Privacy Enhancing Cryptography

Luís T. A. N. Brandão · René Peralta · Angela Robinson

Cryptographic Technology Group, Computer Security Division, National Institute of Standards and Technology

Project Goals

- Follow the progress of emerging PEC technologies
- Promote the use of crypto protocols that enable privacy
- Evaluate the potential for standardization of advanced crypto

Base cryptographic techniques

Privacy-enhancing cryptography (PEC) is made up of various techniques:

ZKPs	SMPC	FHE	Others
Zero-**K**nowledge **P**roofs	**S**ecure **M**ulti**p**arty **C**omputation	**F**ully **H**omomorphic **E**ncryption	**I**dentity-**B**ased **E**ncryption **A**ttribute-**B**ased **E**ncryption **F**unctional **E**ncryption, ...

Basic *gadgets* (building blocks)

ZK proofs and other techniques are often composed by several basic building blocks (commonly referred to as gadgets). Some examples include:

Encipher

Like a randomly *scrambled text*

Hash

Like a *fingerprint* of data ("unique" bit sequence (256 bits).

Commitment

Like a *vault* that hides data until it is open.

Sign

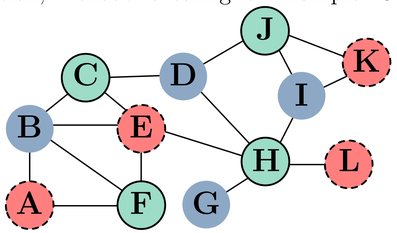
Like a physical signature, but cannot be forged.

Vision and potential impact

- **The Reference Materials approach.** Create and disseminate.
- **Benchmarks.** promote experimentation and deployment of PEC apps.
- **Applications.** user identification, private storage & computation, commercial transactions, ...

Zero-knowledge proofs (ZKPs)

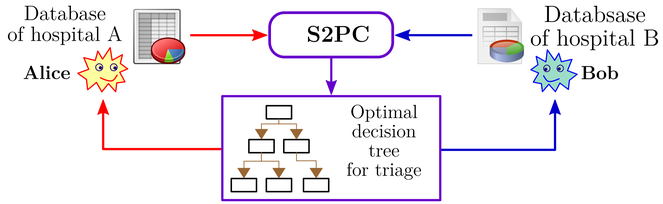
What: one party (the prover) can prove (to a verifier) the knowledge of mathematical solution, without revealing it. Example: Graph 3-colorability.



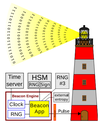
How: Using a *commit–challenge–response* approach. Using random color permutations (e.g. ), and commitments, prove that each edge has two different colors.

Secure multiparty computation (SMPC)

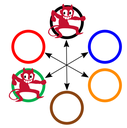
Multiple parties can jointly compute a function of their distributed inputs, while retaining privacy of each input/output.



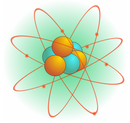
Foreseeable synergies with other projects:



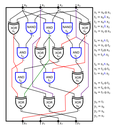
Randomness Beacons



Threshold Cryptography



Post-Quantum Cryptography

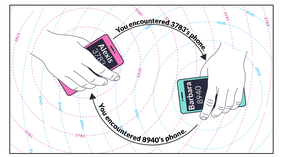


Circuit Complexity

Encounter Metrics

Goal. Measure aggregate levels of encounters within a population while preserving the privacy of individuals.

- Measurements useful for making informed decisions about building occupancy rates and mobility rules.
- We classify *encounters* by distance between persons during time of interaction.



Credit: Victoria Liu

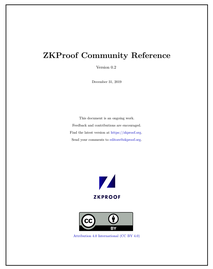
Application. Privacy-preserving exposure notification and automated contact tracing.

- Allows one to obtain a measure of their risk due to past encounters with self-reported COVID-19 positive people.
- The precise engineering of a system for exposure notification should be targeted to particular environments.

The ZKProof initiative

An open-industry academic initiative to mainstream (ZKP) cryptography. The **NIST-PEC team** provides public feedback and develops new material:

- *Comments on the initial ZKProof docs*
- Co-authors of ZKProof Community Ref 0.2
- Comments on the ZkpComRef 0.2
- Talks at various ZKProof events



More about the NIST-PEC project:

- **The PEC Project/Team contact:** crypto-privacy@nist.gov
- **Webpage:** `https://csrc.nist.gov/Projects/pec`
- **See also** the **Special Topics of Privacy and Public Auditability** (STPPA)
- **Poster produced for:** NIST-ITL Virtual Science Day 2020 (October 29)

The first author is a Foreign Guest Researcher at NIST (Contractor via Strativia)