Chair of Communications Engineering
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Forschungspraxis

On the Equivalence of Identification and Authentication

It would be shown that under suitable formulations (preserving all salient features) the two problem of **Identification** (Ahlswede and Dueck, 1989) and Authentication (Simmons, G. J. 1984) are in essence very close to each other. This equivalency was conjectured first by **M. S. Pinsker**. In this research internship the student is expected to address this conjecture. Both problems must be studied separately and then the similar essence of them should be drawn out. In particular the identification codes and authentication codes along with theire relation will be investigated.

Prerequisites

1. Background in Information Theory and Channel Coding
2. Familiarity with fundamentals of Identification Theory

References:

1. Simmons, G. J. 1984, “Message authentication: a game on hypergraphs,” Congressus Numer. 45:161-192.
2. Simmons, G. J. 1982, “A game theory model of digital message authentication,” Congressus Numer., 34, 413-424
3. Simmons, G. J. 1985, “Authentication theory/coding theory,” in: Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science, vol. 196, Springer-Verlag, Berlin, pp. 411-432.
4. E. Gilbert, F. J. MacWilliams and N.J. A. Sloane, 1974, “Codes which detect deception,” Bell System Tech. J., 53, 405-424.
5. R. Ahlswede and G. Dueck, “Identification via channels,” in IEEE Trans. on Inf. Theory, vol. 35, no. 1, pp. 15-29, Jan. 1989, doi: 10.1109/18.42172.
6. L. A. Bassalygo, M. V. Burnashev, “Authentication, Identification, and Pairwise Separated Measures”, Problems Inform. Transmission, 32:1 (1996), 33–39

Advisors

Mohammad Salariseddigh