Observations on the impact of AI on cryptography

Gyöngyvér Márton

Sapientia Hungarian University of Transylvania, Târgu Mures, Romania

mgyongyi@ms.sapientia.ro

Due to the rapid development of artificial intelligence and machine learning in recent years, we have experienced many advantages and challenges of this technology. We see that a tool has been created that greatly facilitates the writing of programs and that everyone, regardless of knowledge or experience, uses with pleasure. It can also be said that, since processing huge amounts of data on remote servers is becoming an everyday practice, new cryptographic solutions are needed to guarantee the security of this data.

In this presentation, we will explore the problems that pose inherent dangers in AI, that is, we will analyze how program codes written with the help of AI affect data security, we will show how AI systems threaten the security of the user's personal data, and we will analyze what recommendations exist regarding the use of cryptographic primitives in AI systems.

References

[1] N. Perry, M. Srivastava, D. Kumar, D. Boneh, Do Users Write More Insecure Code with AI Assistants?, *CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security Pages 2785 - 2799*, 2023.

[2] H. Pearce, B. Ahmad, B. Tan, B. Dolan-Gavitt, R. Karri, Asleep at the Keyboard? Assessing the Security of GitHub Copilot's Code Contributions, *Communications of the ACM, Volume 68, Issue 2 Page 95*, 2025.

[3] H. Taherdoost, T. V. Le, K. Slimani, Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review, *Cryptography, 9(1), 17*, 2025.