AICrypt 2023

3rd Workshop on Artificial Intelligence and Cryptography

April 22nd, 2023
Lyon, France
Event affiliated with Eurocrypt 2023

*** Abstract Submission Deadline: March 3, 2023 ***

https://aicrypt2023.aisylab.com

In recent years, the interplay between artificial intelligence (AI) and security is becoming more prominent and important. This comes naturally because of the need to improve security more efficiently. One specific domain of security that steadily receives more AI applications is cryptography. We already see how AI techniques can improve implementation attacks, attacks on PUFs, hardware Trojan detection, etc. Besides AI's role in cryptography, we believe cryptography for AI to be an emerging and important topic. As we can see an increasing number of attacks on AI systems, one possible research direction could be to investigate which cryptographic techniques can be used to mitigate such threats.

We aim to gather researchers from academia and industry that work on various aspects of cryptography and AI to share their experience and discuss how to strengthen the collaboration. We are especially interested in exploring the transferability of techniques among various cryptographic applications and AI protection mechanisms. Finally, we will discuss the developments happening in the last years, i.e., from the previous AICrypt events.

Topics of Interest

The topics of the workshop encompass all aspects concerning the intersection of AI and cryptography, including but not limited to:

- Deep learning-based cryptanalysis (e.g., neural distinguishers)
- Explainability and interpretability of AI models for cryptanalysis
- Deep learning techniques for Side-Channel Analysis
- AI-assisted design of cryptographic primitives and protocols
- AI-driven attacks on cryptographic protocols
- Cryptographic countermeasures for security and privacy of AI systems

Submissions

We encourage researchers working on all aspects of AI and cryptography to take the opportunity and use AICrypt to share their work and participate in discussions. The authors are invited to submit an extended abstract using the EasyChair submission system. Submitted abstracts for contributed talks will be reviewed by the program committee for suitability and interest to the AICrypt audience. There are no formal proceedings published in this workshop, thus authors can submit extended abstracts related to works submitted or recently published in other venues, or work in progress that they plan to submit elsewhere. Every accepted submission must have at least one author registered for the workshop. All submitted abstracts must follow the original LNCS format with a page limit of up to 2 pages (excluding references). The abstracts should be submitted electronically in PDF format.

Important Dates (AoE)

- Abstract submission deadline: March 3rd, 2023.
- Notification to authors: March 17th, 2023.
- Workshop date: April 22nd, 2023.

Participation

The workshop will be held in Lyon, France, as an event affiliated to Eurocrypt 2023. Further information related to registration is available on the main Eurocrypt website.

Workshop Organizers

- Stjepan Picek, Radboud University, Nijmegen (NL) - stjepan.picek@ru.nl
- Lejla Batina, Radboud University, Nijmegen (NL) - lejla@cs.ru.nl
- Luca Mariot, University of Twente, Enschede (NL) - l.mariot@utwente.nl

Website

https://aicrypt2023.aisylab.com