National Institute of Standards and Technology
U.S. Department of Commerce

Toward Criteria for Standardization of Multi-Party Threshold Schemes for Cryptographic Primitives

Luís T. A. N. Brandão*

Cryptographic Technology Group
National Institute of Standards and Technology (Gaithersburg, USA)

Presentation on August 15, 2020 @ ACAS2020, Virtual event
2nd Workshop on **A**dvanced **C**ryptography **A**pplications and **S**tandards

*At NIST as a Foreign Guest Researcher (Contractor, from Strativia)

Outline

1. Intro NIST standards
2. Update on the NIST Threshold Cryptography project
3. Some thoughts on standardization
4. Concluding remarks

Outline

1. Intro NIST standards
2. Update on the NIST Threshold Cryptography project
3. Some thoughts on standardization
4. Concluding remarks

NIST: Laboratories → Divisions → Groups

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

Aerial photo of Gaithersburg campus (source: Google Maps, August 2019)

NIST: Laboratories → Divisions → Groups

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

Aerial photo of Gaithersburg campus (source: Google Maps, August 2019)

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.

→ **Security Testing, Validation and Measurement (STVM):** validate cryptographic algorithm implementations, cryptographic modules, [...] develop test suites and test methods; [...]

NIST: Laboratories → Divisions → Groups

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

Aerial photo of Gaithersburg campus (source: Google Maps, August 2019)

ITL 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.

→ **Security Testing, Validation and Measurement (STVM):** validate cryptographic algorithm implementations, cryptographic modules, [...] develop test suites and test methods; [...]

- Documents: FIPS, SP 800, NISTIR.
- International cooperation: government, industry, academia, standardization bodies.

Legend: FIPS = Federal Information Processing Standards; SP 800 = Special Publications in Computer Security; NISTIR = NIST Internal or Interagency Report.

NIST standardizes cryptographic primitives

Some examples:

- FIPS 186-5 (draft): RSA, ECDSA and EdDSA signatures
- FIPS 197: AES (block cipher)
- SP 800-56A/B: primitives for DLC/IFC pair-wise key agreement
- SP 800-90 series: DRBGs

Legend: AES (Advanced Encryption Standard); DLC: Discrete-Log Cryptography; DRBG (Deterministic Random Bit Generator); ECDSA (Elliptic Curve Digital Signature Algorithm); EdDSA (Edwards Curve Digital Signature Algorithm); IFC: Integer Factorization Cryptography; RSA (Rivest–Shamir–Adleman).

NIST standardizes cryptographic primitives

Some examples:

- FIPS 186-5 (draft): RSA, ECDSA and EdDSA signatures
- FIPS 197: AES (block cipher)
- SP 800-56A/B: primitives for DLC/IFC pair-wise key agreement
- SP 800-90 series: DRBGs

Legend: AES (Advanced Encryption Standard); DLC: Discrete-Log Cryptography; DRBG (Deterministic Random Bit Generator); ECDSA (Elliptic Curve Digital Signature Algorithm); EdDSA (Edwards Curve Digital Signature Algorithm); IFC: Integer Factorization Cryptography; RSA (Rivest–Shamir–Adleman).

Some guidance on Cryptography Standards:

- NISTIR 7977 (2016): NIST Cryptographic Standards and Guidelines Development Process

  Formalizes several **principles** to follow: transparency, openness, balance, integrity, technical merit, usability, global acceptability, continuous improvement, innovation and intellectual property (and overarching considerations)
- SP 800-175: Guideline for Using Cryptographic Standards in the Federal Government
- FIPS 140-3: Security Requirements for Cryptographic Modules

Development of new standards

Several methods to develop cryptography standards:

- Internal or interagency developed techniques
- Adoption of external standards
- Open call, competition, “competition-like”

Development of new standards

Several methods to develop cryptography standards:

- Internal or interagency developed techniques
- Adoption of external standards
- Open call, competition, "competition-like"

Examples of ongoing standardization projects:

- **Post-quantum Cryptography:** signatures, public-key encryption, key encapsulation
- **Lightweight Cryptography:** ciphers, authenticated encryption, hash functions
- **Threshold Cryptography:** threshold schemes for cryptographic primitives
- ... NIST also has projects for research (e.g., Circuit Complexity) and applications (e.g., Randomness Beacon)

Development of new standards

Several methods to develop cryptography standards:

- Internal or interagency developed techniques
- Adoption of external standards
- Open call, competition, "competition-like"

Examples of ongoing standardization projects:

- **Post-quantum Cryptography:** signatures, public-key encryption, key encapsulation
- **Lightweight Cryptography:** ciphers, authenticated encryption, hash functions
- **Threshold Cryptography:** threshold schemes for cryptographic primitives
- ... NIST also has projects for research (e.g., Circuit Complexity) and applications (e.g., Randomness Beacon)

This presentation: Threshold Cryptography project → "Multi-Party" track

Outline

1. Intro NIST standards
2. Update on the NIST Threshold Cryptography project
3. Some thoughts on standardization
4. Concluding remarks

Why going for a threshold approach?

Crypto can be affected by vulnerabilities

- Attacks can exploit differences between ideal vs. real **implementations**
- **Operators** of cryptographic implementations can go rogue

Why going for a threshold approach?

Crypto can be affected by vulnerabilities

- Attacks can exploit differences between ideal vs. real **implementations**
- **Operators** of cryptographic implementations can go rogue

How to address single-points of failure?

*question-2.html *4296.html

* = clker.com/clipart-

Why going for a threshold approach?

Crypto can be affected by vulnerabilities

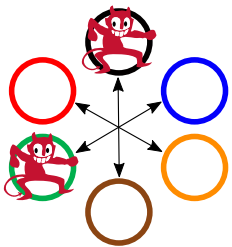
- Attacks can exploit differences between ideal vs. real **implementations**
- **Operators** of cryptographic implementations can go rogue

How to address single-points of failure?

*question-2.html *4296.html

* = clker.com/clipart-

The threshold approach

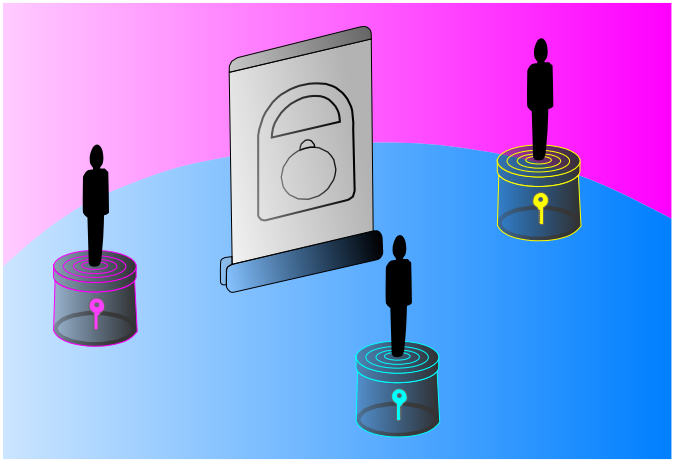


The red dancing devil is from clker.com/clipart-13643.html

At a high-level:

use redundancy & diversity to mitigate the *compromise* of up to a threshold number (f-out-of-n) of components

A depiction of multi-party threshold decryption



Adapted from the original (2020/July/7) from N. Hanacek/NIST.

- **Setup:** The decryption key is *secret shared* across 3 parties
- **Goal:** decrypt a ciphertext in a threshold manner
- **Interaction:** The parties may collaborate, but the *sub-keys* remain secret
- **Result:** The combined outputs derive the decrypted plaintext

The Threshold Cryptography Project at NIST

Scope: standardization of threshold schemes for cryptographic primitives

https://csrc.nist.gov/Projects/Threshold-Cryptography/

The Threshold Cryptography Project at NIST

Scope: standardization of threshold schemes for cryptographic primitives

Steps:

1. March 2019: NISTIR 8214: Threshold Schemes for Cryptographic Primitives: Challenges and Opportunities in Standardization and Validation of Threshold Cryptography
2. March 2019: NTCW 2019: NIST Threshold Cryptography Workshop 2019
3. July 2020: NISTIR 8214A: NIST Roadmap Toward Criteria for Threshold Schemes for Cryptographic Primitives
4. November 2020: MPTS 2020: NIST Workshop on Multi-Party Threshold Schemes

https://csrc.nist.gov/Projects/Threshold-Cryptography/

Characterizing threshold schemes

Characterizing threshold schemes

To reflect on a threshold scheme, start by characterizing **4 main features**:

- Kinds of threshold 
- Communication interfaces 
- Executing platform 
- Setup and maintenance 

The cliparts are from openclipart.org/detail/$*$, with $* \in \{71491, 190624, 101407, 161401, 161389\}$

Characterizing threshold schemes

To reflect on a threshold scheme, start by characterizing **4 main features**:

- Kinds of threshold 
- Communication interfaces 
- Executing platform 
- Setup and maintenance 

The cliparts are from openclipart.org/detail/∗, with ∗ ∈ {71491, 190624, 101407, 161401, 161389}

Each feature spans distinct options that affect security in different ways.

Characterizing threshold schemes

To reflect on a threshold scheme, start by characterizing **4 main features**:

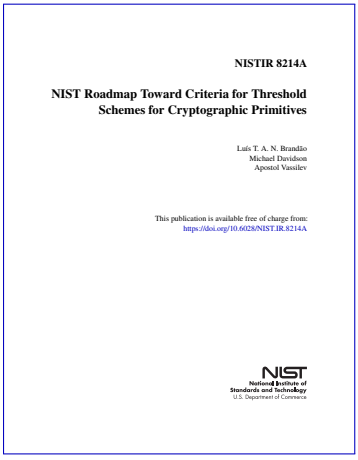
- Kinds of threshold 
- Communication interfaces 
- Executing platform 
- Setup and maintenance 

The cliparts are from openclipart.org/detail/$*$, with $* \in \{71491, 190624, 101407, 161401, 161389\}$

Each feature spans distinct options that affect security in different ways.

A characterization provides a better context for security assertions.

NISTIR 8214A: A roadmap toward criteria


NISTIR 8214A

NIST Roadmap Toward Criteria for Threshold Schemes for Cryptographic Primitives

Luís T. A. N. Brandão
Michael Davidson
Apostol Vassilev

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8214A

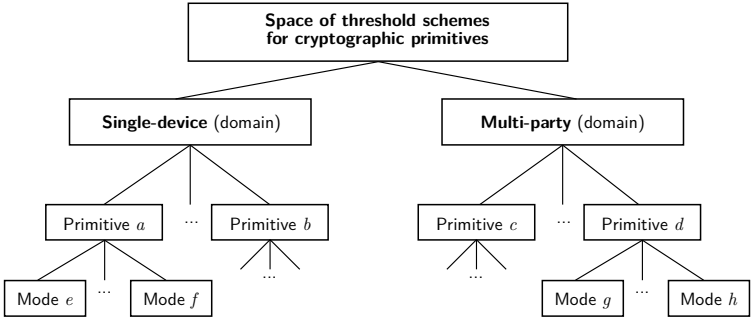
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8214A: NIST Roadmap Toward Criteria for Threshold Schemes for Cryptographic Primitives

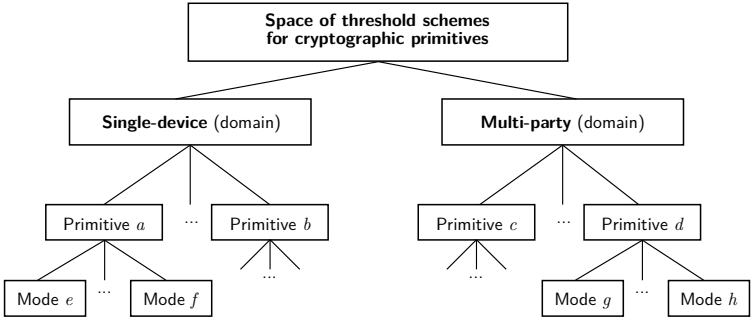

clker.com/clipart-15840.html

1. **Coordinates** (domains, primitives, modes, features)
2. **Features** (security, configurability, validation, modularity)
3. **Phases** (of the development process)
4. **Collaboration** (need feedback from stakeholders)

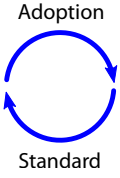
Mapping the space of potential “schemes”



Mapping the space of potential "schemes"



- "*Not every conceivable possibility is suitable for standardization*"
- "*Need to focus on where there is a high need and high potential for adoption*"
- *Best practices*; *minimum defaults*; *interoperability*; *innovation*.



Multi-Party track

Multi-party: separate components; active model (parties may be maliciously compromised).

Current focus on NIST-approved key-based primitives:

Multi-Party track

Multi-party: separate components; active model (parties may be maliciously compromised).

Current focus on NIST-approved key-based primitives:

- Simpler thresholdization: RSA signing/decryption, ECC key-gen, ECC-CDH primitive.
- More complex thresholdization: RSA key-gen, ECDSA signing, EdDSA signing, AES.

Legend of acronyms: AES (Advanced Encryption Standard); Cofactor Diffie-Hellman (CDH); ECC (Elliptic Curve Cryptography); ECDSA (Elliptic Curve Digital Signature Algorithm); EdDSA (Edwards Curve Digital Signature Algorithm); Keygen (key generation); RSA (Rivest–Shamir–Adleman).

Multi-Party track

Multi-party: separate components; active model (parties may be maliciously compromised).

Current focus on NIST-approved key-based primitives:

- Simpler thresholdization: RSA signing/decryption, ECC key-gen, ECC-CDH primitive.
- More complex thresholdization: RSA key-gen, ECDSA signing, EdDSA signing, AES.

Legend of acronyms: AES (Advanced Encryption Standard); Cofactor Diffie-Hellman (CDH); ECC (Elliptic Curve Cryptography); ECDSA (Elliptic Curve Digital Signature Algorithm); EdDSA (Edwards Curve Digital Signature Algorithm); Keygen (key generation); RSA (Rivest–Shamir–Adleman).

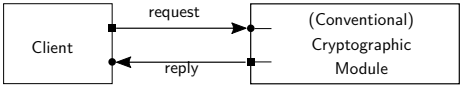
Interchangeability. (A useful notion) Informally, the conventional primitive can be replaced by the threshold version of it, with respect to some subsequent operation, e.g., a threshold signature being verifiable by the conventional verification algorithm, even if not fully equivalent.

Threshold interface modes (in the perspective of the client)

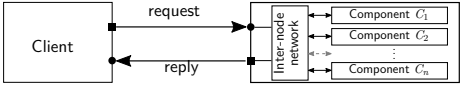
Input/Output interface: client communication with the module / threshold entity?

Threshold interface modes (in the perspective of the client)

Input/Output interface: client communication with the module / threshold entity?



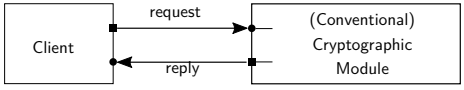
Conventional (non-threshold)



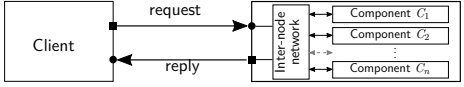
Not-shared-IO

Threshold interface modes (in the perspective of the client)

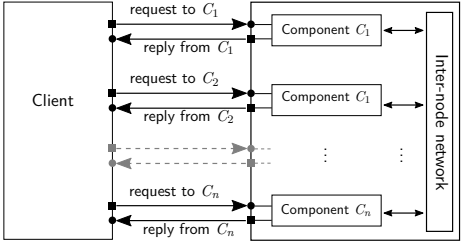
Input/Output interface: client communication with the module / threshold entity?



Conventional (non-threshold)



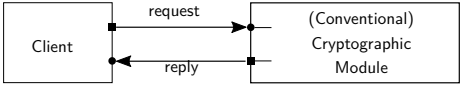
Not-shared-IO



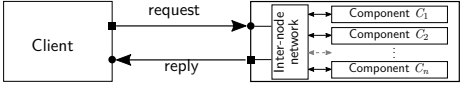
Shared-IO

Threshold interface modes (in the perspective of the client)

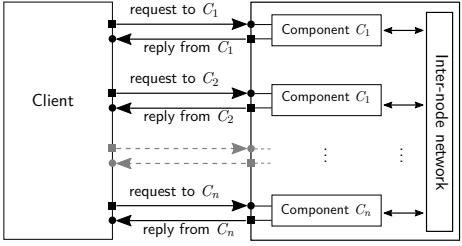
Input/Output interface: client communication with the module / threshold entity?



Conventional (non-threshold)



Not-shared-IO



Shared-IO

- **Example:** Shared-Output may enhance secrecy of the output of a decryption process.
- **Auditability:** can the client prove (or be convinced) the operation was thresholdized?

* **Other modes:** In Shared-I and Shared-O, only the **i**nput and only the **o**utput are shared, respectively.

Development process

A sequence of phases:

1. **Devise criteria for standardization***
2. **Calls for contributions**
3. **Evaluation of threshold schemes**
4. **Publish standards***

* **Note:** The use of “Standards” and “Standardization” does not intend to imply FIPS. Final formats may, for example, include Recommendations and Guidelines (e.g., SP 800), reference definitions, ...

Development process

A sequence of phases:

1. **Devise criteria for standardization***
2. **Calls for contributions**
3. **Evaluation of threshold schemes**
4. **Publish standards***

Each phase is open to public feedback.

Upcoming: NIST Workshop on Multi-Party Threshold Schemes (MPTS2020, November 4–6)

*** Note:** The use of "Standards" and "Standardization" does not intend to imply FIPS. Final formats may, for example, include Recommendations and Guidelines (e.g., SP 800), reference definitions, ...

NIST Workshop on Multi-Party Threshold Schemes

- **When:** November 4–6, 2020, 9am–1pm EST — Virtual event MPTS 2020
- **Goal:** Collect feedback for the multi-party track of the TC project.
- **How:** Invited *talks* ($\sim$20 min each) + Q&A; and submitted *briefs* ($\leq$5 min).
- **Scope:** Criteria for thresholdization of primitives identified in NISTIR 8214A.

For questions or comments related to the workshop, please send an email to workshop-MPTS-2020@nist.gov.

NIST Workshop on Multi-Party Threshold Schemes

- **When:** November 4–6, 2020, 9am–1pm EST — Virtual event MPTS 2020
- **Goal:** Collect feedback for the multi-party track of the TC project.
- **How:** Invited *talks* ($\sim$20 min each) + Q&A; and submitted *briefs* ($\leq$5 min).
- **Scope:** Criteria for thresholdization of primitives identified in NISTIR 8214A.

For questions or comments related to the workshop, please send an email to workshop-MPTS-2020@nist.gov.

NIST Workshop on Multi-Party Threshold Schemes

- **When:** November 4–6, 2020, 9am–1pm EST — Virtual event MPTS 2020
- **Goal:** Collect feedback for the multi-party track of the TC project.
- **How:** Invited *talks* ($\sim$20 min each) + Q&A; and submitted *briefs* ($\leq$5 min).
- **Scope:** Criteria for thresholdization of primitives identified in NISTIR 8214A.

Important dates:

- August 16: Start of online registration: https://csrc.nist.gov/events/2020/mpts2020
- September 30: Deadline for early registration (free)
- September 30: *briefs* submission (title + short abstract)
- October 28: late registration (conditions TBA)

For questions or comments related to the workshop, please send an email to workshop-MPTS-2020@nist.gov.

Some topics of expected feedback

1. configurability (threshold numbers, rejuvenation of components, ...);
2. practical feasibility (computational complexity, setup instantiation, ...);
3. security models (ideal functionalities, game-based definitions, ...);
4. security properties (e.g., termination options, breakdown after threshold, ...);
5. gadgets and modularity;
6. validation suitability.

(For more suggestions, see NISTIR 8214A, Sections 2.1–2.5, 5, 6.1 and 7.2)

(To read offline) More topics toward defining criteria

Some other relevant aspects (from Section 6.1 of NISTIR 8214A):

1. Definition of system model and threat model
2. Description of characterizing features
3. Analysis of efficiency and practical feasibility
4. Existence of open-source reference implementations
5. Concrete benchmarking (threshold vs. conventional; different platforms)
6. Detailed description of operations
7. Example application scenarios
8. Security analysis
9. Automated testing and validation of implementations
10. Disclosure and licensing of intellectual property

We welcome feedback on any of these items.

Outline

1. Intro NIST standards
2. Update on the NIST Threshold Cryptography project
3. Some thoughts on standardization
4. Concluding remarks

What is “advanced cryptography”?

Or maybe ask instead: what is challenging-to-standardize cryptography?

What is “advanced cryptography”?

Or maybe ask instead: what is challenging-to-standardize cryptography?

- Protocols (with distributed systems) instead of single-side primitives?
- Many paradigms/options to choose from?
- Complex techniques/assumptions not previously standardized/scrutinized?
- Uncertainty of adoption or what approach to take?

What is “advanced cryptography”?

Or maybe ask instead: what is challenging-to-standardize cryptography?

- Protocols (with distributed systems) instead of single-side primitives?
- Many paradigms/options to choose from?
- Complex techniques/assumptions not previously standardized/scrutinized?
- Uncertainty of adoption or what approach to take?

Moving toward standardization of Adv.Crypto can anyway benefit from preliminary work:

- Development of collaborative reference material (e.g., see ZKProof)
- Deployment of application use-cases, attesting feasibility and enabling benchmarking
- Promote improved “best practices” and interoperability

Standardization endeavors as processes

What does it entail to standardize "Advanced Cryptography"?

- It's not just detailedly writing a technique into an official document
- It includes the whole process till choosing/devising which technique(s) to standardize

Standardization endeavors as processes

What does it entail to standardize "Advanced Cryptography"?

- It's not just detailedly writing a technique into an official document
- It includes the whole process till choosing/devising which technique(s) to standardize

For example, the process includes deciding:

- how to call for (which types of) contributions;
- what criteria to use to search for and to select items for standardization.

Humans are in the equation

Collaboration between stakeholders is essential:

Humans are in the equation

Collaboration between stakeholders is essential:

- Propose and validate techniques to be considered for standardization
- Motivate use-cases for the modes / applications of interest
- Scrutinize the complex techniques being specified
- Share knowledge

Humans are in the equation

Collaboration between stakeholders is essential:

- Propose and validate techniques to be considered for standardization
- Motivate use-cases for the modes / applications of interest
- Scrutinize the complex techniques being specified
- Share knowledge

Also beware:

- Human resources are finite (both for the standardization bodies and other stakeholders)
- Standardization timelines should allow proper time for public scrutiny and feedback.

Humans are in the equation

Collaboration between stakeholders is essential:

- Propose and validate techniques to be considered for standardization
- Motivate use-cases for the modes / applications of interest
- Scrutinize the complex techniques being specified
- Share knowledge

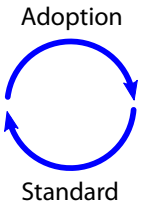
Also beware:

- Human resources are finite (both for the standardization bodies and other stakeholders)
- Standardization timelines should allow proper time for public scrutiny and feedback.

The end game: achieve trustworthy & trusted, globally accepted, adopted ... good standards

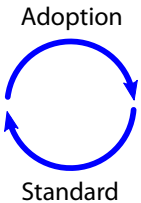
Standardization vs. adoption

What makes a standard *good*? A well-done specification ... and the context.



Standardization vs. adoption

What makes a standard *good*? A well-done specification ... and the context.

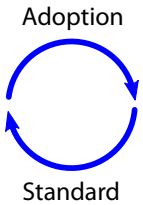


A *good* standard can be a reference for:

- *best practices* and *minimum defaults*;
- *interoperability*;
- validation and certification;
- what to innovate upon.

Standardization vs. adoption

What makes a standard *good*? A well-done specification ... and the context.



A *good* standard can be a reference for:

- *best practices* and *minimum defaults*;
- *interoperability*;
- validation and certification;
- what to innovate upon.

If/when compliance is required, a standard can be *bad* if the technique:

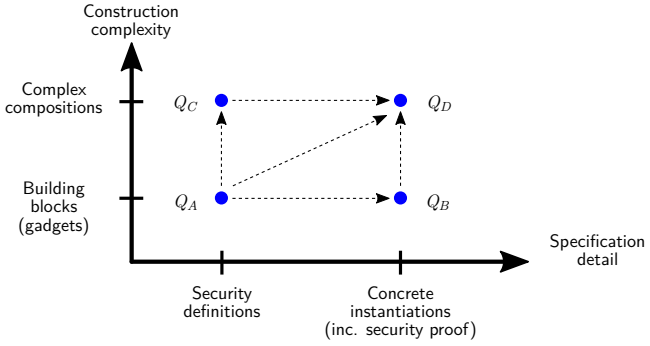
- is obsolete / outdated, or cannot be corrected / withdrawn / replaced (when it should);
- does not lend itself to suitable validation mechanisms.

Modularity and composability

- ideal functionalities vs. concrete protocols of threshold schemes?
- building blocks vs. complex constructions?

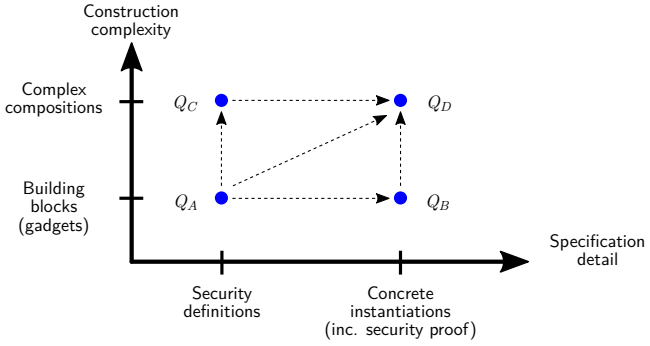
Modularity and composability

- ideal functionalities vs. concrete protocols of threshold schemes?
- building blocks vs. complex constructions?



Modularity and composability

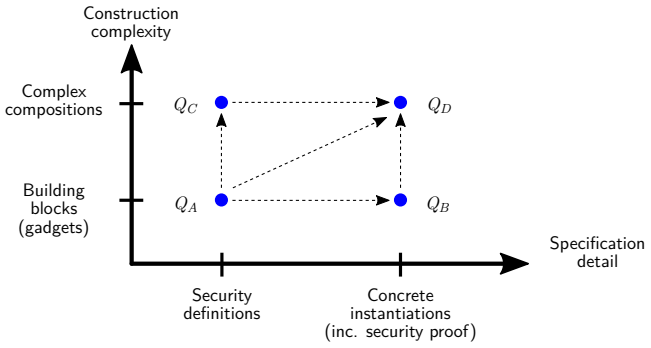
- ideal functionalities vs. concrete protocols of threshold schemes?
- building blocks vs. complex constructions?



Each has a place in the process, e.g.:
- Q_D as a goal;
- Q_C as a criterion;
- Q_B as a module;
- Q_A as a reference definition.

Modularity and composability

- ideal functionalities vs. concrete protocols of threshold schemes?
- building blocks vs. complex constructions?



Each has a place in the process, e.g.:
– Q_D as a goal;
– Q_C as a criterion;
– Q_B as a module;
– Q_A as a reference definition.

Example gadgets:

- secret-sharing
- distributed/correlated RNG
- garbled circuits
- oblivious transfer
- commitments ...

Outline

1. Intro NIST standards
2. Update on the NIST Threshold Cryptography project
3. Some thoughts on standardization
4. Concluding remarks

Concluding remarks

1. NIST has several ongoing standardization initiatives (e.g., PQC, LWC, TC).
2. NIST is interested in accompanying the developments of *advanced cryptography*.
3. Not everything should be standardized, but some things should
   (enable security and interoperability, improve best practices).
4. Official standardization can be preceded by valuable phases (e.g., develop reference material, ...)
5. The development process matters, and it affects the end result of standardization
   Collaboration between stakeholders is essential for a good result.

Concluding remarks

1. NIST has several ongoing standardization initiatives (e.g., PQC, LWC, TC).
2. NIST is interested in accompanying the developments of *advanced cryptography*.
3. Not everything should be standardized, but some things should
   (enable security and interoperability, improve best practices).
4. Official standardization can be preceded by valuable phases (e.g., develop reference material, ...)
5. The development process matters, and it affects the end result of standardization
   Collaboration between stakeholders is essential for a good result.
6. MPTS 2020 (November 4–6): consider contributing with your point of view.
7. It's an exciting time to collaborate toward new standards!

The test of time

Which of today's developing standards will remain,
70 years from now, as building blocks of advanced crypto?

The test of time

Which of today's developing standards will remain,
70 years from now, as building blocks of advanced crypto?

Photo in 1948 *

Photo in 2018: https://www.nist.gov/sites/default/files/documents/2018/06/15/nist_gaithersburg_master_plan_may_7_2018.pdf

Thank you for your attention

Toward Criteria for Standardization of Multi-Party Threshold Schemes for Cryptographic Primitives

Presentation on August 15, 20**20** @ ACAS2020, Virtual event
2nd Workshop on **A**dvanced **C**ryptography **A**pplications and **S**tandards

Feedback is appreciated

luis.brandao@nist.gov

List of Frames