AICrypt 2024

4th Workshop on Artificial Intelligence and Cryptography

May 26th, 2024
Zurich, Switzerland
Event affiliated with Eurocrypt 2024

*** Extended Submission Deadline: April 15, 2024 ***

https://aicrypt2024.aisylab.com

Recently, the synergy between artificial intelligence (AI) and security has gained increasing prominence and significance. This evolution naturally arises from the need to enhance security with greater efficiency. Among the many areas of security benefiting from AI's integration, cryptography stands as a notable field. We are already witnessing the application of AI techniques to address several problems in cryptography, such as enhancing defenses against implementation attacks and hardware Trojans, and investigating attacks on Physical Unclonable Functions (PUFs). Beyond AI's contributions to cryptography, it is also possible to identify the use of cryptography to solve security and privacy issues in AI systems as an emerging and pivotal subject. The mounting frequency of AI system attacks urges us to explore potential research avenues involving cryptographic strategies to counteract these threats. Our objective is to convene experts from both academic and industrial backgrounds, each contributing to diverse facets of cryptography and AI, to facilitate knowledge exchange and foster collaborative efforts. Of particular interest is the exploration of the transferability of techniques across different cryptographic applications and the strengthening of AI security mechanisms. Furthermore, we will delve into recent developments, including those stemming from previous AICrypt events, to provide insights into the evolving landscape of this field.

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 workshop organizers 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: ~~April 5th, 2024.~~ April 15th, 2024 (Extended)
- Notification to authors: April 19th, 2024.
- Workshop date: May 26th, 2024.

Participation

The workshop will be held in Zurich, Switzerland, as an event affiliated to Eurocrypt 2024. 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://aicrypt2024.aisylab.com