Enter the Threshold

The NIST Threshold Cryptography Project

National Institute of Standards and Technology

NIST Threshold Cryptography Workshop 2019 (#NTCW2019)

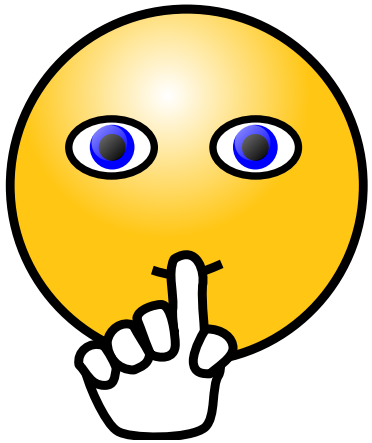
March 11, 2019 @ NIST campus, Gaithersburg MD, USA

Contact email: threshold-crypto@nist.gov

Outline

1. Intro
2. NISTIR (report)
3. NTCW (workshop)

Should we share a secret?



openclipart.org/detail/76603

Should we share a secret?

openclipart.org/detail/76603

"*Three may keep a secret*"

(In: *"Poor Richard's Almanack."* Benjamin Franklin, 1735) [Sau34]

"*Two may keep counsel*"

(In: *"Romeo and Juliet."* William Shakespeare, 1597) [Sha97]

"*For three may kepe counseil*"

(In: *The Ten Commandments of Love*. Geoffrey Chaucer, 1340–1400) [Cha00]

Should we share a secret?

openclipart.org/detail/76603

"*Three may keep a secret, if two of them are dead.*"

(In: *"Poor Richard's Almanack."* Benjamin Franklin, 1735) [Sau34]

"*Two may keep counsel, putting one away.*"

(In: *"Romeo and Juliet."* William Shakespeare, 1597) [Sha97]

"*For three may kepe counseil if twain be away!*"

(In: *The Ten Commandments of Love*. Geoffrey Chaucer, 1340–1400) [Cha00]

Should we share a secret?

Proverbial wisdom tells us to be careful

openclipart.org/detail/76603

"*Three may keep a secret, if two of them are dead.*"

(In: *"Poor Richard's Almanack."* Benjamin Franklin, 1735) [Sau34]

∗/mw02322/Benjamin-Franklin.jpg

"*Two may keep counsel, putting one away.*"

(In: *"Romeo and Juliet."* William Shakespeare, 1597) [Sha97]

∗/mw11574/William-Shakespeare.jpg

"*For three may kepe counseil if twain be away!*"

(In: *The Ten Commandments of Love*. Geoffrey Chaucer, 1340–1400) [Cha00]

∗/mw01262/Geoffrey-Chaucer.jpg

∗ = https://collectionimages.npg.org.uk/large/

Should we share a secret?

Proverbial wisdom tells us to be careful

openclipart.org/detail/76603

"*Three may keep a secret, if two of them are dead.*"

(In: *"Poor Richard's Almanack."* Benjamin Franklin, 1735) [Sau34]

∗/mw02322/Benjamin-Franklin.jpg

"*Two may keep counsel, putting one away.*"

(In: *"Romeo and Juliet."* William Shakespeare, 1597) [Sha97]

∗/mw11574/William-Shakespeare.jpg

"*For three may kepe counseil if twain be away!*"

(In: *The Ten Commandments of Love*. Geoffrey Chaucer, 1340–1400) [Cha00]

∗/mw01262/Geoffrey-Chaucer.jpg

∗ = https://collectionimages.npg.org.uk/large/

Is this relevant today, for modern cryptography?

Should we share a secret?

Proverbial wisdom tells us to be careful

openclipart.org/detail/76603

"*Three may keep a secret, if two of them are dead.*"

(In: *"Poor Richard's Almanack."* Benjamin Franklin, 1735) [Sau34]

∗/mw02322/Benjamin-Franklin.jpg

"*Two may keep counsel, putting one away.*"

(In: *"Romeo and Juliet."* William Shakespeare, 1597) [Sha97]

∗/mw11574/William-Shakespeare.jpg

"*For three may kepe counseil if twain be away!*"

(In: *The Ten Commandments of Love*. Geoffrey Chaucer, 1340–1400) [Cha00]

∗/mw01262/Geoffrey-Chaucer.jpg

∗ = https://collectionimages.npg.org.uk/large/

Is this relevant today, for modern cryptography?

openclipart.org/detail/101407

Yes!

Should we share a secret?

Proverbial wisdom tells us to be careful

openclipart.org/detail/76603

"*Three may keep a secret, if two of them are dead.*"

(In: *"Poor Richard's Almanack."* Benjamin Franklin, 1735) [Sau34]

∗/mw02322/Benjamin-Franklin.jpg

"*Two may keep counsel, putting one away.*"

(In: *"Romeo and Juliet."* William Shakespeare, 1597) [Sha97]

∗/mw11574/William-Shakespeare.jpg

"*For three may kepe counseil if twain be away!*"

(In: *The Ten Commandments of Love*. Geoffrey Chaucer, 1340–1400) [Cha00]

∗/mw01262/Geoffrey-Chaucer.jpg

∗ = https://collectionimages.npg.org.uk/large/

Is this relevant today, for modern cryptography?

openclipart.org/detail/101407

Yes! Cryptography relies on:

- secrecy, correctness, availability ... of cryptographic **keys**
- implementations that use **keys** in an algorithm

Should we share a secret?

Proverbial wisdom tells us to be careful

openclipart.org/detail/76603

"*Three may keep a secret, if two of them are dead.*"

(In: *"Poor Richard's Almanack."* Benjamin Franklin, 1735) [Sau34]

∗/mw02322/Benjamin-Franklin.jpg

"*Two may keep counsel, putting one away.*"

(In: *"Romeo and Juliet."* William Shakespeare, 1597) [Sha97]

∗/mw11574/William-Shakespeare.jpg

"*For three may kepe counseil if twain be away!*"

(In: *The Ten Commandments of Love*. Geoffrey Chaucer, 1340–1400) [Cha00]

∗/mw01262/Geoffrey-Chaucer.jpg

∗ = https://collectionimages.npg.org.uk/large/

Is this relevant today, for modern cryptography?

openclipart.org/detail/101407

Yes! Cryptography relies on:

- secrecy, correctness, availability ... of cryptographic **keys**
- **implementations** that use **keys** in an algorithm

Crypto is affected by implementation vulnerabilities!

Crypto is affected by implementation vulnerabilities!

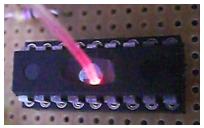
Attacks can exploit differences between ideal vs. real **implementations**

Crypto is affected by implementation vulnerabilities!

Attacks can exploit differences between ideal vs. real **implementations**

“Bellcore attack” (1997)

[BDL97]



[SH07]

Cold-boot attacks (2009)

[HSH+09]

[Don13]

Heartbleed bug (2014)

[DLK+14]

heartbleed.com

“ZigBee Chain reaction” (2017)

[RSWO17]

[RSWO17]

Meltdown & Spectre (2017)

[LSG+18, KGG+18]

meltdownattack.com

Foreshadow (2018)

[BMW+18, WBM+18]

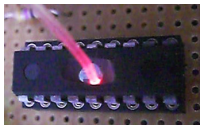
foreshadowattack.eu

Crypto is affected by implementation vulnerabilities!

Attacks can exploit differences between ideal vs. real **implementations**

“Bellcore attack” (1997)

[BDL97]



[SH07]

Cold-boot attacks (2009)

[HSH+09]

[Don13]

Heartbleed bug (2014)

[DLK+14]

heartbleed.com

“ZigBee Chain reaction” (2017)

[RSWO17]

[RSWO17]

Meltdown & Spectre (2017)

[LSG+18, KGG+18]

meltdownattack.com

Foreshadow (2018)

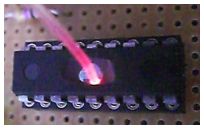
[BMW+18, WBM+18]

foreshadowattack.eu

Also, operators of cryptographic implementations can go rogue

Crypto is affected by implementation vulnerabilities!

Attacks can exploit differences between ideal vs. real **implementations**

"Bellcore attack" (1997)
[BDL97]

[SH07]

Cold-boot attacks (2009)
[HSH+09]

[Don13]

Heartbleed bug (2014)
[DLK+14]

heartbleed.com

"ZigBee Chain reaction" (2017)
[RSWO17]

[RSWO17]

Meltdown & Spectre (2017)
[LSG+18, KGG+18]

meltdownattack.com

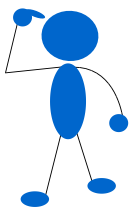
Foreshadow (2018)
[BMW+18, WBM+18]

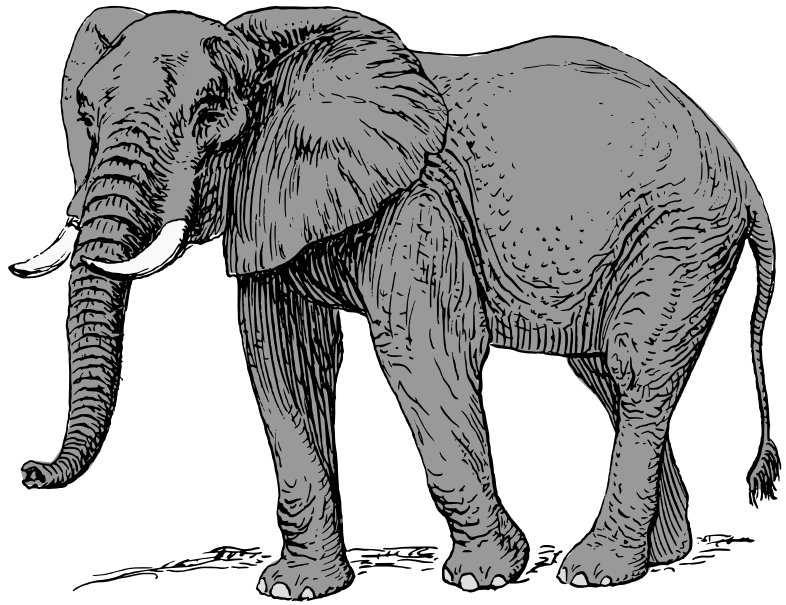
foreshadowattack.eu

Also, operators of cryptographic implementations can go rogue

How can we oppose single-points of failure?


*question-2.html


*4296.html


*colored-elephant.html

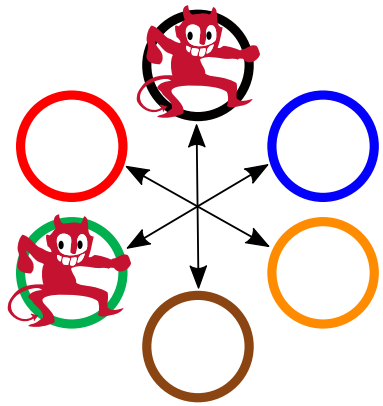
* = clker.com/clipart-

The threshold approach

The threshold approach

At high-level:

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



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

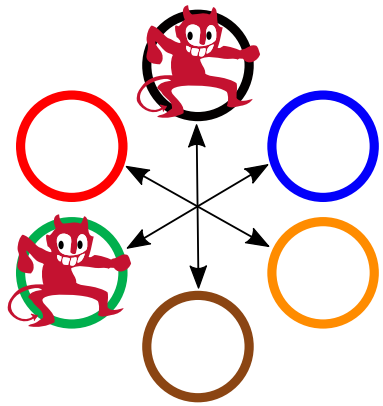
The threshold approach

At high-level:

use redundancy & diversity to mitigate

the *compromise* of up to a threshold

number (f-out-of-n) of components



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

NIST-CSD wants to standardize
threshold schemes for cryptographic primitives

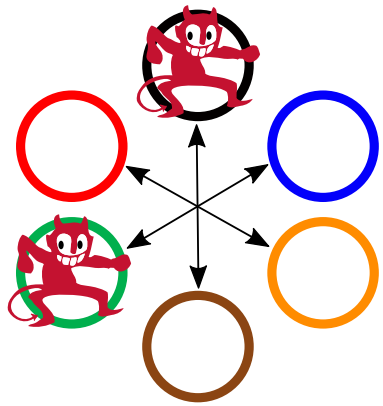
The threshold approach

At high-level:

use redundancy & diversity to mitigate

the *compromise* of up to a threshold

number (f-out-of-n) of components



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

NIST-CSD wants to standardize
threshold schemes for cryptographic primitives

Potential primitives: key-generation, signing, decryption, enciphering, RNGen, ...

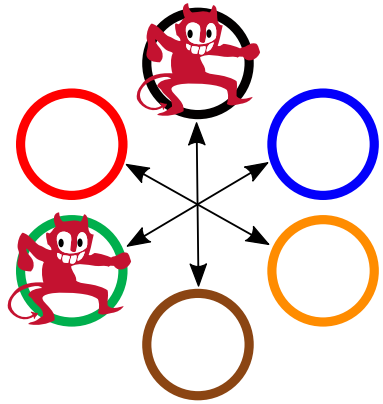
The threshold approach

At high-level:

use redundancy & diversity to mitigate

the *compromise* of up to a threshold

number (f-out-of-n) of components



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

NIST-CSD wants to standardize
threshold schemes for cryptographic primitives

Potential primitives: key-generation, signing, decryption, enciphering, RNGen, ...

- secret keys never in one place;
- operation withstands several compromised components;
- resistance against side-channel attacks
- ...

The NIST Threshold Cryptography Project

The NIST Threshold Cryptography Project

- Project within the NIST Computer Security Division (CSD)
  https://csrc.nist.gov/Projects/Threshold-Cryptography

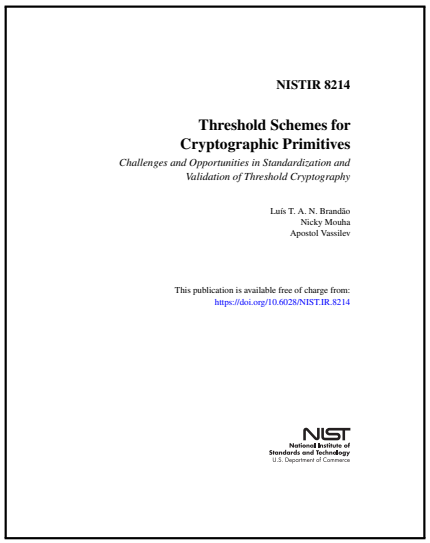
The NIST Threshold Cryptography Project

- Project within the NIST Computer Security Division (CSD)
  https://csrc.nist.gov/Projects/Threshold-Cryptography
- *To drive an open and transparent process towards standardization of threshold schemes for cryptographic primitives.* (See NISTIR 7977 [Gro16])

The NIST Threshold Cryptography Project

- Project within the NIST Computer Security Division (CSD)
  https://csrc.nist.gov/Projects/Threshold-Cryptography
- *To drive an open and transparent process towards standardization of threshold schemes for cryptographic primitives.* (See NISTIR 7977 [Gro16])

NISTIR 8214 (report)


NISTIR 8214

Threshold Schemes for Cryptographic Primitives

Challenges and Opportunities in Standardization and Validation of Threshold Cryptography

Luís T. A. N. Brandão
Nicky Mouha
Apostol Vassilev

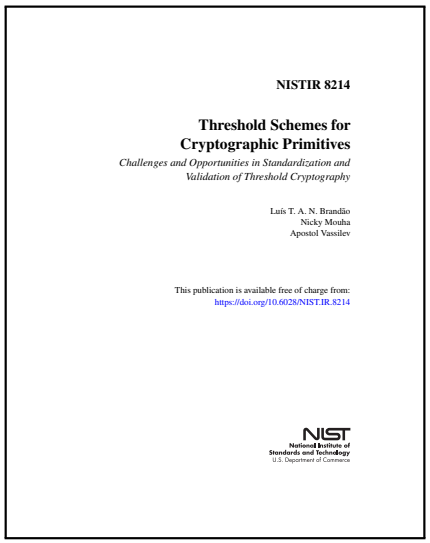
This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8214

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

The NIST Threshold Cryptography Project

- Project within the NIST Computer Security Division (CSD)
  https://csrc.nist.gov/Projects/Threshold-Cryptography
- *To drive an open and transparent process towards standardization of threshold schemes for cryptographic primitives.* (See NISTIR 7977 [Gro16])

NISTIR 8214 (report)



NISTIR 8214

Threshold Schemes for Cryptographic Primitives

Challenges and Opportunities in Standardization and Validation of Threshold Cryptography

Luís T. A. N. Brandão
Nicky Mouha
Apostol Vassilev

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

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

→

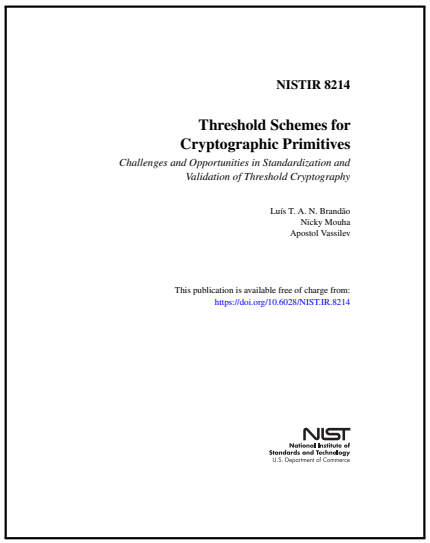
NTCW (workshop)

www.nist.gov/image/surfgaithersburgjpg

The NIST Threshold Cryptography Project

- Project within the NIST Computer Security Division (CSD)
  https://csrc.nist.gov/Projects/Threshold-Cryptography
- *To drive an open and transparent process towards standardization of threshold schemes for cryptographic primitives.* (See NISTIR 7977 [Gro16])

NISTIR 8214 (report)


NISTIR 8214

Threshold Schemes for Cryptographic Primitives

Challenges and Opportunities in Standardization and Validation of Threshold Cryptography

Luís T. A. N. Brandão
Nicky Mouha
Apostol Vassilev

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

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

→

NTCW (workshop)

www.nist.gov/image/surfgaithersburgjpg

→

Move forward

criteria

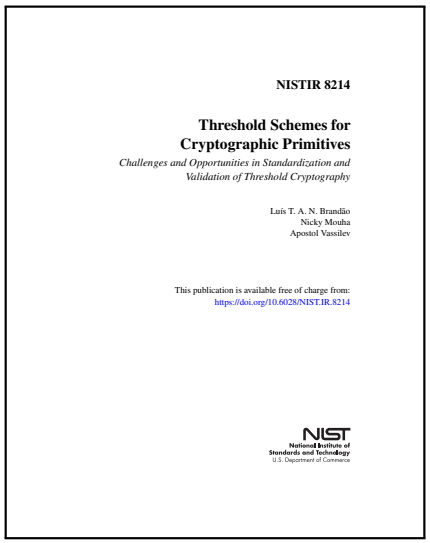
engage

standardize

The NIST Threshold Cryptography Project

- Project within the NIST Computer Security Division (CSD)
  https://csrc.nist.gov/Projects/Threshold-Cryptography
- *To drive an open and transparent process towards standardization of threshold schemes for cryptographic primitives.* (See NISTIR 7977 [Gro16])

NISTIR 8214 (report)


NISTIR 8214

Threshold Schemes for Cryptographic Primitives

Challenges and Opportunities in Standardization and Validation of Threshold Cryptography

Luís T. A. N. Brandão
Nicky Mouha
Apostol Vassilev

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

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

→

NTCW (workshop)

www.nist.gov/image/surfgaithersburgjpg

→

Move forward

criteria

engage

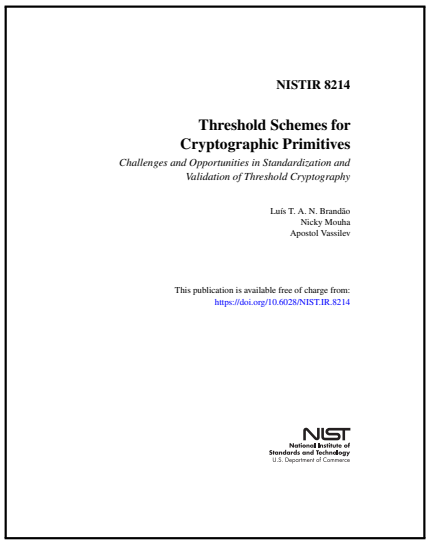
standardize

- Current team: Luís Brandão, Michael Davidson (last month), Nicky Mouha, Apostol Vassilev.

The NIST Threshold Cryptography Project

- Project within the NIST Computer Security Division (CSD)
  https://csrc.nist.gov/Projects/Threshold-Cryptography
- *To drive an open and transparent process towards standardization of threshold schemes for cryptographic primitives.* (See NISTIR 7977 [Gro16])

NISTIR 8214 (report)


NISTIR 8214

Threshold Schemes for Cryptographic Primitives

Challenges and Opportunities in Standardization and Validation of Threshold Cryptography

Luís T. A. N. Brandão
Nicky Mouha
Apostol Vassilev

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

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

→

NTCW (workshop)


www.nist.gov/image/surfgaithersburgjpg

→

Move forward

criteria

engage

standardize

- Current team: Luís Brandão, Michael Davidson (last month), Nicky Mouha, Apostol Vassilev.
- Supported by CSD, e.g., session chairs and speakers at NTCW

Outline

NISTIR 8214

NISTIR 8214

Threshold Schemes for Cryptographic Primitives: Challenges and Opportunities in Standardization and Validation of Threshold Cryptography [BMV19]

NISTIR 8214

Threshold Schemes for Cryptographic Primitives: Challenges and Opportunities in Standardization and Validation of Threshold Cryptography [BMV19]

The report poses diverse initial questions:

- how to characterize threshold schemes?
- what criteria to decide what to standardize?
- ...

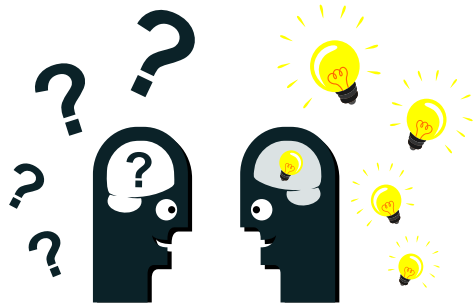


Image adapted from: openclipart.org/detail/283392

NISTIR 8214

Threshold Schemes for Cryptographic Primitives: Challenges and Opportunities in Standardization and Validation of Threshold Cryptography [BMV19]

The report poses diverse initial questions:

- how to characterize threshold schemes?
- what criteria to decide what to standardize?
- ...

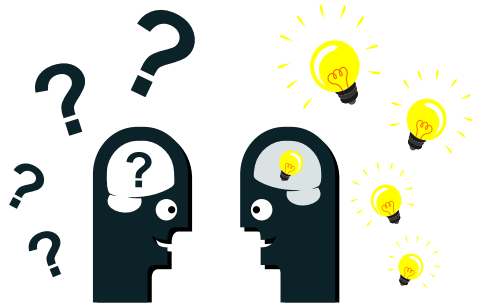


Image adapted from: openclipart.org/detail/283392

Timeline:

- 2018-July: Draft online for public comments
- 2018-October: Received comments from 13 external sources
- 2019-March: Final version online, along with “diff” and received comments

Characterizing threshold schemes

Characterizing threshold schemes

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

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

Characterizing threshold schemes

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

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

Each feature spans distinct options that affect security in a different way.

Characterizing threshold schemes

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

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

Each feature spans distinct options that affect security in a different way.

Other factors: application context, operational pros & cons, conceived attacks, performance.

openclipart.org/detail/281637

clker.com/clipart-10778

Characterizing threshold schemes

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

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

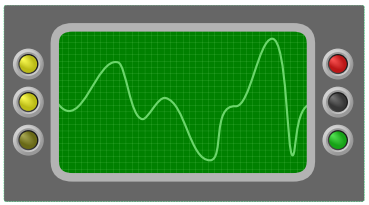
Each feature spans distinct options that affect security in a different way.

Other factors: application context, operational pros & cons, conceived attacks, performance.

openclipart.org/detail/281637

clker.com/clipart-10778

Even if all nodes are initially compromised, (e.g., leaky) a threshold scheme may still be effective, if it increases the cost of exploitation



openclipart.org/detail/172330

(e.g., differential power analysis)

What exactly to standardize?

What exactly to standardize?

A high-dimensionality problem!

What exactly to standardize?

A high-dimensionality problem!

- Security properties and attack types

What exactly to standardize?

A high-dimensionality problem!

- Security properties and attack types
- Flexibility of features and parameters

What exactly to standardize?

A high-dimensionality problem!

- Security properties and attack types
- Flexibility of features and parameters
- Granularity and composability

What exactly to standardize?

A high-dimensionality problem!

- Security properties and attack types
- Flexibility of features and parameters
- Granularity and composability
- Implementation and validation requirements

What exactly to standardize?

A high-dimensionality problem!

- Security properties and attack types
- Flexibility of features and parameters
- Granularity and composability
- Implementation and validation requirements
- ...

Challenge ahead: define **criteria** for standardization

What exactly to standardize?

A high-dimensionality problem!

- Security properties and attack types
- Flexibility of features and parameters
- Granularity and composability
- Implementation and validation requirements
- ...

Challenge ahead: define **criteria** for standardization

Important to engage with stakeholders $\rightarrow$ **workshop**

Outline

Here we are: #NTCW2019

NIST Threshold Cryptography Workshop 2019

(March 11–12, 2019 @ Gaithersburg, USA)

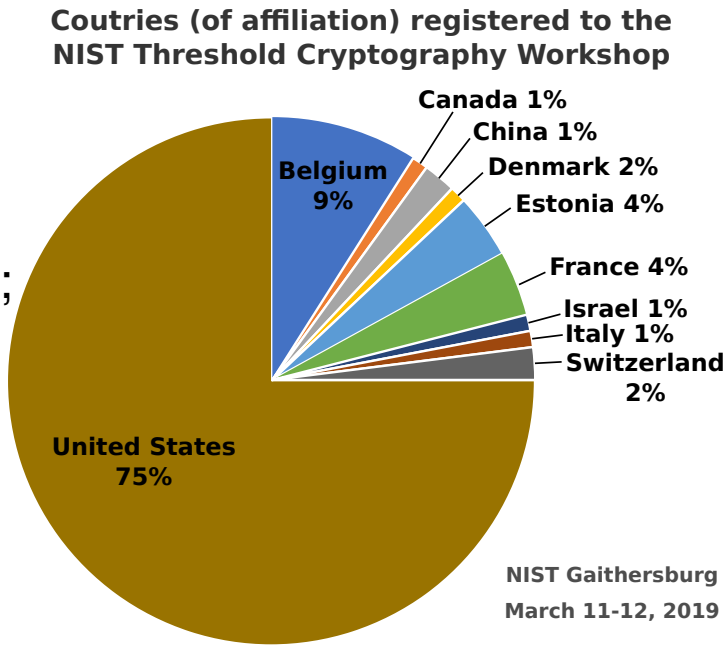
Here we are: #NTCW2019

NIST Threshold Cryptography Workshop 2019

(March 11–12, 2019 @ Gaithersburg, USA)

A platform for open interaction:

- hear about experiences with threshold crypto;
- get to know stakeholders;
- get input to reflect on criteria.



About 80 participants present at NIST

https://csrc.nist.gov/Events/2019/NTCW19

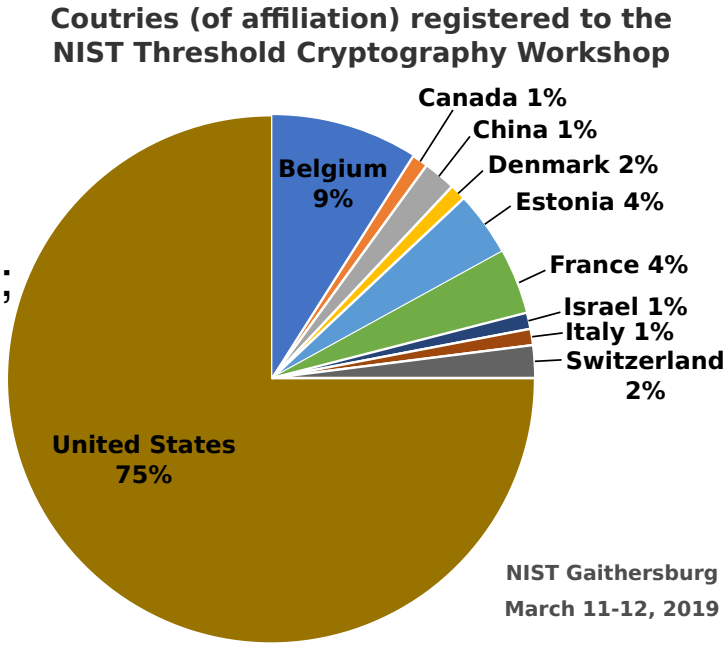
Here we are: #NTCW2019

NIST Threshold Cryptography Workshop 2019

(March 11–12, 2019 @ Gaithersburg, USA)

A platform for open interaction:

- hear about experiences with threshold crypto;
- get to know stakeholders;
- get input to reflect on criteria.



About 80 participants present at NIST

Accepted 15 external submissions:

- 2 panels
- 5 papers
- 8 presentations

https://csrc.nist.gov/Events/2019/NTCW19

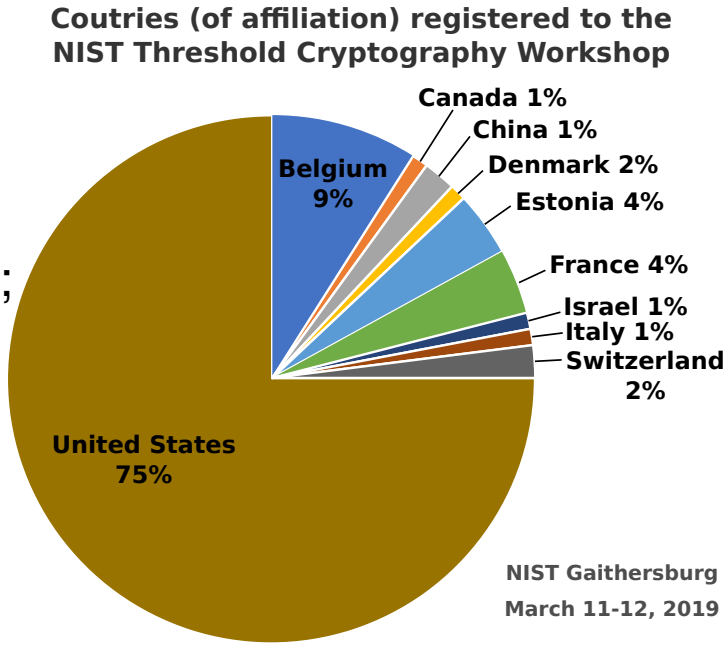
Here we are: #NTCW2019

NIST Threshold Cryptography Workshop 2019

(March 11–12, 2019 @ Gaithersburg, USA)

A platform for open interaction:

- hear about experiences with threshold crypto;
- get to know stakeholders;
- get input to reflect on criteria.



About 80 participants present at NIST

Accepted 15 external submissions:

- 2 panels
- 5 papers
- 8 presentations

Plus:

- NIST talks
- 2 invited keynotes
- 2 feedback moments

https://csrc.nist.gov/Events/2019/NTCW19

Workshop schedule — day 1

What will we be talking about?

Session	**2019-Mar-11**	**Time**†	**Topic** (free abbreviation)	**Source**	#
					1
					2
					3
					4
					5
					6
					7
					8
					9
					10
					11
					12

† Time durations are in minutes

Workshop schedule — day 1

What will we be talking about?

Session	**2019-Mar-11**	**Time**†	**Topic** (free abbreviation)	**Source**	#
—	**08:00–09:00**	**75’**	**Badge pick-up; light refreshments**	**—**	**-**
					1
					2
					3
					4
—	**10:40–11:10**	**30’**	**Morning coffee break**	**—**	**-**
					5
					6
					7
—	**12:25–13:45**	**80’**	**Lunch break (@ heritage room)**	**—**	**-**
					8
					9
					10
—	**15:35–16:05**	**30’**	**Afternoon coffee break**	**—**	**-**
					11
					12

† Time durations are in minutes

Workshop schedule — day 1

What will we be talking about?

Session	**2019-Mar-11**	**Time**†	**Topic** (free abbreviation)	**Source**	#
—	08:00–09:00	75’	Badge pick-up; light refreshments	—	-
Opening	09:00–09:10	10’	**CSD welcoming**	NIST	1
					2
					3
					4
—	10:40–11:10	30’	Morning coffee break	—	-
					5
					6
					7
—	12:25–13:45	80’	Lunch break (@ heritage room)	—	-
					8
					9
					10
—	15:35–16:05	30’	Afternoon coffee break	—	-
					11
					12

† Time durations are in minutes **CSD (computer security division);**

Workshop schedule — day 1

What will we be talking about?

Session	**2019-Mar-11**	**Time**†	**Topic** (free abbreviation)	**Source**	#
—	08:00–09:00	75’	Badge pick-up; light refreshments	—	-
Opening	09:00–09:10	10’	CSD welcoming	NIST	1
I1. Threshold Schemes	09:10–10:40				2
					3
					4
—	10:40–11:10	30’	Morning coffee break	—	-
					5
					6
					7
—	12:25–13:45	80’	Lunch break (@ heritage room)	—	-
					8
					9
					10
—	15:35–16:05	30’	Afternoon coffee break	—	-
					11
					12

† Time durations are in minutes

CSD (computer security division);

Workshop schedule — day 1

What will we be talking about?

Session	**2019-Mar-11**	**Time**†	**Topic** (free abbreviation)	**Source**	#
—	08:00–09:00	75’	Badge pick-up; light refreshments	—	-
Opening	09:00–09:10	10’	CSD welcoming	NIST	1
I1. Threshold Schemes	09:10–10:40	15’	**The TC project**	NIST	2
		50’	**TC prime time?**	**Invited keynote**	3
		25’	**Platform for robust TC**	Subm. pres.	4
—	10:40–11:10	30’	Morning coffee break	—	-
					5
					6
					7
—	12:25–13:45	80’	Lunch break (@ heritage room)	—	-
					8
					9
					10
—	15:35–16:05	30’	Afternoon coffee break	—	-
					11
					12

† Time durations are in minutes

CSD (computer security division); **TC (threshold cryptography); pres. (presentation proposal); Subm. (submitted);**

Workshop schedule — day 1

What will we be talking about?

Session	**2019-Mar-11**	**Time**†	**Topic** (free abbreviation)	**Source**	#
—	08:00–09:00	75’	Badge pick-up; light refreshments	—	-
Opening	09:00–09:10	10’	CSD welcoming	NIST	1
I1. Threshold Schemes	09:10–10:40	15’	The TC project	NIST	2
		50’	TC prime time?	**Invited keynote**	3
		25’	Platform for robust TC	Subm. pres.	4
—	10:40–11:10	30’	Morning coffee break	—	-
I2. NIST Standards	11:10–12:00				5
					6
					7
—	12:25–13:45	80’	Lunch break (@ heritage room)	—	-
					8
					9
					10
—	15:35–16:05	30’	Afternoon coffee break	—	-
					11
					12

† Time durations are in minutes

CSD (computer security division); TC (threshold cryptography); pres. (presentation proposal); Subm. (submitted);

Workshop schedule — day 1

What will we be talking about?

Session	**2019-Mar-11**	**Time**†	**Topic** (free abbreviation)	**Source**	#
—	08:00–09:00	75’	Badge pick-up; light refreshments	—	-
Opening	09:00–09:10	10’	CSD welcoming	NIST	1
I1. Threshold Schemes	09:10–10:40	15’	The TC project	NIST	2
		50’	TC prime time?	**Invited keynote**	3
		25’	Platform for robust TC	Subm. pres.	4
—	10:40–11:10	30’	Morning coffee break	—	-
I2. NIST Standards	11:10–12:00	30’	**NIST crypto standards**	NIST	5
		20’	**Update on EC and PQC**	NIST	6
					7
—	12:25–13:45	80’	Lunch break (@ heritage room)	—	-
					8
					9
					10
—	15:35–16:05	30’	Afternoon coffee break	—	-
					11
					12

† Time durations are in minutes

CSD (computer security division); TC (threshold cryptography); pres. (presentation proposal); Subm. (submitted); **EC (elliptic curves); PQ (post-quantum);**

Workshop schedule — day 1

What will we be talking about?

Session	**2019-Mar-11**	**Time**†	**Topic** (free abbreviation)	**Source**	#
—	08:00–09:00	75’	Badge pick-up; light refreshments	—	-
Opening	09:00–09:10	10’	CSD welcoming	NIST	1
I1. Threshold Schemes	09:10–10:40	15’	The TC project	NIST	2
		50’	TC prime time?	**Invited keynote**	3
		25’	Platform for robust TC	Subm. pres.	4
—	10:40–11:10	30’	Morning coffee break	—	-
I2. NIST Standards	11:10–12:00	30’	NIST crypto standards	NIST	5
		20’	Update on EC and PQC	NIST	6
I3. Threshold PQ	12:00–12:25	25’	**PQ distributed encryption scheme**	Subm. paper	7
—	12:25–13:45	80’	Lunch break (@ heritage room)	—	-
					8
					9
					10
—	15:35–16:05	30’	Afternoon coffee break	—	-
					11
					12

† Time durations are in minutes

CSD (computer security division); TC (threshold cryptography); pres. (presentation proposal); Subm. (submitted); EC (elliptic curves); PQ (post-quantum);

Workshop schedule — day 1

What will we be talking about?

Session	**2019-Mar-11**	**Time**†	**Topic** (free abbreviation)	**Source**	#
—	08:00–09:00	75’	Badge pick-up; light refreshments	—	-
Opening	09:00–09:10	10’	CSD welcoming	NIST	1
I1. Threshold Schemes	09:10–10:40	15’	The TC project	NIST	2
		50’	TC prime time?	**Invited keynote**	3
		25’	Platform for robust TC	Subm. pres.	4
—	10:40–11:10	30’	Morning coffee break	—	-
I2. NIST Standards	11:10–12:00	30’	NIST crypto standards	NIST	5
		20’	Update on EC and PQC	NIST	6
I3. Threshold PQ	12:00–12:25	25’	PQ distributed encryption scheme	Subm. paper	7
—	12:25–13:45	80’	Lunch break (@ heritage room)	—	-
I4. Threshold Signatures	13:45–14:35				8
					9
					10
—	15:35–16:05	30’	Afternoon coffee break	—	-
					11
					12

† Time durations are in minutes

CSD (computer security division); TC (threshold cryptography); pres. (presentation proposal); Subm. (submitted); EC (elliptic curves); PQ (post-quantum);

Workshop schedule — day 1

What will we be talking about?

Session	**2019-Mar-11**	**Time**†	**Topic** (free abbreviation)	**Source**	#
—	08:00–09:00	75’	Badge pick-up; light refreshments	—	-
Opening	09:00–09:10	10’	CSD welcoming	NIST	1
I1. Threshold Schemes	09:10–10:40	15’	The TC project	NIST	2
		50’	TC prime time?	**Invited keynote**	3
		25’	Platform for robust TC	Subm. pres.	4
—	10:40–11:10	30’	Morning coffee break	—	-
I2. NIST Standards	11:10–12:00	30’	NIST crypto standards	NIST	5
		20’	Update on EC and PQC	NIST	6
I3. Threshold PQ	12:00–12:25	25’	PQ distributed encryption scheme	Subm. paper	7
—	12:25–13:45	80’	Lunch break (@ heritage room)	—	-
I4. Threshold Signatures	13:45–14:35	25’	**Adaptively secure threshold sig**	Subm. paper	8
		25’	**Threshold ECDSA using SMPC**	Subm. paper	9
					10
—	15:35–16:05	30’	Afternoon coffee break	—	-
					11
					12

† Time durations are in minutes

CSD (computer security division); TC (threshold cryptography); pres. (presentation proposal); Subm. (submitted); EC (elliptic curves); PQ (post-quantum); **ECDSA (EC digital signature algorithm);**

Workshop schedule — day 1

What will we be talking about?

Session	**2019-Mar-11**	**Time**†	**Topic** (free abbreviation)	**Source**	#
—	08:00–09:00	75’	Badge pick-up; light refreshments	—	-
Opening	09:00–09:10	10’	CSD welcoming	NIST	1
I1. Threshold Schemes	09:10–10:40	15’	The TC project	NIST	2
		50’	TC prime time?	**Invited keynote**	3
		25’	Platform for robust TC	Subm. pres.	4
—	10:40–11:10	30’	Morning coffee break	—	-
I2. NIST Standards	11:10–12:00	30’	NIST crypto standards	NIST	5
		20’	Update on EC and PQC	NIST	6
I3. Threshold PQ	12:00–12:25	25’	PQ distributed encryption scheme	Subm. paper	7
—	12:25–13:45	80’	Lunch break (@ heritage room)	—	-
I4. Threshold Signatures	13:45–14:35	25’	Adaptively secure threshold sig	Subm. paper	8
		25’	Threshold ECDSA using SMPC	Subm. paper	9
I5. Panel DSS	14:35–15:35	60’	**Threshold protocols for DSS**	**Subm. panel**	10
—	15:35–16:05	30’	Afternoon coffee break	—	-
					11
					12

† Time durations are in minutes

CSD (computer security division); TC (threshold cryptography); pres. (presentation proposal); Subm. (submitted); EC (elliptic curves); PQ (post-quantum); ECDSA (EC digital signature algorithm); **DSS (digital signature standard).**

Workshop schedule — day 1

What will we be talking about?

Session	**2019-Mar-11**	**Time**†	**Topic** (free abbreviation)	**Source**	#
—	08:00–09:00	75’	Badge pick-up; light refreshments	—	-
Opening	09:00–09:10	10’	CSD welcoming	NIST	1
I1. Threshold Schemes	09:10–10:40	15’	The TC project	NIST	2
		50’	TC prime time?	**Invited keynote**	3
		25’	Platform for robust TC	Subm. pres.	4
—	10:40–11:10	30’	Morning coffee break	—	-
I2. NIST Standards	11:10–12:00	30’	NIST crypto standards	NIST	5
		20’	Update on EC and PQC	NIST	6
I3. Threshold PQ	12:00–12:25	25’	PQ distributed encryption scheme	Subm. paper	7
—	12:25–13:45	80’	Lunch break (@ heritage room)	—	-
I4. Threshold Signatures	13:45–14:35	25’	Adaptively secure threshold sig	Subm. paper	8
		25’	Threshold ECDSA using SMPC	Subm. paper	9
I5. Panel DSS	14:35–15:35	60’	Threshold protocols for DSS	**Subm. panel**	10
—	15:35–16:05	30’	Afternoon coffee break	—	-
I6. Validation	16:05–16:45	40’	**Crypto validation**	NIST	11
					12

† Time durations are in minutes

CSD (computer security division); TC (threshold cryptography); pres. (presentation proposal); Subm. (submitted); EC (elliptic curves); PQ (post-quantum); ECDSA (EC digital signature algorithm); DSS (digital signature standard).

Workshop schedule — day 1

What will we be talking about?

Session	**2019-Mar-11**	**Time**†	**Topic** (free abbreviation)	**Source**	#
—	08:00–09:00	75’	Badge pick-up; light refreshments	—	-
Opening	09:00–09:10	10’	CSD welcoming	NIST	1
I1. Threshold Schemes	09:10–10:40	15’	The TC project	NIST	2
		50’	TC prime time?	**Invited keynote**	3
		25’	Platform for robust TC	Subm. pres.	4
—	10:40–11:10	30’	Morning coffee break	—	-
I2. NIST Standards	11:10–12:00	30’	NIST crypto standards	NIST	5
		20’	Update on EC and PQC	NIST	6
I3. Threshold PQ	12:00–12:25	25’	PQ distributed encryption scheme	Subm. paper	7
—	12:25–13:45	80’	Lunch break (@ heritage room)	—	-
I4. Threshold Signatures	13:45–14:35	25’	Adaptively secure threshold sig	Subm. paper	8
		25’	Threshold ECDSA using SMPC	Subm. paper	9
I5. Panel DSS	14:35–15:35	60’	Threshold protocols for DSS	**Subm. panel**	10
—	15:35–16:05	30’	Afternoon coffee break	—	-
I6. Validation	16:05–16:45	40’	Crypto validation	NIST	11
I7. Discussion	16:45–17:30	45’	**Open discussion**	NIST	12

† Time durations are in minutes

CSD (computer security division); TC (threshold cryptography); pres. (presentation proposal); Subm. (submitted); EC (elliptic curves); PQ (post-quantum); ECDSA (EC digital signature algorithm); DSS (digital signature standard).

Workshop schedule — day 1

What will we be talking about?

Session	**2019-Mar-11**	**Time**†	**Topic** (free abbreviation)	**Source**	#
—	08:00–09:00	75’	Badge pick-up; light refreshments	—	-
Opening	09:00–09:10	10’	CSD welcoming	NIST	1
I1. Threshold Schemes	09:10–10:40	15’	The TC project	NIST	2
		50’	TC prime time?	**Invited keynote**	3
		25’	Platform for robust TC	Subm. pres.	4
—	10:40–11:10	30’	Morning coffee break	—	-
I2. NIST Standards	11:10–12:00	30’	NIST crypto standards	NIST	5
		20’	Update on EC and PQC	NIST	6
I3. Threshold PQ	12:00–12:25	25’	PQ distributed encryption scheme	Subm. paper	7
—	12:25–13:45	80’	Lunch break (@ heritage room)	—	-
I4. Threshold Signatures	13:45–14:35	25’	Adaptively secure threshold sig	Subm. paper	8
		25’	Threshold ECDSA using SMPC	Subm. paper	9
I5. Panel DSS	14:35–15:35	60’	Threshold protocols for DSS	**Subm. panel**	10
—	15:35–16:05	30’	Afternoon coffee break	—	-
I6. Validation	16:05–16:45	40’	Crypto validation	NIST	11
I7. Discussion	16:45–17:30	45’	Open discussion	NIST	12

† Time durations are in minutes

CSD (computer security division); TC (threshold cryptography); pres. (presentation proposal); Subm. (submitted); EC (elliptic curves); PQ (post-quantum); ECDSA (EC digital signature algorithm); DSS (digital signature standard).

Workshop schedule — day 2

What will we be talking about?

Session	**2019-Mar-12**	**Time**†	**Topic** (free abbreviation)	**Source**	#
					13
					14
					15
					16
					17
					18
					19
					20
					21
					22
					23
					24

Workshop schedule — day 2

What will we be talking about?

Session	2019-Mar-12	Time†	Topic (free abbreviation)	Source	#
—	**08:00–08:45**	**75’**	**Light refreshments**	**—**	**-**
					13
					14
					15
					16
—	**10:25–10:55**	**30’**	**Morning coffee break**	**—**	**-**
					17
—	**12:10–13:30**	**80’**	**Lunch break (@ heritage room)**	**—**	**-**
					18
					19
					20
	15:10–15:40	**30’**	**Afternoon coffee break**	**—**	**-**
					21
					22
					23
					24

† Time durations are in minutes

pres. (presentation proposal); Subm. (submitted); TC (threshold cryptography).

Workshop schedule — day 2

What will we be talking about?

Session	2019-Mar-12	Time†	Topic (free abbreviation)	Source	#
—	08:00–08:45	75’	Light refreshments	—	-
II.1. Threshold circuit design	08:45–10:25				13
					14
					15
					16
—	10:25–10:55	30’	Morning coffee break	—	-
					17
—	12:10–13:30	80’	Lunch break (@ heritage room)	—	-
					18
					19
					20
	15:10–15:40	30’	Afternoon coffee break	—	-
					21
					22
					23
					24

† Time durations are in minutes

pres. (presentation proposal); Subm. (submitted); TC (threshold cryptography).

Workshop schedule — day 2

What will we be talking about?

Session	2019-Mar-12	Time†	**Topic** (free abbreviation)	Source	#
—	08:00–08:45	75’	Light refreshments	—	-
II.1. Threshold circuit design	08:45–10:25	25’	**Tradeoffs shares/area/latency**	Subm. pres.	13
		25’	**Pitfalls of TC in hardware**	Subm. pres.	14
		25’	**TC for combined physical attacks**	Subm. pres.	15
		25’	**VerMI: Verification tool**	Subm. pres.	16
—	10:25–10:55	30’	Morning coffee break	—	-
					17
—	12:10–13:30	80’	Lunch break (@ heritage room)	—	-
					18
					19
					20
	15:10–15:40	30’	Afternoon coffee break	—	-
					21
					22
					23
					24

† Time durations are in minutes

pres. (presentation proposal); Subm. (submitted); TC (threshold cryptography).

Workshop schedule — day 2

What will we be talking about?

Session	**2019-Mar-12**	**Time**†	**Topic** (free abbreviation)	**Source**	#
—	08:00–08:45	75’	Light refreshments	—	-
II.1. Threshold circuit design	08:45–10:25	25’	Tradeoffs shares/area/latency	Subm. pres.	13
		25’	Pitfalls of TC in hardware	Subm. pres.	14
		25’	TC for combined physical attacks	Subm. pres.	15
		25’	VerMI: Verification tool	Subm. pres.	16
—	10:25–10:55	30’	Morning coffee break	—	-
II.2. Panel on TIS	10:55–12:10	75’	**Theory of implementation security**	**Subm. panel**	17
—	12:10–13:30	80’	Lunch break (@ heritage room)	—	-
					18
					19
					20
	15:10–15:40	30’	Afternoon coffee break	—	-
					21
					22
					23
					24

† Time durations are in minutes

pres. (presentation proposal); Subm. (submitted); TC (threshold cryptography).

Workshop schedule — day 2

What will we be talking about?

Session	2019-Mar-12	Time†	**Topic** (free abbreviation)	Source	#
—	08:00–08:45	75’	Light refreshments	—	-
II.1. Threshold circuit design	08:45–10:25	25’	Tradeoffs shares/area/latency	Subm. pres.	13
		25’	Pitfalls of TC in hardware	Subm. pres.	14
		25’	TC for combined physical attacks	Subm. pres.	15
		25’	VerMI: Verification tool	Subm. pres.	16
—	10:25–10:55	30’	Morning coffee break	—	-
II.2. Panel on TIS	10:55–12:10	75’	Theory of implementation security	**Subm. panel**	17
—	12:10–13:30	80’	Lunch break (@ heritage room)	—	-
II.3. Other threshold primitives					18
					19
					20
	15:10–15:40	30’	Afternoon coffee break	—	-
					21
					22
					23
					24

† Time durations are in minutes

pres. (presentation proposal); Subm. (submitted); TC (threshold cryptography).

Workshop schedule — day 2

What will we be talking about?

Session	2019-Mar-12	Time†	**Topic** (free abbreviation)	Source	#
—	08:00–08:45	75’	Light refreshments	—	-
II.1. Threshold circuit design	08:45–10:25	25’	Tradeoffs shares/area/latency	Subm. pres.	13
		25’	Pitfalls of TC in hardware	Subm. pres.	14
		25’	TC for combined physical attacks	Subm. pres.	15
		25’	VerMI: Verification tool	Subm. pres.	16
—	10:25–10:55	30’	Morning coffee break	—	-
II.2. Panel on TIS	10:55–12:10	75’	Theory of implementation security	**Subm. panel**	17
—	12:10–13:30	80’	Lunch break (@ heritage room)	—	-
II.3. Other threshold primitives	13:30–14:20	25’	**Leakage resilient secret-sharing**	Subm. paper	18
		25’	**Symmetric-key encryption**	Subm. paper	19
					20
	15:10–15:40	30’	Afternoon coffee break	—	-
					21
					22
					23
					24

† Time durations are in minutes

pres. (presentation proposal); Subm. (submitted); TC (threshold cryptography).

Workshop schedule — day 2

What will we be talking about?

Session	2019-Mar-12	Time†	Topic (free abbreviation)	Source	#
—	08:00–08:45	75’	Light refreshments	—	-
II.1. Threshold circuit design	08:45–10:25	25’	Tradeoffs shares/area/latency	Subm. pres.	13
		25’	Pitfalls of TC in hardware	Subm. pres.	14
		25’	TC for combined physical attacks	Subm. pres.	15
		25’	VerMI: Verification tool	Subm. pres.	16
—	10:25–10:55	30’	Morning coffee break	—	-
II.2. Panel on TIS	10:55–12:10	75’	Theory of implementation security	**Subm. panel**	17
—	12:10–13:30	80’	Lunch break (@ heritage room)	—	-
II.3. Other threshold primitives	13:30–14:20	25’	Leakage resilient secret-sharing	Subm. paper	18
		25’	Symmetric-key encryption	Subm. paper	19
II.4. TC apps and experience	14:20–16:55	50’	**Multi-Sigs in Bitcoin**	**Invited keynote**	20
		30’	Afternoon coffee break	—	-
					21
					22
					23
					24

† Time durations are in minutes

pres. (presentation proposal); Subm. (submitted); TC (threshold cryptography).

Workshop schedule — day 2

What will we be talking about?

Session	2019-Mar-12	Time†	**Topic** (free abbreviation)	Source	#
—	08:00–08:45	75’	Light refreshments	—	-
II.1. Threshold circuit design	08:45–10:25	25’	Tradeoffs shares/area/latency	Subm. pres.	13
		25’	Pitfalls of TC in hardware	Subm. pres.	14
		25’	TC for combined physical attacks	Subm. pres.	15
		25’	VerMI: Verification tool	Subm. pres.	16
—	10:25–10:55	30’	Morning coffee break	—	-
II.2. Panel on TIS	10:55–12:10	75’	Theory of implementation security	**Subm. panel**	17
—	12:10–13:30	80’	Lunch break (@ heritage room)	—	-
II.3. Other threshold primitives	13:30–14:20	25’	Leakage resilient secret-sharing	Subm. paper	18
		25’	Symmetric-key encryption	Subm. paper	19
II.4. TC apps and experience	14:20–16:55	50’	Multi-Sigs in Bitcoin	**Invited keynote**	20
		30’	Afternoon coffee break	—	-
		25’	**SplitKey case study (national eID)**	Subm. pres.	21
		25’	**TC for cloud & crypto-currencies**	Subm. pres.	22
		25’	**Practice-based recommendations**	Subm. pres.	23
					24

† Time durations are in minutes

pres. (presentation proposal); Subm. (submitted); TC (threshold cryptography).

Workshop schedule — day 2

What will we be talking about?

Session	2019-Mar-12	Time†	Topic (free abbreviation)	Source	#
—	08:00–08:45	75’	Light refreshments	—	-
II.1. Threshold circuit design	08:45–10:25	25’	Tradeoffs shares/area/latency	Subm. pres.	13
		25’	Pitfalls of TC in hardware	Subm. pres.	14
		25’	TC for combined physical attacks	Subm. pres.	15
		25’	VerMI: Verification tool	Subm. pres.	16
—	10:25–10:55	30’	Morning coffee break	—	-
II.2. Panel on TIS	10:55–12:10	75’	Theory of implementation security	**Subm. panel**	17
—	12:10–13:30	80’	Lunch break (@ heritage room)	—	-
II.3. Other threshold primitives	13:30–14:20	25’	Leakage resilient secret-sharing	Subm. paper	18
		25’	Symmetric-key encryption	Subm. paper	19
II.4. TC apps and experience	14:20–16:55	50’	Multi-Sigs in Bitcoin	**Invited keynote**	20
		30’	Afternoon coffee break	—	-
		25’	SplitKey case study (national eID)	Subm. pres.	21
		25’	TC for cloud & crypto-currencies	Subm. pres.	22
		25’	Practice-based recommendations	Subm. pres.	23
Closing	16:55–17:15	20’	**Final remarks**	NIST	24

† Time durations are in minutes

pres. (presentation proposal); Subm. (submitted); TC (threshold cryptography).

Workshop schedule — day 2

What will we be talking about?

Session	**2019-Mar-12**	**Time**†	**Topic** (free abbreviation)	**Source**	#
—	08:00–08:45	75’	Light refreshments	—	-
II.1. Threshold circuit design	08:45–10:25	25’	Tradeoffs shares/area/latency	Subm. pres.	13
		25’	Pitfalls of TC in hardware	Subm. pres.	14
		25’	TC for combined physical attacks	Subm. pres.	15
		25’	VerMI: Verification tool	Subm. pres.	16
—	10:25–10:55	30’	Morning coffee break	—	-
II.2. Panel on TIS	10:55–12:10	75’	Theory of implementation security	**Subm. panel**	17
—	12:10–13:30	80’	Lunch break (@ heritage room)	—	-
II.3. Other threshold primitives	13:30–14:20	25’	Leakage resilient secret-sharing	Subm. paper	18
		25’	Symmetric-key encryption	Subm. paper	19
II.4. TC apps and experience	14:20–16:55	50’	Multi-Sigs in Bitcoin	**Invited keynote**	20
		30’	Afternoon coffee break	—	-
		25’	SplitKey case study (national eID)	Subm. pres.	21
		25’	TC for cloud & crypto-currencies	Subm. pres.	22
		25’	Practice-based recommendations	Subm. pres.	23
Closing	16:55–17:15	20’	Final remarks	NIST	24

† Time durations are in minutes

pres. (presentation proposal); Subm. (submitted); TC (threshold cryptography).

- Contact email: threshold-crypto@nist.gov
- Project webpage: https://csrc.nist.gov/Projects/Threshold-Cryptography
- NISTIR 8214: https://csrc.nist.gov/publications/detail/nistir/8214/final
- NTCW webpage: https://csrc.nist.gov/Events/2019/NTCW19
- Forum: https://groups.google.com/a/list.nist.gov/forum/#!forum/tc-forum
  (register for announcements; we can add your email if you send us a request)

Word cloud based on the NISTIR 8214

- Contact email: threshold-crypto@nist.gov
- Project webpage: https://csrc.nist.gov/Projects/Threshold-Cryptography
- NISTIR 8214: https://csrc.nist.gov/publications/detail/nistir/8214/final
- NTCW webpage: https://csrc.nist.gov/Events/2019/NTCW19
- Forum: https://groups.google.com/a/list.nist.gov/forum/#!forum/tc-forum
  (register for announcements; we can add your email if you send us a request)

Thank you for your attention

Word cloud based on the NISTIR 8214

- Contact email: threshold-crypto@nist.gov
- Project webpage: https://csrc.nist.gov/Projects/Threshold-Cryptography
- NISTIR 8214: https://csrc.nist.gov/publications/detail/nistir/8214/final
- NTCW webpage: https://csrc.nist.gov/Events/2019/NTCW19
- Forum: https://groups.google.com/a/list.nist.gov/forum/#!forum/tc-forum
  (register for announcements; we can add your email if you send us a request)

References

[BDL97] D. Boneh, R. A. DeMillo, and R. J. Lipton. *On the Importance of Checking Cryptographic Protocols for Faults*. In W. Fumy (ed.), Advances in Cryptology — EUROCRYPT '97, pages 37–51, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg. DOI:10.1007/3-540-69053-0˙4.

[BMV19] L. T. A. N. Brandão, N. Mouha, and A. Vassilev. *Threshold Schemes for Cryptographic Primitives — Challenges and Opportunities in Standardization and Validation of Threshold Cryptography*. NISTIR 8214, March 2019. DOI:10.6028/NIST.IR.8214.

[BMW+18] J. v. Bulck, M. Minkin, O. Weisse, D. Genkin, B. Kasikci, F. Piessens, M. Silberstein, T. F. Wenisch, Y. Yarom, and R. Strackx. *Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution*. In 27th USENIX Security Symposium (USENIX Security 18), page 991–1008, Baltimore, MD, 2018. USENIX Association.

[Cha00] G. Chaucer. *The Ten Commandments of Love*, 1340–1400. See "For three may kepe counseil if twain be away!" in the "Secretnesse" stanza of the poem. https://sites.fas.harvard.edu/ chaucer/special/lifemann/love/ten-comm.html. Accessed: July 2018.

[DLK+14] Z. Durumeric, F. Li, J. Kasten, J. Amann, J. Beekman, M. Payer, N. Weaver, D. Adrian, V. Paxson, M. Bailey, and J. A. Halderman. *The Matter of Heartbleed*. In Proceedings of the 2014 Conference on Internet Measurement Conference, IMC '14, pages 475–488, New York, NY, USA, 2014. ACM. DOI:10.1145/2663716.2663755.

[Don13] D. Donzai. *Using Cold Boot Attacks and Other Forensic Techniques in Penetration Tests*, 2013. https://www.ethicalhacker.net/features/root/using-cold-boot-attacks-forensic-techniques-penetration-tests/. Accessed: July 2018.

[Gro16] C. T. Group. *NIST Cryptographic Standards and Guidelines Development Process*. NISTIR 7977, March 2016. DOI:10.6028/NIST.IR.7977.

[HSH+09] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten. *Lest We Remember: Cold-boot Attacks on Encryption Keys*. Commun. ACM, 52(5):91–98, May 2009. DOI:10.1145/1506409.1506429.

[KGG+18] P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom. *Spectre Attacks: Exploiting Speculative Execution*. ArXiv e-prints, January 2018. arXiv:1801.01203.

[LSG+18] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, and M. Hamburg. *Meltdown*. ArXiv e-prints, jan 2018. arXiv:1801.01207.

[RSWO17] E. Ronen., A. Shamir, A.-O. Weingarten, and C. O'Flynn. *IoT Goes Nuclear: Creating a ZigBee Chain Reaction*. IEEE Symposium on Security and Privacy, pages 195–212, 2017. DOI:10.1109/SP.2017.14.

[Sau34] R. Saunders. *Poor Richard's Almanack — 1735*. Benjamin Franklin, 1734.

[SH07] J.-M. Schmidt and M. Hutter. *Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results*, pages 61–67. Verlag der Technischen Universität Graz, 2007.

[Sha97] W. Shakespeare. *An excellent conceited Tragedie of Romeo and Juliet*. Printed by John Danter, London, 1597.

[WBM+18] O. Weisse, J. v. Bulck, M. Minkin, D. Genkin, B. Kasikci, F. Piessens, M. Silberstein, R. Strackx, T. F. Wenisch, and Y. Yarom. *Foreshadow-NG: Breaking the Virtual Memory Abstraction with Transient Out-of-Order Execution*. Technical Report, 2018.