AIT Based Cryptography

Cristian S. Calude

December 4, 2018

Security for cryptographic systems is based on two main approaches: computational security and information-theoretic security.

In the first approach on tries to design a system in such a way that an attacker can not feasibly break it within a reasonable amount of time. These are the most common and used cryptosystems. The weakness is that all proofs of security are based on unproven complexity assumptions.

Security in the second approach is achieved by proving that an attacker can not gain any information about a certain secret even if he has unlimited power. These proofs are based on, but not limit to, time-bounded Kolmogorov complexity.

The project is consists in studying the current solutions and developing new ones base on different complexities, e.g. [**?**, **?**, **?**].

References

[1] L. Antunes, S. Laplante, A. Pinto, L. Salvador. Cryptographic security of individual instances, in Y. Desmedt (Ed.) *Information Theoretic Security*, LNCS 4883, Springer, 2010, 195–210.

[2] C. S. Calude. *Information and Randomness: An Algorithmic Perspective*, 2nd Edition, Revised and Extended, Springer-Verlag, Berlin, 2002.

[3] C. S. Calude, K. Salomaa, T. K. Roblot. Finite state complexity, *Theoretical Computer Science* 412 (2011), 5668–5677.

[4] C. S. Calude, K. Salomaa, T. K. Roblot. State-size hierarchy for FS-complexity, *International Journal of Foundations of Computer Science* 23, 1 (2012) 37–50.

[5] C.S. Calude, L. Staiger, F. Stephan. Finite state incompressible infinite sequences, in T. V. Gopal, M. Agrawal, A. Li, B. S. Cooper (eds).

Proceedings of the 11th Annual Conference on Theory and Applications of Models of Computation, Lecture Notes Comput. Sci. 8402, Springer, 2014, 50–66.

[6] A. Muchnik, Kolmogorov complexity and cryptography, *CoRR* abs/1106.5433, 2011.