Speaker: Mike Rosulek, Oregon State University

Title: **FleXOR: Flexible garbling for XOR gates that beats free-XOR**

Most implementations of Yao's garbled circuit approach for 2-party secure computation use the free-XOR optimization of Kolesnikov & Schneider (ICALP 2008). We introduce an alternative technique called flexible-XOR (fleXOR) that generalizes free-XOR and offers several advantages. First, fleXOR can be instantiated under a weaker hardness assumption on the underlying cipher/hash function (related-key security only, compared to related-key and circular security required for free-XOR) while maintaining most of the performance improvements that free-XOR offers. Alternatively, even though XOR gates are not always "free" in our approach, we show that the other (non-XOR) gates can be optimized more heavily than what is possible when using free-XOR. For many circuits of cryptographic interest, this can yield a significantly (over 30%) smaller garbled circuit than any other known techniques (including free-XOR) or their combinations.

Our garbling schemes can be directly applied in the semi-honest model, as well as compiled into the malicious setting using any existing technique.

Joint work with Vlad Kolesnikov & Payman Mohassel.