Toward Recommendations for Advanced Cryptography

Luís Brandão *

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

Presented at:
5th HomomorphicEncryption.org Standards Meeting
September 02, 2022 @ Geneva, Switzerland

* 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: some PEC tools
- Considerations about standardization / recommendations (including notes on FHE)

PEC = Privacy-Enhancing Cryptography
FHE = Fully-Homomorphic Encryption

Outline

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

Outline

NIST: Laboratories → Divisions → Groups

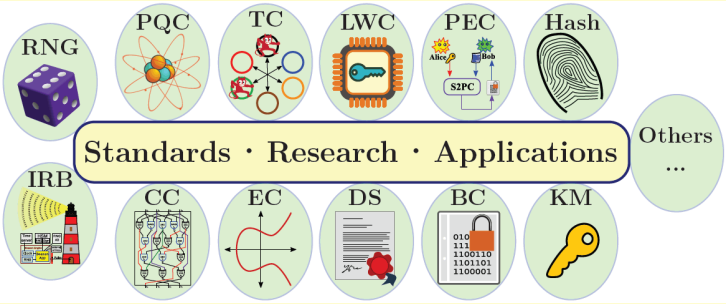
- **Non-regulatory** federal agency (@ U.S. Dept. Commerce)
- **Mission:** ... innovation ... industrial competitiveness ... measurement science, standards, and technology ... economic security ... quality of life.

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**nteragency); **IRB** (**I**nteroperable **R**andomness **B**eacons); **KM** (**K**ey **M**anagement); **LWC** (**L**ight**w**eight **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

On NIST Crypto Standards Development

NIST IR 7977: "NIST Cryptographic Standards and Guidelines Development Process" (2016)

Puts forward various principles to consider:

- Transparency
- Openness
- Balance
- Integrity
- Technical Merit
- Usability
- Global Acceptability
- Continuous Improvement
- Innovation and IP

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

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

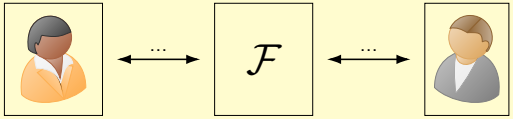
FuE
Functional
Encryption
(Inc. ABE & IBE)

Note: traditional NIST crypto standards cover more-basic primitives. PEC tools (including protocols) require somewhat newer considerations. w.r.t. standards/recommendations.

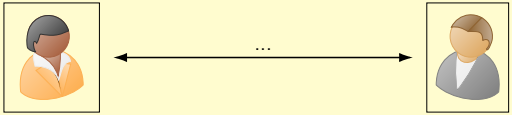
Legend: Symm./PKI: based on symmetric-key or public-key. ABE: attribute-based encryption; IBE: identity-based encryption.

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.



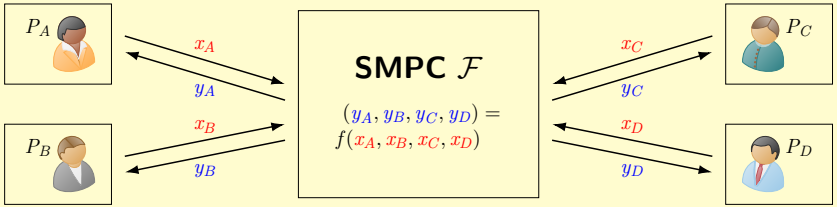
Utility of ideal functionalities: clear formulation of security; security-proof framework (simulatability); composability assurance; modularity.

Next slides: various PEC tools, with simplified illustrations of ideal functionalities.

SMPC (or MPC): Secure Multiparty Computation

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

Illustration of an ideal MPC functionality

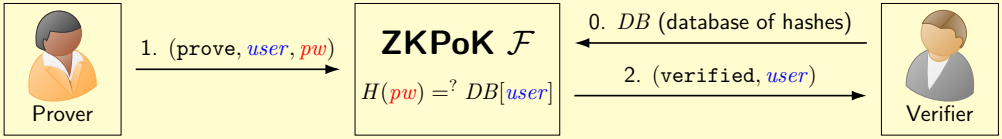


- Privacy of local inputs/outputs
- Correctness of the computation
- Guaranteed output delivery (common nuances: security-with-abort; fairness) ...

ZKPoK: Zero-Knowledge Proof of Knowledge

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

Specific example: illustration of a ZKPoK ideal functionality for "*I know one password whose hash is in your (username-indexed) database*" (ensures ZK and soundness)

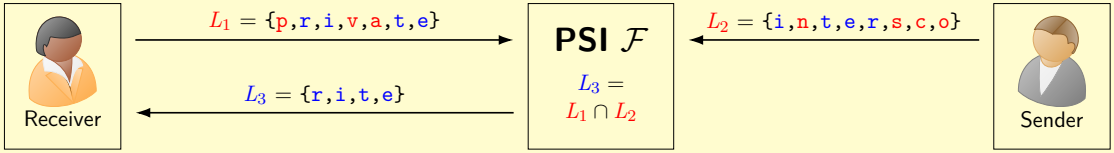


Example applications:

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

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

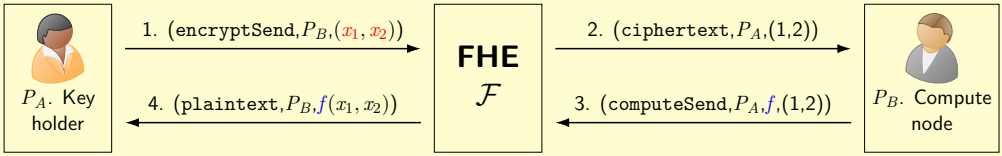
Nuances:

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

FHE: Fully Homomorphic Encryption

A server computes over data encrypted by a client. Later the client decrypts the result.

Illustration of an ideal functionality



- Tuple of operations: `keygen`, `encrypt`, `homom-eval` (add, mult, ...), `decrypt`
- Public-key vs. secret-key encryption
- Various other internal notions: bootstrapping, key-switching, ...

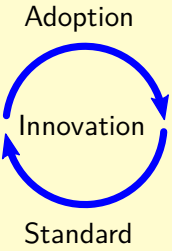
PEC tools come in various flavors

- **MPC:** very general; multi-party; many tradeoffs (system model, thresholds, etc.)
  – The NIST Multi-Party Threshold Crypto project covers some MPC tools/use-cases
- **ZKPs:** many proposed schemes (various assumptions, trusted setups ...); specialized proofs vs. proofs for NP ... also many tradeoffs.
  – NIST-PEC engaged with ZKProof.org to promote development of reference material
- **PSI:** a more concrete MPC app; still a protocol (often 2-parties) with messages
  – NIST-PEC is interested in reference material (concrete applications)
- **FHE:** apparently simpler scope; not multi-party; smaller diversity of assumptions?
  – NIST has been an "observer"

How do these differences warrant differentiated "standardization" approaches?

Outline

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);
- incompatible with validation (required for NIST "essential" crypto)

Note there is also a cost to maintain standards: revise, deprecate, validate, etc.

How should NIST-PEC promote FHE?

A conceivable **NIST Report on FHE** could cover/acknowledge the following.

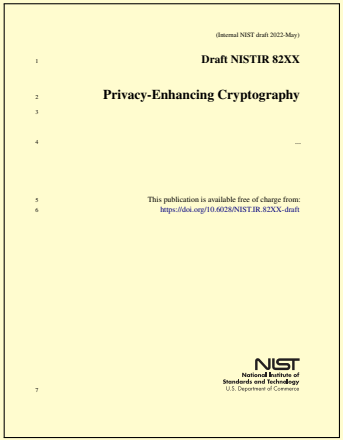
1. FHE as a tuple of algorithms; possible nuances (symmetric and pubkey)
2. Security formulation (intended properties, games, ...) and variety of options
3. Main approaches/concepts, e.g.: lattices/assumptions, bootstrapping, paradigm for homomorphic operations (over Booleans, Fields, ...)
4. State-of-the-art efficiency: what is already practical; what is not
5. Applications that hint at adoptability of a future standard
6. External standardization initiatives, including working groups in SDOs

How helpful would such a report be for stakeholders and for further progress?

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

Concluding remarks

- NIST-PEC appreciates community initiatives that strive for reaching a consensus about recent/advanced (not NIST-standardized) crypto techniques.
- NIST-PEC would take into consideration a potential "standard" emerging from the comunity ... [this is not a promise of producing a standard].
- NIST standards, such as FIPS and SP 800, are open to all / free of charge.
- Other points of interest: PQC and Threshold compatibility; adoptability potential, ...
- What role should NIST-PEC take: observer? report on FHE? more reference material?

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

Toward Recommendations for Advanced Cryptography
Presented at the 5th HomomorphicEncryption.org Standards Meeting
September 02, 2022 @ Geneva (Switzerland)

luis.brandao@nist.gov