PROBLEM UČENJA Z NAPAKAMI IN SODOBNI KRIPTOSISTEMI

TILEN MARC

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Math. Subj. Class. (2020): 94A60, 68P25, 81P94

Sodobni kriptosistemi so osnovani na matematičnih problemih in njihova varnost je zagotovljena samo, dokler ne obstajajo algoritmi, ki bi te probleme učinkovito rešili. V članku predstavimo nedavno vpeljan algoritmičen problem učenja z napakami, ki se izkaže za izjemno uporabnega v kriptografiji, saj omogoča sestavo novih kriptosistemov z zanimivimi in uporabnimi lastnostmi. Taki kriptosistemi veljajo tudi za varne pred nasprotniki, ki imajo dostop do kvantnega računalnika, kar za večino drugih ne velja. Predstavljena sta kvantno varen kriptosistem z javnim ključem in kriptosistem, ki omogoča računanje na šifriranih podatkih, kar je znano pod imenom homomorfno šifriranje. Konstrukcija slednjega je bila odprt problem več desetletij in dosežena šele s pomočjo problema učenja z napakami.

PROBLEM OF LEARNING WITH ERRORS AND MODERN CRYPTOSYSTEMS

Modern cryptosystems are based on mathematical problems and their security is guaranteed only as long as there are no efficient algorithms solving these problems. We present a recently introduced algorithmic problem of learning with errors (LWE). The problem is crafted for the use in cryptography and allows to construct new cryptosystems with interesting and useful properties. Such cryptosystems are considered safe even against adversaries with access to quantum computers, which does not hold for most of the other systems. We explain how to construct two cryptosystems: a quantumly secure cryptographic scheme with public key, and a scheme that enables computation on encrypted data, known as homomorphic encryption. The construction of the latter was a long standing open problem and was solved only recently with the help of LWE problem.

Uvod

Problem učenja z napakami (ang. *learning with errors – LWE*) je vpeljal Regev v [4] kot nov algoritmičen problem in dokazal, da je vsaj tako težek kot nekateri drugi znani problemi. Članek je povzročil pravo revolucijo, saj je bilo v zadnjem desetletju napisanih na tisoče znanstvenih člankov, ki temeljijo na problemu LWE. Regev je bil leta 2018 za svoj prispevek nagrajen s prestižno Gödelovo nagrado, ki jo vsako leto podelijo za doprinos k teoretičnemu računalništvu.

Glavni razlog za priljubljenost problema LWE je njegova uporabnost v kriptografiji. Eden izmed osnovnih temeljev sodobne kriptografije je t. i. asimetrična kriptografija. Ta omogoča, da uporabnik izračuna svoj javni