

Gráfelméleti feladatokon alapuló kriptorendszerek

Márton Gyöngyvér

Sapientia Erdélyi Magyar Tudományegyetem

Marosvásárhelyi Kar, Matematika és Informatika Tanszék

email: mgyongyi@ms.sapientia.ro

Miután az 1978-ban publikált Merkle-Hellman hátizsák feladaton alapuló kriptorendszer feltörhetőségét Adi Shamir megmutatta 1984-ben, a kombinatorikus algebrán alapuló kriptorendszerek kutatása viszonylag visszaesett. A kilencvenes években aztán ismét elkezdtek foglalkozni ezzel az elmélettel, például egy ilyen irányú törekvés a Koblitz és Fellows által publikált Polly Cracker kriptorendszer volt, mely általános szerkesztési sémát adott többváltozós polinomok alkalmazásával, NP-teljes feladatok kriptorendszerekben való alkalmazására. A három színnel színeheztő gráfok, általános gráfokban való perfekt kódok keresésének a problémáin keresztül konkrétan is bemutatták a nyilvános kulcsú kriptorendszerek szerkesztési sémáit. Az utóbbi években azonban Dennis Hofheinz kutatásainak köszönhetően a Polly Cracker kriptorendszer ellen több támadási algoritmus is napvilágot látott. További kutatásokat ebben a témában a budapesti műszaki egyetem kutatóinak publikációja jelenti, melyben gráf izomorfizmusok alkalmazásával digitális aláírási sémát mutatnak be. Jelen előadásban ezen eredmények felvázolásáról lesz elsősorban szó.

Hivatkozások

- [1] N. Koblitz, *Algebraic Aspects of Cryptography*, Springer, 1999.
- [2] M.R. Fellows, N. Koblitz, Combinatorically based cryptosystem for children (and adults). *Congressus Numerantium*, **99**, 2000.
- [3] D. Hofheinz, *Public key encryption from a mathematical perspective*, International School on Mathematical Cryptology, Barcelona, 2008.
- [4] L. Szöllősi, T. Marosits, G. Fehér, and A. Recski, Fast Digital Signature Algorithm Based on Subgraph Isomorphism, *Lecture Notes in Computer Science, Cryptology and Network Security*, CANS2007.