

Let's talk about multi-party threshold schemes

Computer Security Division,
National Institute of Standards and Technology (Gaithersburg, USA)

Presentation* at [MPTS 2020](#)
NIST Workshop on **M**ulti-**P**arty **T**hreshold **S**chemes
November 4, 2020, Virtual event

*Luís T. A. N. Brandão — At NIST as a Foreign Guest Researcher (Contractor, from Strativia).

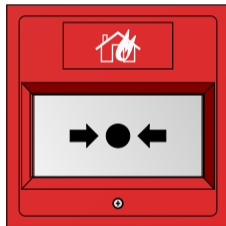
Opinions expressed in this presentation are from the speaker and are not to be construed as official views of NIST.

1. Workshop logistics
2. The TC project at NIST
3. Collecting feedback
4. Concluding remarks

1. Workshop logistics
2. The TC project at NIST
3. Collecting feedback
4. Concluding remarks

In case of fire alarm:

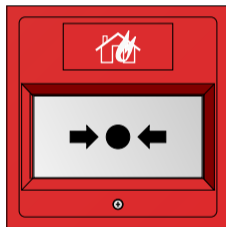
Please leave orderly into the exterior parking lot ...



clker.com/clipart-alarm.html

In case of fire alarm:

Please leave orderly into the exterior parking lot ...



clker.com/clipart-alarm.html

Ups, wrong script, this is a virtual event! ...

Workshop with free attendance, using “Webex events”

Roles: Host (and co-hosts), panelists, attendees, presenter.



[thenounproject.com/term/
screen-teleconference/601579/](https://thenounproject.com/term/screen-teleconference/601579/)

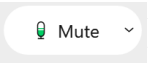
Workshop with free attendance, using “Webex events”

Roles: Host (and co-hosts), panelists, attendees, presenter.



[thenounproject.com/term/
screen-teleconference/601579/](https://thenounproject.com/term/screen-teleconference/601579/)

- ▶ **Hosts (one at a time):** The TC team (reach out to Luís, Michael, Apostol, René or Dustin if having some difficulty during the workshop)
- ▶ **Panelists:** All speakers in the other 17 talks and 11 briefs. Can show video.
- ▶ **Attendees:** Cannot show video, but can send messages to panelists+hosts.
- ▶ **Presenter (one at a time):** Can show slides; role is assigned by the host.

- ▶ Please mute yourself ( Mute) while not presenting
- ▶ Two modes of sending text-messages:
 - ▶ **Chat**: logistic notes or comments to be addressed by a host or panelist
 - ▶ **Q&A**: questions/notes to be asked to the **presenters** (as time allows)
- ▶ Q&A: co-hosts will try to relay some “Q&A” questions to the presenter
- ▶ Audio-visuals in workshop website (after the event):
 - ▶ We’re trying to record the entire video to later publish it online
 - ▶ Slides will also be available (when speakers provide them)



- ▶ We assume presenters speak in personal capacity ... affiliations can be mentioned
- ▶ Timing:
 - ▶ Each day: 6 talks, various briefs [, possible time for open comments]
 - ▶ Each talk: uninterrupted ~20 min; then ~5 min Q&A.
 - ▶ Each brief: uninterrupted ~ 5 min.
- ▶ Some connectivity issues may occur ... we will be flexible

1. Workshop logistics
2. The TC project at NIST
3. Collecting feedback
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

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

* = ctker.com/clipart-

Why going for a threshold approach?

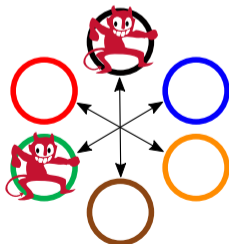
Crypto can be affected by vulnerabilities

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

How to address
single-points
of failure?



The threshold approach

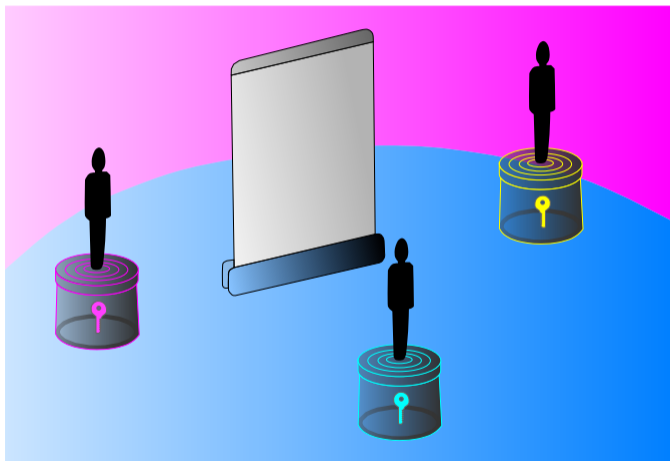


The red dancing devil is from
ctker.com/clipart-13643.html

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 their *key shares* remain secret
- ▶ **Result:** The combined outputs derive the decrypted plaintext

The Threshold Cryptography Project at NIST



Scope: standardization of threshold schemes for cryptographic primitives

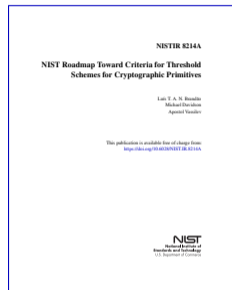
<https://csrc.nist.gov/Projects/Threshold-Cryptography/>

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/>

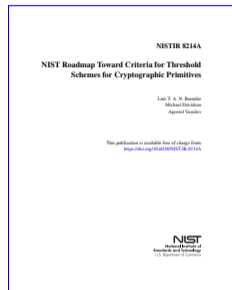


NISTIR 8214A: NIST Roadmap Toward Criteria for Threshold Schemes for Cryptographic Primitives



clipart.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)



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



clipart.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)

- ▶ *“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.*

- ▶ Separate components (parties), possibly dynamic membership;
- ▶ Arbitrary inter-communication environment;
- ▶ Active model: parties can be maliciously compromised.

- ▶ Separate components (parties), possibly dynamic membership;
- ▶ Arbitrary inter-communication environment;
- ▶ Active model: parties can be maliciously compromised.

Thresholdization complexity:

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

* EdDSA signing

- ▶ Separate components (parties), possibly dynamic membership;
- ▶ Arbitrary inter-communication environment;
- ▶ Active model: parties can be maliciously compromised.

Thresholdization complexity:

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

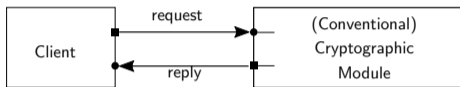
* EdDSA signing

Modularity is an important consideration:

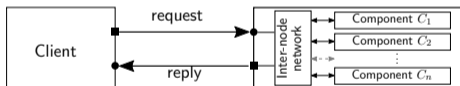
- ▶ secret-sharing, oblivious transfer, garbled circuits, consensus/broadcast ...

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

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

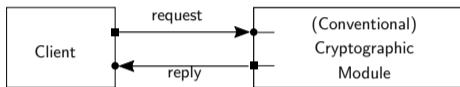


Conventional (non-threshold)

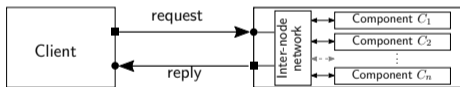


Threshold Not-shared-IO

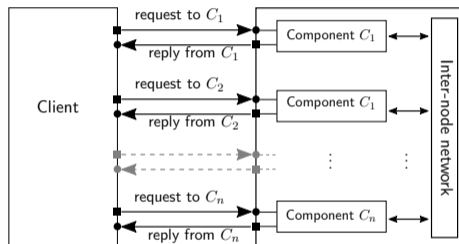
Input/Output interface: client communication with the module / threshold entity?



Conventional (non-threshold)

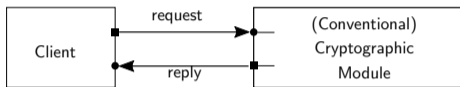


Threshold Not-shared-IO

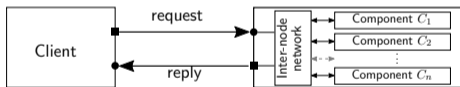


Threshold Shared-IO

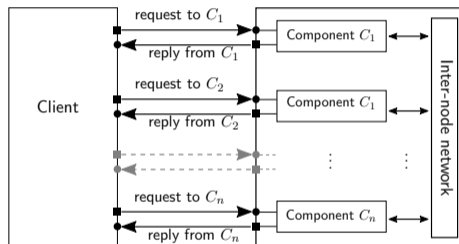
Input/Output interface: client communication with the module / threshold entity?



Conventional (non-threshold)



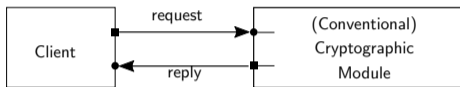
Threshold Not-shared-IO



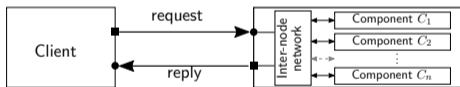
Threshold Shared-IO

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

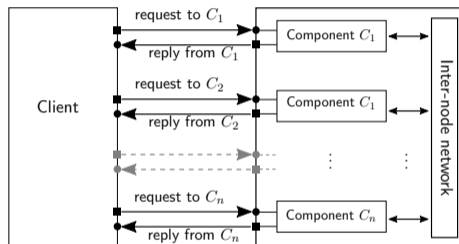
Input/Output interface: client communication with the module / threshold entity?



Conventional (non-threshold)



Threshold Not-shared-IO



Threshold Shared-IO

- ▶ **Example:** Shared-Output mode 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 input and only the output are shared, respectively.

Notions of interoperability (client's perspective)

Client's perspective of functional properties of a crypto primitive.

Client's perspective of functional properties of a crypto primitive.

- ▶ **Functional equivalence.** Same input/output distribution
 - ▶ Decryption: threshold decryption must give same result as conventional decryption
- ▶ **Functional interchangeability.** Compatibility of operations (need-not be equivalent)
 - ▶ Key-gen: RSA integers forced to be Blum integers (product of two primes $\equiv 3 \pmod{4}$)
 - ▶ Signatures: deterministic vs. probabilistic (secret randomness), with same verification

Client's perspective of functional properties of a crypto primitive.

- ▶ **Functional equivalence.** Same input/output distribution
 - ▶ Decryption: threshold decryption must give same result as conventional decryption
- ▶ **Functional interchangeability.** Compatibility of operations (need-not be equivalent)
 - ▶ Key-gen: RSA integers forced to be Blum integers (product of two primes $\equiv 3 \pmod{4}$)
 - ▶ Signatures: deterministic vs. probabilistic (secret randomness), with same verification

Latitude of applicability? Open question per primitive ... feedback is useful

A sequence of phases:

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

* to evaluate or compare, to call for proposals, to standardize, ...

[†] **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, ...

1. Workshop logistics
2. The TC project at NIST
3. Collecting feedback
4. Concluding remarks

Opportunity to hear experts' views on diverse threshold topics/primitives/settings of interest.

Invited **talks** spanning diverse topics of interest; submitted "**briefs**" to complement.

Opportunity to hear experts' views on diverse threshold topics/primitives/settings of interest.

Invited **talks** spanning diverse topics of interest; submitted "**briefs**" to complement.

Intended to serve as basis to:

1. Systematize various ideas / topics of criteria (will be open to public comments)
2. Motivate further feedback by the community

Opportunity to hear experts' views on diverse threshold topics/primitives/settings of interest.

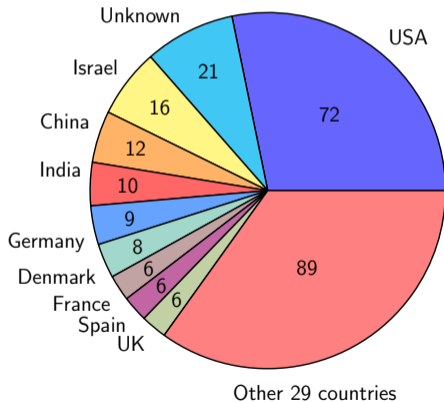
Invited **talks** spanning diverse topics of interest; submitted "**briefs**" to complement.

Intended to serve as basis to:

1. Systematize various ideas / topics of criteria (will be open to public comments)
2. Motivate further feedback by the community
3. Possibly derive a number of posterior questions to pose to the community
4. Possibly organize more-focused consultations

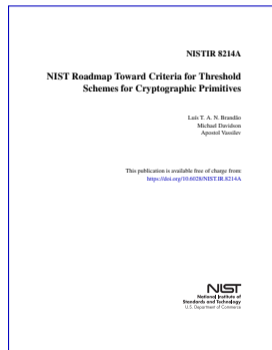
Registration stats (preliminary)

236 registrations across 38⁺ countries:

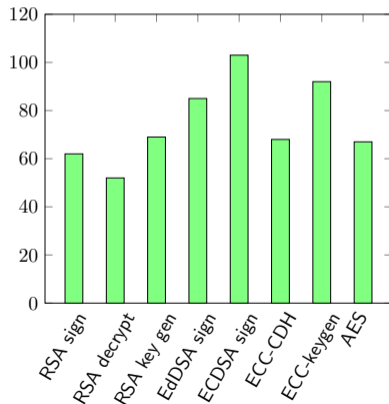


Familiarity with NISTIR 8214A?

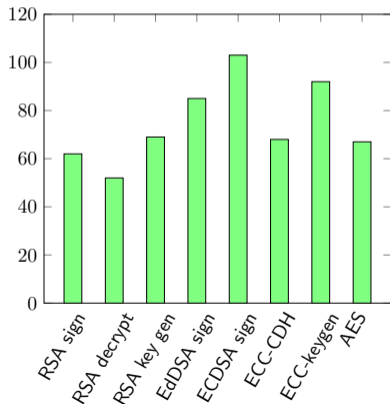
Yes: 100; No: 128; N/A: 8.



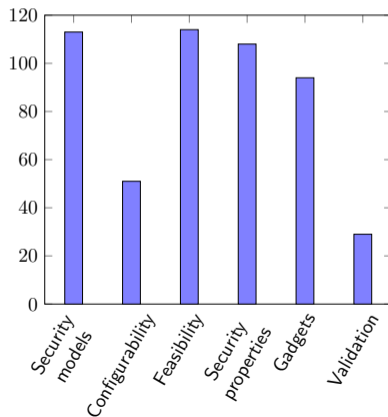
In which primitives are you most interested in?



In which primitives are you most interested in?



What threshold-related topics are of most interest to you?



MPTS schedule 1st day (November 4)

#	Hour	Speaker(s)	Topic (not the title)
	09:30–09:35	—	Virtual arrival
1a1	09:35–10:00	Luís Brandão	Workshop introduction
1a2	10:00–10:25	Berry Schoenmakers	Publicly verifiable secret sharing
1a3	10:25–10:50	Ivan Damgård	Active security with honest majority
	10:50–11:05	—	Break
1b1	11:05–11:30	Tal Rabin	MPC in the YOSO model
1b2	11:30–11:55	Nigel Smart	Threshold HashEdDSA (deterministic)
1b3	11:55–12:20	Chelsea Komlo	Threshold Schnorr (probabilistic)
	12:20–12:30	—	Break
1c1	12:30–12:36	Yashvanth Kondi	Threshold Schnorr (deterministic)
1c2	12:36–12:42	Akira Takahashi	PQ Threshold signatures
1c3	12:42–12:48	Jan Willemson	PQ Threshold schemes
1c4	12:48–12:54	Saikrishna Badrinarayanan	Threshold bio-authentication

All times are expressed in Eastern Standard Time (EST) timezone.

MPTS schedule 2nd day (November 5)

#	Hour	Speaker(s)	Topic (not the title)
	09:30–09:35	—	Virtual arrival
2a1	09:35–10:00	Yehuda Lindell	Diverse multiparty settings
2a2	10:00–10:25	Ran Canetti	General principles (composability, ...)
2a3	10:25–10:50	Yuval Ishai	Pseudorandom correlation generators
	10:50–11:05	—	Break
2b1	11:05–11:30	Emmanuela Orsini & Peter Scholl	Oblivious transfer extension
2b2	11:30–11:55	Vladimir Kolesnikov	Garbled circuits
2b3	11:55–12:20	Xiao Wang	Global scale threshold AES
	12:20–12:30	—	Break
2c1	12:30–12:36	Xiao Wang	Garbled circuits
2c2	12:36–12:42	Frank W. & Dan B. & Omer S.	MPC Alliance
2c3	12:42–12:48	Jakob Pagter	MPC-based Key-management
2c4	12:48–12:54	Phillip Hallam-Baker	Threshold key infrastructure
2c5	12:54–13:00	Ronald Tse	Framework for threshold cryptography

All times are expressed in Eastern Standard Time (EST) timezone.

MPTS schedule 3rd day (November 6)

#	Hour	Speaker(s)	Topic (not the title)
	09:30–09:35	—	Virtual arrival
3a1	09:35–10:00	JP Aumasson & Omer Shlomovits	Attacks to deployed threshold signatures
3a2	10:00–10:25	Kris Shrishak	Threshold ECDSA
3a3	10:25–10:50	Nikolaos Makriyannis	Threshold ECDSA
	10:50–11:05	—	Break
3b1	11:05–11:30	Schuyler Rosefield	Distributed RSA key generation
3b2	11:30–11:55	Muthu Venkitasubramanian	Distributed RSA key generation
3b3	11:55–12:20	Marcella Hastings	Implementation frameworks
	12:20–12:30	—	Break
3c1	12:30–12:36	Damian Straszak	Threshold ECDSA
3c2	12:36–12:42	Jack Doerner	Threshold ECDSA
	12:42–13:00 ⁺	Various	Final comments

All times are expressed in Eastern Standard Time (EST) timezone.

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

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

- ▶ Propose and validate techniques to be considered for standardization
- ▶ Explain use-cases that benefit from standardization of threshold schemes for particular primitives/modes
- ▶ Scrutinize complex techniques proposed by other stakeholders
- ▶ Share knowledge

- ▶ Propose and validate techniques to be considered for standardization
- ▶ Explain use-cases that benefit from standardization of threshold schemes for particular primitives/modes
- ▶ Scrutinize complex techniques proposed by other stakeholders
- ▶ Share knowledge

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

The object (threshold schemes) is substantially different from that of previous/ongoing “competitions” (AES, SHA, PQC, LWC):

- ▶ We know the primitives being enhanced ... e.g., not developing a new block-cipher.
- ▶ It's “standard” to have proofs of security for SMPC
- ▶ Distributed protocols (“advanced cryptography”?)

The development process matters, and it can affect the end result of standardization. Collaboration with stakeholders is essential for a good result.

1. Workshop logistics
2. The TC project at NIST
3. Collecting feedback
4. Concluding remarks

1. NIST has an ongoing standardization initiative for threshold schemes.
2. Goal: enable threshold-based implementations/operations of cryptographic primitives
3. It's not full-blown SMPC, but may benefit from generic tools/gadgets therefrom
4. Not everything should be standardized, but some things should (enable security and interoperability, improve best practices).
5. After the workshop, consider (anyone in the audience) sending us additional feedback on criteria for threshold schemes.

1. NIST has an ongoing standardization initiative for threshold schemes.
2. Goal: enable threshold-based implementations/operations of cryptographic primitives
3. It's not full-blown SMPC, but may benefit from generic tools/gadgets therefrom
4. Not everything should be standardized, but some things should (enable security and interoperability, improve best practices).
5. After the workshop, consider (anyone in the audience) sending us additional feedback on criteria for threshold schemes.
6. It's an exciting time to collaborate toward new standards!

Let's talk about multi-party threshold schemes

Presentation on November 4, 2020 @ MPTS 2020, Virtual event
NIST Workshop on **Multi Party Threshold Schemes 2020**

Email the threshold crypto team: threshold-crypto@nist.gov

Check the MPTS 2020 webpage: <https://csrc.nist.gov/events/2020/mpts2020>

Join the public TC forum: <https://list.nist.gov/tc-forum>

Follow updates of the NIST TC project: <https://csrc.nist.gov/Projects/Threshold-Cryptography>

Disclaimer. Opinions expressed in this presentation are from the author(s) and are not to be construed as official or as views of the U.S. Department of Commerce. The identification of any commercial product or trade names in this presentation does not imply endorsement of recommendation by NIST, nor is it intended to imply that the material or equipment identified are necessarily the best available for the purpose.

Disclaimer. Some external-source images and cliparts were included/adapted in this presentation with the expectation of such use constituting licensed and/or fair use.

- 1 Cover
- 2 Outline
- 3 In case of fire alarm:
- 4 Tele-conference roles
- 5 Tele-conference how to
- 6 Talks and briefs
- 7 Outline
- 8 Why going for a threshold approach?
- 9 A depiction of multi-party threshold decryption
- 10 The Threshold Cryptography Project at NIST
- 11 NISTIR 8214A: A roadmap toward criteria
- 12 Multi-Party track
- 13 Threshold interface modes (client's perspective)
- 14 Notions of interoperability (client's perspective)
- 15 Development process
- 16 Outline
- 17 MPTS workshop as a source of feedback
- 18 Registration stats (preliminary)
- 19 Registration answers
- 20 MPTS schedule 1st day (November 4)
- 21 MPTS schedule 2nd day (November 5)
- 22 MPTS schedule 3rd day (November 6)
- 23 Some topics of wanted feedback
- 24 Collaboration with stakeholders is essential
- 25 What kind of standardization effort?
- 26 Outline
- 27 Concluding remarks
- 28 Thank you for your attention

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); FIPS (Federal Information Processing Standard); IFC (Integer Factorization Cryptography); NIST (National Institute of Standards and Technology); NISTIR (NIST Internal or Interagency Report); RSA (Rivest–Shamir–Adleman); SP (Special Publication).

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); FIPS (Federal Information Processing Standard); IFC (Integer Factorization Cryptography); NIST (National Institute of Standards and Technology); NISTIR (NIST Internal or Interagency Report); RSA (Rivest-Shamir-Adleman); SP (Special Publication).

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