Emerging Advanced Cryptography
Opportunities and Challenges

Presented* at

The Future Cryptography Conference

May 21, 2025 | Tallinn (Estonia)

* Luís Brandão: NIST Associate (Foreign Guest Researcher†, Contractor from Strativia). Expressed opinions are from the speaker.
†Cryptographic Technology Group, Information Technology Laboratory, (United States) National Institute of Standards and Technology (NIST).

About this Presentation

1. **Aitäh** kutse esst esinema @ The `Future Cryptography` Conference

   Thank you for the invitation

About this Presentation

1. **Aitäh** kutse esst esinema @ The `Future Cryptography` Conference
   Thank you for the invitation
2. **Goals:**
   2.1 Provide an intro/context about NIST (crypto)*
   2.2 Disseminate the Threshold Call (an expedition into advanced cryptography)
   2.3 Suggest a few topics of anticipated interest

* Disclaimer: I'm at NIST as a Foreign Guest Researcher (non-employee), Contractor from Strativia

About this Presentation

1. **Aitäh** kutse esst esinema @ The `Future Cryptography` Conference
   Thank you for the invitation
2. **Goals:**
   2.1 Provide an intro/context about NIST (crypto)*
   2.2 Disseminate the Threshold Call (an expedition into advanced cryptography)
   2.3 Suggest a few topics of anticipated interest
3. The slide-deck will be available

* Disclaimer: I'm at NIST as a Foreign Guest Researcher (non-employee), Contractor from Strativia

Outline

1. Intro on NIST Crypto
2. Threshold Call and related explorations
3. Thoughts on (Emerging?) Opportunities and Challenges

Outline

National Institute of Standards and Technology

- **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)

National Institute of Standards and Technology

- **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 ($\approx 7 \times 10^3$ staff):** Laboratories $\rightarrow$ Divisions $\rightarrow$ Groups

National Institute of Standards and Technology

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

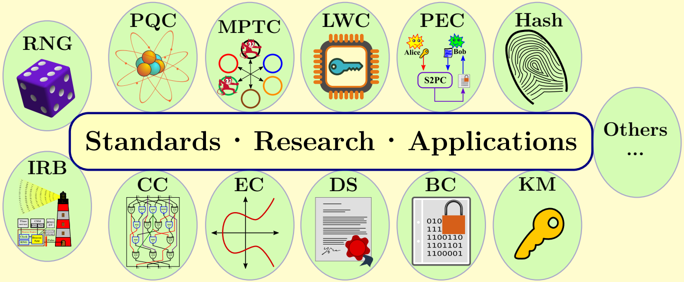
NIST name and address plate (source: nist.gov)

- **NIST ($\approx 7 \times 10^3$ staff):** Laboratories $\rightarrow$ Divisions $\rightarrow$ Groups

ITL INFORMATION TECHNOLOGY LABORATORY $\rightarrow$ **Computer Security Division (CSD)**

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

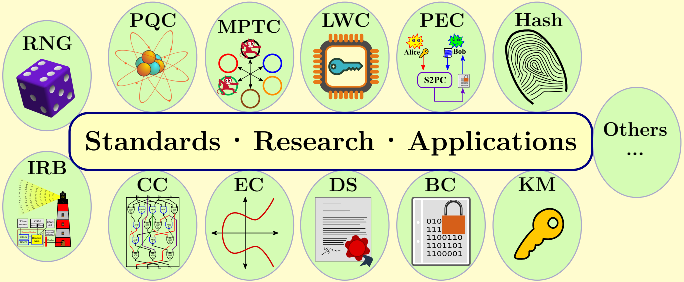
Activities in the “Crypto” Group



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. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**rypto). **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.

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

Activities in the “Crypto” Group

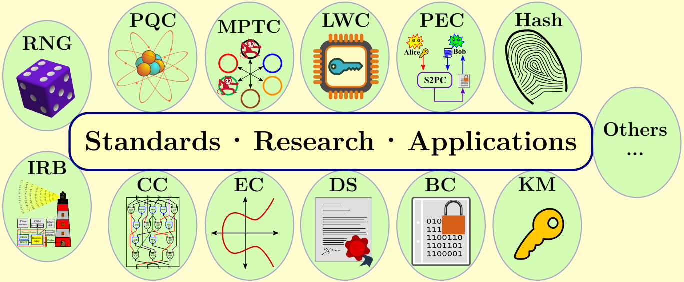


- **Public documentation:** FIPS; Special Publications (SP 800); NIST Reports (IR).
- **International cooperation:** government, industry, academia, standardization bodies.

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. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**rypto). **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.

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

Activities in the "Crypto" Group



Example recent publications:

- FIPS 202/3/4/...: PQC standards
- SP 800-232: Lightweight Crypto
- SP 800-227: KEM recommendations
- IR 8547: PQC transition
- IR 8214C: Threshold Call
- IR 8552: Accordion requirements

- **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. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**rypto). **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** = **Sp**ecial **P**ublications in Computer Security.

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

A variety of NIST Crypto Projects

- **PQC:** [standardization] "**post-quantum**" signatures and key-encapsulation
- **LWC:** [standardization] "**lightweight**" authenticated encryption, hash, XOF

Legend: **LWC** = **L**ight**w**eight **C**ryptography. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**ryptography. **PEC** = **P**rivacy-**E**nhancing **C**ryptography. **PQC** = **P**ost-**Q**uantum **C**ryptography. **XOF** = e**X**tendable **O**utput **F**unction.

A variety of NIST Crypto Projects

- **PQC:** [standardization] "**post-quantum**" signatures and key-encapsulation
- **LWC:** [standardization] "**lightweight**" authenticated encryption, hash, XOF
- **PEC:** [exploratory] "**privacy-enhancing**" (advanced) features/functionalities
- **MPTC:** [exploratory] "**multi-party threshold**" schemes for crypto primitives
- **...** various others: https://www.nist.gov/itl/csd/cryptographic-technology

Legend: **LWC** = **L**ight**w**eight **C**ryptography. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**ryptography. **PEC** = **P**rivacy-**E**nhancing **C**ryptography. **PQC** = **P**ost-**Q**uantum **C**ryptography. **XOF** = e**X**tendable **O**utput **F**unction.

A variety of NIST Crypto Projects

- **PQC:** [standardization] "**post-quantum**" signatures and key-encapsulation
- **LWC:** [standardization] "**lightweight**" authenticated encryption, hash, XOF
- **PEC:** [exploratory] "**privacy-enhancing**" (advanced) features/functionalities
- **MPTC:** [exploratory] "**multi-party threshold**" schemes for crypto primitives
- **...** various others: https://www.nist.gov/itl/csd/cryptographic-technology

There is a vast area for developments in both Standardization and Exploratory projects

Legend: **LWC** = **L**ightweight **C**ryptography. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**ryptography. **PEC** = **P**rivacy-**E**nhancing **C**ryptography. **PQC** = **P**ost-**Q**uantum **C**ryptography. **XOF** = e**X**tendable **O**utput **F**unction.

Outline

1. Intro on NIST Crypto
2. Threshold Call and related explorations
3. Thoughts on (Emerging?) Opportunities and Challenges

Multi-Party Threshold Cryptography: NIST Project

Cryptographic primitives:


Signing

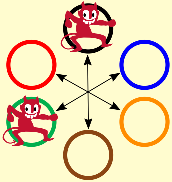
Encryption


KeyGen


Hashing

etc.

Threshold schemes (for cryptographic primitives):



https://csrc.nist.gov/projects/threshold-cryptography

Multi-Party Threshold Cryptography: NIST Project

Cryptographic primitives:


Signing

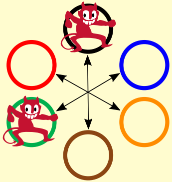

Encryption


KeyGen


Hashing

etc.

Threshold schemes (for cryptographic primitives):



1. Split (**secret-share**) the secret/private-key across multiple parties.
2. Use **MPC** to perform needed operation (with split key), e.g., sign.

   (MPC = secure multiparty computation ... or call it "Threshold Cryptography")

https://csrc.nist.gov/projects/threshold-cryptography

Multi-Party Threshold Cryptography: NIST Project

Cryptographic primitives:


Signing

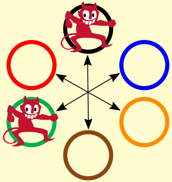
Encryption


KeyGen


Hashing

etc.

Threshold schemes (for cryptographic primitives):



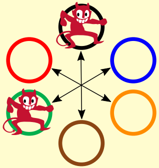
1. Split (**secret-share**) the secret/private-key across multiple parties.
2. Use **MPC** to perform needed operation (with split key), e.g., sign.
   (MPC = secure multiparty computation ... or call it "Threshold Cryptography")

- **"Threshold" (f):** Operation is secure if number of corrupted parties is $\leq f$.
- **Decentralized** trust about key **(not reconstructed)**: avoids single-point of failure.

https://csrc.nist.gov/projects/threshold-cryptography

The NIST Call for *Multi-Party Threshold Schemes*

A public call for input, to form a body of reference material:

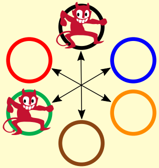


- It deals with **threshold** schemes
- It stands at the **threshold** of advanced cryptography

The NIST Call for *Multi-Party Threshold Schemes*

A public call for input, to form a body of reference material:

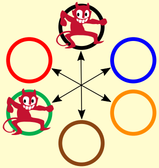
- It deals with **threshold** schemes
- It stands at the **threshold** of advanced cryptography



Fits in the **"Reference Materials"** approach of the **exploratory** NIST projects on Privacy-Enhancing Cryptography (PEC) and Multi-Party Threshold Cryptography (MPTC).

The NIST Call for *Multi-Party Threshold Schemes*

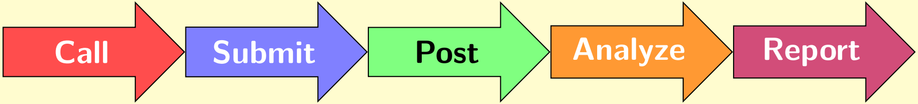
A public call for input, to form a body of reference material:



- It deals with **threshold** schemes
- It stands at the **threshold** of advanced cryptography

Fits in the **“Reference Materials”** approach of the **exploratory** NIST projects on Privacy-Enhancing Cryptography (PEC) and Multi-Party Threshold Cryptography (MPTC).

Establishes a process: (not a competition for selection of a standard)



A scope organized into two classes

- **Class N: <u>N</u>IST-standardized primitives** (Sign, PKE, Symm, KeyGen)

  KeyGen = Key Generation; PKE = Public-Key Encryption; Symm = Symmetric

- **Class S: <u>S</u>pecial others** (those above; FHE, ZKPoK, Gadgets)

  FHE = Fully-Homomorphic Encryption; ZKP = Zero-Knowledge Proof

A scope organized into two classes

- **Class N: NIST-standardized primitives** (Sign, PKE, Symm, KeyGen)

  KeyGen = Key Generation; PKE = Public-Key Encryption; Symm = Symmetric

- **Class S: Special others** (those above; FHE, ZKPoK, Gadgets)

  FHE = Fully-Homomorphic Encryption; ZKP = Zero-Knowledge Proof

Each class is organized into various categories

	Sign	PKE	Symmetric	KeyGen	**FHE**	**ZKPoK**	**Gadgets**
NIST specified	N1	N2	N3	N4			
Special others	S1	S2	S3	S4	**S5**	**S6**	**S7**

(Using the notation updated in the 2nd public draft)

Phases and Deadlines

* (Public comments due by 2025-May-30)

Phase	Subphase	Required?	When
0. Call	0.1: Public Drafts (1st and 2nd*)	—	2023/2025
	0.2: Final version	**Yes**	X_0

Phases and Deadlines

* (Public comments due by 2025-May-30)

Phase	Subphase	Required?	When
0. Call	0.1: Public Drafts (1st and 2nd*)	—	2023/2025
	0.2: Final version	**Yes**	X_0
1. Previews	1.1: Preview 1	Encouraged	$X_1 \gtrsim X_0 + 2$
	1.2: Preview 2	Encouraged	$X_2 \gtrsim X_1 + 3$

- **Preview:** abstract of a planned submission, followed by public presentation

Phases and Deadlines

* (Public comments due by 2025-May-30)

Phase	Subphase	Required?	When
0. Call	0.1: Public Drafts (1st and 2nd*)	—	2023/2025
	0.2: Final version	**Yes**	X_0
1. Previews	1.1: Preview 1	Encouraged	$X_1 \gtrsim X_0 + 2$
	1.2: Preview 2	Encouraged	$X_2 \gtrsim X_1 + 3$
2. Packages	2.1: Preliminary submission	Encouraged	$X_3 \gtrsim X_2 + 1$
	2.2: Regular submission	**Yes**	$X_4 \gtrsim X_3 + 2$ $\gtrsim X_0 + 8$

- **Preview:** abstract of a planned submission, followed by public presentation
- **Package:** specification, implementation, experimental evaluation

Phases and Deadlines

* (Public comments due by 2025-May-30)

Phase	Subphase	Required?	When
0. Call	0.1: Public Drafts (1st and 2nd*)	—	2023/2025
	0.2: Final version	**Yes**	X_0
1. Previews	1.1: Preview 1	Encouraged	$X_1 \gtrsim X_0 + 2$
	1.2: Preview 2	Encouraged	$X_2 \gtrsim X_1 + 3$
2. Packages	2.1: Preliminary submission	Encouraged	$X_3 \gtrsim X_2 + 1$
	2.2: Regular submission	**Yes**	$X_4 \gtrsim X_3 + 2$ $\gtrsim X_0 + 8$
3. Analysis	3.1: Public presentations	**Yes**	2026
	3.2: Package updates	—	—
	3.3: NIST-MPTC report	**Yes**	($\approx$ 2027)

- **Preview:** abstract of a planned submission, followed by public presentation
- **Package:** specification, implementation, experimental evaluation
- **Analysis:** including series of presentations

Other notes on exploratory activities

MPTS 2025

- **NIST Workshop on Multi-Party Threshold Scheme 2025**
- Fully virtual, **2025-{Oct or Nov}** (exact dates TBA)
- Will host the "1st Previews" (plans) of Threshold Call submissions

Other notes on exploratory activities

MPTS 2025

- **NIST Workshop on Multi-Party Threshold Scheme 2025**
- Fully virtual, **2025-{Oct or Nov}** (exact dates TBA)
- Will host the "1st Previews" (plans) of Threshold Call submissions

PEC Project

- Accompany the progress of emerging Privacy-Enhancing Cryptography
- In scope: MPC, FHE, ZKP, PSI, PIR, Special Sigs, ...
- Special Topics on Privacy Enhancing Cryptography (STPPA) series

FHE = Fully-Homomorphic Encryption. MPC = (Secure) Multi-Party Computation. PIR = Private Information Retrieval. PSI = Private Set Intersection. ZKP = Zero-Knowledge Proof.

Other notes on exploratory activities

MPTS 2025

- **NIST Workshop on Multi-Party Threshold Scheme 2025**
- Fully virtual, **2025-{Oct or Nov}** (exact dates TBA)
- Will host the "1st Previews" (plans) of Threshold Call submissions

PEC Project

- Accompany the progress of emerging Privacy-Enhancing Cryptography
- In scope: MPC, FHE, ZKP, PSI, PIR, Special Sigs, ...
- Special Topics on Privacy Enhancing Cryptography (STPPA) series

FHE = Fully-Homomorphic Encryption. MPC = (Secure) Multi-Party Computation. PIR = Private Information Retrieval. PSI = Private Set Intersection. ZKP = Zero-Knowledge Proof.

Past Events

- WPEC 2024: Workshop on Privacy-Enhancing Cryptography 2024
- MPTS 2023: Workshop on Multi-Party Threshold Schemes 2023
- Many other diverse set of talks at the NIST Crypto Reading Club

Outline

1. Intro on NIST Crypto

2. Threshold Call and related explorations

3. Thoughts on (Emerging?) Opportunities and Challenges

The NIST Stone Test Wall (thinking about the future)

Photo in 2018

Photo in 1948

"*Constructed [in **1948**] to study the **performance of stone subjected to weathering**. It contains 2352 individual samples of stone, of which 2032 are domestic stone from 47 [U.S.] states, and 320 are stones from 16 foreign countries.*"

https://www.nist.gov/el/materials-and-structural-systems-division-73100/nist-stone-wall

The NIST Stone Test Wall (thinking about the future)

Photo in 2018 Photo in 1948

"*Constructed [in **1948**] to study the **performance of stone subjected to weathering**. It contains 2352 individual samples of stone, of which 2032 are domestic stone from 47 [U.S.] states, and 320 are stones from 16 foreign countries.*"

https://www.nist.gov/el/materials-and-structural-systems-division-73100/nist-stone-wall

How about crypto building blocks?

Signing

Encryption

KeyGen

Hashing

RNG

...

The NIST Stone Test Wall (thinking about the future)

Photo in 2018

Photo in 1948

*"Constructed [in **1948**] to study the **performance of stone subjected to weathering**. It contains 2352 individual samples of stone, of which 2032 are domestic stone from 47 [U.S.] states, and 320 are stones from 16 foreign countries."*

https://www.nist.gov/el/materials-and-structural-systems-division-73100/nist-stone-wall

How about crypto building blocks? Signing Encryption KeyGen Hashing RNG . . .

- Which of **today's crypto standards** will remain valid ≈ 75 years from now?
- Which **new blocks** should we develop/standardize to enable good crypto walls?
- Which **walls** (complex compositions) can be safely created out of building blocks?

The NIST Stone Test Wall (thinking about the future)

Photo in 2018

Photo in 1948

"Constructed [in ***1948****] to study the* ***performance of stone subjected to weathering****. It contains 2352 individual samples of stone, of which 2032 are domestic stone from 47 [U.S.] states, and 320 are stones from 16 foreign countries."*

https://www.nist.gov/el/materials-and-structural-systems-division-73100/nist-stone-wall

How about crypto building blocks?

Signing

Encryption

KeyGen

Hashing

RNG

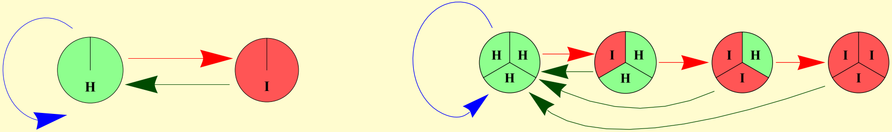
. . .

- Which of **today's crypto standards** will remain valid ≈ 75 years from now?
- Which **new blocks** should we develop/standardize to enable good crypto walls?
- Which **walls** (complex compositions) can be safely created out of building blocks?

... And what ***crypto weather*** do we need to be prepared for?

Reliability of long-lived threshold systems?

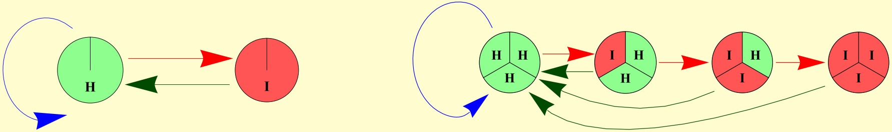
Intrusion models with proactive recovery:



Legend: H = healthy; I = intruded. Diagrams from doi:10.1007/s13173-012-0062-x

Reliability of long-lived threshold systems?

Intrusion models with proactive recovery:



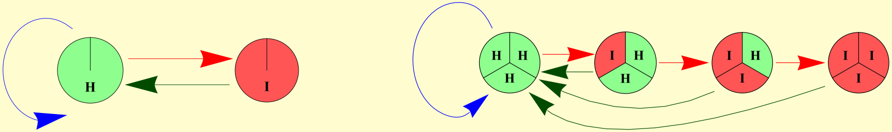
Legend: H = healthy; I = intruded. Diagrams from doi:10.1007/s13173-012-0062-x

What happens in settings of continued intrusion?

- In the long-run, larger attack surface may imply larger probability of global compromise
- Mitigation: identifiable abort, proactive rejuvenation (e.g., secret-**re**sharing)

Reliability of long-lived threshold systems?

Intrusion models with proactive recovery:



Legend: H = healthy; I = intruded. Diagrams from doi:10.1007/s13173-012-0062-x

What happens in settings of continued intrusion?

- In the long-run, larger attack surface may imply larger probability of global compromise
- Mitigation: identifiable abort, proactive rejuvenation (e.g., secret-**re**sharing)

Important to assess: Is a proposed system suitable for a deployment setting?

Trust versus trustworthiness

It is important to match **trust** with **trustworthiness**

Trust versus trustworthiness

It is important to match **trust** with **trustworthiness**

- Decrease **trust** requirements, by clever use of advanced crypto, e.g.:
  - MPC allows collaboration while avoiding "sharing" unneeded data
  - ZKP allows verifying correct behavior of another party
  - FHE allows delegating computation (with data-confidentiality)

Trust versus trustworthiness

It is important to match **trust** with **trustworthiness**

- Decrease **trust** requirements, by clever use of advanced crypto, e.g.:
  - MPC allows collaboration while avoiding “sharing” unneeded data
  - ZKP allows verifying correct behavior of another party
  - FHE allows delegating computation (with data-confidentiality)
- Increase **trustworthiness**, e.g., via:
  - Standardization process and verified specification
  - Validation/certification of implementations

Other brief notes

Validation	**Known-answer test (KAT) / test-vectors?** How to deal with: ▶ **Non-determinism** in distributed systems? ▶ **Floating**-point operations? (different results across compilers/processors) ▶ Combinatorial explosion of parametrizations

Related: Check the NIST Cryptographic Algorithm Validation Program (CAVP)

Other brief notes

Validation

Known-answer test (KAT) / test-vectors? How to deal with:

- **Non-determinism** in distributed systems?
- **Floating**-point operations? (different results across compilers/processors)
- Combinatorial explosion of parametrizations

Related: Check the NIST Cryptographic Algorithm Validation Program (CAVP)

QV/QR

Quantum-vulnerable (QV) / quantum-resistant (QR) solutions?

- Envisioned deprecation of QV (2035?)
- QV has good references for what to functionally achieve as QR
- In the future, which settings may remain suitable for QV?

Concluding remarks

1. **Advanced** crypto $\overset{?}{\Rightarrow}$ advanced processes for standardization/certification
2. **Threshold Call:** an approach for exploring advanced crypto (prior to standards)
3. **Aim:** Devise recommendations about advanced cryptography (PEC + MPTC)
   (Will support future processes.) PEC = Privacy-Enhancing Crypto. MPTC = Multi-Party Threshold Crypto
4. **Ample room for participation:** Give feedback $\rightarrow$ Submit $\rightarrow$ Analyze
5. **Privacy-preserving applications:** a key space for adoption of Future Crypto
6. **MPTS 2025:** Participate (virtual event) to hear/speak thorougher elaborations

Tänan tähelepanu eest!

Thank you for your attention!

Questions?

PEC Project **MPTC Project** **Threshold Call**

Subscribe to the PEC-Forum and MPTC-Forum to receive announcements.

Emerging Advanced Cryptography: Opportunities and Challenges

Presented at The Future Cryptography Conference

May 21, 2025 @ Tallinn (Estonia) — luis.brandao@nist.gov