Cryptology ePrint Archive: Report 2011/353

Hidden Pair of Bijection Signature Scheme

Masahito Gotaishi and Shigeo Tsujii

Abstract: A new signature system of multivariate public key cryptosys- tem is proposed. The new system, Hidden Pair of Bijection (HPB), is the advanced version of the Complementary STS system. This system real- ized both high security and quick signing. Experiments showed that the cryptanalysis of HPB by Gr? obner bases has no less complexity than the random polynomial systems. It is secure against other way of cryptanal- ysis eﬀective for Complementary STS. On the other hand, since it is based on bijections, signatures exist for any message, unlike other cryptosystems based on non-bijections such as HFE or Unbalanced Oil and Vinegar.

Category / Keywords: public-key cryptography / Multivariate Public Key Cryptosystem, Digital Signature, Bijection, Rainbow

Date: received 1 Jul 2011

Contact author: gotaishi at tamacc chuo-u ac jp