CAREER panel summary and reviews

Second submission

CAREER: Pushing the Practicality of Secure Multiparty Computation

Panel recommendation: Highly Competitive

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

Panel summary

1. Proposal summary

The focus of this proposal is on Multi-party computation (MPC): a cryptographic tool that allows a set of mutually untrusted parties to compute any function jointly without revealing anything except for the output. MPC is a well studied topic with many advances in recent years that have made it more practical. The main intellectual merit of this proposal is to provide efficient solutions without sacrificing privacy (i.e. in the malicious setting), allow optimizations in the systems level (i.e. cache usage while execution) and explore applications when large amounts of data and participants are involved.

The proposal includes well integrated educational and outreach plans. On the educational side new classes and hands-on projects are proposed. The PI has a record of creating mentorship material that will expand as part of this proposal. Finally, the PI commits to open sourcing the developed code and work towards standardization of underlying techniques.

2. Intellectual merit

Strengths

All the panel participants agree that the potential intellectual merit of this proposal is strong, well thought out and nicely presented. MPC is an important cryptographic tool and the proposed research tasks may significantly advance the area. For example, the ideas on Task 2 on customized zero-knowledge proofs for 2party computation are very interesting and can have implications beyond MPC, while the ideas on Task 4 on the topic of MPC with unbalanced inputs are a nice trade-off in the setting that can lead to efficiency improvements.

The proposed ideas are well explained and include convincing evaluation plans. It is positively noted that for certain applications, evaluation will happen in collaboration with industrial partners.

All the panel participants agree that the PI is well qualified to do the proposed research and has access to all required resources and departmental support.

Weaknesses

Some of the reviewers had specific comments for certain tasks, i.e. additional related work to be discussed and clarifications between communication and computation tasks and benefits of batching and parallelization during implementation. More details can be found in the individual reviews. However, it is noted that the panel considered these issues of only minor impact and they did not affect the overall evaluation of the proposal.

3. Broader impacts

Strengths

Given the increasing popularity of MPC methods, the broader impacts of this work are important and could have large societal impact if MPC tools end up being more widely adopted. The deployment plan can have impact in various fields including federated relational databases and confidential settlements like non-disclosure agreements (NDA) which can also foster multi-disciplinary collaborations.

The educational plan is well thought out and directly related to the proposed research.

The reviewers appreciate the efforts of the PI to maintain open-source implementations and his commitment to continue doing so.

There is commitment from industrial partners for the evaluation and deployment of the proposed tasks.

Weaknesses

The panel agreed that the plan for the engagement of underrepresented communities is somewhat weak.

4. Relevance to SaTC

The proposal fits very well within the SaTC vision as it can enhance the scientific foundations of MPC - an important building block for privacy preserving computations.

5. Suggested improvements

The proposal is generally very well written. In the individual reviews there exist a few directions for improvement in regards to related work discussions and clarification of evaluation goals.

6. Conclusions

Overall this is a very strong proposal that can push the boundaries of MPC research. The PI is very well qualified to solve the presented challenges and has already shown significant commitment to standardization, education and outreach efforts.

7. Panel recommendation

Highly competitive

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

PANEL RECOMMENDATION: Highly Competitive

Review 1

Rating: Very Good

Intellectual merit

The PI proposes to develop more efficient techniques for secure multi-party computation (SMPC) and addresses different challenges such in different settings such as two party secure circuit evaluation, zero knowledge proofs for two party computation, protocols for unbalanced data case where one party has bigger data than the others.

Strengths

- The PI has a well designed research plan for almost all of the cryptographic protocol development tasks.
- The PI has extensive prior work on all of the proposed areas.
- Strong evaluation plan is provided for almost all of the tasks.

Weaknesses

- It was not clear to me whether the large embedding of the server in the context of unbalanced inputs will be practical for other parties that may not have enough computational power.
- I found some of the discussion with respect to application areas less developed. Based on the cryptographic improvements mentioned, I do not see how SQL queries that involve joins can be built for very large datasets. I suspect the reported results (e.g., more than half million records) are for scenarios where there is no multi-joins. In addition, the incentive issues identified in legal deployment setting may not be simply solved with the proposed cryptographic innovations, and tools that combined SMPC and incentives may be needed.

Broader impacts

The PI has strong existing collaboration with many companies and organizations. If the proposed research is successful, it may lead to quick industry adoption.

The PI proposes to also submit solutions to NIST challenges. This could potentially lead to adoption of the developed solutions.

Finally, the PI proposes research and education integration via hands-on labs, new curriculum development and student advising.

Summary statement

The PI proposes many potentially useful and innovative solutions to improve the performance of the SMPC tools. My minor concern is that for some applications mentioned there are additional challenges that may not be addressed by the proposed cryptographic solutions.

Review 2

Rating: Very Good

Intellectual merit

Strengths

1. The proposed project will study two distinct paradigms for malicious two-party computation, i.e., the authenticated garbling paradigm and the GMW-compiler with zero-knowledge proofs tailored for proving non-black-box garbling which can reduce the overhead due to malicious security to the minimal level.
2. The project also considers MPC on big data, and will study a new deployment model that can utilize existing content distribution networks and thus provides enormous opportunities for improved performance based on variations of pseudorandom correlation generators. The instantiation of MPC for big data will provide nontrivial contributions to the community and practical usage.
3. Considering the multi-parting setting, the PI proposes to study generic compilers to obtain malicious security efficiently with system-aware protocol designs, which will bring nontrivial contributions to real-world multi-parting settings.
4. The proposed research activities have an emphasis on real-world deployment and collaboration with industries, which will largely demonstrate the effectiveness of the proposed approaches and analyses.

Weaknesses

1. The proposed protocol for squeezing the last bit of the performance is less clear, and it would be good to discuss for different applications how the design would be constructed and what's the concrete challenges for different applications.
2. For the scalable MPC for big data, it is less clear how much the parallelization and batching will help the efficiency and how much the designed new models will contribute. It would be good to discuss it more clearly.
3. Large industrial collaborations are mentioned, and it would be good to make the concrete application and collaborated problems clear since the protocol design depends on the data type and application itself.

Broader impacts

Strengths

1. The plans of producing high-quality materials for MPC education at different levels and types of audiences are solid and very important.
2. The planned hands-on MPC lab project materials like the SEED labs will be very helpful and contribute to both education and industry deployment.
3. The collaboration with local lawyers and broad outreach plan is solid and concrete.
4. The social impact of using MPC to identify frequent offenders from confidential settlements is novel and suitable for the proposed research activities.

Weaknesses

1. The outreach activities considering the underrepresented communities are not discussed. Given that the research topic on enhancing security and privacy with MPC is related to every individual, it would be good to consider how to support education and career development for the underrepresented groups during the research development.

Summary statement

This proposal aims to push the practicality of secure multiparty computation by developing maliciously secure two-party computation protocols as efficient and scalable as their semi-honest counterparts, improving MPC efficiency when used for big data via proposing new deployment model and improved RAM-based MPC protocols, and developing new classes of protocols that can scale MPC to hundreds of parties and compute huge statements even when the adversary can corrupt the majority of participants.

Overall, the proposal is well-written, and the proposed research activities are concrete and novel. The target problem is of great importance, and the large industrial collaborations are promising for real-world deployment. The education and outreach plans are concrete and reasonable. Some proposed models and protocols can be more clear, but this doesn’t hurt the contribution and logic of the proposed project.

Review 3

Rating: Excellent

Intellectual merit

Strengths

On the one hand, this is a very focused proposal on multi-party computation but on the other hand it covers very many cryptographic techniques. However, the PI clearly shows how the proposed advances build on his unique past contributions. These advances are also clearly spelled out and substantive. The ideas while diverging in their objectives and application areas are well-integrated with respect to their techniques.

Weaknesses

When the proposal mentions efficiency or cost, it is not clear to me whether that is communication or computation. It seems it also varies between the different approaches compared. However, total latency of an MPC may change depending on the system environment (e.g., same data center vs. data centers connected by WAN).

Broader impacts

Strengths

The PI lists many ways how the research can have broader impact. The PI maintains one of the most used MPC toolkits which has tremendous impact in the past already of which the PI lists some examples. This also provides ample opportunity for future broader impact and is very positively noted. The PI also list several industry contacts that can help transition the research results.

Additional solicitation-specific review criteria

Strengths

The PI integrates education and research well. The educational lab for MPC is a great idea and should find many adopters.

Summary statement

Very well done proposal.

Review 4

Rating: Very Good

Intellectual merit

The intellectual merit of this project is to advance the state of the art of multiparty computation (MPC). MPC is a well and long studied problem in the areas of cryptography and applied security where a plethora of existing works have investigated a number of schemes under different features/assumptions and security requirements.

The proposed work can advance the state of the art by exploring distinct paradigms of MPC, such as efficient 2PC in the malicious setting, MPC for large data and MPC for many parties. Under the proposed applications, it can additionally advance cross-disciplinary connections between law/policy and CS.

The proposed activities explore creative approaches to tackle known problems in the MPC literature. The proposed tasks are generally original and creative. The tasks proposed in Thrust 1 seem very well thought and with lots of preliminary results already. In Thrusts 2 & 3 although proposed tasks seem original, some relevant related works that take alternative approaches in solving the problem are missing and would be useful to include for comparison and better understanding of the importance of the given approaches.

The plan for carrying out the proposed activities is well though and includes a promising system evaluation and real world deployment plan (including collaborations with industry, NIST and medical institutions).

The PI is well qualified to perform the proposed research and has adequate resources within his department and via collaborations.

Broader impacts

MPC is an important cryptographic mechanism that has started having the potential to transform certain real-world computations in various applications which has important privacy gains for users. The results of the project can push towards this direction. The PI has a well thought educational and outreach plan including proposed tasks beyond his institution to the wider cryptographic/security communities. Some of the proposed deployment applications can have broader impacts beyond computer science to healthcare data and policy settlements.

The PI has already a solid record of outreach and educational/mentoring activities.

Summary statement

This project can bring MPC protocols closer to practice by proposing a number of techniques and efforts to specific application scenarios. The proposed tasks are generally intellectually novel, well organized and with a measurable success plan. The implementation, educational and outreach/diversity plans are very well thought and show the commitment of the PI in the area.