (MPC), and in particular, developing new algorithmic approaches that will achieve enhanced performance and security. In addition, the proposal lays out a plan for exploring applications of MPC in collaboration with domain experts in law and healthcare databases. This is an excellent proposal.

For the big data section, I'm skeptical that the proposed work will end up with actually scalable protocols, at least in comparison to what is achievable when relying on trusted hardware or just plaintext protocols. If I understand the approach correctly, it requires hiding all access patterns (via ORAM or similar) to the dataset. It would have been good to see some concrete dataset sizes that the PI thought would be tractable.

Another potential limitation is the focus on general-purpose MPC. While this is beneficial in terms of ease-of-use for deployments (which is very important), it would seem less likely to allow high performance compared to application-specific constructions.

The broader impacts of the proposal are very nice. I particularly liked the effort to work with domain experts on applications of the PI's techniques. This is really critical to the prospect of making MPC useful in the real world, and will be immensely challenging as the proposal seems to recognize.

Intellectual merits

1. What is the potential for the proposed activity to advance knowledge and understanding within its own field or across different fields?

The proposal is likely to improve our understanding of building faster, general purpose MPC. It also proposes multi-disciplinary investigations of applications, which could be influential elsewhere.

2. To what extent do the proposed activities suggest and explore creative, original, or potentially transformative concepts?

The overarching goal is what most in the MPC community have been striving for (increased efficiency), but the proposal lays out a compelling set of research tasks that seem likely to help make good progress.

3. Is the plan for carrying out the proposed activities well-reasoned, well-organized, and based on a sound rationale? Does the plan incorporate a mechanism to assess success?

The proposal lays out a clear evaluation plan, and metrics for success.

4. How well qualified is the individual, team, or organization to conduct the proposed activities?

The PI is well qualified, with significant prior work in this area. The PI has also already begun the needed collaborations for his application-oriented work.

5. Are there adequate resources available to the PI (either at the home organization or through collaborations) to carry out the proposed activities?

Yes.

Broader impacts

1. What is the potential for the proposed activity to benefit society or advance desired societal outcomes (Broader Impacts)?

The PI has a track record of releasing and maintaining open source libraries that others end up using. The research protocols themselves may be impactful should they achieve efficiency for particular applications. The proposal also mentions curriculum development, encouraging undergraduate research, and organizing a cryptography workshop for non-cryptographers.

2. To what extent do the proposed activities suggest and explore creative, original, or potentially transformative concepts?

The proposed activities are creative, and the focus on impact in terms of good open-source code bases, outreach to other communities could be transformative.

3. Is the plan for carrying out the proposed activities well-reasoned, well-organized, and based on a sound rationale? Does the plan incorporate a mechanism to assess success?

The broader impacts agenda is well-planned.

4. How well qualified is the individual, team, or organization to conduct the proposed activities?

The PI is well-qualified, and in particular has already started the inter-disciplinary collaborations that will be needed for aspects of the broader impact agenda.

5. Are there adequate resources available to the PI (either at the home organization or through collaborations) to carry out the proposed activities?

Yes.

Additional solicitation-specific review criteria

The educational and research agenda have good synergy.

The proposal seems to clearly lay out a foundation for a career in applied and theoretical cryptography focusing on MPC. The research tasks are compelling and complementary, ranging from theory to application.

The chair's letter indicated that the department would provide sufficient support for the PI.

Summary statement

The proposal is overall excellent, laying out a compelling plan for research on improving MPC's practical utility. Some research thrusts seem unlikely to achieve practicality, but this is a minor point (and the results would probably be of theoretical interest, if they work out, anyway). The exploration of applications and the broader impact agenda more generally are creative and potentially transformative.

Review 3

Rating: Very Good

Intellectual merit

The most interesting part of the proposal to me were its ideas to resolve problems in other disciplines by using ideas from multiparty computation. Particularly, section 6.3 (identifying frequent offenders) involves a very interesting collaboration with a colleague at the Northwestern Law School. Another project is being applied to network of local hospitals.

There is also a project a new compiler, though the proposal would have benefited from clearer explanations here (e.g., on par with those for the previously-mentioned projects).

Broader impacts

Given the application-oriented focus of the research, the application to non-disclosure agreements could have a massive impact on society.

Additional solicitation-specific review criteria

The integrated education plan is adequate though perhaps not as ambitious as one might expect for a CAREER proposal. The letter from his chair explains a high-level picture of the PI's collaboration with academics in other disciplines, though did not address the integrated education plan in detail either.

Summary statement

The PI is involved in projects with collaborators in different disciplines, which is difficult. In particular, the collaboration with legal scholars is potentially transformative if successful.

Review 4

Multiple Rating: (Very Good/Good)

Intellectual merit

This proposal is a very comprehensive approach to the problem of pushing secure multiparty computation (SMPC) to practice. The PI approaches the problem from three different aspects: efficient compilers for malicious security, efficient protocols for computing over large datasets, and concrete security analysis. One might argue that these are the three fundamental roadblocks that stand in the way of making MPC truly practical.

The problems described in the proposal are technically challenging and will require substantial original advances to be solved. I would have preferred to see an arching "theme" connecting them, but they rather read as a set of disjoint problems that are important to improve MPC. The methodology and approach to the problems could have been a bit more detailed.

The PI already has an impressive record in this area and is definitely qualified to run the described research program.

Broader impacts

Improving MPC protocols has great societal importance. The PI details some of the possible applications in the proposal, and it is exciting to see actual possible deployment in practice (e.g NDA and sexual harassment). The PI's educational plan and outreach is standard.

Summary statement

This is a good proposal that could benefit from an unifying theoretical theme connecting the research problems the PI wants to work on.