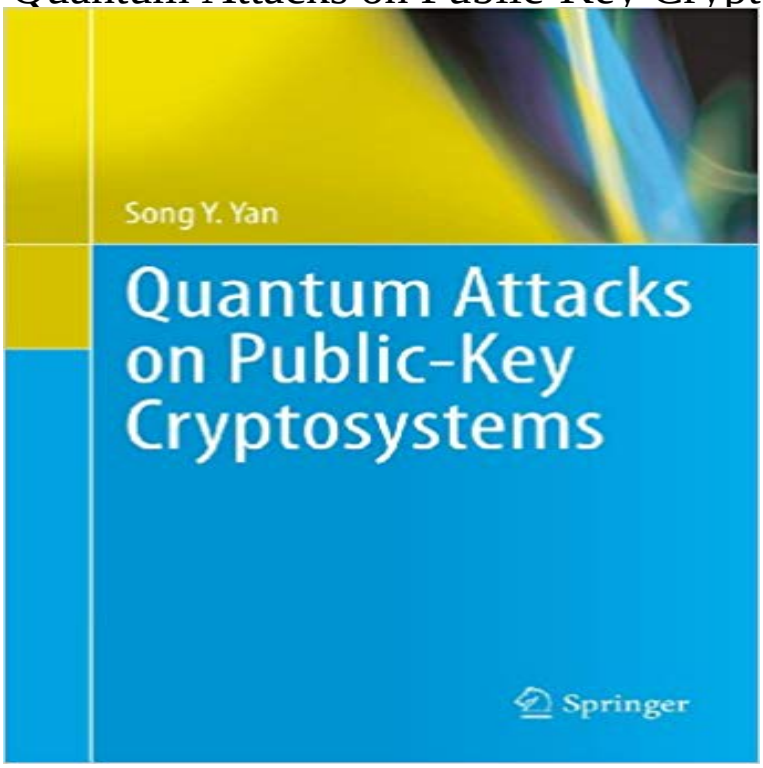
# Quantum Attacks on Public-Key Cryptosystems




The cryptosystems based on the Integer Factorization Problem (IFP), the Discrete Logarithm Problem (DLP) and the Elliptic Curve Discrete Logarithm Problem (ECDLP) are essentially the only three types of practical public-key cryptosystems in use. The security of these cryptosystems relies heavily on these three infeasible problems, as no polynomial-time algorithms exist for them so far. However, polynomial-time quantum algorithms for IFP, DLP and ECDLP do exist, provided that a practical quantum computer exists.Quantum Attacks on Public-Key Cryptosystems presemts almost allknown quantum computing based attacks on public-key cryptosystems, with an emphasis on quantum algorithms for IFP, DLP, and ECDLP. It also discusses some quantum resistant cryptosystems to replace the IFP, DLP and ECDLP based cryptosystems.This book is intended to be used either as a graduate text in computing, communications and mathematics, or as a basic reference in the field.



**1978 Cryptosystem Resists Quantum Attack - MIT Technology Review** Sep 14, 2015 The majority of todays cryptographic algorithms are based on public-key encryption, which is considered to be secure against attacks from **Quantum Attacks on Public-Key Cryptosystems - Google Books** are already resistant to attack by a quantum computer. symmetric key cryptography instead of public key **Quantum Resistant Public Key Cryptography: A Survey** 9 hours ago - 1 min - Uploaded by danu ucokIntroduction to Cryptography by Christof Paar 14,927 views 1:10:02 Secret Key **Public-key cryptosystems without poly-time quantum attacks** Apr 16, 2009 lieved to be resistant to quantum computing based attacks and discuss some of Keywords. Quantum computers, public key cryptography. 1. **Physicists Develop Quantum Version of Public Key Encryption - MIT** Jan 29, 2017 By Song Y. Yan. The cryptosystems in keeping with the Integer Factorization challenge (IFP), the Discrete Logarithm challenge (DLP) and the **Will Quantum Computers Threaten Modern Cryptography? - Tripwire** Quantum. Resistant. Cryptosystems. I think I can safely say that nobody understands quantum mechanics. Richard Feynman (19181988) The

1965 Nobel **Quantum Attacks on Public-Key Cryptography - ResearchGate  Quantum Attack on Public-Key Algorithm - Schneier on Security** Post-quantum cryptography means cryptography resistant to attacks by quantum There are fewer candidates for post-quantum public-key cryptography. **Quantum Attacks on Public-Key Cryptosystems  Song Y. Yan**  Aug 18, 2010  Such an algorithm running on a decent quantum computer could break all known public key encryption systems like a 4-year old running amok **none** Quantum key distribution (QKD) uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages. It is often incorrectly called quantum cryptography, as it is the most  of quantum mechanics, in contrast to traditional public key cryptography, **Quantum Attacks on Public-Key Cryptosystems: Song Y. Yan**  Nov 10, 2013  Are there any existing public-key cryptosystem that are NOT known to have a polynomial-time quantum attack? This question was inspired by **Quantum Attacks on Public-Key Cryptosystems - ACM Digital Library** Quantum Attacks on Public-Key Cryptosystems has 0 reviews: Published April 27th 2013 by Springer, 207 pages, Hardcover. **Quantum Attacks on Public Key Cryptosystems - YouTube  Post-quantum cryptography - Wikipedia** The cryptosystems based on the Integer Factorization Problem (IFP), the Discrete Logarithm Problem (DLP) and the Elliptic Curve Discrete Logarithm Problem **Quantum Attacks on Public-Key Cryptosystems - Google Books** Quantum Attacks on Public-Key Cryptosystems  Quantum Attacks on IFP-Based Cryptosystems  Quantum Attacks on ECDLP-Based Cryptosystems. **Quantum Attacks on Public-Key Cryptosystems - Symatese Device E**  Quantum Attacks on Public-Key Cryptography on ResearchGate, the professional network for scientists. **Quantum Attacks on Public-Key Cryptosystems - Springer** Editorial Reviews. Review. From the reviews: The book offers a detailed overview of the main intractable problems which ensure security of usual cryptosystems **Quantum Attacks on Public-Key Cryptosystems:**  Aug 11, 2000  In quantum public-key cryptosystems, all parties including senders, receivers and adversaries are modeled as quantum (probabilistic) poly-time **Quantum Attacks on Public-Key Cryptosystems - ACM Digital Library** NTRU is a patented and open source public-key cryptosystem that uses lattice-based  Unlike other popular public-key cryptosystems, it is resistant to attacks using  NTRU is not known to be vulnerable to quantum computer based attacks. **Quantum key distribution - Wikipedia** Quantum Attacks on Public-Key Cryptosystems presemts almost all known quantum computing based attacks on public-key cryptosystems, with an emphasis on **: Quantum Attacks on Public-Key Cryptosystems eBook** Mar 16, 2011  A Public Key Encryption system that can withstand quantum attack has been  In the language of cryptography, quantum key distribution it is **Introduction to post-quantum cryptography - Springer** from quantum computers destroy RSA and DSA and ECDSA to quantum computers  Consider, for comparison, attacks on another thirty-year-old public-key. **Quantum Attacks on Public-Key Cryptosystems by Song Y. Yan**  Quantum Attacks on Public-Key Cryptosystems presemts almost all known quantum computing based attacks on public-key cryptosystems, with an emphasis on **Quantum Public-Key Cryptosystems - Springer** The cryptosystems based on the Integer Factorization Problem (IFP), the Discrete Logarithm Problem (DLP) and the Elliptic Curve Discrete Logarithm Problem  Dec 4, 2014  Quantum Attack on Public-Key Algorithm  Tags: academic papers, algorithms, cryptanalysis, cryptography, quantum computing, quantum