NIST Threshold Workshop 2019 — 1st day

All talks take place in the Green Auditorium in the Main Building (101) at the NIST campus in Gaithersburg, MD, USA
Attendees need to pre-register to attend the conference. Badge pick-up (for on time and late arrivals) is done in front of the Green auditorium.

Session	Hour	Time†	1st day of workshop (Monday, March 11, 2019)	Source	#
---	08:00-09:00	60	**Badge pick-up; light refreshments available**	---	-
Opening	09:00-09:10	10	**NIST Computer Security Division welcoming. Matthew Scholl** (NIST, USA)	NIST	1
I.1. Threshold Schemes (Chair: Rene Peralta, NIST)	09:10-09:25	15	**Enter the Threshold (The NIST Threshold Cryptography Project). Luís Brandão** (NIST, USA)	NIST	2
	09:25-10:15	50	**Threshold Cryptography: Ready for Prime Time? Hugo Krawczyk** (IBM Research, USA)	**Invited Keynote**	3
	10:15-10:40	25	**Platform for Robust Threshold Cryptography.** Christian Cachin (University of Bern, Switzerland), Hugo Krawczyk (IBM Research, USA), Tal Rabin (IBM Research, USA), **Jason Resch** (IBM, USA), Chrysoula Stathakopoulou (IBM research, Zurich, Switzerland)	Submitted Presentation	4
---	10:40-11:10	30	**Coffee break**	---	-
I.2. NIST Standards (Chair: Andrew Regenscheid, NIST)	11:10-11:40	30	**The NIST Standardization Approach on Cryptography – Past, Present, and Future. Lily Chen** (NIST, USA)	NIST	5
	11:40-12:00	20	**NIST Status Update on Elliptic Curves and Post-Quantum Crypto. Dustin Moody** (NIST, USA)	NIST	6
I.3. Threshold Post-Quantum (Chair: Daniel Apon, NIST)	12:00-12:25	25	**Adding Distributed Decryption and Key Generation to a Ring-LWE Based CCA Encryption Scheme.** Michael Kraitsberg (Unbound Technology, Israel), Yehuda Lindell (Bar-Ilan University, Israel; Unbound Technology, Israel), Valery Osheter (Unbound Technology, Israel), **Nigel P. Smart** (KU Leuven, Belgium; University of Bristol, UK), Younes Talibi Alaoui (KU Leuven, Belgium)	Submitted Paper	7
---	12:25-13:45	80	**Lunch (at the Heritage room)**	---	-
I.4. Threshold Signatures (Chair: Daniel Apon, NIST)	13:45-14:10	25	**Fully Distributed Non-Interactive Adaptively-Secure Threshold Signature Scheme with Short Shares: Efficiency Considerations and Implementation.** Benoît Libert (CNRS and ENS de Lyon, France), Marc Joye (OneSpan, Belgium), Moti Yung (Google Inc. and Columbia University, USA), **Fabrice Mouhartem** (ENS de Lyon, France)	Submitted Paper	8
	14:10-14:35	25	**A Multiparty Computation Approach to Threshold ECDSA.** Jack Doerner (Northeastern University, USA), **Yashvanth Kondi** (Northeastern University, USA), Eysa Lee (Northeastern University, USA), abhi shelat (Northeastern University, USA)	Submitted Paper	9
I.5. Panel on Threshold for DSS (Chair: Hugo Krawczyk, IBM Research)	14:35-15:35	60	**Threshold Protocols for the Digital Signature Standard.** Moderator: **Hugo Krawczyk** (IBM Research, USA); Panelists: **Rosario Gennaro** (CUNY, USA), **abhi shelat** (Northeastern University, USA), **Samuel Ranellucci** (Unbound Tech, Israel)	Submitted Panel	10
---	15:35-16:05	30	**Coffee break**	---	-
I.6. Validation (Chair: Michael Cooper, NIST)	16:05-16:45	40	***Quo Vadis*, Crypto Validation? Apostol Vassilev** (NIST, USA)	NIST	11
I.7. Discussion (Chair: Michael Cooper, NIST)	16:45-17:30	45	**Open discussion.** Moderator: **Nicky Mouha** (NIST, USA)	NIST	12

† Time durations are in minutes

Expected speakers are highlighted in **bold**.

Available shuttles:

- For guests at the Courtyard by Marriot Hotel, Gaithersburg, a shuttle will be available (both days) at 7:30am for Hotel → NIST, and at 5:45pm (Monday) or 5:30pm (Tuesday) for NIST → Hotel
- A NIST shuttle to NIST departs from the Shady grove Metro Station, Bus Bay C **(**go right when exiting the station**)** at 15 and 45 minutes past the hour.
- A NIST shuttle to Shady Grove Metro Station departs from the NIST Building 101 at 5 and 35 minutes past the hour. The last NIST shuttle leaves NIST at 6:00 p.m.
- See https://www.nist.gov/about-nist/visit/getting-nist-gaithersburg for further details

See online updates at the conference webpage: https://csrc.nist.gov/Events/2019/NTCW19

NIST Threshold Workshop 2019 — 2nd day

All talks take place in the Green Auditorium in the Main Building (101) at the NIST campus in Gaithersburg, MD, USA
Attendees need to pre-register to attend the conference. Badge pick-up (for on time and late arrivals) is done in front of the Green auditorium.

Session	Hour	Time†	2nd day of workshop (Tuesday, March 12, 2019)	Source	#
---	08:00-08:45	45	**Badge pick-up; light refreshments available**	---	-
II.1. Threshold Circuit Design (Chair: Meltem S. Turan, NIST)	08:45-09:10	25	**Optimized Threshold Implementations: Number of Shares and Area/Latency Trade-off.** Dušan Božilov (NXP Semiconductors, Belgium; COSIC KU Leuven and imec, Belgium), Miroslav Knežević (NXP Semiconductors, Belgium), **Ventzislav Nikov** (NXP Semiconductors, Belgium)	Submitted Presentation	13
	09:10-09:35	25	**The pitfalls of threshold cryptography in hardware.** **Marco Macchetti** (Kudelski Group, Switzerland), Karine Villegas (Kudelski Group, Switzerland), Claudio Favi (Kudelski Group, Switzerland)	Submitted Presentation	14
	09:35-10:00	25	**Threshold Cryptography against Combined Physical Attacks.** **Lauren De Meyer** (KU Leuven, Belgium)	Submitted Presentation	15
	10:00-10:25	25	**VerMI: Verification Tool for Masked Implementations.** **Victor Arribas** (KU Leuven, imec-COSIC, Belgium), Svetla Nikova (KU Leuven, imec-COSIC, Belgium), Vincent Rijmen (KU Leuven, imec-COSIC, Belgium)	Submitted Presentation	16
---	10:25-10:55	30	**Coffee break**	---	-
II.2. Panel on TIS (Chairs: Svetla Nikova and Vincent Rijmen, KU Leuven)	10:55-12:10	75	**Theory of Implementation Security Panel.** Moderators: **Svetla Nikova** (KU Leuven, Belgium), **Vincent Rijmen** (KU Leuven, Belgium). Panelists: **Nigel Smart** (KU Leuven, Belgium), **Ventzislav Nikov** (NXP Semiconductors, Belgium), **Mike Hutter** (Rambus, USA), **Junfeng Fan** (Open Security Research, China), **Ruggero Susella** (ST Microelectronics, Italy), **Emmanuel Prouff** (ANSSI, France)	Submitted Panel	17
---	12:10-13:30	80	**Lunch (at the Heritage room)**	---	-
II.3. Other Threshold Primitives (Chair: John Kelsey, NIST)	13:30-13:55	25	**Efficient Leakage Resilient Secret Sharing.** Peihan Miao (UC Berkeley, USA), Akshayaram Srinivasan (UC Berkeley, USA), **Prashant Nalini Vasudevan** (UC Berkeley, USA)	Submitted Paper	18
	13:55-14:20	25	**DiSE: Distributed Symmetric-key Encryption. Shashank Agrawal** (Visa Research, USA), Payman Mohassel (Visa Research, USA), Pratyay Mukherjee (Visa Research, USA), Peter Rindal (Visa Research, USA)	Submitted Paper	19
II.4. Threshold Cryptography Applications and Experience (Chair: Michael Davidson, NIST)	14:20-15:10	50	**Challenges for Multisignature and Threshold Signature Implementation in a Bitcoin Context.** **Andrew Poelstra** (Blockstream, USA)	**Invited Keynote**	20
	15:10-15:40	30	**Coffee break**	---	-
	15:40-16:05	25	**SplitKey Case Study.** **Maximiliaan van de Poll** (Cybernetica AS, Estonia), **Aivo Kalu** (Cybernetica AS, Estonia)	Submitted Presentation	21
	16:05-16:30	25	**Practical Threshold Cryptography for Cloud and Cryptocurrencies.** **Jakob Pagter** (Sepior, Denmark)	Submitted Presentation	22
	16:30-16:55	25	**Practice Based Recommendations for Standardization of Threshold Cryptography.** **Daniel Shumow** (Microsoft Research, USA)	Submitted Presentation	23
Closing	16:55-17:15	20	**Final remarks.** Moderator: **Luís Brandão** (NIST, USA)	NIST	24

† Time durations are in minutes

Expected speakers are highlighted in **bold**.

Available shuttles:

- For guests at the Courtyard by Marriot Hotel, Gaithersburg, a shuttle will be available (both days) at 7:30am for Hotel → NIST, and at 5:45pm (Monday) or 5:30pm (Tuesday) for NIST → Hotel
- A NIST shuttle to NIST departs from the Shady grove Metro Station, Bus Bay C **(**go right when exiting the station**)** at 15 and 45 minutes past the hour.
- A NIST shuttle to Shady Grove Metro Station departs from the NIST Building 101 at 5 and 35 minutes past the hour. The last NIST shuttle leaves NIST at 6:00 p.m.
- See https://www.nist.gov/about-nist/visit/getting-nist-gaithersburg for further details

See online updates at the conference webpage: https://csrc.nist.gov/Events/2019/NTCW19

NIST Threshold Cryptography Workshop 2019

(March 11–12, Gaithersburg Md., USA)

Invited keynote 1 (Monday, March 11)

Speaker: Hugo Krawczyk (IBM Research, USA)

Title: Threshold Cryptography: Ready for Prime Time?

Abstract: The trend in trust decentralization together with the ever increasing value of digital assets (cryptocurrencies, blockchains, mega data repositories, key (mis)management, intellectual property, privacy, etc.) and the need to protect these assets for secrecy and availability, make threshold cryptography a most relevant technology whose time has come. We need to see more targeted applications as well as software platforms on which to build solutions that take into account real-world considerations such as asynchronous networks, support for diversified architectures, hardware enclaves, and more. Additionally, we need to refresh the set of techniques supporting threshold cryptography with advances in areas such as multi-party computation, quantum-resistant primitives, and blockchain-inspired consensus protocols. In addition to arguing these points, the talk will discuss some recent applications of threshold cryptography in the domain of key and password management, blockchain, and how threshold cryptography can be relevant to the #metoo movement.

Bio: Hugo Krawczyk is an IBM Fellow and Distinguished Research Staff Member with the Cryptography Group at the IBM T.J. Watson Research Center whose interests span theoretical and applied aspects of cryptography. He has contributed to the cryptographic design of numerous Internet standards, particularly IPsec, IKE, and SSL/TLS, and is a co-inventor of the HMAC message authentication algorithm. His most recent work in this area includes designs for TLS 1.3, the next generation TLS, and HKDF, the emerging standard for key derivation adopted by TLS 1.3, Signal, WhatsApp, Facebook Messenger and more. He has contributed to multiple areas of cryptography including to the theory and practice of key exchange, threshold and proactive cryptosystems, password authentication, and search on encrypted data. He is a Fellow of the International Association of Cryptologic Research (IACR) and the recipient of the 2015 RSA Conference Award for Excellence in the Field of Mathematics, the 2018 Levchin Prize for Contributions to Real-World Cryptography, and of multiple IBM awards, including two corporate awards.

Invited keynote 2 (Tuesday, March 12)

Speaker: Andrew Poelstra (Blockstream, USA)

Title: Challenges for Multisignature and Threshold Signature Implementation in a Bitcoin Context

Abstract: Bitcoin, started in 2009, is a digital currency in which all activity is publicly verifiable. Coins are controlled by spending policies expressed in *Bitcoin Script*, a simple stack-based programming language which supports hash preimage challenges and digital signatures. Included in Bitcoin Script is a basic form of threshold ECDSA signature: a list of public keys and a threshold is specified; the coins can then be moved if threshold-many valid ECDSA signatures are provided in sequence.

This threshold scheme is inefficient in terms of both signature size and verification time (both linear in the threshold size), which are the two most important considerations for cryptosystems designed for inclusion on blockchains. Being explicitly specified, they also represent a fungibility loss as threshold-controlled coins are visibly distinct from non-threshold-controlled coins. However, they achieve several practical goals which have proved difficult to preserve in more efficient threshold schemes: they are noninteractive; they require no persistent state during signing; they work in the plain public-key model and require no interactive key setup; their security follows immediately from the security of the underlying ECDSA scheme even when signing counterparties are considered to be adversarial.

In this talk we describe our work in developing a multisignature scheme for Bitcoin, called MuSig, which supports an extension to threshold signatures, over the last several years. We describe how consideration of both practical use cases and formal security models guided the evolution of our goals, and the unexpected tradeoffs that we found ourselves forced to make.

Bio: Andrew Poelstra is a Mathematician at Blockstream. He has dabbled in software development for the last twenty years, in open-source cryptography for ten. He became involved in Bitcoin in late 2011, and joined Blockstream cofounders Greg Maxwell and Pieter Wuille in developing the high-performance cryptography library libsecp256k1. His latest major project has been Mimble Wimble which is described as a blockchain design with no script support and blinded amounts. Like proverbial black holes, transaction outputs have no hair. This simplicity allows aggressive compaction and aggregation, resulting in a blockchain with much better scalability than any other design to date. He has a Bachelor of Science in Mathematics from Simon Fraser University. While completing his Masters of Arts at the University of Texas at Austin, he wrote and co-wrote several papers about Bitcoin, practical cryptography and mathematics.

Accepted panels:

- *Threshold Protocols for the Digital Signature Standard.* Moderator: Hugo Krawczyk[1]. Panelists: Rosario Gennaro[2], abhi shelat[3], Samuel Ranellucci[4]. ([1] IBM Research, USA; [2]CUNY, USA; [3] Northeastern University, USA; [4] Unbound Tech, Israel)
- *Theory of Implementation Security Panel.* Moderators: Svetla Nikova[1], Vincent Rijmen[1]. Panelists: Nigel Smart[1], Ventzislav Nikov[2], Mike Hutter[3], Junfeng Fan[4], Ruggero Susella[5], Emmanuel Prouff[6]. ([1] KU Leuven, Belgium; [2] NXP, Belgium; [3] Rambus, USA; [4] Open Security Research; [5] ST Microelectronics, China; [6] ANSSI, France)

Accepted papers:

- *Adding Distributed Decryption and Key Generation to a Ring-LWE Based CCA Encryption Scheme.* Michael Kraitsberg[3], Yehuda Lindell[1,3], Valery Osheter[3], Nigel P. Smart[2,4], Younes Talibi Alaoui[2]. ([1] Bar-Ilan University, Israel; [2] KU Leuven, Belgium; [3] Unbound Technology, Israel; [4] University of Bristol, UK)
- *Fully Distributed Non-Interactive Adaptively-Secure Threshold Signature Scheme with Short Shares: Efficiency Considerations and Implementation.* Benoît Libert[1,2], Marc Joye[3], Moti Yung[4],

Fabrice Mouhartem[2]. ([1] CNRS, France; [2] ENS de Lyon, France; [3] OneSpan, Belgium; [4] Google Inc. and Columbia University, USA)

- *A Multiparty Computation Approach to Threshold ECDSA.* Jack Doerner, Yashvanth Kondi, Eysa Lee, abhi shelat. (Northeastern University, USA)
- *Efficient Leakage Resilient Secret Sharing.* Peihan Miao, Akshayaram Srinivasan, Prashant Nalini Vasudevan. (UC Berkeley, USA)
- *DiSE: Distributed Symmetric-key Encryption.* Shashank Agrawal, Payman Mohassel, Pratyay Mukherjee, Peter Rindal. (Visa Research, USA)

Accepted presentation proposals:

- *Platform for Robust Threshold Cryptography.* Christian Cachin[1], Hugo Krawczyk[2], Tal Rabin[2], Jason Resch[3], Chrysoula Stathakopoulou[4]. ([1] University of Bern, Switzerland; [2] IBM Research, USA; [3] IBM, USA; [4] IBM research, Zurich, Switzerland)
- *Optimized Threshold Implementations: Number of Shares and Area/Latency Trade-off.* Dušan Božilov[1,2], Miroslav Knežević[1], Ventzislav Nikov[1]. ([1] NXP Semiconductors, Belgium; [2] COSIC KU Leuven and imec, Belgium)
- *The pitfalls of threshold cryptography in hardware.* Marco Macchetti, Karine Villegas, Claudio Favi. (Kudelski Group, Switzerland)
- *Threshold Cryptography against Combined Physical Attacks.* Lauren De Meyer. (KU Leuven, Belgium)
- *VerMI: Verification Tool for Masked Implementations.* Victor Arribas, Svetla Nikova, Vincent Rijmen. (KU Leuven, imec-COSIC, Belgium)
- *SplitKey Case Study.* Maximiliaan van de Poll, Aivo Kalu. (Cybernetica AS, Estonia)
- *Practical Threshold Cryptography for Cloud and Cryptocurrencies.* Jakob Pagter. (Sepior, Denmark)
- *Practice Based Recommendations for Standardization of Threshold Cryptography.* Daniel Shumow. (Microsoft Research, USA)

NIST presentations:

- *NIST Computer Security Division welcoming*. Matthew Scholl
- *Enter the Threshold (The NIST Threshold Cryptography Workshop)*. Luís Brandão
- *The NIST Standardization Approach on Cryptography ─ Past, Present, and Future*. Lily Chen
- *NIST Status Update on Elliptic Curves and Post-Quantum Crypto*. Dustin Moody
- *Quo Vadis, Crypto Validation?* Apostol Vassilev
- *Open discussion*. Nicky Mouha

Organization (NIST Computer Security Division)

- Co-chairs and program committee: Luís Brandão, Nicky Mouha, Apostol Vassilev
- Administrative contact: Sara Kerman
- (Non-panel) Session Chairs: Rene Peralta, Andrew Regenscheid, Daniel Apon, Michael Cooper, Meltem Sönmez Turan, John Kelsey, Michael Davidson

NIST Threshold Workshop 2019 — Program schedule

All talks take place in the Green Auditorium in the Main Building (101) at the NIST campus in Gaithersburg, MD, USA
Attendees need to pre-register to attend the conference. Badge pick-up (for on time and late arrivals) is done in front of the Green auditorium.

Session	Hour	Time†	1st day of workshop (Monday, March 11, 2019)	Source	#
---	08:00-09:00	60	**Badge pick-up; light refreshments available**	---	-
Opening	09:00-09:10	10	**NIST Computer Security Division welcoming. Matthew Scholl** (NIST, USA)	NIST	1
I.1. Threshold Schemes (Chair: Rene Peralta, NIST)	09:10-09:25	15	**Enter the Threshold (The NIST Threshold Cryptography Project). Luís Brandão** (NIST, USA)	NIST	2
	09:25-10:15	50	**Threshold Cryptography: Ready for Prime Time? Hugo Krawczyk** (IBM Research, USA)	**Invited Keynote**	3
	10:15-10:40	25	**Platform for Robust Threshold Cryptography.** Christian Cachin (University of Bern, Switzerland), Hugo Krawczyk (IBM Research, USA), Tal Rabin (IBM Research, USA), **Jason Resch** (IBM, USA), Chrysoula Stathakopoulou (IBM research, Zurich, Switzerland)	Submitted Presentation	4
---	10:40-11:10	30	**Coffee break**	---	-
I.2. NIST Standards (Chair: Andrew Regenscheid, NIST)	11:10-11:40	30	**The NIST Standardization Approach on Cryptography ─ Past, Present, and Future. Lily Chen** (NIST, USA)	NIST	5
	11:40-12:00	20	**NIST Status Update on Elliptic Curves and Post-Quantum Crypto. Dustin Moody** (NIST, USA)	NIST	6
I.3. Threshold Post-Quantum (Chair: Daniel Apon, NIST)	12:00-12:25	25	**Adding Distributed Decryption and Key Generation to a Ring-LWE Based CCA Encryption Scheme.** Michael Kraitsberg (Unbound Technology, Israel), Yehuda Lindell (Bar-Ilan University, Israel; Unbound Technology, Israel), Valery Osheter (Unbound Technology, Israel), **Nigel P. Smart** (KU Leuven, Belgium; University of Bristol, UK), Younes Talibi Alaoui (KU Leuven, Belgium)	Submitted Paper	7
---	12:25-13:45	80	**Lunch (at the Heritage room)**	---	-
I.4. Threshold Signatures (Chair: Daniel Apon, NIST)	13:45-14:10	25	**Fully Distributed Non-Interactive Adaptively-Secure Threshold Signature Scheme with Short Shares: Efficiency Considerations and Implementation.** Benoît Libert (CNRS and ENS de Lyon, France), Marc Joye (OneSpan, Belgium), Moti Yung (Google Inc. and Columbia University, USA), **Fabrice Mouhartem** (ENS de Lyon, France)	Submitted Paper	8
	14:10-14:35	25	**A Multiparty Computation Approach to Threshold ECDSA.** Jack Doerner (Northeastern University, USA), **Yashvanth Kondi** (Northeastern University, USA), Eysa Lee (Northeastern University, USA), abhi shelat (Northeastern University, USA)	Submitted Paper	9
I.5. Panel on Threshold for DSS (Chair: Hugo Krawczyk, IBM Research)	14:35-15:35	60	**Threshold Protocols for the Digital Signature Standard.** Moderator: **Hugo Krawczyk** (IBM Research, USA); Panelists: **Rosario Gennaro** (CUNY, USA), **abhi shelat** (Northeastern University, USA), **Samuel Ranellucci** (Unbound Tech, Israel)	Submitted Panel	10
---	15:35-16:05	30	**Coffee break**	---	-
I.6. Validation (Chair: Michael Cooper, NIST)	16:05-16:45	40	***Quo Vadis*, Crypto Validation? Apostol Vassilev** (NIST, USA)	NIST	11
I.7. Discussion (Chair: Michael Cooper, NIST)	16:45-17:30	45	**Open discussion.** Moderator: **Nicky Mouha** (NIST, USA)	NIST	12

† Time durations are in minutes

Expected speakers are highlighted in **bold**.

Session	Hour	Time†	2nd day of workshop (Tuesday, March 12, 2019)	Source	#
---	08:00-08:45	45	**Badge pick-up; light refreshments available**	---	-
II.1. Threshold Circuit Design (Chair: Meltem S. Turan, NIST)	08:45-09:10	25	**Optimized Threshold Implementations: Number of Shares and Area/Latency Trade-off.** Dušan Božilov (NXP Semiconductors, Belgium; COSIC KU Leuven and imec, Belgium), Miroslav Knežević (NXP Semiconductors, Belgium), **Ventzislav Nikov** (NXP Semiconductors, Belgium)	Submitted Presentation	13
	09:10-09:35	25	**The pitfalls of threshold cryptography in hardware. Marco Macchetti** (Kudelski Group, Switzerland), Karine Villegas (Kudelski Group, Switzerland), Claudio Favi (Kudelski Group, Switzerland)	Submitted Presentation	14
	09:35-10:00	25	**Threshold Cryptography against Combined Physical Attacks. Lauren De Meyer** (KU Leuven, Belgium)	Submitted Presentation	15
	10:00-10:25	25	**VerMI: Verification Tool for Masked Implementations. Victor Arribas** (KU Leuven, imec-COSIC, Belgium), Svetla Nikova (KU Leuven, imec-COSIC, Belgium), Vincent Rijmen (KU Leuven, imec-COSIC, Belgium)	Submitted Presentation	16
---	10:25-10:55	30	**Coffee break**	---	-
II.2. Panel on TIS (Chairs: Svetla Nikova and Vincent Rijmen, KU Leuven)	10:55-12:10	75	**Theory of Implementation Security Panel.** Moderators: **Svetla Nikova** (KU Leuven, Belgium), **Vincent Rijmen** (KU Leuven, Belgium). Panelists: **Nigel Smart** (KU Leuven, Belgium), **Ventzislav Nikov** (NXP Semiconductors, Belgium), **Mike Hutter** (Rambus, USA), **Junfeng Fan** (Open Security Research, China), **Ruggero Susella** (ST Microelectronics, Italy), **Emmanuel Prouff** (ANSSI, France)	Submitted Panel	17
---	12:10-13:30	80	**Lunch (at the Heritage room)**	---	-
II.3. Other Threshold Primitives (Chair: John Kelsey, NIST)	13:30-13:55	25	**Efficient Leakage Resilient Secret Sharing.** Peihan Miao (UC Berkeley, USA), Akshayaram Srinivasan (UC Berkeley, USA), **Prashant Nalini Vasudevan** (UC Berkeley, USA)	Submitted Paper	18
	13:55-14:20	25	**DiSE: Distributed Symmetric-key Encryption. Shashank Agrawal** (Visa Research, USA), Payman Mohassel (Visa Research, USA), Pratyay Mukherjee (Visa Research, USA), Peter Rindal (Visa Research, USA)	Submitted Paper	19
II.4. Threshold Cryptography Applications and Experience (Chair: Michael Davidson, NIST)	14:20-15:10	50	**Challenges for Multisignature and Threshold Signature Implementation in a Bitcoin Context. Andrew Poelstra** (Blockstream, USA)	**Invited Keynote**	20
	15:10-15:40	30	**Coffee break**	---	-
	15:40-16:05	25	**SplitKey Case Study. Maximiliaan van de Poll** (Cybernetica AS, Estonia), **Aivo Kalu** (Cybernetica AS, Estonia)	Submitted Presentation	21
	16:05-16:30	25	**Practical Threshold Cryptography for Cloud and Cryptocurrencies. Jakob Pagter** (Sepior, Denmark)	Submitted Presentation	22
	16:30-16:55	25	**Practice Based Recommendations for Standardization of Threshold Cryptography. Daniel Shumow** (Microsoft Research, USA)	Submitted Presentation	23
Closing	16:55-17:15	20	**Final remarks.** Moderator: **Luís Brandão** (NIST, USA)	NIST	24

† Time durations are in minutes

Expected speakers are highlighted in **bold**.

Available shuttles:

- For guests at the Courtyard by Marriot Hotel, Gaithersburg, a shuttle will be available (both days) at 7:30am for Hotel → NIST, and at 5:45pm (Monday) or 5:30pm (Tuesday) for NIST → Hotel
- A NIST shuttle to NIST departs from the Shady grove Metro Station, Bus Bay C **(**go right when exiting the station**)** at 15 and 45 minutes past the hour.
- A NIST shuttle to Shady Grove Metro Station departs from the NIST Building 101 at 5 and 35 minutes past the hour. The last NIST shuttle leaves NIST at 6:00 p.m.
- See https://www.nist.gov/about-nist/visit/getting-nist-gaithersburg for further details