Enabling Privacy, Trust and Security in Emerging Technologies using Zero-Knowledge Proofs

Supervisors

prof. dr hab. Stefan Dziembowski (IDEAS NCBR)

dr hab. inż. Josef Pieprzyk, prof. IPI PAN

Description

Emerging technologies, such as artificial intelligence (AI) and blockchain, have gained widespread adoption among users. However, the increasing usage of these technologies in daily life has given rise to concerns surrounding users' privacy, correctness of computations, and the authenticity of resulting data. For instance, recent advances in AI models have made it possible to produce digital media that are nearly indistinguishable from human-generated content. This has led to the need to verify the trustworthiness and authenticity of media, in certain applications such as news reports. Moreover, in many AI applications, users are required to share their private data to be processed by the AI model, raising concerns about privacy.

Zero-knowledge proofs (ZKP) are cryptographic tools that enable a prover to demonstrate the truth of a statement to a verifier without revealing additional information. This property makes ZKP an appealing solution for applications that require security and privacy, such as privacy-preserving machine learning (PPML) [1], blockchain-based platforms, and verifiable computations (VC) [2]. However, current ZKP protocols may experience computational and communication overheads, which hinder their scalability and efficiency, making them unsuitable for use as infrastructure in various applications. To tackle these challenges, this project aim at investigation of innovative techniques for designing efficient and scalable protocols based on ZKP, which incorporate verifiable computation techniques. This will allow for the provision of proofs of valid computation (e.g. valid history of edits from a referenced origin in digital media scenario).

The research necessitates a sound understanding of privacy concerns and challenges within cryptographic protocols. Familiarity with software programming languages, such as Python, and hardware programming languages, such as Verilog, would be helpful for implementation purposes. Furthermore, a comprehensive knowledge of general cryptography, security, and the privacy challenges, in addition to a profound understanding of blockchain fundamentals, smart contracts, and zero-knowledge proofs is essential.

Requirements

- MSc degree in computer science or related field
- Good knowledge in cryptography, multi-party computation (MPC), zero-knowledge proof (ZKP), blockchain technology, and different encryption schemes.
- Practical experience with programming in at least one of the following languages: Python, C++, JavaScript, Verilog, Solidity.
- Advanced skills in written and spoken English
- Publication track record in major Cryptography venues (e.g. CRYPTO, EuroCrypt, S&P) **is a plus**

References

[1] Mohassel, P., & Zhang, Y. (2017, May). Secureml: A system for scalable privacy-preserving machine learning. In 2017 IEEE symposium on security and privacy (S&P) (pp. 19-38). IEEE.

[2] Wahby, R. S., Howald, M., Garg, S., Shelat, A., & Walfish, M. (2016, May). Verifiable asics. In 2016 IEEE Symposium on Security and Privacy (S&P) (pp. 759-778). IEEE.