Engagements cryptographiques sur des données anonymisables

Charlène Jojon*[1,2]

[1]LIFO, Université d'Orléans, INSA Centre Val de Loire – INSA - Institut National des Sciences Appliquées – France

[2]Inria Saclay – INRIA Saclay Ile-de-France, INRIA Saclay Île de France – France

Résumé

Local Differential Privacy (LDP) mechanisms consist of (locally) adding controlled noise to data in order to protect the privacy of their owner. In this paper, we introduce a new cryptographic primitive called LDP commitment. Usually, a commitment ensures that the committed value cannot be modified before it is revealed. In the case of an LDP commitment, however, the value is revealed after being perturbed by an LDP mechanism. Opening an LDP commitment therefore requires a proof that the mechanism has been correctly applied to the value, to ensure that the value is still usable for statistical purposes. We also present a security model for this primitive, in which we define the hiding and binding properties. Finally, we present a concrete scheme for an LDP staircase mechanism (generalizing the randomized response technique), based on classical cryptographic tools and standard assumptions. We provide an implementation in Rust that demonstrates its practical efficiency (the generation of a commitment requires just a few milliseconds). On the application side, we show how our primitive can be used to ensure simultaneously privacy, usability and traceability of medical data when it is used for statistical studies in an open science context. We consider a scenario where a hospital provides sensitive patients data signed by doctors to a research center after it has been anonymized, so that the research center can verify both the provenance of the data (i.e. verify the doctors' signatures even though the data has been noised) and that the data has been correctly anonymized (i.e. is usable even though it has been anonymized). In collaboration with: Xavier Bultel, LIFO, Université d'Orléans, INSA Centre Val de Loire, INRIA; Céline Chevalier, CRED, Université Panthéon-Assas, DIENS, École normale supérieure, PSL University, CNRS, INRIA; Diandian Liu, LIFO, Université d'Orléans, INSA Centre Val de Loire, INRIA; Benjamin Nguyen, LIFO, Université d'Orléans, INSA Centre Val de Loire, INRIA.

*Intervenant