PhD Resarch Plan

Cryptographic Protocol Security Analysis Based on Algorithmic Information Theory

Summary

The goal of this work is the application of Algorithmic Information Theory (AIT) to the analysis of cryptographic primitives, namely: one-way functions, pseudo-random generators, and extractors. Based on this study and on recent work on the usage of AIT as a tool in the analysis of symmetric protocols [PSMA], the individual security of asymmetric cipher systems will be finally analyzed.

Introduction

In Algorithmic Information Theory (AIT), not to be confused with Information Theory, the length of the smallest algorithm that produces a given string x, also called the Kolmogorov complexity of x, is used as a measure of the information contained in x. Only very recently has AIT been used to prove the security of *individual* instances of cryptographic protocols.

The Kolmogorov complexity is a rigorous measure of the amount of information that an individual object contains; it is the length of the shortest description of the object, see [LV97]. For instance, random strings are those that not be compressed further and, as such contain maximum information.

A function f is *one-way* if it satisfies the following conditions

- The description of f is known and $f(x)$ is computable in polynomial time.
- Given y in the co-domain of f, it computationally unfeasible to find any x such that $f(x) = y$, i.e., a polynomial algorithm will succeed only with negligible probability.

Using AIT to analyze one-way functions, it is easy to see that

1. $K(x) = K(y)$ [1]
2. $K^t(y) \leq K^t(f) + K^t(x)$ where t is a polynomial in $|x|$.

It is not known whether such functions exist, but if they do, P≠NP. Thus the proof of the existence of one-way functions is apparently beyond the current analytical powers of Mathematics and Computer Science.

It is however interesting to study under what assumptions about f we have $K^t(x) = K^t(x|y)$. It is conjectured that the functions associated with the following problems are one-way

1. Quadratic residue problem.
2. Discrete logarithm problem: $f(p, g, x) = \langle p, g, g^x (\operatorname{mod} p)\rangle$, where g is a generator of Z_p^*, for some prime p.
3. RSA cypher $f(p, q, e, y) = \langle pq, e, y^e (\operatorname{mod} pq)\rangle$, where $y \in Z_{(pq)^*}$, $e \in Z_{(pq)}$ is prime relatively with $(p-1)(q-1)$, with p and q primes.

[1] $K(x) \leq K(f) + K(y) \leq 2 \times K(f) + K(x)$. Mustn't we also impose that f is injective? Otherwise we may have $K(x > K(y)$.

Pseudo-random generators are deterministic algorithms that output finite strings from an input which is called the "initial seed"; the goal is to use a short string, which is truly random, and expand it, creating a longer string which is polynomially indistinguishable from a true random string. It is known that if "hard" functions exist, pseudo-random generators also exist. Important goals of the research in this area are

– Prove the unconditional existence of pseudo-random generators.

– Reduce the length of the initial seed.

– Obtain longer output sequences.

– Get an output string which is harder to distinguish from truly random strings.

Let $g : \Sigma^{\log n} \to \Sigma^n$ be a pseudo-random function generator and let $g(y) = x$. The Kolmogorov complexity of x and y satisfy

1. $K(y) \leq \log n$

2. $K(x) \leq K(y) + K(g) \leq \log n + K(g)$

If x is indistinguishable from a random string, one has $K(g) \geq n - \log n - \delta$, where δ represents the randomness deficiency of x. One of the goals of this work is to use Algorithmic Complexity Theory to characterize the properties of those functions g.

An *extractor* is an algorithm that outputs a pseudo-random string from an input which has some minimum entropy. Another goal of this work is to characterize the properties of he extractors, using the Kolmogorov complexity as an analysis tool. In general terms we want to show that: if A is the set of strings with some entropy, and $x \in \Sigma^n$ is the output of the extractor, then $K(x|A) = n$.

Two sequences x and y are distinguishable by some program p which always outputs 0 or 1, if $p(x) \neq p(y)$; two sequences x and y are k-indistinguishable if they are not distinguished by any program p with length k or less.

Goals

The main goal of this work is to characterize a basic set of cryptographic primitives, using the Algorithmic Information Theory as the fundamental tool of research. Those cryptographic primitives should include

– One-way functions.

- Pseudo-random generators.

- Extractors.

- Indistinguishability.

- Basic communication protocols.

Based on that characterization, it should be possible to analyze the protocols obtainable by composition of those primitives, or whose security depends on its existence.

The deep study of those cryptographic primitives should also allow the student to define and build new cryptographic protocols.

This work also includes the following tasks:

- Study of the following areas: algorithmic complexity (and its variants) and of cryptographic primitives.

- Use algorithmic complexity and its variants to characterize the properties and the security of those cryptographic primitives.

- Analyze the known cryptographic protocols which can be obtained by composition of primitives.

- Create new, hopefully useful, new protocols, obtained again, by composition.

During this work we expect the publication of 2 papers in international refereed journals and 3 papers in international conferences.

21 de Janeiro de 2008

(Luís Filipe Antunes and Armando B. Matos)

Referências

[AFvM01] L. Antunes, L. Fortnow, and D. van Melkebeek. Computational depth. In *Proceedings of the 16th IEEE Conference on Computational Complexity*, pages 266–273, 2001.

[AFV03] L. Antunes, L. Fortnow, and N. V. Vinodchandran. Using depth to capture average-case complexity. In *14th International Symposium on Fundamentals of Computation Theory*, volume 2751 of *Lecture Notes in Computer Science*, pages 303-310. Springer, Berlin, 2003.

[Ben88] C. H. Bennett. Logical depth and physical complexity. In R. Herken, editor, *The Universal Turing Machine: A Half-Century Survey*, pages 227–257. Oxford University Press, 1988.

[LV97] M. Li and P. Vitányi. *An introduction to Kolmogorov complexity and its applications*. Springer, 2nd edition, 1997.

[GP99] O. Goldreich and E. Petrank. Quantifying Knowledge Complexity. *Computational Complexity*, Vol 8, pages 50-98, 1999.

[GMR89] S. Goldwasser and S. Micali and C. Rackoff The knowledge complexity of interactive proof systems. In *SIAM J. Comput.*, pages 186–208, 1989.

[PSMA] A. Pinto, A. Souto, Armando Matos and L. Antunes. Commitment and Authentication Systems. Proc. International Conference on Information Theoretic Security. Lecture Notes in Computer Science. Springer, 2007. To appear.