



Technology Opportunity, Ref. No. 13/043

Method and apparatus for public-key cryptography based on error correcting codes

A new technique for implementing public-key cryptography based on error-correcting codes is presented. It allows to increase the public key security of the classical McEliece cryptosystem and to use widespread classes of codes, as Reed-Solomon codes, in the place of classical Goppa codes. This gives significant advantages in terms of security and key size.

Keywords Code-based cryptography, Public-key cryptography, McEliece cryptosystem
Secure communications.

Inventors Marco Baldi, Marco Bianchi and Franco Chiaraluce, Università Politecnica delle Marche; Davide Schipani and Joachim Rosenthal, University of Zurich.

Reference in preparation

Background The importance of code-based cryptosystems is continuously increasing. Due to their extremely low complexity and because they are among the few techniques that will resist attacks exploiting quantum computers, they are expected to replace classical cryptosystems (like RSA, DSA and ECDSA) in the foreseeable future. A promising candidate for code-based cryptosystems is the classical McEliece cryptosystem that is able to resist attacks based on quantum computers and allows easy encryption and decryption procedures. However, the key size needed for achieving a satisfactory level of security is quite large, and this is one of the main reasons that have limited its use in practical applications. The classical McEliece cryptosystem is based on Goppa codes, while the use of other families of codes, as cyclic codes and Reed-Solomon codes, could help to reduce the key size for a fixed security level. However, previous attempts of replacing Goppa codes with such alternatives have compromised the system security.

Invention The invention consists in a variation of the McEliece cryptosystem which increases its public key security, allowing the use of families of codes alternative to classical Goppa codes. By using the invented variant of the McEliece cryptosystem, the same security level can be achieved with significantly shorter public keys. The adoption of families of codes alternative to Goppa codes also allows to exploit optimized software and hardware, already developed for widespread coding schemes.

Fields of Use Cryptography, secure communications, secure network protocols, e-commerce, home banking.

Patent Status Patent application filed

Contact *Unitetra, Technology Transfer of University Zurich, Dr. W. Henggeler, Möhrlistrasse 23, CH-8006 Zürich, +41 44 634 44 01, mail@unitetra.ch*