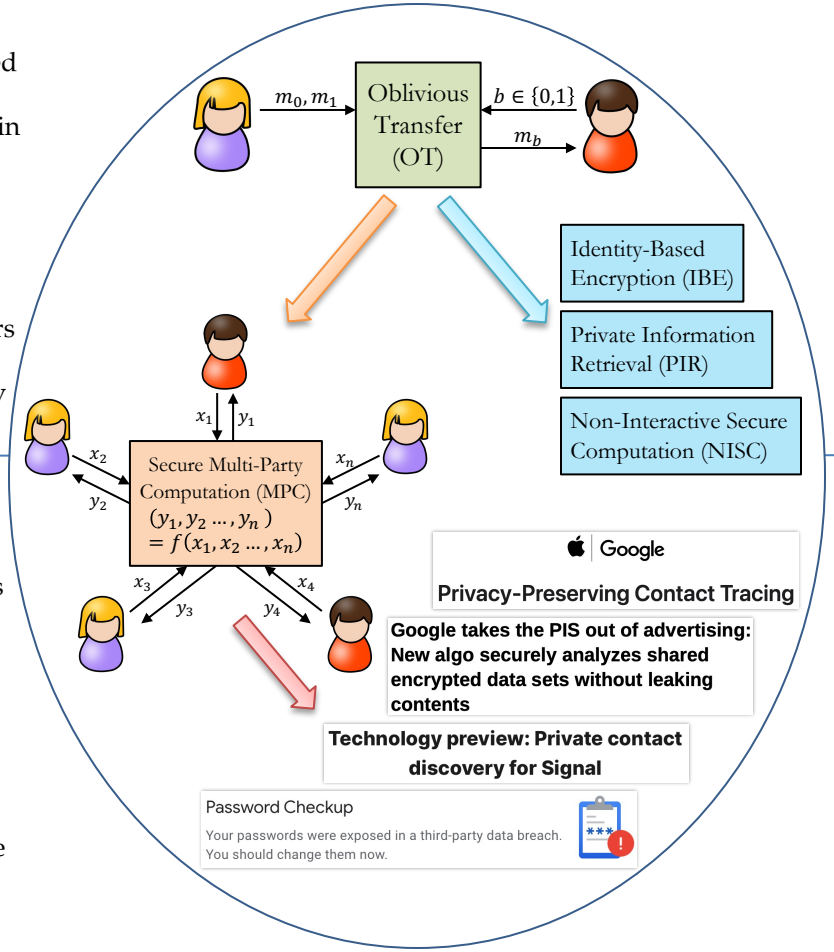
SaTC: CORE: Small: Expanding the Realm of Oblivious Transfer: New Tools for Cryptography

Challenge:

- Efficient oblivious transfer (OT) with advanced functionality and strengthened security are crucial for lowering the communication and computation costs in various cryptographic systems.
- Private set intersection (PSI) with high efficiency and enriched functionality, which has close connection to OT, is in need in many real-world applications.
- It is important to understand the barriers (e.g., lower bounds on the assumptions or communication complexity) that may exist against the above two goals.

Solution:

- We introduced a new technique for amortizing the cost of multiple rate-1 OTs from pairing assumptions. This has also led to significant communication improvements in unbalanced PSI and single-server private information retrieval (PIR).
- We initiated the study of updatable PSI (UPSI) and designed efficient protocols, which allows parties to efficiently compute the intersection of their private sets on a regular basis with sets that constantly get updated.



Scientific Impact:

- New OT tools will play an integral role in the design of privacy-preserving computation. They can be better leveraged in big-data applications, accelerating their adoption in practice.
- OT is closely related to many areas in cryptography (e.g., secure multi-party computation). Advances in OT will deepen our understanding of efficient constructions and fundamental limits in these areas, which is a longer-term intellectual merit of this project.

Broader Impact and Broader Participation:

- This project will facilitate the adoption of privacy-preserving technologies in more industry settings.
- In the longer term, this project will raise awareness of privacy issues and push service providers to provide privacy transparency to their consumers.
- The PI is actively involved in Break Through Tech (BTT) Chicago to increase gender equality in computer science. The PI mentored two female undergraduate students in Summer 2021 and participated in the eCSR (explore Computer Science Research) 2021 workshop.
- The PI co-organized a Mentoring Workshop at CRYPTO 2021.

Award Number: 2055358
Institution: University of Illinois Chicago
PI: Peihan Miao (peihan@uic.edu)