An Overview of PQC Workshops/Projects and Standardization Concerns in China

Hong Xiang, Tao Xiang
Chongqing University
Zheng-feng Zhang
Institute of Software Chinese Academy of Sciences
Zheng-fu Han
University of Science and Technology of China

OUTLINE

1. National Strategies
2. Projects/Workshops
3. Impact to Standards
4. Markets for PQC

National Strategies

中华人民共和国中央人民政府
The Central People's Government of the People's Republic of China
www.GOV.cn

Feb. 2006, Chinese government announced "the Outline of the National Medium and Long Term Program for Science and Technology Development (2006-2020)"

http://www.gov.cn/jrzg/2006-02/09/content_183787.htm

Key Domain Primary Direction

"Focus on developing the security technologies for national infrastructure networks and key information systems, …, including cyber trustworthy systems and new encryption schemes"

National Strategies

中华人民共和国中央人民政府
The Central People's Government of the People's Republic of China
www.GOV.cn

Fundamental Research

"Basic mathematical problems, and emergent issues raised from new frontier interdisciplines such as … quantum-related problems, …"

Crucial Science Project

"Quantum information, …, will deeply impact our daily life in the coming 20-30 years and the rules it plays will be beyond our imaginations…"

Program Mgt. of PQC-related

中华人民共和国科学技术部
Ministry of Science and Technology of the People´s Republic of China

→ "973" Project

国家自然科学基金委员会
National Natural Science Foundation of China

→ Natural Science Fund

国家商用密码管理办公室
www.oscca.gov.cn

→ Cryptography Open Fund

"973"Project Funding

中华人民共和国科学技术部
Ministry of Science and Technology of the People's Republic of China

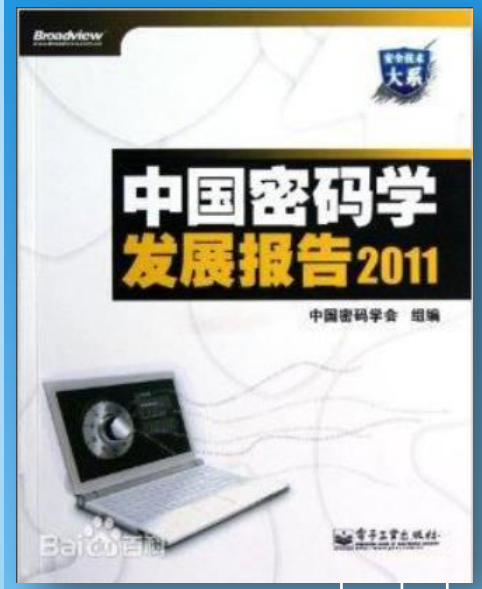
- "973" Project: Studies on key mathematical problems raised from the modern cryptography and their applications (2013-2017)
- "973" Project: over 10 quantum-related research projects were approved in the last three years
- "973" Project: these projects cover R&D on quantum devices, quantum control, quantum circuit…

NSFC Funding

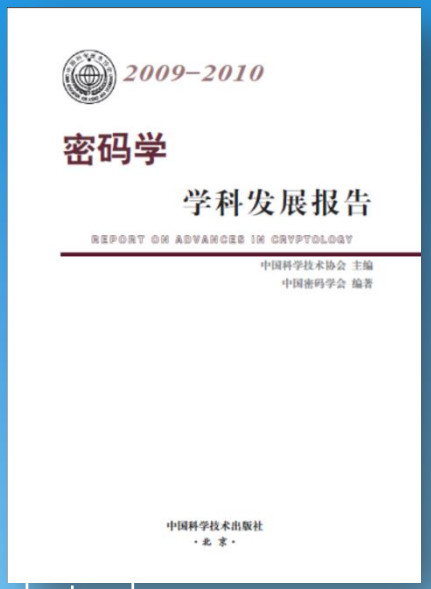
国家自然科学基金委员会 National Natural Science Foundation of China

- NSFC Key Program: "Studies on Theories and Technologies for Lattice-based Quantum Resistant Public Encryption Scheme" (2016-2019)
- NSFC Key Program: "Studies on theories and key technologies of Public Encryption Scheme against Quantum Computer" (2014-2018)
- NSFC General Program: All PQC families (Lattice-based, MPKC, Secure Hash, Code-based, …)

PQC Workshops in China since 2010



Workshops subject to PQC , conducted by many organizations, such as Chinese Association for Cryptography Research (CACR), Chinese Association for Science and Technology(CAST) , etc., have been held since 2010. Some of interested topics are selected in the publications "Chinese Cryptography Report" (2011, 2012)",and "Report on Advanced in Cryptography" (2011,2016)



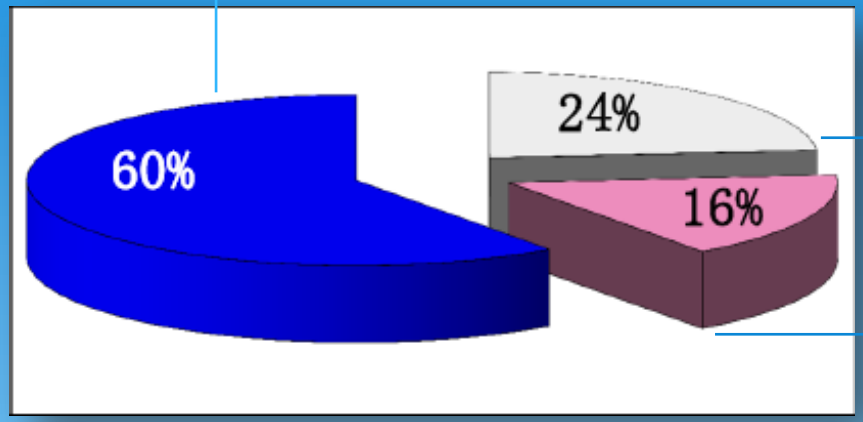
- Security of quantum computing-based encryption schemes
- Advanced in PKC
- Advanced in FHE

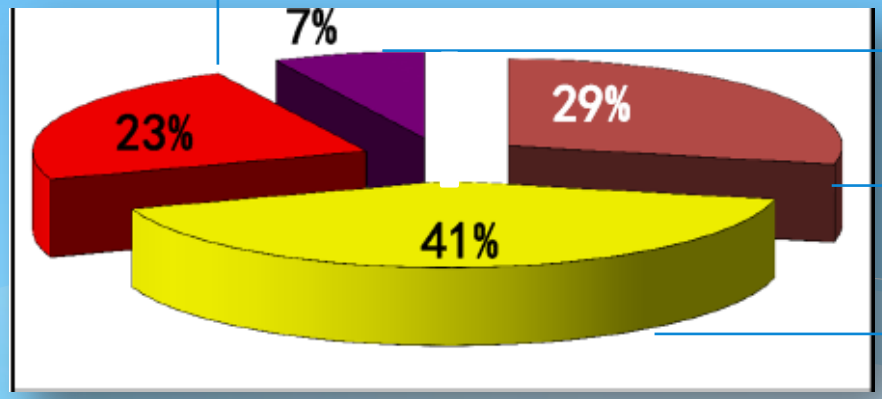
Distribution of PQC Workload

- Over 20 institutes, more than 500 researchers working on PQC
- Over 10 key projects are processing

Distribution of Existing Std.

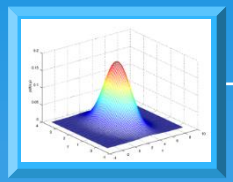
- Over 100 National standards have been published
- Over 150 National standards waiting for reviewing





- Self-made National Standards
- Referring to International Standards
- Adopting International Standards
- Technological Standards
- others
- Management Standards
- Testing & Assessing Standards

Impact to Info. Security standards



MPC

Secure Harsh

Lattice based

Code-based

- PQC algorithms Std.
- PQC-based Tech. Std.
- PQC-based App. Std.
- PQC-based Mgt. Std.
- …

WG 1

WG 2

WG 3

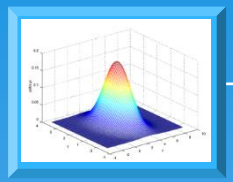
WG 4

WG 5

WG 6

WG 7

Impact to other standards



MPC

Secure Harsh

Lattice based

Code-based

- PQC algorithms Std.
- PQC-based Tech. Std.
- PQC-based App. Std.
- PQC-based Mgt. Std.
- …

Mob. Internet

Cloud Computing

Internet Of Thing

Smart Manufacturing

Potential PQC Markets in China

The global e-commercial giant Alibaba creates a new online-shopping festival “Double 11” in 2014

2014.11.11 Traded over 50 billions RMB

2015.11.11 Traded over 90 billions RMB giant

2016.11.11 ?

Potential PQC Markets in China

Tencent Corp. creates a popular game named "Red cyber wallet donation" in the end of 2014

"Red-Cyber-Wallet"

2015 Spring Festival: 5-million people involved

2016 Spring Festival: 500-million people involved, 32 billions Lucky-Cyber-Wallets traded

Potential PQC Markets in China

Circulation of digital certificate has growth fast in the last five years in China

SUMMERIZATION

National Strategies

- Key Domain & Primary Direction
- Fundamental Research
- Crucial Science Project

Project & Workshops

- “973” Project
- NSFC Key Program
- Open Fund for Cryptography

Impact to Existed Std.

- Cover all spectrum of existed std.
- From 5G, Cloud Computing, IOT, to CPS…

Potential Markets

- Fast growth of applications related next generation of PKC
- Huge amount of cyber- population

Q & A