Title

Secure Mobile Applications based on NTRU

Description

Modern mobile devices have an urgent need for a new-generation public-key cryptographic system. This system should provide sufficient security for mobile devices without degrading performance due to their limited resources. NTRU is a decent model for this. We validate it through experimental studies and apply NTRU to protect a peer-to-peer communication app.

Abstract

Nowadays, people use mobile devices for a variety of applications, such as e-commerce, online banking, and private messaging. All require high levels of security. Public-key (or asymmetric-key) cryptographic algorithms are more secure than symmetric-key algorithms, so they are ideal for these mobile applications. However, traditional public-key cryptographic algorithms such as RSA and Elliptic Curve Cryptosystems (ECC) are too heavy-load for mobile devices as they run very slowly there. Therefore, modern mobile devices have an urgent need for a new-generation public-key cryptographic system. This new system should provide sufficient security protections for mobile devices applications without degrading their performance due to their limited resources available.

Based on our research, we found that NTRU is a decent model for this new public-key system. NTRU uses a cipher mechanism based on polynomials. Its security depends on the Shortest Vector Problem (SVP) within a block, which has many advantages over other cipher mechanisms such as discrete logarithms and integer factorization. Security-wise, NTRU algorithm even has the ability to resist quantum attacks, while RSA and ECC have no such capability.

We validated the results found in Al-Bakri et. al. ["Securing peer-to-peer mobile communications using public key cryptography: New security strategy", International Journal of Physical Sciences, Vol. 6, no. 4 (2011): 930-938] that NTRU is faster than ECC and RSA, except in our study we found it to be true on modern Android devices, rather than those relatively obsolete and limited devices studied in the referenced paper. In fact, as key sizes increase, this difference grows when comparing equivalent levels of security, meaning that the benefits of NTRU will be even greater in the future. Our conclusion is based on our experimental studies or performance evaluations.

We also apply NTRU to protect a peer-to-peer communication mobile application on top of an Android device. We demonstrate that NTRU can protect the confidentiality, integrity, and authentication of a peer-to-peer messaging app effectively and efficiently. This android mobile app is similar to other messaging apps, such as WhatsApp, but it uses NTRU as the underlying cryptographic algorithm.

Keywords

Mobile security, NTRU, Public-key cryptography, Performance, Peer-to-peer