NIST's Views on Standardization of Advanced Cryptography

René Peralta (*)

ZKProof Policy @ DC

November 30th, 2023

(*) Thanks to Luis Brandao.

Outline

1. NIST
2. Advanced Cryptography: PEC
3. Advanced Cryptography: MPTS and ZK

(Slides will be publicly available)

Crypto = Cryptography. NIST = National Institute of Standards and Technology. PEC = Privacy-Enhancing Crytpography.

Outline

Crypto = Cryptography. NIST = National Institute of Standards and Technology. PEC = Privacy-Enhancing Crytpography.

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

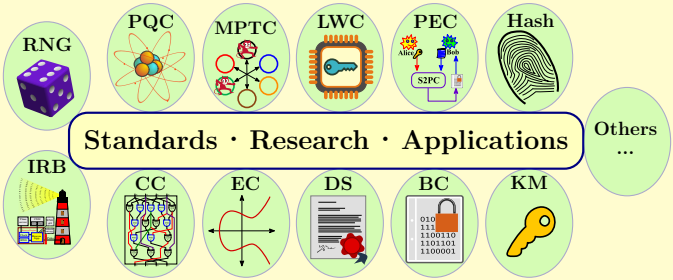
- **Non-regulatory** federal agency (@ U.S. Dept. Commerce)
- **Mission:** ... innovation ... industrial competitiveness ... measurement science, standards and technology, ... economic security ... quality of life.

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.*

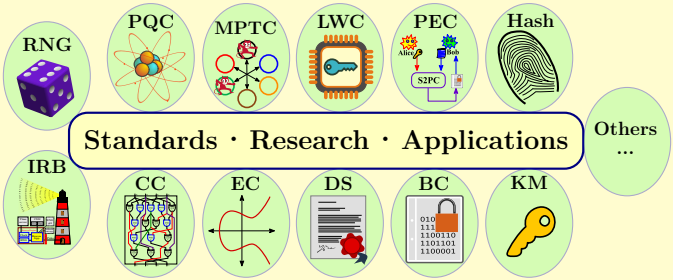
Activities in the “Crypto” Group



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 (denoting that the public NIST report was developed internally at NIST or in an interagency collaboration, respectively. **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

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 (denoting that the public NIST report was developed internally at NIST or in an interagency collaboration, respectively. **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

Outline

1. NIST
2. Advanced Cryptography: PEC
3. Advanced Cryptography: MPTS and ZK

Crypto = Cryptography. NIST = National Institute of Standards and Technology. PEC = Privacy-Enhancing Crytpography.

Advanced cryptography

- For our purposes, advanced cryptography refers to cryptographic techniques that go beyond encryption, hashing, digital signatures, and establishment of shared secret keys.

Advanced cryptography

- For our purposes, advanced cryptography refers to cryptographic techniques that go beyond encryption, hashing, digital signatures, and establishment of shared secret keys.
- There are many areas that fall within this category: ZKP, MPC, FHE, ...

Advanced cryptography

- For our purposes, advanced cryptography refers to cryptographic techniques that go beyond encryption, hashing, digital signatures, and establishment of shared secret keys.
- There are many areas that fall within this category: ZKP, MPC, FHE, ...
- Can NIST produce and maintain standards in all these areas? Do we have the resources?

Advanced cryptography

- For our purposes, advanced cryptography refers to cryptographic techniques that go beyond encryption, hashing, digital signatures, and establishment of shared secret keys.
- There are many areas that fall within this category: ZKP, MPC, FHE, ...
- Can NIST produce and maintain standards in all these areas? Do we have the resources?
- What are the risks?

Advanced cryptography

- For our purposes, advanced cryptography refers to cryptographic techniques that go beyond encryption, hashing, digital signatures, and establishment of shared secret keys.
- There are many areas that fall within this category: ZKP, MPC, FHE, ...
- Can NIST produce and maintain standards in all these areas? Do we have the resources?
- What are the risks?
- Which of these techniques are mature enough for standards?

Advanced cryptography

- For our purposes, advanced cryptography refers to cryptographic techniques that go beyond encryption, hashing, digital signatures, and establishment of shared secret keys.
- There are many areas that fall within this category: ZKP, MPC, FHE, ...
- Can NIST produce and maintain standards in all these areas? Do we have the resources?
- What are the risks?
- Which of these techniques are mature enough for standards?
- Should we be pursuing new standards for **quantum-breakable** primitives?

Privacy-Enhancing Cryptography (PEC): NIST Project

Cryptography used to **enhance privacy**.

Privacy-Enhancing Cryptography (PEC): NIST Project

Cryptography used to **enhance privacy**.

Goals:

1. Accompany the progress of **emerging *PEC tools***.

ZKP	**MPC**	**FHE**	**PSI**	**GRS**	**FnE**	**PIR**	**StE**
Zero- **K**nowledge **P**roofs	(**S**ecure) **M**ultiparty **C**omputation	**F**ully **H**omomorphic **E**ncryption	**P**rivate **S**et **I**ntersection	**G**roup and **R**ing **S**ignatures	**Fun**ctional **E**ncryption (Inc. ABE & IBE)	**P**rivate **I**nformation **R**etrieval	**St**ructured **E**ncryption (Symm./Pub.)

Legend: ABE: attribute-based encryption. IBE: identity-based encryption. Inc.: including. PEC: privacy-enhancing cryptography. Symm./pub.: symmetric-key or public-key based.

Privacy-Enhancing Cryptography (PEC): NIST Project

Cryptography used to **enhance privacy**.

Goals:

1. Accompany the progress of **emerging *PEC tools***.
2. Promote development of PEC **reference material**.

PEC tools
STPPA (series of talks)
PEC use-case suite
Threshold schemes
ZKProof collaboration
Encounter metrics
Email list (PEC Forum)

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

ZKP	**MPC**	**FHE**	**PSI**	**GRS**	**FnE**	**PIR**	**StE**
Zero- **K**nowledge **P**roofs	(**S**ecure) **M**ultiparty **C**omputation	**F**ully **H**omomorphic **E**ncryption	**P**rivate **S**et **I**ntersection	**G**roup and **R**ing **S**ignatures	**Fun**ctional **E**ncryption (Inc. ABE & IBE)	**P**rivate **I**nformation **R**etrieval	**St**ructured **E**ncryption (Symm./Pub.)

Legend: ABE: attribute-based encryption. IBE: identity-based encryption. Inc.: including. PEC: privacy-enhancing cryptography. Symm./pub.: symmetric-key or public-key based.

Privacy-Enhancing Cryptography (PEC): NIST Project

Cryptography used to **enhance privacy**.

Goals:

1. Accompany the progress of **emerging *PEC tools***.
2. Promote development of PEC **reference material**.
3. **Exploratory work** to assess potential for recommendations, standardization; ...

PEC tools
STPPA (series of talks)
PEC use-case suite
Threshold schemes
ZKProof collaboration
Encounter metrics
Email list (PEC Forum)

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

ZKP	**MPC**	**FHE**	**PSI**	**GRS**	**FnE**	**PIR**	**StE**
Zero- **K**nowledge **P**roofs	(**S**ecure) **M**ultiparty **C**omputation	**F**ully **H**omomorphic **E**ncryption	**P**rivate **S**et **I**ntersection	**G**roup and **R**ing **S**ignatures	**Fu**nctional **E**ncryption (Inc. ABE & IBE)	**P**rivate **I**nformation **R**etrieval	**St**ructured **E**ncryption (Symm./Pub.)

Legend: ABE: attribute-based encryption. IBE: identity-based encryption. Inc.: including. PEC: privacy-enhancing cryptography. Symm./pub.: symmetric-key or public-key based.

When is it time to standardize a technology?

- Let the market speak?

When is it time to standardize a technology?

- Let the market speak?
- Ask industry?

When is it time to standardize a technology?

- Let the market speak?
- Ask industry?
- Ask academia?

When is it time to standardize a technology?

- Let the market speak?
- Ask industry?
- Ask academia?
- Let stakeholders state their needs?

When is it time to standardize a technology?

- Let the market speak?
- Ask industry?
- Ask academia?
- Let stakeholders state their needs?
- Wait for the killer application to show up?

When is it time to standardize a technology?

- Let the market speak?
- Ask industry?
- Ask academia?
- Let stakeholders state their needs?
- Wait for the killer application to show up?
- Let NIST decide on an ad-hoc basis?

When is it time to standardize a technology?

- Let the market speak?
- Ask industry?
- Ask academia?
- Let stakeholders state their needs?
- Wait for the killer application to show up?
- Let NIST decide on an ad-hoc basis?

I think "all of the above" is the right approach. But this requires NIST being able to read these external gauges.

When is it time to standardize a technology?

- Let the market speak?
- Ask industry?
- Ask academia?
- Let stakeholders state their needs?
- Wait for the killer application to show up?
- Let NIST decide on an ad-hoc basis?

I think "all of the above" is the right approach. But this requires NIST being able to read these external gauges. An alternative: "do not lead, follow other standard development organizations".

Outline

1. NIST
2. Advanced Cryptography: PEC
3. Advanced Cryptography: MPTS and ZK

Crypto = Cryptography. NIST = National Institute of Standards and Technology. PEC = Privacy-Enhancing Crytpography.

Process

- **Goals**
  - Collect and curate reference material.
  - Devise recommendations.
  - Gain trust through transparency.
- **Not a competition**
- **Ample room for participation:** Give feedback $\rightarrow$ Submit $\rightarrow$ Analyze

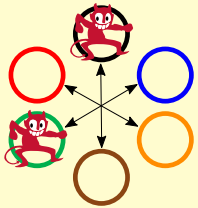
NIST Call for Multi-Party Threshold Schemes

- NISTIR 8214C: Initial public **draft** (**Jan 2023**) $\Rightarrow$ Revised version (**late 2023**).
- Submission deadline (expected $\approx$ **2nd-half 2024**)

NIST Call for Multi-Party Threshold Schemes

- NISTIR 8214C: Initial public **draft** (**Jan 2023**) ⇒ Revised version (**late 2023**).
- Submission deadline (expected ≈ **2nd-half 2024**)

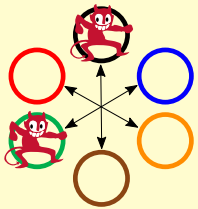
Calling for submissions of threshold schemes



(And gadgets for modular use)

NIST Call for Multi-Party Threshold Schemes

- NISTIR 8214C: Initial public **draft** (**Jan 2023**) ⇒ Revised version (**late 2023**).
- Submission deadline (expected ≈ **2nd-half 2024**)



Calling for submissions of threshold schemes for:

- **[Cat1] Selected NIST-standardized primitives**
- **[Cat2] Other primitives (including FHE, IBE/ABE, ZKP)**

  (And gadgets for modular use)

FHE = Fully-homomorphic encryption.
IBE/ABE = Identity/Attribute-based encryption.
ZKP = Zero-knowledge proof.

Ongoing work on Zero-Knowledge Proofs

Engagement with ZKProof

- Since 2019: Contribution to Community Reference document.
- Since 2019: Participation in the ZKProof Editors team
- Since 2023: Participation in the ZKProof Standards Committee

The **"NIST Threshold Call"** has a **ZKP subcategory**.

- Focused on **ZKPs of knowledge** of secret keys ...
- ... but we expect ZKP submissions to be applicable to broader use-cases
- Submission deadline will be set to 2nd semester of 2024

Thank you!

NIST's Views on Standardization of Advanced Cryptography

Presented at ZKProof Policy @ DC | November 30th @ Washington DC (USA)

PEC team: peralta@nist.gov, luis.brandao@nist.gov, angela.robinson@nist.gov

Threshold Call (Draft)

MPTS 2023 (Sept. 26–28)

MPTC-Forum (email list)

PEC-Forum (email list)