Elements of Symmetric Cryptography in the NIST Threshold Call

Virtual presentation[†] on January 4th, 2024

@ ALPSY Research Retreat

Workshop on **Al**gebraic Aspects in the Design and Cry**p**tanalysis of Modern **Sy**mmetric Cryptography

(Hosted by Innsbruck University @ Obergurgl, Austria)

[†] Luís Brandão: at NIST as a Foreign Guest Researcher (non-employee), contractor from Strativia. Presented from Maryland, USA. Expressed opinions are from the speaker/author and should not be construed as official NIST views.

This presentation

Thank you Christian for the invitation to give this talk!

We appreciate the opportunity to connect with the International research community!

Goal/angle:

- Highlight possibilities of useful research contribution/collaboration
- Convey perspective from NIST projects: Threshold Crypto, Circuit Complexity, ...

Slides will be made available

Outline

1. NIST Crypto Intro
2. The “Threshold Call” (at a high level)
3. Symmetric Crypto in the Threshold Call
4. Circuit Complexity
5. Concluding remarks

Legend: Crypto = Cryptography. NIST = National Institute of Standards and Technology.

Outline

1. NIST Crypto Intro
2. The “Threshold Call” (at a high level)
3. Symmetric Crypto in the Threshold Call
4. Circuit Complexity
5. Concluding remarks

Legend: Crypto = Cryptography. NIST = National Institute of Standards and Technology.

NIST:

- **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)**

NIST: Laboratories → Divisions → Groups

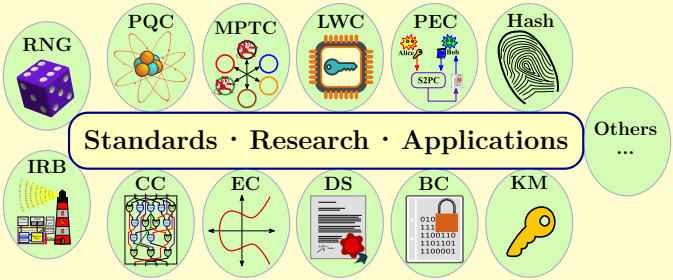
- **Non-regulatory** federal agency (@ U.S. Dept. Commerce)
- **Mission:** ... innovation ... industrial competitiveness ... measurement science, standards, and technology ... economic security ... quality of life.

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.*

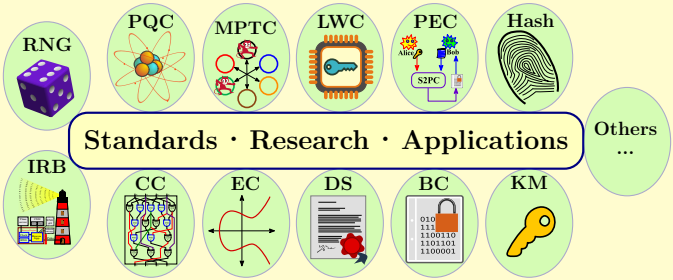
Activities in the “Crypto” Group



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 **C**omputer **S**ecurity. **TC** = [Multi-Party] **T**hreshold **C**rypto).

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

On the PEC and MPTC projects

PEC: Privacy-Enhancing Cryptography

MPTC: Multi-Party Threshold Cryptography

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

MPTC: Multi-Party Threshold Cryptography

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. Inc.: Including. Symm./pub.: symmetric-key or public-key based.

MPTC: Multi-Party Threshold Cryptography

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

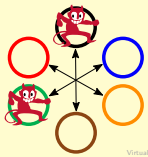
- Crypto (that can be) used to enhance privacy. (Emphasis on non-standardized tools)

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	**Fn**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. Symm./pub.: symmetric-key or public-key based.

MPTC: Multi-Party Threshold Cryptography

- *Threshold Schemes* for diverse 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., decrypt.



NIST Crypto Standardization/Exploratory Projects

- **PQC:** [standardization] "**Post-Quantum**" signatures and key-encapsulation
- **LWC:** [standardization] "**LightWeight**" **a**uth. **e**nc. w/ **a**ssoc. **d**ata, and hashing

Legend: AEAD = **A**uth[enticated] **E**nc[ryption] w[ith] **A**ssoc[iated] **D**ata. **CTG** = **C**ryptographic **T**echnology **G**roup. **LWC** = **L**ightweight **C**ryptography. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**ryptography. **NIST** = **N**ational **I**nstitute of **S**tandards and **T**echnology. **PEC** = **P**rivacy-**E**nhancing **C**ryptography. **PQC** = **P**ost-**Q**uantum **C**ryptography.

NIST Crypto Standardization/Exploratory Projects

- **PQC:** [standardization] "**Post-Quantum**" signatures and key-encapsulation
- **LWC:** [standardization] "**LightWeight**" **a**uth. **e**nc. w/ **a**ssoc. **d**ata, and hashing
- **PEC:** [exploratory] "**Privacy-Enhancing**" (advanced) features/functionalities
- **MPTC:** [exploratory] "**Multi-Party Threshold**" schemes for crypto primitives

Legend: AEAD = **A**uth[enticated] **E**nc[ryption] w[ith] **A**ssoc[iated] **D**ata. **CTG** = **C**ryptographic **T**echnology **G**roup. **LWC** = **L**ightweight **C**ryptography. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**ryptography. **NIST** = **N**ational **I**nstitute of **S**tandards and **T**echnology. **PEC** = **P**rivacy-**E**nhancing **C**ryptography. **PQC** = **P**ost-**Q**uantum **C**ryptography.

NIST Crypto Standardization/Exploratory Projects

- **PQC:** [standardization] "**Post-Quantum**" signatures and key-encapsulation
- **LWC:** [standardization] "**LightWeight**" **a**uth. **e**nc. w/ **a**ssoc. **d**ata, and hashing
- **PEC:** [exploratory] "**Privacy-Enhancing**" (advanced) features/functionalities
- **MPTC:** [exploratory] "**Multi-Party Threshold**" schemes for crypto primitives
- **...** (various other projects in the NIST "Crypto group" [CTG])

Legend: AEAD = **A**uth[enticated] **Enc**[ryption] w[ith] **Assoc**[iated] **D**ata. **CTG** = **C**ryptographic **T**echnology **G**roup. **LWC** = **L**ightweight **C**ryptography. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**ryptography. **NIST** = **N**ational **I**nstitute of **S**tandards and **T**echnology. **PEC** = **P**rivacy-**E**nhancing **C**ryptography. **PQC** = **P**ost-**Q**uantum **C**ryptography.

NIST Crypto Standardization/Exploratory Projects

- **PQC:** [standardization] "**Post-Quantum**" signatures and key-encapsulation
- **LWC:** [standardization] "**LightWeight**" **a**uth. **e**nc. w/ **a**ssoc. **d**ata, and hashing
- **PEC:** [exploratory] "**Privacy-Enhancing**" (advanced) features/functionalities
- **MPTC:** [exploratory] "**Multi-Party Threshold**" schemes for crypto primitives
- **...** (various other projects in the NIST "Crypto group" [CTG])

The "Threshold Call" (from MPTC+PEC): to gather **reference material** for public analysis ... aiming for **recommendations** (in a 1st phase), including about PEC.

Legend: AEAD = **A**uth[enticated] **Enc**[ryption] w[ith] **Assoc**[iated] **D**ata. **CTG** = **C**ryptographic **T**echnology **G**roup. **LWC** = **L**ightweight **C**ryptography. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**ryptography. **NIST** = **N**ational **I**nstitute of **S**tandards and **T**echnology. **PEC** = **P**rivacy-**E**nhancing **C**ryptography. **PQC** = **P**ost-**Q**uantum **C**ryptography.

Some NIST Crypto "Standardization" Updates

- **Post-Quantum (PQ):** Selected 4 PQC-schemes for standardization.
  - [Aim] Standards in 2024: ML-KEM, ML-DSA, SLH-DSA. (FN-DSA still in development)
  - July 2023: 40 new PQ-signature submissions/candidates under analysis.
- **Lightweight (LWC):** Selected ASCON for standardization
  - [Aim] Draft Standard in 2024: AEAD and XOF
    (as a Special Publication: SP 800 series)

Legend: **AEAD** = **A**uthenticated **E**ncryption with **A**ssociated **D**ata. **DSA** = **D**igital **S**ignature **A**lgorithm. **Feb** = **Feb**ruary. **FIPS** = **F**ederal **I**nformation **P**rocessing **S**tandards. **Jan** = **Jan**uary. **KEM** = **K**ey **E**ncapsulation **M**ethod. **LWC** = **L**ightweight **C**ryptography. **ML** = **M**odule **L**attice-based. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**ryptography. **Oct** = **Oct**ober. **PEC** = **P**rivacy-**E**nhancing **C**ryptography. **PQC** = **P**ost-**Q**uantum **C**ryptography. **SLH** = **S**tateless **H**ash-based. **SP** = **S**pecial **P**ublication (800 series) [in Computer Security]. **XOF** = **E**xtendable **O**utput **F**unction.

Some NIST Crypto "Standardization" Updates

- **Post-Quantum (PQ):** Selected 4 PQC-schemes for standardization.
  - [Aim] Standards in 2024: ML-KEM, ML-DSA, SLH-DSA. (FN-DSA still in development)
  - July 2023: 40 new PQ-signature submissions/candidates under analysis.
- **Lightweight (LWC):** Selected ASCON for standardization
  - [Aim] Draft Standard in 2024: AEAD and XOF
    (as a Special Publication: SP 800 series)
- **Threshold Call (MPTC/PEC):** Jan. 2023, Published Draft Call
  - Sep. 2023: MPTS workshop (gathered more public feedback)
  - [Aim] Finalize Call in 1st half of 2024; submissions deadline within 2nd half of 2024.

Legend: **AEAD** = Authenticated Encryption with Associated Data. **DSA** = Digital Signature Algorithm. **Feb** = February. **FIPS** = Federal Information Processing Standards. **Jan** = January. **KEM** = Key Encapsulation Method. **LWC** = Lightweight Cryptography. **ML** = Module Lattice-based. **MPTC** = Multi-Party Threshold Cryptography. **Oct** = October. **PEC** = Privacy-Enhancing Cryptography. **PQC** = Post-Quantum Cryptography. **SLH** = Stateless Hash-based. **SP** = Special Publication (800 series) [in Computer Security]. **XOF** = Extendable Output Function.

Some NIST Crypto "Standardization" Updates

- **Post-Quantum (PQ):** Selected 4 PQC-schemes for standardization.
  - [Aim] Standards in 2024: ML-KEM, ML-DSA, SLH-DSA. (FN-DSA still in development)
  - July 2023: 40 new PQ-signature submissions/candidates under analysis.

- **Lightweight (LWC):** Selected ASCON for standardization
  - [Aim] Draft Standard in 2024: AEAD and XOF
    (as a Special Publication: SP 800 series)

- **Threshold Call (MPTC/PEC):** Jan. 2023, Published Draft Call
  - Sep. 2023: MPTS workshop (gathered more public feedback)
  - [Aim] Finalize Call in 1st half of 2024; submissions deadline within 2nd half of 2024.

Legend: **AEAD** = **A**uthenticated **E**ncryption with **A**ssociated **D**ata. **DSA** = **D**igital **S**ignature **A**lgorithm. **Feb** = **Feb**ruary. **FIPS** = **F**ederal **I**nformation **P**rocessing **S**tandards. **Jan** = **Jan**uary. **KEM** = **K**ey **E**ncapsulation **M**ethod. **LWC** = **L**ightweight **C**ryptography. **ML** = **M**odule **L**attice-based. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**ryptography. **Oct** = **Oct**ober. **PEC** = **P**rivacy-**E**nhancing **C**ryptography. **PQC** = **P**ost-**Q**uantum **C**ryptography. **SLH** = **S**tateless **H**ash-based. **SP** = **S**pecial **P**ublication (800 series) [in Computer Security]. **XOF** = **X**tendable **O**utput **F**unction.

Outline

1. NIST Crypto Intro
2. The “Threshold Call” (at a high level)
3. Symmetric Crypto in the Threshold Call
4. Circuit Complexity
5. Concluding remarks

Legend: Crypto = Cryptography. NIST = National Institute of Standards and Technology.

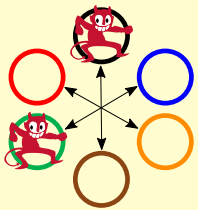
NIST Call for Multi-Party Threshold Schemes

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

NIST Call for Multi-Party Threshold Schemes

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

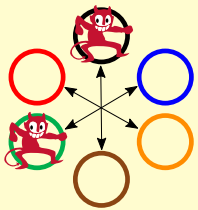
Calling for submissions of threshold schemes



(And gadgets for modular use)

NIST Call for Multi-Party Threshold Schemes

- NISTIR 8214C: Initial public **draft** (**Jan 2023**) ⇒ Revised version (**early 2024**).
- 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.

Category Cat1 of NIST Call for Multi-Party Threshold Schemes

Subcategory: Type	Families of specifications	NIST references
C1.1: **Signing**		
C1.2: **PKE**		
C1.3: **2KA**		
C1.4: **Symmetric**		
C1.5: **Keygen**		

Category Cat1 of NIST Call for Multi-Party Threshold Schemes

Too many acronyms, we know. (Legend further below)

Subcategory: Type
C1.4: **Symmetric** AES encipher/decipher, KDM/KC (for 2KE) FIPS 197, SP 800-56C Rev2, ...

Legend: 2KA: **pair**-wise **k**ey-agreement. **2KE**: **pair**-wise **k**ey-establisment. **AES**: **A**dvanced **E**ncryption **S**tandard. **CDH**: cofactor **D**iffie–**H**ellman. **ECC**: **E**lliptic-curve **c**ryptography (or, if used as an adjective, **EC**-based). **ECDSA**: **E**lliptic-curve **D**igital **S**ignature **A**lgorithm. **EdDSA**: **Ed**wards-curve **D**igital **S**ignature **A**lgorithm. **E**lliptic-curve based **K**ey-**E**stablishment. **FIPS**: **F**ederal **I**nformation **P**rocessing **S**tandard. **KC**: **K**ey-**c**onfirmtion. **KDM**: **K**ey-**d**erivation **m**echanism. **Keygen**: **K**ey-**gen**eration. **MQV**: Menezes-Qu-Vanstone. **PKE**: **p**ublic-key **e**ncryption. **RSA**: **R**ivest–**S**hamir–**A**dleman (signature and encryption schemes). **RSADSA**: **RSA** digital signature algorithm. **SP 800**: **S**pecial **P**ublication (in Computer Security).
Note: In the 2nd column, each item within a subcategory is itself called a family of specifications, since it may include diverse primitives or modes/variants.

Category Cat1 of NIST Call for Multi-Party Threshold Schemes

Too many acronyms, we know. (Legend further below)

Subcategory: Type	Families of specifications	NIST references
C1.1: **Signing**	EdDSA sign, ECDSA sign, RSADSA sign	FIPS 186-5 (see also NISTIR 8214B)
C1.2: **PKE**	RSA decrypt, RSA encrypt (a secret value)	SP 800-56B Rev2
C1.3: **2KA**	ECC-CDH, ECC-MQV	SP 800-56A Rev3
C1.4: **Symmetric**	AES encipher/decipher, KDM/KC (for 2KE)	FIPS 197, SP 800-56C Rev2, ...
C1.5: **Keygen**	ECC keygen, RSA keygen, bitstring keygen	(corresponding references above)

Legend: 2KA: **pair**-wise **k**ey-agreement. **2KE**: **pair**-wise **k**ey-establisment. **AES**: **A**dvanced **E**ncryption **S**tandard. **CDH**: cofactor **D**iffie–**H**ellman. **ECC**: **E**lliptic-curve **c**ryptography (or, if used as an adjective, **EC**-based). **ECDSA**: **E**lliptic-curve **D**igital **S**ignature **A**lgorithm. **EdDSA**: **Ed**wards-curve **D**igital **S**ignature **A**lgorithm. **E**lliptic-curve based **K**ey-**E**stablishment. **FIPS**: **F**ederal **I**nformation **P**rocessing **S**tandard. **KC**: **K**ey-**c**onfirmtion. **KDM**: **K**ey-**d**erivation **m**echanism. **Keygen**: **K**ey-**gen**eration. **MQV**: Menezes-Qu-Vanstone. **PKE**: **p**ublic-**k**ey **e**ncryption. **RSA**: **R**ivest–**S**hamir–**A**dleman (signature and encryption schemes). **RSADSA**: **RSA** digital signature algorithm. **SP 800**: **S**pecial **P**ublication (in Computer Security). **Note:** In the 2nd column, each item within a subcategory is itself called a family of specifications, since it may include diverse primitives or modes/variants.

Also to be added to Category Cat1

Primitives from NIST draft standards emerging from the PQC and LWC projects:

- **ML-KEM** (KYBER-based) Draft FIPS 203: ***M**odule-**L**attice-Based KEM Standard*
- **ML-DSA** (DILITHIUM-based) Draft FIPS 204: ***M**odule-**L**attice-Based DSA*
- **SLH-DSA** (SPHINCS-based) Draft FIPS 205: ***S**tate**l**ess **H**ash-Based DSA*
- **FN-DSA** (Falcon-based): Upcoming Draft FIPS
- **AEAD and XOF standards** (ASCON-based): Draft upcoming in 2024

Legend: AEAD = **A**uthenticated **E**ncryption with **A**ssociated **D**ata. DSA = **D**igital **S**ignature **A**lgorithm. FIPS = **F**ederal **I**nformation **P**rocessing **S**tandard [Publication]. KEM = **K**ey-**E**ncapsulation **M**echanism. ML = **M**odule **L**attice. SLH = **S**tate**L**ess **h**ash. XOF = e**x**tendable **O**utput **F**unction.

Category Cat2 of the NIST “Threshold” Call

Subcategory: Type
C2.1: **Signing**
C2.2: **PKE**
C2.3: **Key-agreem.**
C2.4: **Symmetric**
C2.5: **Keygen**

Note: While TF-QR is desired for any type of scheme, some examples show just TF to highlight that it is welcome even if not QR.

Legend: agreem. = **agreem**ent. **Keygen** = **key-gen**eration. **PKE** = **p**ublic-key **e**ncryption. **PRF** = **p**seudorandom **f**unction [family]. **PRP** = **p**seudorandom **p**ermutation [family]. **QR** = **q**uantum **r**esistant. **TF** = **t**hreshold-**f**riendly. **ZKPoK** = **z**ero **k**nowledge **p**roof **o**f **k**nowledge.

Category Cat2 of the NIST "Threshold" Call

TF = **t**hreshold **f**riendly. QR = **q**uantum **r**esistant.

Subcategory: Type	Example types of schemes	Example primitives
C2.4: **Symmetric**	TF blockcipher/PRP	Encipher/decipher
|	TF key-derivation / key-confirmation	PRF and hash function

Note: While TF-QR is desired for any type of scheme, some examples show just TF to highlight that it is welcome even if not QR

Legend: agreem. = **agreem**ent. **Keygen** = **key-gen**eration. **PKE** = **p**ublic-key **e**ncryption. **PRF** = **p**seudorandom **f**unction [family]. **PRP** = **p**seudorandom **p**ermutation [family]. **QR** = **q**uantum **r**esistant. **TF** = **t**hreshold-**f**riendly. **ZKPoK** = **z**ero **k**nowledge **p**roof **o**f **k**nowledge.

Category Cat2 of the NIST “Threshold” Call

Subcategory: Type
C2.6: **Advanced**
C2.7: **ZKPoK**
C2.8: **Gadgets**

Note: While TF-QR is desired for any type of scheme, some examples show just TF to highlight that it is welcome even if not QR

Legend: agreem. = **agreem**ent. **Keygen** = **key-gen**eration. **PKE** = **p**ublic-key **e**ncryption. **PRF** = **p**seudorandom **f**unction [family]. **PRP** = **p**seudorandom **p**ermutation [family]. **QR** = **q**uantum **r**esistant. **TF** = **t**hreshold-**f**riendly. **ZKPoK** = **z**ero **k**nowledge **p**roof **o**f **k**nowledge.

Category Cat2 of the NIST "Threshold" Call

TF = **t**hreshold **f**riendly. QR = **q**uantum **r**esistant.

Subcategory: Type	Example types of schemes	Example primitives
C2.6: **Advanced**	TF-QR **f**ully-**h**omomorphic **e**ncryption (FHE)	Decryption; Keygen
|	TF identity-based and attribute-based encryption	Decryption; Keygens

Note: While TF-QR is desired for any type of scheme, some examples show just TF to highlight that it is welcome even if not QR

Legend: agreem. = **agreem**ent. **Keygen** = **key-gen**eration. **PKE** = **p**ublic-key **e**ncryption. **PRF** = **p**seudorandom **f**unction [family]. **PRP** = **p**seudorandom **p**ermutation [family]. **QR** = **q**uantum **r**esistant. **TF** = **t**hreshold-**f**riendly. **ZKPoK** = **z**ero **k**nowledge **p**roof **o**f **k**nowledge.

Category Cat2 of the NIST “Threshold” Call

Subcategory: Type	Example types of schemes	Example primitives
C2.7: **ZKPoK**	**Z**ero-**k**nowledge **p**roof **o**f **k**nowledge of private key	ZKPoK.Generate

Note: While TF-QR is desired for any type of scheme, some examples show just TF to highlight that it is welcome even if not QR

Legend: agreem. = **agreem**ent. **Keygen** = **key-gen**eration. **PKE** = **p**ublic-**k**ey **e**ncryption. **PRF** = **p**seudorandom **f**unction [family]. **PRP** = **p**seudorandom **p**ermutation [family]. **QR** = **q**uantum **r**esistant. **TF** = **t**hreshold-**f**riendly. **ZKPoK** = **z**ero **k**nowledge **p**roof **o**f **k**nowledge.

Category Cat2 of the NIST “Threshold” Call

Subcategory: Type	Example types of schemes	Example primitives
C2.8: **Gadgets**	Garbled circuit (GC)	GC.generate; GC.evaluate

Note: While TF-QR is desired for any type of scheme, some examples show just TF to highlight that it is welcome even if not QR

Legend: agreem. = **agreem**ent. **Keygen** = **key-gen**eration. **PKE** = **p**ublic-key **e**ncryption. **PRF** = **p**seudorandom **f**unction [family]. **PRP** = **p**seudorandom **p**ermutation [family]. **QR** = **q**uantum **r**esistant. **TF** = **t**hreshold-**f**riendly. **ZKPoK** = **z**ero **k**nowledge **p**roof **o**f **k**nowledge.

Category Cat2 of the NIST "Threshold" Call

TF = **t**hreshold **f**riendly. QR = **q**uantum **r**esistant.

Subcategory: Type	Example types of schemes	Example primitives
C2.1: **Signing**	TF succinct & verifiably-deterministic signatures	Sign
|	TF-QR signatures	Sign
C2.2: **PKE**	TF-QR **p**ublic-**k**ey **e**ncryption (PKE)	Decrypt/Encrypt (a secret value)
C2.3: **Key-agreem.**	TF Low-round multi-party key-agreement	Single-party primitives
C2.4: **Symmetric**	TF blockcipher/PRP	Encipher/decipher
|	TF key-derivation / key-confirmation	PRF and hash function
C2.5: **Keygen**	Any of the above	Keygen
C2.6: **Advanced**	TF-QR **f**ully-**h**omomorphic **e**ncryption (FHE)	Decryption; Keygen
|	TF identity-based and attribute-based encryption	Decryption; Keygens
C2.7: **ZKPoK**	**Z**ero-**k**nowledge **p**roof **o**f **k**nowledge of private key	ZKPoK.Generate
C2.8: **Gadgets**	Garbled circuit (GC)	GC.generate; GC.evaluate

Note: While TF-QR is desired for any type of scheme, some examples show just TF to highlight that it is welcome even if not QR

Legend: agreem. = **agreem**ent. **Keygen** = **key-gen**eration. **PKE** = **p**ublic-**k**ey **e**ncryption. **PRF** = **p**seudorandom **f**unction [family]. **PRP** = **p**seudorandom **p**ermutation [family]. **QR** = **q**uantum **r**esistant. **TF** = **t**hreshold-**f**riendly. **ZKPoK** = **z**ero **k**nowledge **p**roof **o**f **k**nowledge.

Main components of a submission package

Check	#	Item
☐	M1	Written specification (S1–S16)
☐	M2	Reference implementation (Src1–Src4)
☐	M3	Execution instructions (X1–X7)
☐	M4	Experimental evaluation (Perf1–Perf5)
☐	M5	Additional statements

Main components of a submission package

Check	#	Item
☐	M1	Written specification (S1–S16)
☐	M2	Reference implementation (Src1–Src4)
☐	M3	Execution instructions (X1–X7)
☐	M4	Experimental evaluation (Perf1–Perf5)
☐	M5	Additional statements

A submission package can propose various **objects** (schemes/gadgets).

Each **component** will then map all such **objects**.

Outline

1. NIST Crypto Intro
2. The “Threshold Call” (at a high level)
3. Symmetric Crypto in the Threshold Call
4. Circuit Complexity
5. Concluding remarks

Legend: Crypto = Cryptography. NIST = National Institute of Standards and Technology.

Symmetric Crypto in Cat1

Subcategory "C1.4 Symmetric" (with NIST standardized primitives)

- **Enciphering:** AES, ASCON-AEAD
- **MAC'ing:** HMAC, KMAC, CMAC
- **Hashing:** SHA2, SHA3, ASCON-XOF

Symmetric Crypto in Cat1

Subcategory "C1.4 Symmetric" (with NIST standardized primitives)

- **Enciphering:** AES, ASCON-AEAD
- **MAC'ing:** HMAC, KMAC, CMAC
- **Hashing:** SHA2, SHA3, ASCON-XOF

Notes:

- Primitives not designed for threshold-friendliness. How to efficiently thresholdize?
- MPTS 2023: at least one team will submit a Threshold-AES package (based on garbled circuits; might apply stacked garbling [branching] and lookup tables)

Legend: AEAD = **A**uthenticated **E**ncryption with **A**ssociated **D**ata. AES = **A**dvanced **E**ncryption **S**tandard. CMAC = Cipher-based **MAC**. HMAC = Keyed-**H**ash **MAC**. KMAC = Keccak-based **MAC**. MAC = **M**essage **A**uthentication **C**ode. MPTS = **M**ulti **P**arty **T**hreshold **S**chemes (Workshop). SHA = **S**ecure **H**ash **A**lgorithm. XOF = e**x**tendable **O**utput **F**unction.

Symmetric Crypto in Cat2

- C2.4: **Symmetric:** Threshold-friendlier symmetric primitives
- C2.8: **Gadgets:** e.g., *-friendly hashing, for:
  - C2.6: **Advanced:** Fully Homomorphic Encryption (FHE), ...
  - C2.7: **ZKP:** Zero-Knowledge Proofs of Knowledge

Symmetric Crypto in Cat2

- C2.4: **Symmetric:** Threshold-friendlier symmetric primitives
- C2.8: **Gadgets:** e.g., *-friendly hashing, for:
  - C2.6: **Advanced:** Fully Homomorphic Encryption (FHE), ...
  - C2.7: **ZKP:** Zero-Knowledge Proofs of Knowledge

Notes

- In the threshold paradigm: How much more efficient can symmetric crypto get?
- More broadly (advanced crypto): friendliness for MPC, ZKP, FHE, ...

Example ZKPoKs of interest (related to Cat1)

Related type	Related (sub)sub-category: Primitive	Example ZKPoK (including consistency with public commitments of secret-shares, when applicable)
Keygen	5.1.1: ECC keygen	of discrete-log (s or d) of pub key Q
|	5.1.2: RSA keygen	of factors (p, q), or group order ϕ, or decryption key d
|	5.1.3: AES keygen	of secret key k (with regard to secret-sharing commitments)
PKE	5.2.1: RSA encryption	of secret plaintext m (encrypted)
|	5.2.2: RSA decryption	of secret-shared plaintext m (after SSO-threshold decryption)
Symmetric	1.4.1: AES enciphering	of secret key k (with regard to plaintext/ciphertext pair)
|	1.4.2: Hashing in KDM	of secret pre-image Z

Source: Table 12 or NISTIR 8214C ipd

Legend: AES = Advanced Encryption Standard. Cat1 = Category 1. ECC = Elliptic-Curve Cryptography. ipd = initial public draft. keygen = key-generation. KDM = key-derivation mechanism. RSA = Rivest-Shamir Adleman. SSO = Secret-shared output. NISTIR = NIST Internal[ly developed, public] Report. ZKPoK = Zero-knowledge proof of knowledge.

Other considerations on Symmetric Crypto

- Threshold Deterministic-EdDSA (in Cat 1): secret nonce is the SHA3-hashing of a secret key. A threshold-friendlier PRF would be useful.
- {PQC,LWC} vs. initial {MPTC,PEC} processes: different expectations.
- Analysis of Threshold Call submissions to focus more on reduction proofs / provable MPC, rather than on unproven heuristic constructions.
- Symmetric Crypto is also of interest to other NIST projects (e.g., Circuit Complexity, next slides).

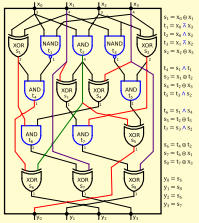
Outline

1. NIST Crypto Intro
2. The “Threshold Call” (at a high level)
3. Symmetric Crypto in the Threshold Call
4. Circuit Complexity
5. Concluding remarks

Legend: Crypto = Cryptography. NIST = National Institute of Standards and Technology.

The NIST Circuit Complexity project

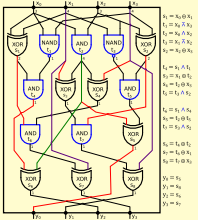
- A project (René, Meltem, Luís) in the NIST "Crypto Group".
- Why? *"... Optimization of circuits leads to efficiency improvement in a wide range of algorithms."*
- Open to host foreign guest researchers (1^+ year)



https://csrc.nist.gov/projects/circuit-complexity

The NIST Circuit Complexity project

- A project (René, Meltem, Luís) in the NIST "Crypto Group".
- Why? *"... Optimization of circuits leads to efficiency improvement in a wide range of algorithms."*
- Open to host foreign guest researchers (1^+ year)



Main goals:

1. **Improve understanding** of the circuit complexity of Boolean functions (BFs) and vectorial BFs
2. **Develop new techniques** for constructing better circuits for use by academia and industry.

1. Background
2. Research directions
3. Results
4. Collaborators

https://csrc.nist.gov/projects/circuit-complexity

Boolean circuits as reference material

The NIST circuit library

- AES Implementations
- SHA256
- Finite field multiplication
- Binary polynomial multiplication
- Boolean functions
- Linear maps

Example list of circuits of one type (AES)

AES Implementations

AES S-Boxes	Links	#ANDs	#XOR + #XNOR	#Gates	Depth	AND-Depth
S-Box 1	SLP, Graph	32	83	115	28	6
S-Box 2	SLP	32	81	113	27	6
S-Box 3	SLP, Graph	34	94	128	16	4
S-Box inverse 1	SLP	34	87	121	21	4
S-Box inverse 2	SLP, Graph	34	93	127	16	4

AES Cipher	Links	#ANDs	#XNOR	#XOR	#Gates	Depth	AND-Depth
AES-128(k,m)	SLP	6400	844	21 356	28 600	326	60
AES-128(0,m)	SLP	5120	1620	14 652	21 392	325	60

The AES circuit above is constructed using: (i) the S-Box implementation "forward 2" (doi:10.1007/s00145-012-9124-7 further improved in 2013 by 2 XORs); and (ii) the MixColumn circuit by Maximov in 2019 (ia.cr/2019/833).

(Example: AES SBox with 32 AND gates)

We'd like to expand this library

Some research interest in circuit complexity

1. AND-optimization of Boolean functions
2. AND-optimization of vectorial Boolean functions
3. XOR-optimization of linear maps
4. Recurrence relations for binary polynomial multiplication

Lots of interesting fundamental research to do:

- We haven't departed much from $\{\texttt{AND}, \texttt{XOR}, \mathbb{1}\}$ basis.
- Can AES SBox be implemented with fewer than 32 AND gates?
- OMA: Prove that $x_0 * f(x_1, ..., x_n)$ requires **o**ne **m**ore **A**ND gate than f.

Circuit File Format: Upcoming Reference

We intend to specify a reference (not a "standard") for a circuit file format.

Toy example:

Figure 1. Circuit for the majority of three bits

```
1 begin CIRCUIT MAJ3
2 # Description: The majority of three bits
3 Inputs: x1:x3; Outputs: y1; Internal:t1:t3
4 GateSyntax: GateName Output Inputs
5 begin SLP
6   XOR t1 x1 x2;  XOR t2 x1 x3;  AND t3 t1 t2;  XOR y1 t3 x1
7 end SLP end CIRCUIT
```

The colors distinguishing between input, intermediate and output variables are used as an aid, but is not required to interpret the circuit. The line numbers on the left are part of the file format. Both the colors and the line numbers can appear automatically when opening the file in an text editor that can interpret the circuit format.

Circuit File Format: More examples

AES SBox (G113, A32, D27, AD6)

```
begin circuit AES-SBOX-FWD-G113-A32-D27-AD6

# Description: AES Sbox Forward
# References: Based on doi:10.1007/s00145-012-
# Tally: 8 inputs, 8 outputs, 113 gates, 32 AN
# Depth(Gate): 27; Depth(AND): 6

Inputs: U0:U7
Outputs: S0:S7
Internal: t1:t105
GateSyntax: GateName Output Inputs

begin SLP
XOR t1 U3 U5
XOR t2 U0 U6
XOR t3 U0 U3
XOR t4 U0 U5
...
end SLP
end circuit
```

Binary Poly Mult with 11 terms

```
begin circuit Mult-Binary-Poly-11-terms

# Description: Multiplication of two Binary Polynomials with 11 terms
# References: doi:10.1109/TC.2018.2874662
# Tally: 22 inputs, 21 outputs, 186 gates, 78 AND, 108 XOR
# Depth(Gate): 7; Depth(AND): 1

# Input polynomials are A = f0 + f1*X + f2*X^2 + ... + f10*X^10 and B
# Output polynomial is the product A*B = h0 + h1*X + h2*X^2 + ... + h2
# Coefficients are over GF2

Inputs: f0:f10 g0:g10
Outputs: h0:h20
Internal: t1:t165
GateSyntax: GateName Output Inputs

begin SLP
AND t1 f2 g2
AND t2 f2 g0
AND t3 f2 g1
...
```

Circuit File Format: rationale

Why:

- Uniform format for circuits in the NIST Circuit Library
- Interoperability for public calls (e.g., the Threshold Call)
- Include desired features

Some intended features:

- Human readable/editable .txt format
- Succinct specification of ranges of variables
- Modularity: multiple circuits and subcircuits per file
- Loops and branching: FOR, IF
- Parser to unroll circuits

Masked Circuits (for block-ciphers)

Plan: create a library of masked circuits
(When masking, the probing of a single wire does not reveal secret info)

- **Public call:** will ask for masked AES circuits (and maybe others?)
- **Optimization:** 3 metrics (#rand, #gates, depth) $\times$ 3 masking degrees (1,2,3)
- **Timeline:** not before the Multi-Party Threshold Call is published.

Expected result: public library; a reference for subsequent side-channel attack experiments/discussion.

See details of project scope at: https://csrc.nist.gov/projects/masked-circuits

Outline

1. NIST Crypto Intro
2. The “Threshold Call” (at a high level)
3. Symmetric Crypto in the Threshold Call
4. Circuit Complexity
5. Concluding remarks

Legend: Crypto = Cryptography. NIST = National Institute of Standards and Technology.

Selected remarks

- **Symmetric Crypto** is in scope of the Threshold Call
  - Various optimization paradigms: *-friendly, with $* \in \{$FHE, ZKP, MPC, ...$\}$.
- The process is an **exploration**, before promising standards
  - A gathering of **reference material** (not a competition for a selection).
  - Evaluation will aim to devise **recommendations** for subsequent processes
- Other NIST projects are also interested in symmetric crypto / circuits
- Community **participation** is essential (feedback; submissions; analyses)

NIST May Have Funds for a Guest Researcher

Come collaborate in the NIST exploration of Advanced Cryptography

- Conduct joint research with other NIST researchers.
- Bring your perspective into the NIST standardization process.
- Example projects: MPTC, PEC, Circuit Complexity.

PEC = Privacy-Enhancing Cryptography; MPTC = Multi-Party Threshold Cryptography.

NIST May Have Funds for a Guest Researcher

Come collaborate in the NIST exploration of Advanced Cryptography

- Conduct joint research with other NIST researchers.
- Bring your perspective into the NIST standardization process.
- Example projects: MPTC, PEC, Circuit Complexity.

PEC = Privacy-Enhancing Cryptography; MPTC = Multi-Party Threshold Cryptography.

NIST May Have Funds for a Guest Researcher

Come collaborate in the NIST exploration of Advanced Cryptography

- Conduct joint research with other NIST researchers.
- Bring your perspective into the NIST standardization process.
- Example projects: MPTC, PEC, Circuit Complexity.

PEC = Privacy-Enhancing Cryptography; MPTC = Multi-Party Threshold Cryptography.

— Initial contacts: {rene.peralta, luis.brandao} @ nist (dot) gov

— Check also online the "Foreign Guest Researcher Program" at nist.gov

Thank you for your attention! Questions?

Elements of Symmetric Cryptography in the NIST Threshold Call

Presented at ALPSY Research Retreat | January 4th, 2024

We appreciate followup comments: luis.brandao@nist.gov

Threshold Call (IR 8213 ipd)

MPTC project

PEC project

Circuit Complexity