

---

# How to protect privacy with cryptographic methods

Duong Hieu Phan<sup>\*1</sup>

<sup>1</sup>Télécom Paris – Télécom Paris, Télécom-Paris – France

## Résumé

Cryptography traditionally supports data confidentiality, integrity, and authenticity. However, when cryptographic protocols are deployed in emerging applications such as cloud services or big data, the demand for security grows beyond these requirements. Data nowadays are being extensively stored in the cloud, and users also need to trust the authorities/cloud servers that run powerful applications. Collecting user data, combined with powerful tools (e.g., machine learning), can come with a huge risk of mass surveillance or of undesirable data-driven strategies for profit making while ignoring users' needs. Privacy protection, which allows individuals to have control over how their personal data is collected and used, therefore, becomes more and more critical. New techniques should be developed, first, to protect personal privacy, and, second, to reduce centralized trust in authorities or in technical solutions providers. In this talk, we discuss privacy-preserving solutions with techniques in cryptography.

---

\*Intervenant