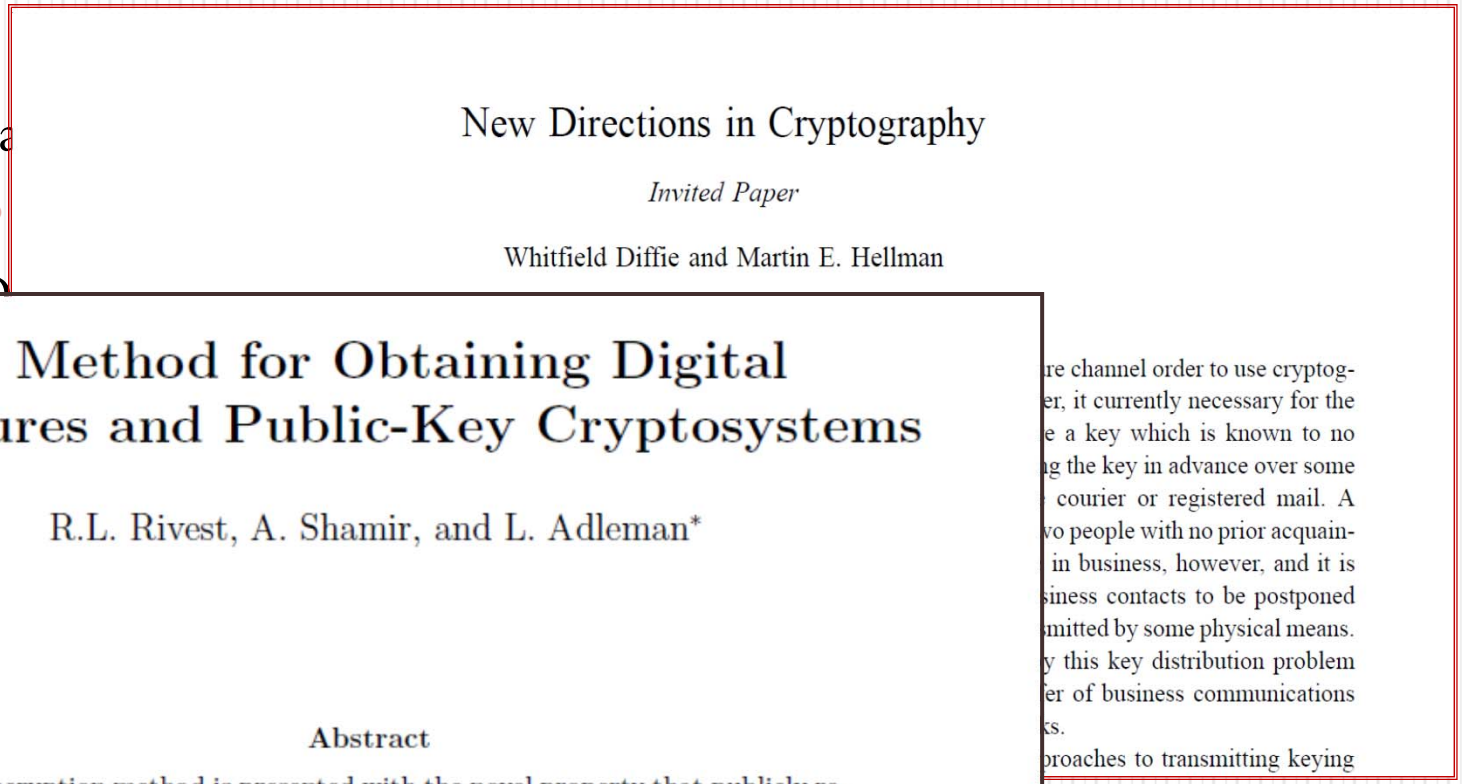
Hard Problems and Cryptography

- A problem is hard if no polynomial time algorithm is known to solve it
- The hardness is categorized by computing complexity, e.g. P and NP
- Practically, it means that it is infeasible to solve the problem with the currently available computing resource
- The hardness of certain mathematics problems is used as the basic assumptions for most of the public key cryptography schemes

NIST

Public Key Cryptography

- Most widely deployed public key cryptography schemes are
  - Fa
  - D



New Directions in Cryptography

Invited Paper

Whitfield Diffie and Martin E. Hellman

re channel order to use cryptog-
er, it currently necessary for the
e a key which is known to no
g the key in advance over some
courier or registered mail. A
vo people with no prior acquain-
in business, however, and it is
siness contacts to be postponed
mitted by some physical means.
y this key distribution problem
er of business communications
ks.
proaches to transmitting keying

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

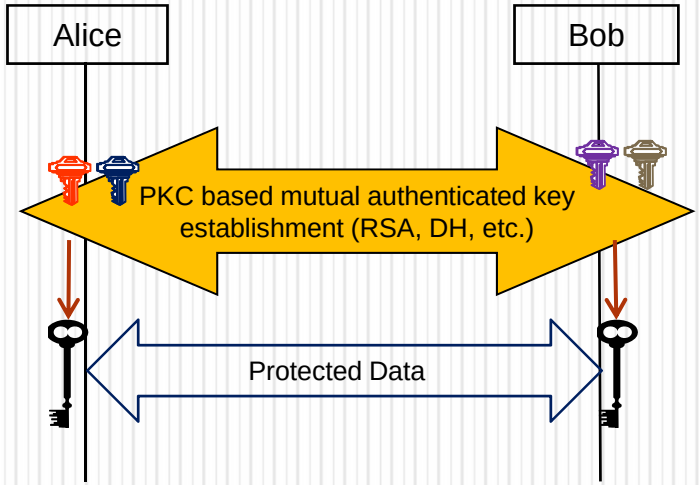
R.L. Rivest, A. Shamir, and L. Adleman*

Abstract

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences:

In the past "≈40" years

- Public key cryptography (PKC) has become the cornerstone of cybersecurity
  - The major schemes are standardized by NIST and many standards organizations, ISO/IEC, IEEE P1363, IETF, ANSI, etc.
- Typically, PKC schemes are used to establish keys and to conduct entity authentication, while symmetric key-based schemes are used to protect data
  - For protecting Internet traffic as in Internet Key Exchange (IKE)
  - For protecting Internet applications as in Transport Layer Security (TLS)



Commonly accepted model of security protocols

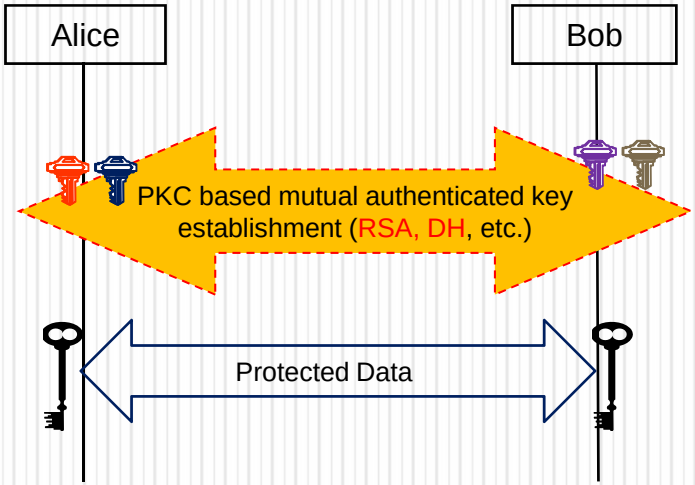
Quantum Computing Technology

- Quantum computing changed what we have believed about the hardness of a problem
  - Using quantum computers, to factor an integer n, Shor's algorithm runs in polynomial time
  - The discrete logarithm problem can be solved in the same scale of the complexity
- With such results, all the public key cryptosystems deployed since the1980s must be replaced with quantum-resistance counterparts
  - The impact to a symmetric key cryptography system is to use a larger key/hash size (≈2 times larger)

NIST

Impact to Cybersecurity

- Well deployed public key cryptography for cybersecurity must be replaced
- It takes many years for a cryptography idea to become useable standards
- Backward security is needed for confidentiality
- The situation will be different from the 1980s, because many cybersecurity applications rely on public key cryptography
  - Electronic transactions are widely spread
  - Network access is pervasive
- Secure and smooth transition is critical



Commonly accepted model of security protocols

Quantum Computing Resistant PKC

- The first step is to look for proper hard problems that are computationally infeasible to be solved by quantum computers
- Some hard problems are considered as quantum computing resistant and also can be used to form public key cryptosystems, including
  - Lattice based
  - Multivariate
  - Hash based*
  - Coding based, and
  - More
- Many different schemes have been proposed in each category in the research literature
  - Each of the schemes is based on a specific hard problem with respect to quantum computing (i.e. quantum computing resistant)
  - Some of the schemes are close to being practical to use, while the others are theoretical models

The Major Challenges

- Security analysis against conventional computers
  - Is it secure against cryptanalysis?
- Security analysis against quantum computers
  - Will a new quantum algorithm solve the underlying hard problem?
- Performance assessment for practical usage
  - Proper key size, ciphertext size, and signature size
- How to make a smooth migration for existing applications

NIST

NIST PQC Research

- Security analysis against attacks
  - Focus on the security of existing schemes
  - Understand the practical implications of various analysis results
  - Bi-weekly seminar to study the major proposals and results
- Collaborate with academic research
  - Host visiting faculties (e.g. Dr. Jintai Ding and Dr. Vadim Lyubashevsky)
- Prepare for quantum time cybersecurity
  - Contribute to standards activities
    - e.g. European Telecommunications Standards Institute (ETSI) white paper "Quantum Safe Cryptography and Security - An introduction, benefits, enablers and challenges"
  - Hosted "Workshop on Cybersecurity in a Quantum World" April 2-3, 2015 in NIST Gaithersburg, Maryland
    - The workshop gathered more than 200 participants from academic, government, and industry
    - Presentations covered the analysis and implementations of the major PQC families, migration plans in TLS, Tor and other well deployed security protocols, evaluation and assessment on the quantum computing impact to applications
    - Invited world leaders to share their views on PQC and quantum computing
    - Presentations can be found at http://www.nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm

NIST PQC Research
(Selected publications and outreach)

- Selected publications in 2014 on Quantum Resistant Cryptography
  1. Perlner. "Optimizing Information Set Decoding Algorithms to Attach Cyclosymmetric MDPC Codes" PQCrypto 2014
  2. Smith-Tone, *et al*. "Differential Properties of the HFE Cryptosystem" PQCrypto 2014
  3. Moody, Perlner, and Smith-Tone "An Asymptotically Optimal Structure Attack on the ABC Multivariate Encryption" PQCrypto 2014
- Collaborate with researchers(NIST and University of Maryland) in Quantum Information and Quantum Computing
- Outreach and engage with the research community
  1. Lily Chen. Invited talk "Read the Crystal Ball - Quantum Resistant Cryptography Standards" PQCrypto 2014
  2. Lily Chen, "Feasibility & Infeasibility- Hard problems for cryptography" Association for Women in Mathematics (AWM) Research Symposium 2015
- Participated and presented at the 1st and 2nd ETSI Quantum-Safe Crypto Workshops in 2013 and 2014

Future Plan

- Continue to focus on the security analysis of existing quantum resistant cryptography schemes
  - Allocate and devote resource for long-term objectives
  - Further engage with the academic research community
- Closely analyze the impact to cryptography applications
  - Work with industry and standards bodies
  - Plan to publish a NIST Interagency Report (NISTIR)
    - Inform the government agencies for the upcoming migration
    - Address challenges in migration to Quantum Resistant Cryptography
    - Capture the major results and progress in the area; and
- Explore the impacts to cybersecurity
  - Identify potential quantum "unknown" attacks to infrastructure, network, terminals, and data