1. Record Nr. UNINA9910709596903321

Autore	Chen Lily
Titolo	Report on post-quantum cryptography / / Lily Chen; Stephen Jordan; Yi-Kai Liu; Dustin Moody; Rene Peralta; Ray Perlner; Daniel Smith-Tone
Pubbl/distr/stampa	Gaithersburg, MD : , : U.S. Dept. of Commerce, National Institute of Standards and Technology, , 2016
Descrizione fisica	1 online resource (15 pages) : illustrations (black and white)
Collana	NISTIR ; ; 8105
Altri autori (Persone)	ChenLily JordanStephen LiuYi-Kai MoodyDustin PeraltaRene PerlnerRay Smith-ToneDaniel
Soggetti	Public key cryptography Quantum computing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	April 2016. Contributed record: Metadata reviewed, not verified. Some fields updated by batch processes. Title from PDF title page (viewed April 30, 2016).
Nota di bibliografia	Includes bibliographical references.
Sommario/riassunto	In recent years, there has been a substantial amount of research on quantum computers machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and

networks. This Internal Report shares the National Institute of Standards and Technology (NIST) s current understanding about the status of quantum computing and post-quantum cryptography, and outlines NIST s initial plan to move forward in this space. The report also recognizes the challenge of moving to new cryptographic infrastructures and therefore emphasizes the need for agencies to focus on crypto agility.