Kryptologie

10. April 2014

1. Vortrag: Kryptographische Protokolle

1. Überblick: kryptographische Protokolle
   (a) Kryptosysteme (symmetrisch, asymmetrisch)
   (b) Authentifikationsprotokolle
   (c) Zero-Knowledge-Protokolle
   (d) Signatur-Protokolle
   (e) Schlüsselaustauschprotokolle
   (f) Secret-Sharing-Protokolle
2. Secret-Sharing-Protokoll von Adi Shamir

Literatur: [Sha79], [Buc10], [BNS10], [Mol12], [BFKR15, Abschnitt I. 4. Seite 53 ff.].

2. Vortrag: CFRZ-Secret-Sharing-Protokoll

1. CFRZ-Secret-Sharing-Protokoll erklären und beweisen
2. Vergleich mit dem Secret-Sharing-Protokoll von Shamir
3. Erweiterung zu einem symmetrischen Kryptosystem

Literatur: [Sha79], [FMR13], [Mol12].

3. Vortrag: Gruppentheoretisches Diffie-Hellman Protokoll

1. Diffie-Hellmann Schlüsselaustauschprotokoll
   (a) zahlentheoretisch (diskretes Logarithmus Problem)
   (b) gruppentheoretisch (Ko-Lee et al. Protokoll)
      i. Konjugationssuchproblem
      ii. Plattformgruppe: Zopfgruppen

Literatur: [DH76], [KLC+00], [MSU08], [BFKR15, Abschnitt III. 11. Seite 279 ff.].

Literatur

[BFKR15] G. Baumslag, B. Fine, M. Kreuzer, and G. Rosenberger. *A Course in Mathematical Cryptography.* 2014/15.

[BNS10] A. Beutelspacher, H. B. Neumann, and T. Schwarzpaul. *Kryptografie in Theorie und Praxis.* Vieweg+Teubner, second edition, 2010.

[Buc10] J. Buchmann. *Einführung in die Kryptographie.* Springer, 2010.

[DH76] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT 22:644 – 654, 1976.

[FMR13] B. Fine, A. Moldenhauer, and G. Rosenberger. A secret sharing scheme based on the closest vector theorem and a modification to a private key cryptosystem. *Groups Complexity Cryptology 5*, pages 223 – 238, 2013.

[KLC+00] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, and C. Park. New public-key cryptosystem using braid groups. *CRYPTO 2000, Springer Lecture Notes in Computer Science 1880*, pages 166 – 184, 2000.

[Mol12] A. Moldenhauer. Untersuchung der Secret-Sharing-Protokolle von Shamir und Panagopoulos, sowie die Entwicklung eines neuen Secret-Sharing-Protokolls. Master's thesis, 2012.

[MSU08] A. Myasnikov, V. Shpilrain, and A. Ushakov. *Group-based Cryptography.* Advanced Courses in Mathematics - CRM Barcelona. Birkhäuser Basel, 2008.

[Sha79] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.