Doctoral School of Information and Biomedical Technologies
Polish Academy of Sciences (TIB PAN)

SUBJECT:

Applied cryptography and privacy protection

SUPERVISOR:

Mirosław Kutyłowski, miroslaw.kutylowski@nask.pl, NASK PIB, Kolska 12, 01-045 Warszawa
(remote supervision from Wrocław)

DESCRIPTION:

The real impact and strength of cryptographic techniques depends very much on multiple factors and interaction of the cryptographic schemes with the environment. According to the famous statement: "cryptography will not be broken, it will be bypassed". is In particular, we have to deal with the situations such as implementations errors opening door for attacks (e.g. by side-channel analysis), malicious participants and devices deviating from protocol description in an invisible way, or even powerful adversaries with unknown attack capabilities.

Nevertheless, the situation is not hopeless. The general goal is to design schemes and their implementation strategies that are secure by-design in the E2E model, where every involved component and agent may be faulty or malicious. Such solutions will not protect unconditionally, but typically may provide an undeniable proof of adversarial activities and indicate the party responsible.

The proposed research topics contain but are not limited to identity management, privacy protection technologies, long period security and crypto assets creation and management. Interaction between practice and European ICT regulations are in particular focus.

BIBLIOGRAPHY:

IACR publications (conference proceedings, eprint, journals) …