Fostering Standards for Privacy Enhancing Cryptography

Luís Brandão *

Cryptographic Technology Group
National **I**nstitute of **S**tandards and **T**echnology

Presented on May 19, 2022 @ Boston, USA
Privacy-Enhancing Technology Summit North America

Based on joint work with René Peralta and Angela Robinson.

* At NIST as a Foreign Guest Researcher (Strativia Contractor). Expressed opinions are from the speaker, not to be construed as official NIST views.

This presentation?

- A pre-standards perspective: the ***reference material*** approach (in the PEC project)
- A cryptography focus: ideal functionalities, some PEC tools
- Some considerations: modularity, adoptability, insights, ...

Outline

1. NIST-PEC intro
2. PEC tools/nuances
3. Considerations

NIST: Laboratories → Divisions → Groups

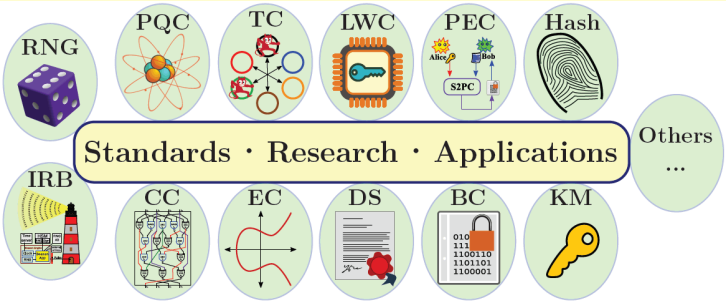
- **Non-regulatory** federal agency (@ U.S. Deptm. Commerce)
- **Mission:** ... innovation ... industrial competitiveness ... measurement science, standards, and technology ... economic security ... quality of life.

NIST name and address plate (source: nist.gov)

INFORMATION TECHNOLOGY LABORATORY → **Computer Security Division (CSD):**

→ **Cryptographic Technology Group (CTG):** research, develop, engineer, and produce guidelines, recommendations and best practices for cryptographic algorithms, methods, and protocols.

Activities in the “Crypto” Group



- Public documentation: FIPS; Special Publications (SP 800); NIST Reports (IR).
- International cooperation: government, industry, academia, standardization bodies.

Legend: **BC** (**B**lock **C**iphers); **CC** (**C**ircuit **C**omplexity); **Crypto** (**Crypto**graphy); **DS** (**D**igital **S**ignatures); **EC** (**E**lliptic **C**urves); **FIPS** (**F**ederal **I**nformation **P**rocessing **S**tandards); **IR** (**I**nternal or **I**neragency); **IRB** (**I**nteroperable **R**andomness **B**eacons); **KM** (**K**ey **M**anagement); **LWC** (**L**ightweight **C**rypto); **PEC** (**P**rivacy-**E**nhancing **C**rypto); **PQC** (**P**ost-**Q**uantum **C**rypto); **RNG** (**R**andom-**N**umber **G**eneration); **SP 800** (**S**pecial **P**ublications in Computer Security); **TC** ([Multi-Party] **T**hreshold **C**rypto).

More details at https://www.nist.gov/itl/csd/cryptographic-technology

The NIST Privacy Enhancing Cryptography (PEC) project

- Within the NIST Cryptographic Technology Group (CTG).
- PEC ≈ **c**ryptography (that can be) used to **e**nhance **p**rivacy.

  Focus on non-standardized high-level special-featured techniques

STPPA series

PEC use-case suite

Encounter metrics

ZKProof collaboration

Workshops

https://csrc.nist.gov/projects/pec

Goals:

- Accompany the progress of emerging PEC tools (≈ primitives, protocols, techniques).
- Develop reference material to support the use of crypto to enable privacy.
- Evaluate the potential for guidance/standardization about PEC tools.

https://csrc.nist.gov/projects/pec

Toward Standards for PEC?

It's tempting to just ask: <u>when</u> should PEC be standardized ?

The question deserves some in-depth reflection (what/how/...?)

1. **Domain space:** Identify/clarify/distinguish major techniques: general (e.g., SMPC), particular (e.g., PSI), building blocks (e.g., OT). There is a large space of tradeoffs.

2. **(Mis)understanding:** What do PEC tools actually provide when applied?

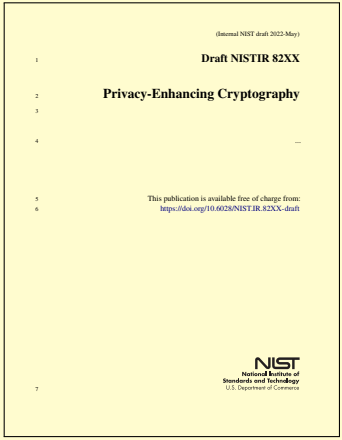
3. **Toward standards (?) / alternatives: reference material** (definitions, descriptions, implementations, characterization, applicability); **recommendations** & **guidelines**

Legend: SMPC = Secure Multiparty Computation. PSI = Private Set Intersection. OT = Oblivious Transfer

Upcoming NIST Report on PEC

- Enumerate and explain various “PEC tools”
- Acknowledge their terminology, building blocks, nuances
- Distill insights useful toward “recommendations”

A draft will be open for public comments


(Internal NIST draft 2022-May)

Draft NISTIR 82XX

Privacy-Enhancing Cryptography

...

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.82XX-draft

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Outline

“PEC Tools”

SMPC
Secure
Multi**p**arty
Computation

ZKP
Zero-
Knowledge
Proofs

FHE
Fully
Homomorphic
Encryption

PSI
Private
Set
Intersection

GRS
Group and
Ring
Signatures

StE
Structured
Encryption
(Symm./PKI)

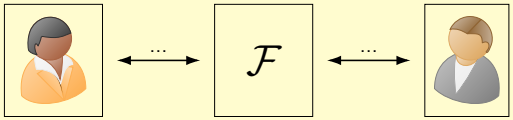
PIR
Private
Information
Retrieval

FuE
Functional
Encryption
(Inc. ABE & IBE)

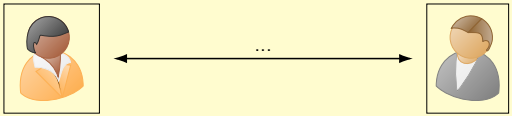
Legend: Symm./PKI: based on symmetric-key or public-key. ABE: attribute-based encryption; IBE: identity-based encryption.

Ideal functionalities ($\mathcal{F}$)

Ideal world: uses an incorruptible trusted party to define the desired functionality ($\mathcal{F}$), and thus its security properties.



Real world: A set of procedures that satisfies (*emulates*) the properties of the ideal execution, but without a trusted party.

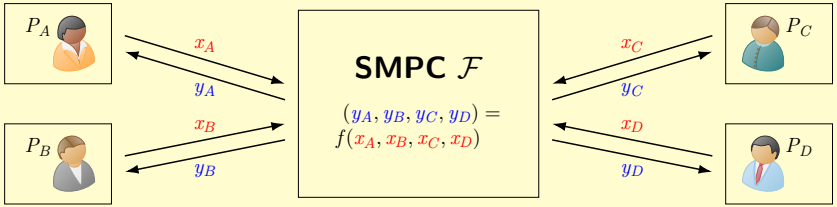


Utility of ideal functionalities: clear formulation of security; security-proof framework (simulatability); composability assurance; modularity.

Next slides: various PEC tools, with simplified illustrations of ideal functionalities. Over-simplified: omitting setup, session ids, nuances, ...

SMPC (or MPC): Secure Multiparty Computation

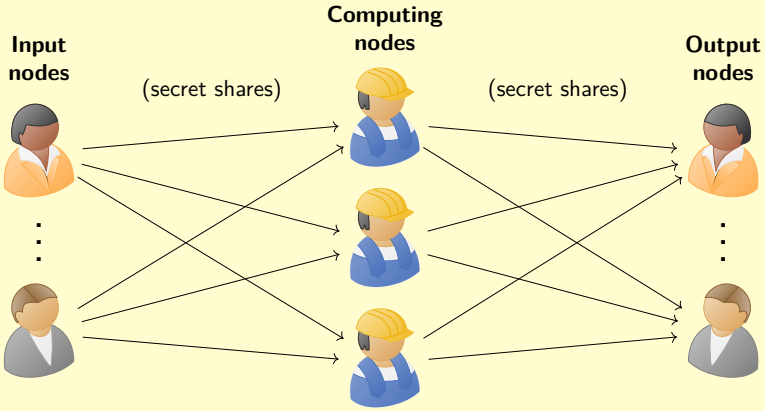
Illustration of an ideal functionality $\mathcal{F}$



Multiple parties with privacy constraints can securely compute a function over their private inputs.

- Privacy of local inputs/outputs
- Correctness of the computation
- Guaranteed output delivery (common nuances: security-with-abort; fairness) ...

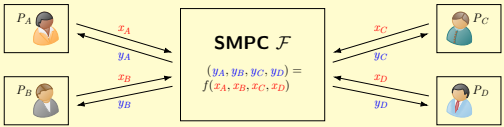
SMPC, by an external (secret-shared) set of parties

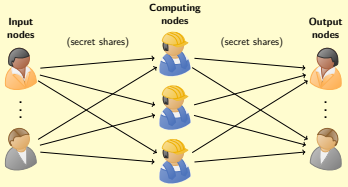


The computing nodes compute (SMPC) over **secret-shared** data.

SMPC nuances

Wait: Was there a mismatch across the past two slides?





- No mediator (when $\mathcal{F}$ disappears)
- Parties retain control of their input
- Everyone decides when to SMPC
- Online agreem./synch. more difficult

- SMPC done by the computing nodes
- Parties secret-share their input
- Delegated consent for future computations
- Comp. nodes facilitate interoperability

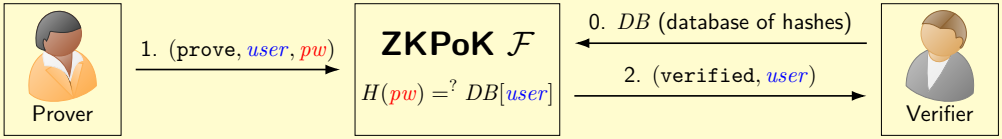
Both are possible. It's important to distinguish them.

ZKPoK: Zero-Knowledge Proof of Knowledge

Prove knowledge of a secret (called *witness*), without disclosing it to the verifier.

Example: ZK-prove knowledge of a password pw (pre-image of a hash $H(pw)$ stored by the verifier)

Illustration of an ideal functionality $\mathcal{F}$ (ensuring ZK and soundness)



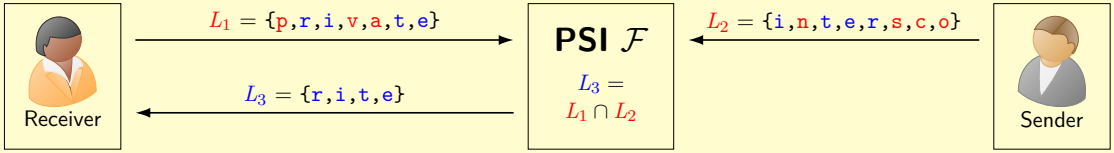
Other example applications:

- correct behavior in an SMPC
- knowledge of secret key wrt public key
- regulatory compliance over encrypted data

zkproof.org is an open initiative for promoting interoperable, secure and practical ZKPs

(Minor slide update on 2022-May-26)

PSI: Private Set Intersection



Two parties find their common elements, without revealing the others

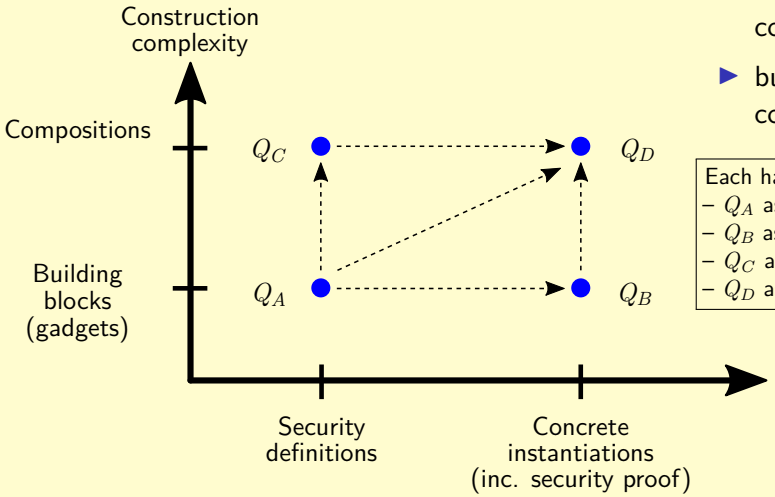
Examples: private contact discovery, leaked-password check, multi-state vote registration

Nuances:

- May leak the length of the lists; more than 2 parties; ...
- Computation over the intersection (special case of MPC)

Outline

Modularity and composability



- ideal functionalities vs. concrete protocols?
- building blocks vs. complex constructions?

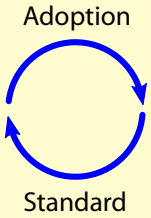
Each has a place in the process, e.g.:
– Q_A as a reference definition;
– Q_B as a module;
– Q_C as a criterion/template;
– Q_D as a goal.

Some insights

- **Ideal functionalities** enable a simple, modular reflection. But even that requires thinking it through, e.g., who owns the inputs?, who decides when to compute?
- **Where is the privacy?** Use of a **P**EC tool does not guarantee an application enhances/preserves privacy (might it be degraded?). It requires proper use.
- **Who is empowered?**
  - **Users?**: PEC for more user autonomy in authentication, proof of attributes, PSI, ...
  - **Companies?**: PEC for new possible collaborations that leverage user data, ...
- PEC can raise **trustworthiness** to the level of reasonable **trust** (e.g., analogy with end-to-end encryption, blind mediator).
- **A relevant duo:** privacy & [public] auditability. PEC tools allow it.

Adoptability of standards

- *Not every conceivable possibility is suitable for standardization.*
- *Need to focus on high need and high potential for adoption.*
- *Best practices*; *minimum defaults*; *interoperability*; *innovation*.



If/when compliance is required, a standard can be *impractical* if the technique:

- is obsolete/outdated, or cannot be corrected/withdrawn/replaced (when it should);
- does not lend itself to suitable validation mechanisms.

Useful before PEC standards

- Technical understanding of **PEC tools** and their nuances
- Need to conceptualize / contextualize **privacy application goals**
- Develop **reference material** (also promotes **transparency** of rationale)
- **Assess solutions vs. problems** (clarify potential for adoption of standards)
- **Public feedback** is necessary (tools, applications, privacy/auditability concerns)
- Various **recommendations** are likely feasible before **standards**

Thank you for your attention!

Questions?

More resources about the NIST-PEC project:

- **Website:** https://csrc.nist.gov/projects/pec
- **Forum:** https://list.nist.gov/pec-forum
- **Email:** crypto-privacy@nist.gov

Fostering Standards for Privacy Enhancing Cryptography

Presented at Privacy-Enhancing Technology Summit North America, May 19, 2022 @ Boston

luis.brandao@nist.gov

Index of Slides