Good morning, everyone! My name is Han Yongxin and I'm from UCLA. My presentation topic is "Quantum2FA: Efficient Quantum-Resistant Two-Factor Authentication Scheme for Mobile Devices."

The first part is introduction.

Smart-card based password authentication has been the most widely used two-factor authentication (2FA) mechanism for security. Most of them are built on the difficulty of conventional hard problems which are no longer hard in the quantum era. So we proposed Quantum2FA.

Now I will introduce the evaluation metric and the underlying security model.

Generally, a practical scheme in the quantum era should meet the following two important criteria: Quantum security and efficiency.

We use a practical evaluation framework for 2FA under conventional computers, which is composed of 12 evaluation criteria.

We also consider the capabilities of the adversary.

As for attacks, we consider quantum attacks and extend the traditional attacks to the quantum setting.

In all, our security goals and corresponding attacks are comprehensive.

Now I will summarize the contributions.

We propose Quantum2FA, a Ring-LWE-based two-factor authentication scheme. It is quantum-resistant and efficient on the smart card. We divide the proposed scheme into four parts: registration phase, log-in phase, verification phase, and password-changing phase. The security of our scheme is on the basis of the Ring-LWE problem.

Formal security analysis demonstrates that the proposed scheme Quantum2FA is secure against attacks from both classical and quantum computers.

We implement Quantum2FA on a micro controller. Comparison results show that Quantum2FA is not only more secure but also offers better computation efficiency than the state-of-the-art traditional 2FA schemes.

The last part is the conclusion.

We have proposed a secure and efficient smart-card-based password authentication scheme for the mobile devices. As far as we know, Quantum2FA is the first 2FA scheme that is secure against attacks from both quantum and conventional computers.

We believe that achieving practical two-factor authentication is of broad interest, and our work constitutes an important step forward in this direction and will spark interest for new quantum-resistant 2FA research.

Q&A

RLWE provides a cryptographic scheme against quantum computing attacks. Traditional public-key cryptography algorithms, such as RSA and DSA, may become insecure against quantum computers, while RLWE structure is stronger under quantum attacks.

RLWE is considered to be secure even under classical attacks, and it provides a fairly high level of security even in the absence of a quantum computer.

That's the reason why we chose RLWE for the algorithm.