Connections between graph theory and cryptography

Natalia Tokareva
Sobolev Institute of Mathematics, Novosibirsk, Russia
Novosibirsk State University, Novosibirsk, Russia
tokareva@math.nsc.ru

It is not a secret that modern cryptography is highly connected with discrete mathematics. Many well-known cryptographic algorithms such as RSA, ElGamal, elliptic curve methods, etc. are directly based on mathematical results. In fact there is a lot of other cryptographic methods (may be not so famous but no less important) that are constructed by using optimal combinatorial and algebraic structures. Among them are symmetric ciphers AES, CAST, Grain, several stream ciphers, hash functions, statistical methods of cryptanalysis, cryptographic protocols, etc.

In this talk we discuss connections between cryptographic methods and graph theory. We consider such topics as:

- sparse graphs and mobile security systems;
- hash functions and random graphs;
- cycles of large period and linear recurrent sequences;
- cryptographic Boolean functions and strongly regular graphs;
- metrical properties of Cayley graphs and bent functions;
- automorphisms of colored graphs and S-boxes;
- zero-knowledge proof of graph isomorphism.