UNIVERSIDAD COMPLUTENSE MADRID

Facultad de Informática

ANUNCIO DE CONFERENCIA

POSGRADO

How to verify computation in the blink of an eye

Matteo Campanelli
IMDEA Software

Facultad de Informática
Sala de Grados - lunes 1 de julio de 2019 - 16:00
Entrada libre hasta completar el aforo

Resumen:

Trust but verify, they say. If a math-savvy friend did your calculus homework for you, you would do well to have a look at it before you hand it in. Likewise, you want to verify work from third party machines you have no control over. Example: you commissioned TheBigTech (tm) cloud to run a large simulation SIM, whose results you are eager to get recognized for. Issue: you lack the means to rerun and check SIM (after all, that is why you are delegating!). Commissioning more parties may be costly or not a solution. This talk is on how Verifiable Computation (VC)—a mix of theory and systems—solved this problem: the cloud gives us a proof that its work is correct, e.g. that no HW glitch or competitor could have tampered with it. Such a proof is succinct—much more so than the abstract you are reading. You can store it in 100 bytes and verify it in microseconds on a laptop. And VC is secure: a "wrong" proof would pass as good with probability of less than 10^{-35}. I will discuss: - applications of VC (and its "cryptographic" cousins, zkSNARKs, core of the cryptocurrency ZCash), - intuitions on how it works, - resources/APIs for anyone hoping to use VC or learn about it.

Sobre Matteo Campanelli:

Matteo Campanelli joined IMDEA Software as a post-doctoral researcher in 2018. The same year he obtained his Ph.D. from the City University of New York where he worked at the intersection between decision theory, complexity and cryptography. His current research interests are in theoretical and practical aspects of probabilistic proof systems. He was a visiting student at Aarhus University (2016) and at the Stanford Research Institute (2017). Besides cryptographic research he has developed software for Libreoffice and machine learning models for ads quality at Google. He made the mistake of appearing on a few improv comedy stages in NYC; he was never able to surf.