

Emerging FHE: from Multiple Perspectives into a Clarifying Progress

HES7: 7th HomomorphicEncryption.org Standards Meeting

2024-Oct-13, Salt Lake City, USA

Luís Brandão^{*}

* NIST Foreign Associate (Guest Researcher, non-employee), Contractor from Strativia. Expressed opinions are from the speaker.
The work from the PEC-team is joint with René Peralta and Angela Robinson.

Preamble — This presentation

1. **Thank you** for the invite to give this update at HES7

HES7 = 7th HomomorphicEncryption.Org Standards Meeting

2. **Goals:**

- ▶ Briefly convey the NIST-PEC interest and perspective on FHE
- ▶ Share some topics of reflection

3. The slide-deck will be **publicly available**



Outline

1. **NIST-PEC Intro**
2. **Our FHE Info Sources**
3. **What we Care About**
4. **Reflection**

FHE = Fully **H**omomorphic **E**ncryption

NIST = **N**ational **I**nstitute of **S**tandards and **T**echnology.

PEC = **P**rivacy-**E**nhancing **C**ryptography.

Outline

1. **NIST-PEC Intro**
2. Our FHE Info Sources
3. What we Care About
4. Reflection

FHE = Fully Homomorphic Encryption

NIST = National Institute of Standards and Technology.

PEC = Privacy-Enhancing Cryptography.

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)

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)

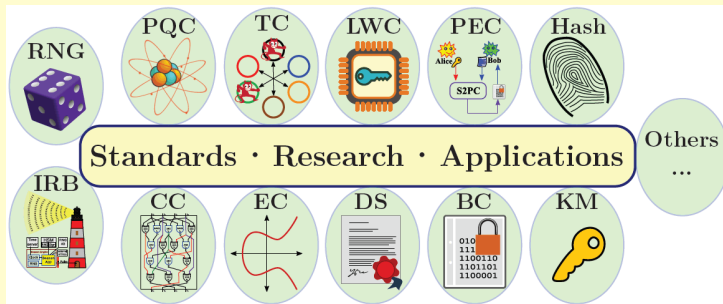


INFORMATION
TECHNOLOGY
LABORATORY

→ **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 = Block Ciphers. CC = Circuit Complexity. **Crypto** = **C**ryptography. DS = Digital Signatures. EC = Elliptic Curves. FIPS = Federal Information Processing Standards. IR = Internal or Interagency (denoting that the public NIST report was developed internally at NIST or in an interagency collaboration, respectively). IRB = Interoperable Randomness Beacons. KM = Key Management. LWC = Lightweight Crypto. PEC = Privacy-Enhancing Crypto. PQC = Post-Quantum Crypto. RNG = Random-Number Generation. SP 800 = Special Publications in Computer Security. TC = [Multi-Party] Threshold Crypto).

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

Intro: NIST has various Crypto Projects

- ▶ **PQC:** [standardization] “**post-quantum**” signatures and key-encapsulation
- ▶ **LWC:** [standardization] “**lightweight**” **Auth. Enc.** w/ **Assoc. Data**, and hashing

Legend: **AEAD** = Auth[enticated] Enc[ryption] w[ith] Assoc[iated] Data. **CTG** = Cryptographic Technology Group. **LWC** = Lightweight Cryptography. **MPTC** = Multi-Party Threshold Cryptography. **NIST** = National Institute of Standards and Technology. **PEC** = Privacy-Enhancing Cryptography. **PQC** = Post-Quantum Cryptography.

Intro: NIST has various Crypto Projects

- ▶ **PQC:** [standardization] “**post-quantum**” signatures and key-encapsulation
- ▶ **LWC:** [standardization] “**lightweight**” **Auth. Enc.** w/ **Assoc. Data**, and hashing
- ▶ **PEC:** [exploratory] “**privacy-enhancing**” (advanced) features/functionality
- ▶ **MPTC:** [exploratory] “**multi-party threshold**” schemes for crypto primitives
- ▶ ... (various other projects in the NIST “Crypto group” [CTG])

Legend: **AEAD** = Auth[enticated] Enc[ryption] w[ith] Assoc[iated] Data. **CTG** = Cryptographic Technology Group. **LWC** = Lightweight Cryptography. **MPTC** = Multi-Party Threshold Cryptography. **NIST** = National Institute of Standards and Technology. **PEC** = Privacy-Enhancing Cryptography. **PQC** = Post-Quantum Cryptography.

Intro: NIST has various Crypto Projects

- ▶ **PQC:** [standardization] “**post-quantum**” signatures and key-encapsulation
- ▶ **LWC:** [standardization] “**lightweight**” **Auth. Enc.** w/ **Assoc. Data**, and hashing
- ▶ **PEC:** [exploratory] “**privacy-enhancing**” (advanced) features/functionality
- ▶ **MPTC:** [exploratory] “**multi-party threshold**” schemes for crypto primitives
- ▶ ... (various other projects in the NIST “Crypto group” [CTG])

PEC and MPTC are interested in FHE (and other techniques).

Legend: **AEAD** = Auth[enticated] Enc[ryption] w[ith] Assoc[iated] Data. **CTG** = Cryptographic Technology Group. **LWC** = Lightweight Cryptography. **MPTC** = Multi-Party Threshold Cryptography. **NIST** = National Institute of Standards and Technology. **PEC** = Privacy-Enhancing Cryptography. **PQC** = Post-Quantum Cryptography.

On the PEC and MPTC projects

Exploratory work to assess potential for recommendations, and standardization processes.

Main approach: promote development of **reference material**.

On the PEC and MPTC projects

Exploratory work to assess potential for recommendations, and standardization processes.

Main approach: promote development of **reference material**.

PEC: Privacy-Enhancing Cryptography

- ▶ Crypto (that can be) used to enhance privacy [emphasis on non-standardized tools].

MPTC: Multi-Party Threshold Cryptography

- ▶ *Threshold Schemes* for diverse Cryptographic Primitives

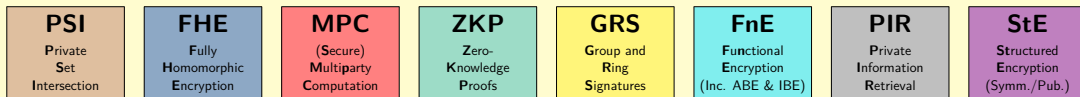
On the PEC and MPTC projects

Exploratory work to assess potential for recommendations, and standardization processes.

Main approach: promote development of **reference material**.

PEC: Privacy-Enhancing Cryptography

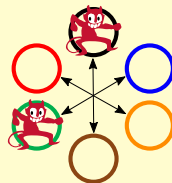
- ▶ Crypto (that can be) used to enhance privacy [emphasis on non-standardized tools].



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

MPTC: Multi-Party Threshold Cryptography

- ▶ *Threshold Schemes* for diverse Cryptographic Primitives



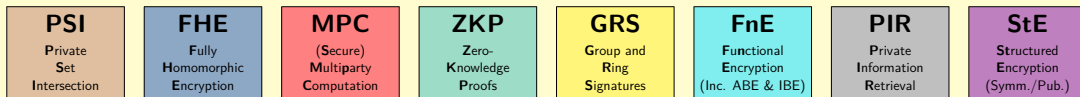
On the PEC and MPTC projects

Exploratory work to assess potential for recommendations, and standardization processes.

Main approach: promote development of **reference material**.

PEC: Privacy-Enhancing Cryptography

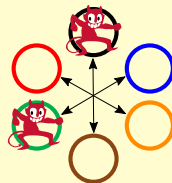
- ▶ Crypto (that can be) used to enhance privacy [emphasis on non-standardized tools].



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

MPTC: Multi-Party Threshold Cryptography

- ▶ *Threshold Schemes* for diverse Cryptographic Primitives
- ▶ The NIST Threshold Call considers MPC, FHE, ZKP and various gadgets.



Outline

1. NIST-PEC Intro
2. **Our FHE Info Sources**
3. What we Care About
4. Reflection

FHE = Fully Homomorphic Encryption

NIST = National Institute of Standards and Technology.

PEC = Privacy-Enhancing Cryptography.

Where have we been “hearing” about FHE

In NIST crypto activities:

1. **Workshops**: WPEC 2024, MPTS 2023, STPPA6
2. The **Threshold Call**
3. Addressing other **PEC tools**

In contact with / observing external initiatives:

4. FHE-related events (HES **meetings**, ...)
5. Governance-level documentation and initiatives

Check the PEC/FHE webpage:



<https://csrc.nist.gov/projects/pec/fhe>

NIST Crypto Workshops covering FHE

NIST organize workshops with participation from academia, industry, and gov

Mindset: reference material (all media available online), learning, signal-to-noise, ...

- ▶ **WPEC 2024** (Sep 24–26) [**W**orkshop on **P**rivacy-**E**nhancing **C**ryptography]
 - ▶ Included one day with **a session on FHE**, and another on PEC (inc. FHE) in Gov.
- ▶ **MPTS 2023** (Sep 26-28) [**W**orkshop on **M**ulti-**P**arty **T**hreshold **S**chemes]
 - ▶ Included talks on comments about **FHE in the Threshold Call**
- ▶ **STPPA6** (July 25, 2023) [**S**pecial **T**opics on **P**rivacy and **P**ublic **A**uditability, Event #6]
 - ▶ **Theme:** Community Efforts on Advanced Cryptographic Techniques
 - ▶ Included talks about **HES and the ISO/IEC efforts**

NIST Threshold Call

<https://csrc.nist.gov/projects/pec/threshold>



- ▶ Expects submissions of FHE schemes (subcategory C2.6), in 2025
- ▶ Submitters can motivate and choose a benchmark that benefits their scheme.
(The [Draft](#) Threshold Call exemplifies FHE of AES as one use case.)
- ▶ Incorporates FHE (and threshold decryption, ...) in a large/wide process,
 - promoting a gathering of **resources** for **analysis**,
 - aiming to support future NIST **documentation** (recommendations, ...).

PEC synergies

When exploring PEC, FHE also appears in connection with other techniques.

- ▶ FHE used to enable MPC, PSI, PIR, encrypted search, ...
- ▶ FHE's verifiability enabled by ZKPs.
- ▶ FHE to complement other PETs (e.g., differential privacy).
- ▶ FHE using lattices, relatable to assumptions accepted for NIST standardized PQC.



Legend: FHE = Fully-Homomorphic Encryption. MPC = Secure Multiparty Computation. NIST = National Institute of Standards and Technology. PEC = Privacy-Enhancing Cryptography. PET = Private-Enhancing Technology. PIR = Private Information Retrieval. PSI = Private Set Intersection. ZKP = Zero Knowledge Proof. PQC = Post-Quantum Cryptography.

HES meetings

NIST welcomes community initiatives such as HomomorphicEncryption.Org Standardization (HES), promoting **technical consensus**, creating **reference material** for the community, and clarifying the **needs and path for standardization**.

- ▶ **HES1** (2017 @ Redmond, USA) and community standard proposal:
 - ▶ Participation* on the 1st HES meeting (working groups)
 - ▶ Collaboration on writeup with community proposal of HE security standard.
- ▶ **Invited talks ('22, '23, '24):** An opportunity to disseminate NIST's perspective
 - ▶ **HES5** (2022 @ Geneva, Switzerland): [Talk](#) on advanced cryptography
 - ▶ **HES6** (2023 @ Seoul, South Korea): [Talk](#) on threshold Call
 - ▶ **HES7** (2024 @ Salt Lake City, USA): [Talk](#) on PEC/FHE perspective

In Gov documentation, initiatives

Further acknowledgment of FHE in various gov-level documents, initiatives, ...

- ▶ National Strategy to Advance Privacy-Preserving Data Sharing and Analytics ([PPDSA](#))
- ▶ UK/US PETs [Prize Challenge](#)
- ▶ UN PETs Lab/Guide
- ▶ US PETs Lab (NIST+Census)
- ▶ NIH [webinars/workshop](#) on FHE
- ▶ ... (non-exhaustive list)

Outline

1. NIST-PEC Intro
2. Our FHE Info Sources
3. **What we Care About**
4. Reflection

FHE = Fully Homomorphic Encryption

NIST = National Institute of Standards and Technology.

PEC = Privacy-Enhancing Cryptography.

C. What we care about (if thinking about future standards)

1. **Understanding/explainability:**

taxonomy, building blocks, education (reference material)

2. **Technical consensus:**

From community initiatives, working groups, dedicated workshops, ...

3. **Standards' adoptability:**

Applications, feasibility, interoperability, security ...

4. **Industry maturity:** development stage of dedicated hardware, open-source libraries, reference material, real-world deployments, pilots

5. **Post-quantum security:** (NSM [10](#) (2022), NCCoE)

Outline

1. NIST-PEC Intro
2. Our FHE Info Sources
3. What we Care About
4. **Reflection**

FHE = Fully Homomorphic Encryption

NIST = National Institute of Standards and Technology.

PEC = Privacy-Enhancing Cryptography.

Some observations:

1. FHE is a **sound** cryptographic technology, receiving a lot of attention!
2. Increasingly noticeable FHE **momentum** (from multiple initiatives)
3. **Community**-based **open** documentation is very useful (such as from HES)
4. Standardization **process** > standardizing > standard (document)
(and maintenance, implementation validation and guidance)
5. A challenge: On human resources **availability** / **speed** of the process

Some observations:

1. FHE is a **sound** cryptographic technology, receiving a lot of attention!
2. Increasingly noticeable FHE **momentum** (from multiple initiatives)
3. **Community**-based **open** documentation is very useful (such as from HES)
4. Standardization **process** > standardizing > standard (document)
(and maintenance, implementation validation and guidance)
5. A challenge: On human resources **availability** / **speed** of the process
(NIST-PEC would benefit from integrating an FHE specialist)

NIST-PEC approach:

1. **Not a driver** of developing technical FHE documentation
2. Interested in the **process and outcomes** of community/standardization activities
3. Improve the **signal-to-noise ratio** (identifying FHE as sound technology)
4. Expects to receive **FHE submissions to the Threshold Call**, to support a phase of analysis that will then facilitate informed recommendations/statements about FHE.
5. Long time idea: A **NIST report on PEC**, including FHE (mostly at high-level): terminology, security properties, applications, adoptability, ...

A PEC/FHE Webpage

A Recent **FHE** [webpage](#) within the PEC project webpage (feedback welcome)

A screenshot of a web browser displaying the NIST Fully-Homomorphic Encryption (FHE) webpage. The browser's address bar shows the URL 'https://csrc.nist.gov/projects/pec/fhe'. The page title is 'Fully-Homomorphic Encryption'. The main text describes FHE as a main tool of Privacy-Enhancing Cryptography (PEC), alongside Multi-Party Computation (MPC), Zero-Knowledge Proofs (ZKP), Private-Set Intersection (PSI), and others. It mentions the NIST PEC project. A green button with a plus icon and the text '+ expand all' is visible. Below the text are four gray rectangular buttons: 'FHE Applications', 'FHE Info Sources', 'FHE Conceptualization', and 'FHE Techniques'.

→ ↻ <https://csrc.nist.gov/projects/pec/fhe> ☆ 🔍 Search

Fully-Homomorphic Encryption

Fully-Homomorphic Encryption (FHE) is a main tool of Privacy-Enhancing Cryptography (PEC), alongside with Multi-Party Computation ([MPC](#)), Zero-Knowledge Proofs ([ZKP](#)), Private-Set Intersection (PSI), and [others](#). The NIST [PEC project](#) is accompanying FHE developments and initiatives toward future useful standards.

[+ expand all](#)

- [FHE Applications](#)
- [FHE Info Sources](#)
- [FHE Conceptualization](#)
- [FHE Techniques](#)

A “list” of many FHE applications?

Suggestion/challenge: Elaborate a “list” of 100 concrete FHE applications. Clarify:

- ▶ FHE “killer apps” in multiple areas: health, finances, gaming, crypto, AI, ...?
- ▶ Use cases *where we should be doing **X**, **achievable with FHE**, but we are not doing it because of lack of a standard, and that has the cost **Y** (loss of privacy, inefficiency, ...)*
- ▶ Use cases and development for the public good / with social responsibility.
- ▶ Uses “for the people”, e.g., support people’s agency over their privacy.

Would ease making a case for adoptability

Vision: Future NIST FHE Standard and Recommendations?

A reflection on how:

1. Would leverage a **community-developed standard**
2. Would be an **open/free document**
3. It might select a subset of possible parametrizations (per security level)
4. Would be facilitated by the **Threshold Call** analysis and emerging considerations
5. Would emerge from collaboration. Note: The Crypto Group can host visits and/or consider integrating guest researchers on FHE.

Thank you for your attention!

Emerging FHE: from Multiple Perspectives into a Clarifying Progress

Presented at **HES7**: 7th HomomorphicEncryption.org Standards Meeting 2024

October 13, 2024 @ Salt Lake City, USA — luis.brandao@nist.gov

Useful links

- ▶ **WPEC 2024 Webpage:** <https://csrc.nist.gov/events/2024/wpec2024>
- ▶ **PEC Website:** <https://csrc.nist.gov/projects/pec>
- ▶ **Subscribe to the PEC-Forum:** <https://csrc.nist.gov/projects/pec/email-list>

Page intentionally blank

Other NIST Series of Crypto Talks

- ▶ **NIST Crypto Reading Club:** crypto-club-questions@nist.gov

<https://csrc.nist.gov/projects/crypto-reading-club>



- ▶ **NIST PQC Seminar:** pqc-seminars@nist.gov

<https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline/pqc-seminars>



- ▶ **Special Topics on Privacy and Public Auditability:** pec-stppa@nist.gov

<https://csrc.nist.gov/projects/pec/stppa>



- ▶ (Upcoming) **Threshold Crypto Seminar:** threshold-crypto@nist.gov

Once the Threshold Call final version is released



See “Other NIST-hosted presentations/workshops” list at <https://csrc.nist.gov/projects/crypto-reading-club>