Peikert, Chris

Lattice cryptography for the internet. (English) Zbl 1383.94037

Mosca, Michele (ed.), Post-quantum cryptography. 6th international workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1–3, 2014. Proceedings. Berlin: Springer (ISBN 978-3-319-11658-7/pbk). Lecture Notes in Computer Science 8772, 197-219 (2014).

Summary: In recent years, lattice-based cryptography has been recognized for its many attractive properties, such as strong provable security guarantees and apparent resistance to quantum attacks, flexibility for realizing powerful tools like fully homomorphic encryption, and high asymptotic efficiency. Indeed, several works have demonstrated that for basic tasks like encryption and authentication, lattice-based primitives can have performance competitive with (or even surpassing) those based on classical mechanisms like RSA or Diffie-Hellman. However, there still has been relatively little work on developing lattice cryptography for deployment in real-world cryptosystems and protocols.

In this work we take a step toward that goal, by giving efficient and practical lattice-based protocols for key transport, encryption, and authenticated key exchange that are suitable as "drop-in" components for proposed Internet standards and other open protocols. The security of all our proposals is provably based (sometimes in the random-oracle model) on the well-studied "learning with errors over rings" problem, and hence on the conjectured worst-case hardness of problems on ideal lattices (against quantum algorithms).

One of our main technical innovations (which may be of independent interest) is a simple, low-bandwidth reconciliation technique that allows two parties who "approximately agree" on a secret value to reach exact agreement, a setting common to essentially all lattice-based encryption schemes. Our technique reduces the ciphertext length of prior (already compact) encryption schemes nearly twofold, at essentially no cost.

For the entire collection see [Zbl 1296.94005].

MSC:

94A60 Cryptography
68M11 Internet topics

Full Text: DOI