Cryptography Endeavors at NIST
Standardization and Beyond

Presented* at Portugal Crypto Day 2024

December 13, 2024 | Lisboa (Portugal)

* **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. **Obrigado** pelo convite para apresentar @ Portugal Crypto Day 2024

   Thank you for the invitation

About this Presentation

1. **Obrigado** pelo convite para apresentar @ Portugal Crypto Day 2024

   Thank you for the invitation

2. **Goals:**

   2.1 Convey a NIST-related perspective* of working with Crypto

   2.2 Disseminate some of the ongoing crypto projects

   2.3 Convey openness to collaboration and public feedback

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

About this Presentation

1. **Obrigado** pelo convite para apresentar @ Portugal Crypto Day 2024

   Thank you for the invitation

2. **Goals:**

   2.1 Convey a NIST-related perspective* of working with Crypto

   2.2 Disseminate some of the ongoing crypto projects

   2.3 Convey openness to collaboration and public feedback

3. The slide-deck will be **publicly available** (via the organizers)

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

Outline

1. Intro on NIST Crypto
2. The PEC and MPTC Projects
3. The Threshold Call
4. Notes on Interaction

MPTC = Multi-Party Threshold Cryptography.
NIST = National Institute of Standards and Technology.
PEC = Privacy-Enhancing Cryptography.

Outline

MPTC = Multi-Party Threshold Cryptography.
NIST = National Institute of Standards and Technology.
PEC = Privacy-Enhancing Cryptography.

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 (≈ 7000 persons):** 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.

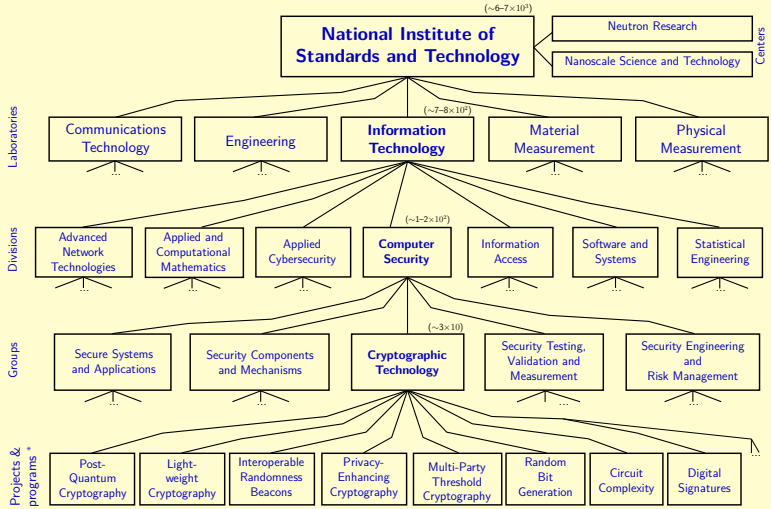
NIST name and address plate (source: nist.gov)

- **NIST (≈ 7000 persons):** Laboratories $\rightarrow$ Divisions $\rightarrow$ Groups

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.*

The Crypto Group within the NIST organization



* (Some projects / programs involve various groups, divisions or labs.)

(in parenthesis: estimate of approximate number of people, inc. employees and associates)

The NIST Stone Test Wall

Photo in 2018

"*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 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

Photo in 2018

"*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 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

Photo in 2018

"*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 states, and 320 are stones from 16 foreign countries.*"

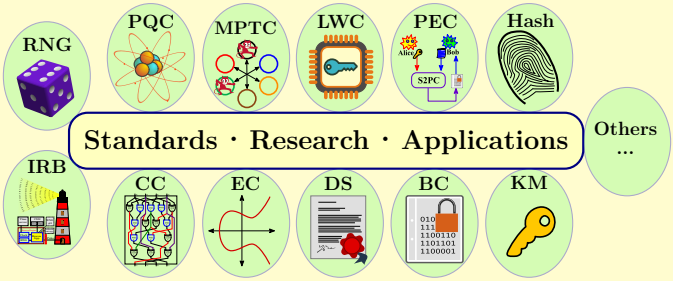
https://www.nist.gov/el/materials-and-structural-systems-division-73100/nist-stone-wall

How about crypto building blocks:

Signing 
Encryption 
KeyGen 
Hashing 
RNG 

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

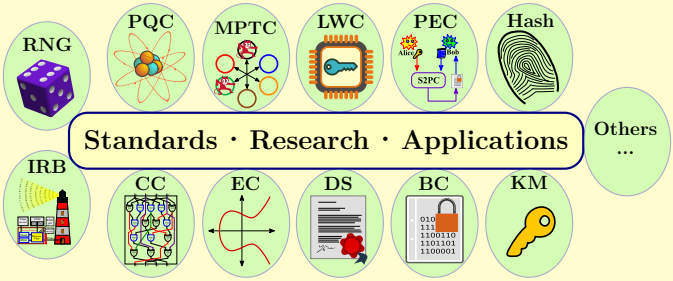
Activities in the “Crypto” Group



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** = Multi-Party **T**hreshold **C**rypto). **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.

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**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.

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

Recent/ongoing "competition-like" projects/processes

PQC = Post-Quantum Cryptography

(Digital signatures and public-key encryption)

- **Withstand future quantum computers**
- 2016: Call for algorithms (received 82)
- 2024: Standards: FIPS 203, 204, 205
- More standards upcoming
- Migration to PQC is a huge effort

https://csrc.nist.gov/projects/post-quantum-cryptography

Recent/ongoing "competition-like" projects/processes

PQC = Post-Quantum Cryptography

(Digital signatures and public-key encryption)

- **Withstand future quantum computers**
- 2016: Call for algorithms (received 82)
- 2024: Standards: FIPS 203, 204, 205
- More standards upcoming
- Migration to PQC is a huge effort

https://csrc.nist.gov/projects/post-quantum-cryptography

LWC = Lightweight Cryptography

(Authenticated encryption and others)

- **Primitives for constrained devices**
- 2018: Call for algorithms (received 57)
- 2024: Draft standard: SP 800-232 ipd
- AEAD = **A**uth. **E**nc. w/ **A**ssoc. **D**ata
- XOF = E**x**tendable **O**utput **F**unction

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

Recent/ongoing "competition-like" projects/processes

PQC = Post-Quantum Cryptography

(Digital signatures and public-key encryption)

- **Withstand future quantum computers**
- 2016: Call for algorithms (received 82)
- 2024: Standards: FIPS 203, 204, 205
- More standards upcoming
- Migration to PQC is a huge effort

https://csrc.nist.gov/projects/post-quantum-cryptography

LWC = Lightweight Cryptography

(Authenticated encryption and others)

- **Primitives for constrained devices**
- 2018: Call for algorithms (received 57)
- 2024: Draft standard: SP 800-232 ipd
- AEAD = **A**uth. **E**nc. w/ **A**ssoc. **D**ata
- XOF = E**x**tendable **O**utput **F**unction

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

Multi-year efforts, with intense public/community participation ⇒ New standards

A variety of NIST Crypto Projects

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

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.

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**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.

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

MPTC = Multi-Party Threshold Cryptography.
NIST = National Institute of Standards and Technology.
PEC = Privacy-Enhancing Cryptography.

Privacy-Enhancing Cryptography (PEC): NIST Project

Cryptography usable to **enhance privacy**

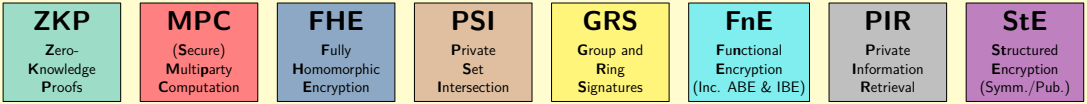
(emphasis on non-standardized tools)

Privacy-Enhancing Cryptography (PEC): NIST Project

Cryptography usable to **enhance privacy**
(emphasis on non-standardized tools)

Goals:

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



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

Privacy-Enhancing Cryptography (PEC): NIST Project

Cryptography usable to **enhance privacy**
(emphasis on non-standardized tools)

Goals:

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

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.)

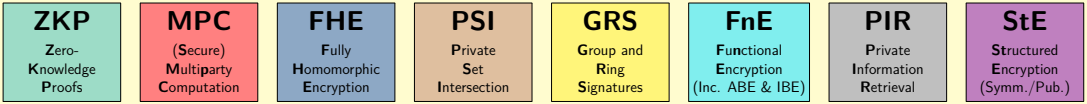
Legend: ABE: attribute-based encryption. IBE: identity-based encryption. PEC: privacy-enhancing cryptography. Symm./pub.: symmetric-key or public-key based.

Privacy-Enhancing Cryptography (PEC): NIST Project

Cryptography usable to **enhance privacy**
(emphasis on non-standardized tools)

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, ...



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

Privacy-Enhancing Cryptography (PEC): NIST Project

Cryptography usable to **enhance privacy**
(emphasis on non-standardized tools)

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
Fully-Homomophic Encryption (FHE)
Zero-Knowledge Proof (ZKP)
Multi-Party Computation (MPC)
STPPA (Series of Talks)
PEC Use-Case Suite
Encounter Metrics
Email List (PEC Forum)

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

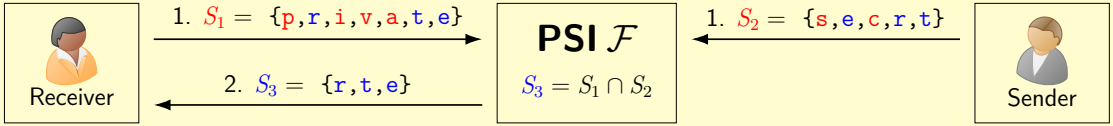
ZKP	MPC	FHE	PSI	GRS	FnE	PIR	StE
Zero-Knowledge Proofs	(Secure) Multiparty Computation	Fully Homomorphic Encryption	Private Set Intersection	Group and Ring Signatures	Functional Encryption (Inc. ABE & IBE)	Private Information Retrieval	Structured Encryption (Symm./Pub.)

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

One PEC example: Private-Set Intersection (PSI)

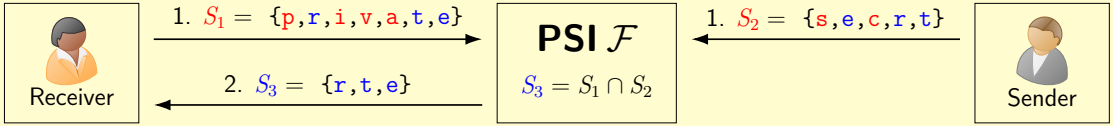
One PEC example: Private-Set Intersection (PSI)

Obtain the intersection of two sets, without disclosing the non-intersecting elements.



One PEC example: Private-Set Intersection (PSI)

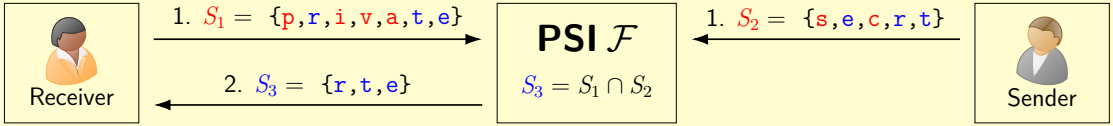
Obtain the intersection of two sets, without disclosing the non-intersecting elements.



(The middle box is an abstraction; there is no actual intermediary)

One PEC example: Private-Set Intersection (PSI)

Obtain the intersection of two sets, without disclosing the non-intersecting elements.

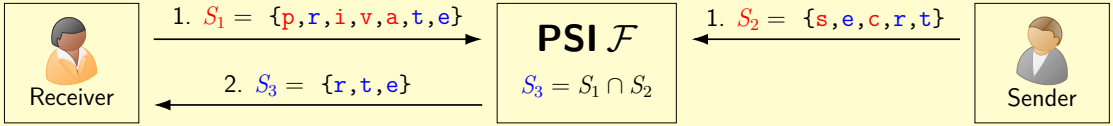


(The middle box is an abstraction; there is no actual intermediary)

- **Insecure:** Compare **hashes** (usual non-cryptographer's intuition)
- **Secure:** Compare **Oblivious-PRF** outputs (PRF = **P**seudo**r**andom **f**unction)

One PEC example: Private-Set Intersection (PSI)

Obtain the intersection of two sets, without disclosing the non-intersecting elements.



(The middle box is an abstraction; there is no actual intermediary)

- **Insecure:** Compare **hashes** (usual non-cryptographer's intuition)
- **Secure:** Compare **Oblivious-PRF** outputs (PRF = **P**seudo**r**andom **f**unction)

- **Generalizations:** Circuit-PSI (only learn $f(S_3)$), multi-party (≥ 2), ...
- Check "**The First PSI day**" organized within WPEC 2024 (NIST workshop)

Multi-Party Threshold Cryptography: NIST Project

Cryptographic primitives:


Signing

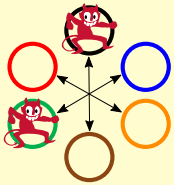
Encryption


KeyGen


Hashing

etc.

Threshold schemes (for cryptographic primitives):



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

Multi-Party Threshold Cryptography: NIST Project

Cryptographic primitives:


Signing

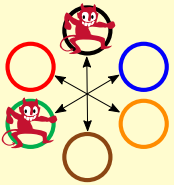
Encryption


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

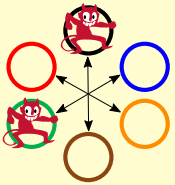

KeyGen


Hashing

etc.

Threshold schemes (for cryptographic primitives):

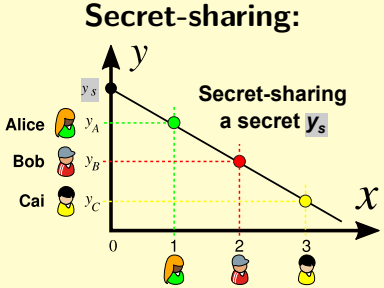
1. Split (**secret-share**) the secret/private-key across multiple parties.
2. Use **MPC** to perform needed operation (with split key), e.g., sign.
   (MPC = secure multiparty computation ... or call it "Threshold Cryptography")



- **"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

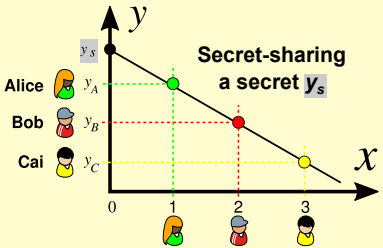
Basics of a Threshold Scheme



Splits the key into secret shares

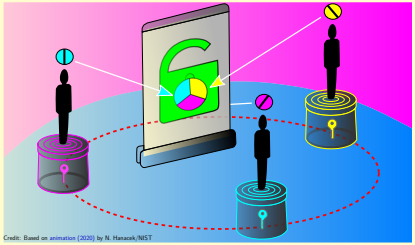
Basics of a Threshold Scheme

Secret-sharing:



Splits the key into secret shares

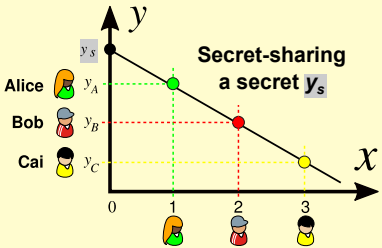
Multi-party computation (MPC)



Operates without recombining the key

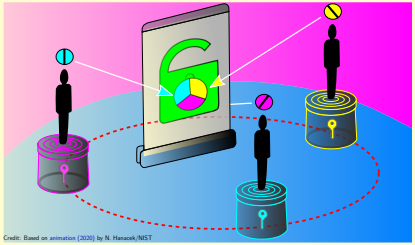
Basics of a Threshold Scheme

Secret-sharing:

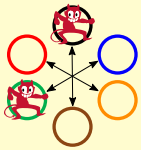


Splits the key into secret shares

Multi-party computation (MPC)



Operates without recombining the key

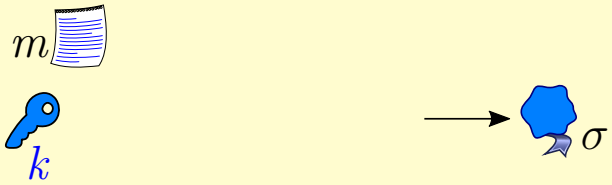


Participation threshold: the operation needs k parties in agreement

Corruption threshold: system secure even if f parties are malicious

Simple(st) example: Threshold n-of-n RSA signatures

Threshold signature (with $n = 3$):

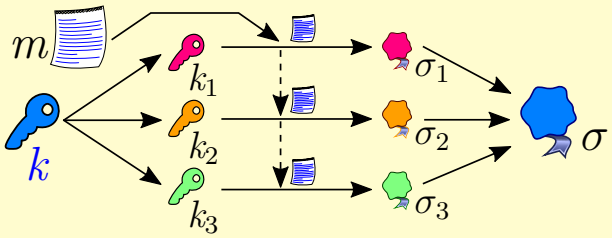


Textbook RSA:

- **Private** signing key: k
- **Priv.** $\phi = (p-1) \times (q-1)$
- **Public:** $N = p \cdot q$; $e =_\phi k^{-1}$
- **Signature:** $\sigma =_N m^k$

Simple(st) example: Threshold n-of-n RSA signatures

Threshold signature (with $n = 3$):

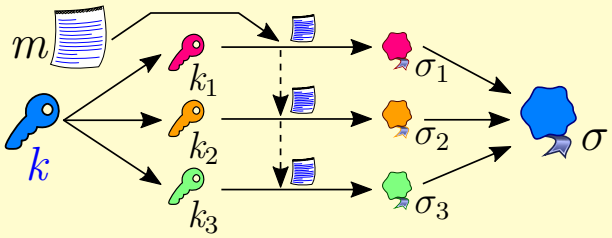


Textbook RSA:

- **Private** signing key: k
- **Priv.** $\phi = (p-1) \times (q-1)$
- **Public:** $N = p \cdot q$; $e =_\phi k^{-1}$
- **Signature:** $\sigma =_N m^k$

Simple(st) example: Threshold n-of-n RSA signatures

Threshold signature (with $n = 3$):



Textbook RSA:

- **Private** signing key: k
- **Priv.** $\phi = (p-1) \times (q-1)$
- **Public:** $N = p \cdot q$; $e =_\phi k^{-1}$
- **Signature:** $\sigma =_N m^k$

1. **Secret-share the key k:** $k \to k_1, k_2, k_3 : k_1 + k_2 + k_3 = k \bmod \phi$
2. **Produce partial signatures:** $\sigma_i = m^{k_i} \bmod N$, for $i = 1, 2, 3$
3. **Obtain final signature:** $\sigma = \sigma_1 \cdot \sigma_2 \cdot \sigma_3 = m^{k_1+k_2+k_3} = m^k \bmod N$

Threshold schemes can get more complicated

Threshold schemes can get more complicated

Feel free to ignore the next technical terms ... just want to convey some diversity

Threshold schemes can get more complicated

Feel free to ignore the next technical terms ... just want to convey some diversity

- **Threshold EdDSA/Schnorr:** Commitments, ZKPs, ...

  EdDSA = Edwards-Curve **Digital Signature** Algorithm; ZKP = Zero-Knowledge Proof

- **Threshold ECDSA, distributed RSA KeyGen:** Oblivous transfer, AHE, ...

  AHE = Additively-Homomorphic Encryption; ECDSA = Elliptic-Curve **Digital Signature** Algorithm; RSA = Rivest–Shamir–Adleman

- **Threshold AES:** Garbled circuits, oblivious transfer, ... AES = Advanced Encryption Standard

- **Other building blocks:** Reliable broadcast, threshold-friendly hash functions, ...

Threshold schemes can get more complicated

Feel free to ignore the next technical terms ... just want to convey some diversity

- **Threshold EdDSA/Schnorr:** Commitments, ZKPs, ...

  EdDSA = Edwards-Curve **Digital Signature** Algorithm; ZKP = Zero-Knowledge Proof

- **Threshold ECDSA, distributed RSA KeyGen:** Oblivous transfer, AHE, ...

  AHE = Additively-Homomorphic Encryption; ECDSA = Elliptic-Curve **Digital Signature** Algorithm; RSA = Rivest–Shamir–Adleman

- **Threshold AES:** Garbled circuits, oblivious transfer, ...

  AES = Advanced Encryption Standard

- **Other building blocks:** Reliable broadcast, threshold-friendly hash functions, ...

Other primitives (not standardized by NIST) can be more *threshold friendly*

(easier in practice to thresholdize, or amenable to "better" threshold schemes)

Outline

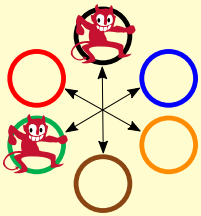
1. Intro on NIST Crypto
2. The PEC and MPTC Projects
3. The Threshold Call
4. Notes on Interaction

MPTC = Multi-Party Threshold Cryptography.
NIST = National Institute of Standards and Technology.
PEC = Privacy-Enhancing Cryptography.

The NIST Call for *Multi-Party Threshold Schemes*

NISTIR 8214C ipd (**i**nitial **p**ublic **d**raft) [Jan 2023]. Soon 2nd public draft.

Calling for submissions of threshold schemes for:

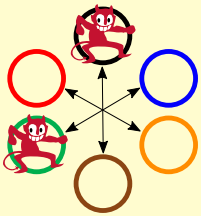


The NIST Call for *Multi-Party Threshold Schemes*

NISTIR 8214C ipd (**i**nitial **p**ublic **d**raft) [Jan 2023]. Soon 2nd public draft.

Calling for submissions of threshold schemes for:

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

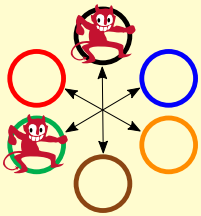


ZKP = Zero-Knolwedge Proof; FHE = Fully-Homomoprhic Encryption

The NIST Call for *Multi-Party Threshold Schemes*

NISTIR 8214C ipd (**i**nitial **p**ublic **d**raft) [Jan 2023]. Soon 2nd public draft.

Calling for submissions of threshold schemes for:



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

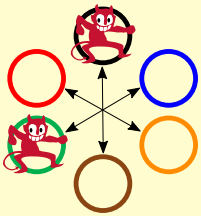
  (And auxiliary gadgets)

ZKP = Zero-Knolwedge Proof; FHE = Fully-Homomoprhic Encryption

The NIST Call for *Multi-Party Threshold Schemes*

NISTIR 8214C ipd (**i**nitial **p**ublic **d**raft) [Jan 2023]. Soon 2nd public draft.

Calling for submissions of threshold schemes for:



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

  (And auxiliary gadgets)

ZKP = Zero-Knolwedge Proof; FHE = Fully-Homomoprhic Encryption

— **Submissions (2025):** specification + reference implementation + evaluation

— Soon upcoming revised version of the Threshold Call: NISTIR 8214C

— More detailed info: https://csrc.nist.gov/projects/threshold-cryptography

Category Cat1 of the NIST Threshold Call

- **C1.1: Signing** (pre- and post-quantum)
- **C1.2: Public-Key Encryption** (pre- and post-quantum)
- **C1.3: Key-Agreement** (pre-quantum)
- **C1.4: Symmetric** (key-based [e.g., block-cipher] and key-less [e.g., hash])
- **C1.5: Key-Generation** (for all the above)

Note: The subcategory indices may still be updated in the final version

Category Cat2 of the NIST Threshold Call

- **C2.1–C2.5: Signing, PKE, KA, Symmetric, KeyGen** [topics as in Cat1]

  (PKE = Public-Key Encryption, KA = Key-Agreement, KeyGen = Key-Generation)

- **C2.6: Fully-Homomorphic Encryption**
- **C2.7: Zero-Knowledge Proofs (of knowledge of a secret key)**
- **C2.7: "Gadgets" (e.g., garbled circuits)**

Will explore advanced cryptography not traditionally covered by NIST standards

Note: The subcategory indices may still be updated in the final version

Assorted notes about the NIST Threshold Call

1. **Setup:** A gathering of reference material (not a competition for a selection).
2. **Interchangeability:** Threshold result usable as if it was conventionally generated. See our NISTIR 8214B (notes on Threshold Schnorr/EdDSA).
3. **Threshold-friendliness:** a perspective beyond usual efficiency.
4. **Expected:** The process will clarify relevant system models, best practices, ...
5. **Aim:** Devise recommendations about advanced cryptography (PEC + MPTC). (Will support future processes.) PEC = Privacy-Enhancing Crypto. MPTC = Multi-Party Threshold Crypto
6. **Ample room for participation:** Give feedback → Submit → Analyze.

Outline

1. Intro on NIST Crypto
2. The PEC and MPTC Projects
3. The Threshold Call
4. Notes on Interaction

MPTC = Multi-Party Threshold Cryptography.
NIST = National Institute of Standards and Technology.
PEC = Privacy-Enhancing Cryptography.

NIST Series of Crypto Talks

(To subscribe, check each webpage)

NIST hosts many talks by external researchers. Virtual attendance allowed.

- **NIST Crypto Reading Club:** crypto-club-questions@nist.gov
  https://csrc.nist.gov/projects/crypto-reading-club
  See also the "Other NIST-hosted Presentations" container.

- **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

- **Threshold Cryptography Seminar** (Expected in 2025, after initial MPTC submissions)

Some references on NIST Crypto Processes

- **NISTIR 7977:** Cryptographic Standards and Guidelines Development Process
- **NIST Computer Security Resource Center** (CSRC):
  Access to publications (standards, ...), presentations, events ...

- **Crypto Pub Review Project:** Ongoing review of past standards
- **Recent and soon upcoming NIST Workshops:**
  - Sep 24–26: Workshop on Privacy-Enhancing Cryptography 2024
  - Jan 16: Special Topics on Privacy & Public Auditability #7: Special Types of Encryption
  - Feb 25–26: Workshop on Guidance for Key-Encapsulation Mechanisms

Assorted remarks

- **Bad:** It's very easy to get "home-made crypto" wrong
- **Good:** International/community interaction, with thorough public scrutiny
- **Advanced cryptography:**
  - What/when/whether to standardize?
    — Complexification challenge (many options, parameters, metrics, ...)
  - PEC and MPTC follow the "**Reference Materials**" approach
    — Threshold Call, Exploratory workshops
  - Many opportunities for **privacy-preserving apps**

Cryptographers are welcome

The NIST Crypto Group can host visits and/or consider integrating a Foreign Guest Researcher ($\approx$ post-doc) expert on MPC / FHE / ZKP / Threshold Crypto.

The NIST Stone Test Wall

Come place a new "block" in the Crypto Standards Wall

Obrigado pela atenção!

Thank you for your attention!

Questions or Perguntas?

PEC Project

MPTC Project

Threshold Call

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

Cryptography Endeavors at NIST: Standardization and Beyond

Presented at the Portugal Crypto Day 2024

December 13, 2024 @ Lisboa (Portugal) — luis.brandao@nist.gov