Understanding the Complexity of Concurrent Security

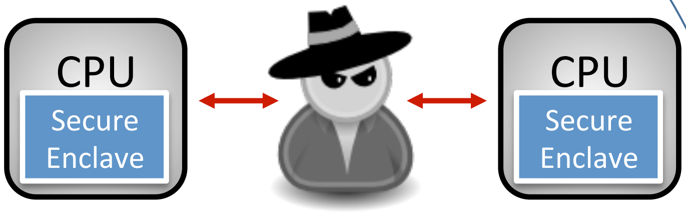
Challenge:

- Identify **minimal complexity** to achieve **concurrent security** that relies on the underlying cryptographic primitives in a **black-box** manner (i.e. construction and reduction should only rely on the input/ output behavior of the primitive).

Solution:

- Identified minimal primitives sufficient to guarantee concurrent security in a black-box way.
- Concurrently secure protocols for arbitrary functionalities under minimal assumptions in the Common Reference String model and Tamper Proof Hardware Token.
- First constructions of concurrently secure protocols in the plain model without setup against adaptive corruptions under standard assumptions.

How to prevent
man-in-the-middle attacks
with secure hardware?



Good local properties that guarantee global composition:

1. Security should not rely on the knowledge of programs incorporated by adversary
2. Security should not rely on programmability of tokens
3. Security should only rely on input/output behavior of cryptographic primitives (i.e. black-box)

Scientific Impact:

- Simplifying constructions for achieving concurrent security via a unified approach under minimal computational assumptions.
- A new framework to model tokens that enable design of concurrently secure protocols. Prior works fail to guarantee adequate security in the concurrent setting.

Broader Impact:

- Framework to incorporate and design concurrently secure protocols using the Intel Software Guard Extension (SGX).
- Understand leakage resilience guarantees of protocols that are secure against adaptive corruptions.

NSF CNS – 1526377, University of Rochester,
Muthuramakrishnan Venkitasubramaniam
email: muthuv@cs.rochester.edu