A Brief Retrospective Look at the Cayley-Purser Public-key Cryptosystem, 19 Years Later

Douglas Stinson, University of Waterloo

Sarah Flannery won the *EU Young Scientist of the Year Award* for 1999 for her proposal of a public-key cryptosystem based on 2 by 2 matrices with entries from Z_n, where n is the product of two distinct primes p and q. The cryptosystem she proposed was named the *Cayley-Purser algorithm*. Unfortunately, the cryptosystem turned out not to be secure, but there are some interesting mathematical aspects of this cryptosystem that I will discuss in my talk, including attacks on the system.

Keywords: public-key cryptography