WELCOME TO ISCwsISC 2021

Second ISC Winter School on Information Security and Cryptology
February 2021 (Virtual Event)

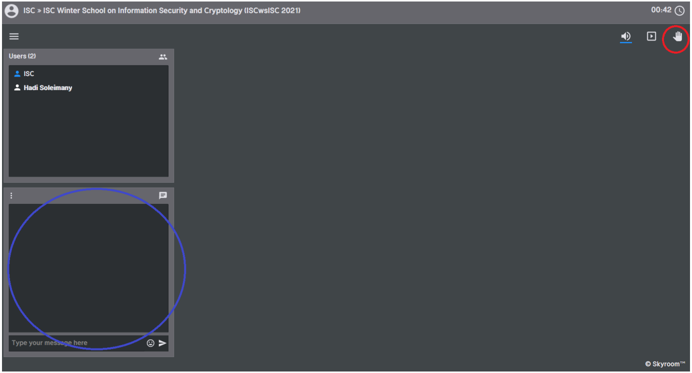
انجمن رمز ایران
Iranian Society of Cryptology

Cyberspace Research Institute

Technical Content

- 5 main topics:
  - Fault attacks and countermeasures
  - Timing attacks and countermeasures
  - Power analysis attacks and countermeasures
  - White-box cryptography
  - Design from the implementation perspective

Skyroom



ISC » ISC Winter School on Information Security and Cryptology (ISCwsISC 2021)

00:42

Users (2)

ISC

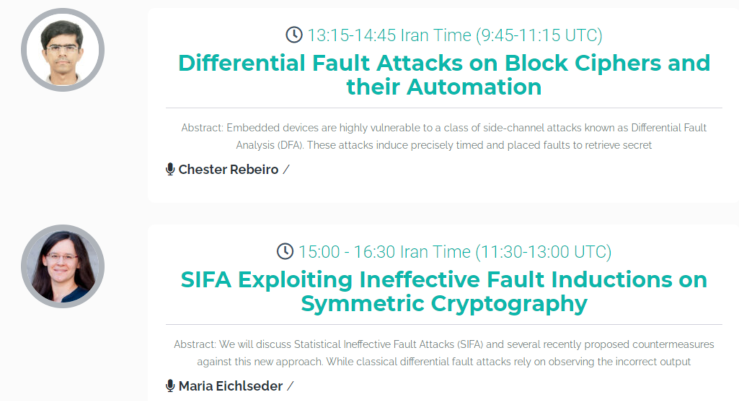
Hadi Soleimany

Type your message here

© Skyroom™

- To raise your hand during a session, select Raise Hand from the top right.
- You can also write your question in the Chat Box located in bottom left.

Program Day 1 (Monday): Fault Attacks



13:15-14:45 Iran Time (9:45-11:15 UTC)

Differential Fault Attacks on Block Ciphers and their Automation

Abstract: Embedded devices are highly vulnerable to a class of side-channel attacks known as Differential Fault Analysis (DFA). These attacks induce precisely timed and placed faults to retrieve secret

Chester Rebeiro /

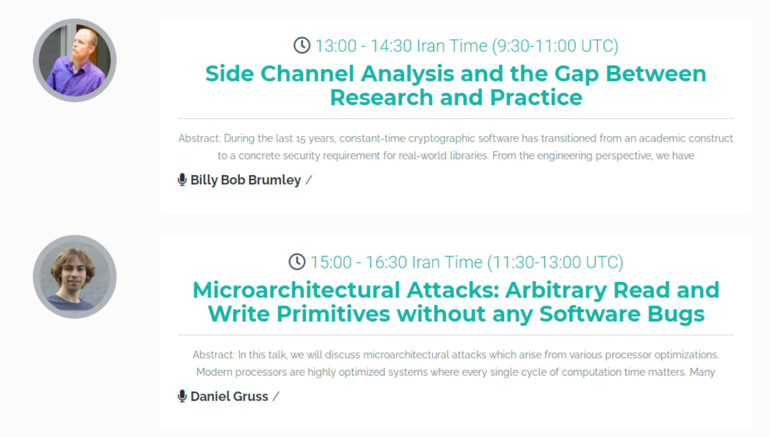
15:00 - 16:30 Iran Time (11:30-13:00 UTC)

SIFA Exploiting Ineffective Fault Inductions on Symmetric Cryptography

Abstract: We will discuss Statistical Ineffective Fault Attacks (SIFA) and several recently proposed countermeasures against this new approach. While classical differential fault attacks rely on observing the incorrect output

Maria Eichlseder /

Program Day 2 (Tuesday): Timing Attack



13:00 - 14:30 Iran Time (9:30-11:00 UTC)

Side Channel Analysis and the Gap Between Research and Practice

Abstract: During the last 15 years, constant-time cryptographic software has transitioned from an academic construct to a concrete security requirement for real-world libraries. From the engineering perspective, we have

Billy Bob Brumley /

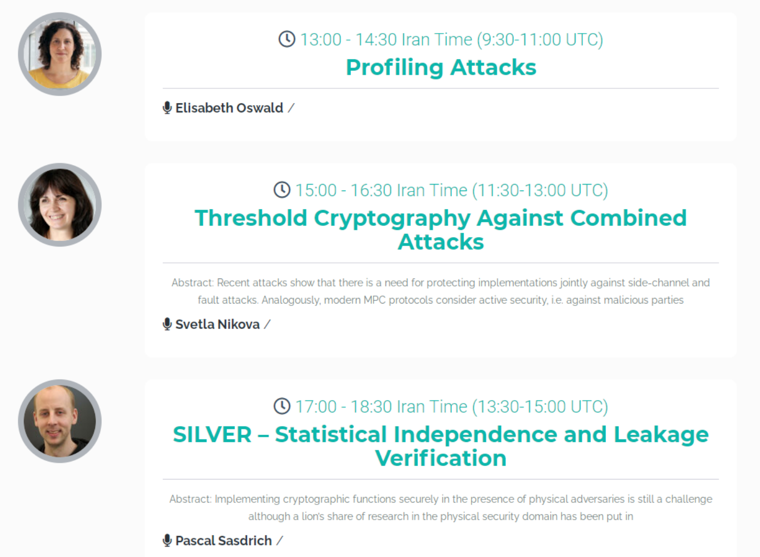
15:00 - 16:30 Iran Time (11:30-13:00 UTC)

Microarchitectural Attacks: Arbitrary Read and Write Primitives without any Software Bugs

Abstract: In this talk, we will discuss microarchitectural attacks which arise from various processor optimizations. Modern processors are highly optimized systems where every single cycle of computation time matters. Many

Daniel Gruss /

Program Day 3 (Wednesday): Power Analysis Attacks



13:00 - 14:30 Iran Time (9:30-11:00 UTC)

Profiling Attacks

Elisabeth Oswald /

15:00 - 16:30 Iran Time (11:30-13:00 UTC)

Threshold Cryptography Against Combined Attacks

Abstract: Recent attacks show that there is a need for protecting implementations jointly against side-channel and fault attacks. Analogously, modern MPC protocols consider active security, i.e. against malicious parties

Svetla Nikova /

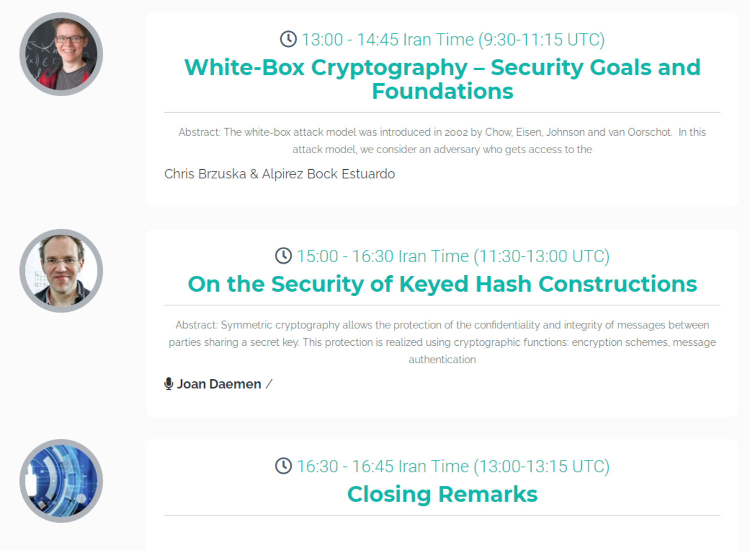
17:00 - 18:30 Iran Time (13:30-15:00 UTC)

SILVER – Statistical Independence and Leakage Verification

Abstract: Implementing cryptographic functions securely in the presence of physical adversaries is still a challenge although a lion's share of research in the physical security domain has been put in

Pascal Sasdrich /

Program Day 4 (Thursday): White-box Cryptography and Design



🕓 13:00 - 14:45 Iran Time (9:30-11:15 UTC)

White-Box Cryptography – Security Goals and Foundations

Abstract: The white-box attack model was introduced in 2002 by Chow, Eisen, Johnson and van Oorschot. In this attack model, we consider an adversary who gets access to the

Chris Brzuska & Alpirez Bock Estuardo

🕓 15:00 - 16:30 Iran Time (11:30-13:00 UTC)

On the Security of Keyed Hash Constructions

Abstract: Symmetric cryptography allows the protection of the confidentiality and integrity of messages between parties sharing a secret key. This protection is realized using cryptographic functions: encryption schemes, message authentication

🎙 **Joan Daemen** /

🕓 16:30 - 16:45 Iran Time (13:00-13:15 UTC)

Closing Remarks

More points

- Videos will be available in ISC Aparat channel: https://www.aparat.com/Irancrypt

More points

- Videos will be available in ISC Aparat channel: https://www.aparat.com/Irancrypt
- Slides will be added in the winter school website: http://iscwsisc2021.sbu.ac.ir/

More points

- Videos will be available in ISC Aparat channel: https://www.aparat.com/Irancrypt
- Slides will be added in the winter school website: http://iscwsisc2021.sbu.ac.ir/
- ISC pre-school event that involves introduction lectures by experienced researchers was held between 1 February and 4 February 2021.

More points

- Videos will be available in ISC Aparat channel: https://www.aparat.com/Irancrypt
- Slides will be added in the winter school website: http://iscwsisc2021.sbu.ac.ir/
- ISC pre-school event that involves introduction lectures by experienced researchers was held between 1 February and 4 February 2021.
    - Slides are available in the website: http://iscwsisc2021.sbu.ac.ir/fa/

More points

- Videos will be available in ISC Aparat channel: https://www.aparat.com/Irancrypt
- Slides will be added in the winter school website: http://iscwsisc2021.sbu.ac.ir/
- ISC pre-school event that involves introduction lectures by experienced researchers was held between 1 February and 4 February 2021.
  - Slides are available in the website: http://iscwsisc2021.sbu.ac.ir/fa/
  - Videos are available in ISC Aparat channel

More points

- Videos will be available in ISC Aparat channel: https://www.aparat.com/Irancrypt
- Slides will be added in the winter school website: http://iscwsisc2021.sbu.ac.ir/
- ISC pre-school event that involves introduction lectures by experienced researchers was held between 1 February and 4 February 2021.
    - Slides are available in the website: http://iscwsisc2021.sbu.ac.ir/fa/
    - Videos are available in ISC Aparat channel
- Feel free to contact us if you have any questions or problem (email address: iscwsisc2021@sbu.ac.ir)

Acknowledgments

We thank all people who contributed to ISCwsISC 2021:

- All the members of the Programme Committee:
  - Haleh Amintoosi, Ferdowsi University of Mashhad
  - Nasour Bagheri, Shahid Rajaee Teacher Training University
  - Reza Ebrahimi Atani, University of Guilan
  - Shahram Khazei, Sharif University of Technology
  - Mahtab Mirmohseni, Sharif University of Technology
  - Farokhlagha Moazami, Shahid Beheshti University (General chair)
  - Mohammad Ali Orumiehchiha, Research Center for Development of Advanced Technologies
  - Raziye Salarifard, Shahid Beheshti University
  - Mahmoud Salmasizadeh, Sharif University of Technology
  - Hadi Soleimany, Shahid Beheshti University

Acknowledgments

We thank all people who contributed to ISCwsISC 2021:

- Speakers of pre-school event:Meysam Bashirpour, Ali Jahanian, Farokhlagha Moazami, Amir Moradi, Mohammad Ali Orumiehchiha, Raziye Salarifard, Mehri Yahyayi.

Acknowledgments

We thank all people who contributed to ISCwsISC 2021:

- Speakers of pre-school event:Meysam Bashirpour, Ali Jahanian, Farokhlagha Moazami, Amir Moradi, Mohammad Ali Orumiehchiha, Raziye Salarifard, Mehri Yahyayi.
- Session chairs: Reza Ebrahimi Atani, Nasour Bagheri, Sadegh Dorri, Shahram Khazei, Massoud Masoumi, Atefeh Musavi, Mohammad Ali Orumiehchiha, Mahmoud Salmasizadeh, Somayeh Timarchi.

Acknowledgments

We thank all people who contributed to ISCwsISC 2021:

- Speakers of pre-school event:Meysam Bashirpour, Ali Jahanian, Farokhlagha Moazami, Amir Moradi, Mohammad Ali Orumiehchiha, Raziye Salarifard, Mehri Yahyayi.
- Session chairs: Reza Ebrahimi Atani, Nasour Bagheri, Sadegh Dorri, Shahram Khazei, Massoud Masoumi, Atefeh Musavi, Mohammad Ali Orumiehchiha, Mahmoud Salmasizadeh, Somayeh Timarchi.
- All those at Cyberspace Research Institute who have helped, including: Maryahm Heidari, Milad Seddigh, Amir Hossein Saffari and Sara Zarei.

Thank you very much and Enjoy ISCwsISC 2021!