MPTS 2020 final comments

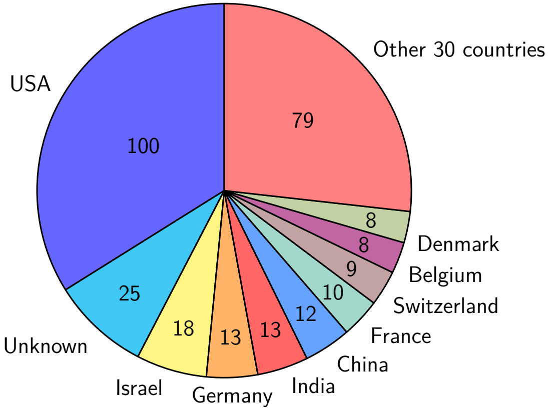
Computer Security Division,
National **I**nstitute of **S**tandards and **T**echnology (Gaithersburg, USA)

Presentation* at MPTS 2020
NIST Workshop on **M**ulti-**P**arty **T**hreshold **S**chemes
November 6, 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.

Registration stats (updated November 5)

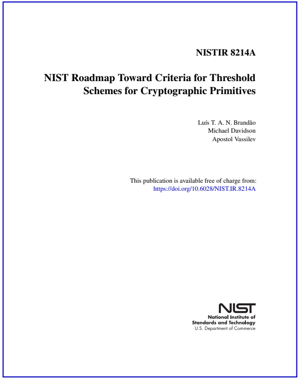
292 registrations across 40$^+$ countries:



(The USA count includes 20 from NIST)

Familiarity with NISTIR 8214A?

Yes: 121; **No:** 165; **N/A:** 6.



NISTIR 8214A

NIST Roadmap Toward Criteria for Threshold Schemes for Cryptographic Primitives

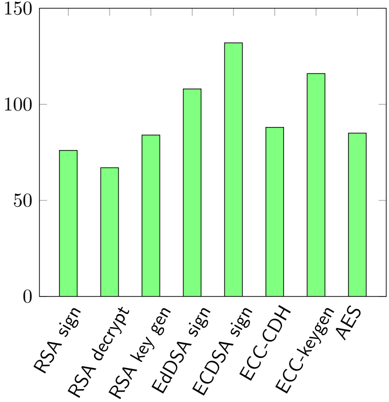
Luís T. A. N. Brandão
Michael Davidson
Apostol Vassilev

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

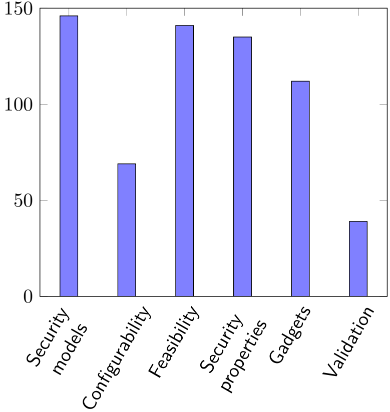
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Registration answers

In which primitives are you most interested in?



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



Answers were not mandatory

Recalling why this workshop:

Hear experts on diverse threshold topics/primitives/settings of interest, to:

1. Support an internal systematization of ideas/topics to advance the TC project (namely to develop criteria for multi-party threshold schemes)
2. Motivate further feedback by the community

Feedback collection may continue:

- Derive posterior questions to pose to the community
- Organize more-focused consultations

Thank you for participating!

Close to 300 registrations; 17 invited talks; 11 briefs.

We hope you remain interested in engaging with the TC project.

Some resources:

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

Next: mini-briefs

Thank you for participating!

Close to 300 registrations; 17 invited talks; 11 briefs.

We hope you remain interested in engaging with the TC project.

Some resources:

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

Next: mini-briefs

- Use the "raise-hand" feature to signal interest in leaving a final comment ($\leq$ 1 min)
- The host will temporarily upgrade your role to panelist (for voice+video capability)
- We'll be flexible with the end time (13:00+) based on the number of intended comments