Mathematics of Post-Quantum Cryptography

Algebraic Cryptography Center at Stevens Institute of Technology

---

Jintai Ding

(University of Cincinnati)

Random Quadratics over Odd-Characteristic Medium-Sized Fields

Abstract:

We present a new MPKC (multivariate public key cryptosystem) whose hidden central map is a small number of random quadratics over a medium-sized extension field of a \emph{small odd prime field}, with an extra ``embedding" modifier (essentially fixing some variables to zero). The combination of these known ideas makes for better efficiency and scalability than all the other multivariate encryption schemes still standing.

Switching to odd characteristics affects how an attacker can make use of field equations. This makes an especially large difference when attacking HFE and related MPKCs using Groebner Basis algorithms. Extensive empirical tests (using the best commercially available F4 implementation in MAGMA) suggests that our new construction is indeed secure against algebraic attacks using Groebner basis algorithms. The ``embedding" serves both to narrow down choices of pre-images and to guard against a possible Kipnis-Shamir type (rank) attack. We may hence reasonably argue that for practical sizes, prior attacks take exponential time.

We demonstrate that our construction is in fact efficient by implementing practical-sized examples of our new MPKC with 3 variables (``3RQ") over \GF{31}. To be precise, 3RQ is $>10\times$ as fast publicly available optimized RSA-1024 code in both C and optimized assembly.

Algebraic Cryptography Center

STEVENS Institute of Technology