Cryptography for private electronic traffic pricing

Ruben De Smet

Vrije Universiteit Brussel, Brussel, Belgium

(Joint work with Kris Steenhaut and An Braeken)

Due to road congestion and pollution during peak-hours, some governments are interested in implementing "traffic pricing" policies. In these schemes, your usage of the public road is taxed based on the time and location of use. The potential implications regarding the privacy of the driver are not to be overlooked.

Zero-knowledge proofs (ZKPs) can help in protecting the driver's privacy. In this talk, we go over the notion of zero-knowledge proofs, and how they can be instantiated over elliptic curves. Finally, we show how a ZKP can offer a more efficient traffic pricing scheme compared to a naive, privacy-violating send-it-all scheme.

Vrije Universiteit Brussel, ETRO (Electronics and Informatics), Pleinlaan 2, 1000 Brussel, Belgium
rubedesm@vub.be