Criptografia e Tópicos Relacionados

Programa

12 de julho

09:00-09:30
Joan Daemen: "Efficient block ciphers by the use of error-correcting codes: AES" (Palestra por tele-conferência)

09:30-10:00
Filipe Casal: "Kolmogorov One-way Functions"

10:00-10:30
António Lázaro: "Dos Primórdios da Criptografia em Portugal"

13 de julho

11:00-11:30
Paulo Mateus: "Criptografia quântica"

11:30-12:00
Guilherme Ramos: "Symbolic Probabilistic Analysis of Side-Channel Information"

12:00-12:30
André Souto: "Quantum bit-string oblivious transfer protocols"

Efficient block ciphers by the use of error-correcting codes: AES

(apresentação por teleconferência)

Joan Daemen

Ever since the introduction of the block cipher Data Encryption Standard (DES) in the seventies, block ciphers have been the workhorses of cryptography. A block cipher can be described as a permutation operating on bitstrings of a particular length, parameterized by a secret key. Block ciphers can be used for encryption, authentication and even hashing. For someone that knows the key, the permutation should be easy to compute and for someone who does not know the key, the permutation should be hard to predict.

Traditionally block ciphers were constructed as the iteration of a so-called round function, that consists of a non-linear substitution layer (of so-called S-boxes) and a permutation layer just moving bits around. These are called substitution-permutation networks (SPN). DES can be seen as an exponent of that method.

After the breaking of DES by differential and linear cryptanalyis in the early nineties, we came up with a paradigm to build block ciphers offering better resistance against attacks: the wide trail strategy. Block ciphers designed according to this strategy have an additional element in the round function: the mixing layer. There is an interesting link between these mixing layers and error-correcting codes. In the talk I will discuss this using the Advanced Encryption Standard, the best known wide trail design, as an example.

Kolmogorov One-way Functions

Filipe Casal

Dep. Matemática, Instituto Superior Técnico, U Lisboa, Portugal and
Centro de Matemática, Aplicações Fundamentais e
Investigação Operacional (CMAF-CIO), U Lisboa, Portugal

One-way functions are polynomially computable functions that are hard to invert, meaning that given an image it should not exist an efficient algorithm to compute its pre-image. One-way functions are not known to exist. However their existence has major consequences in mathematics, as well as in everyones daily lives: on one hand their existence implies that $\mathsf{P} \neq \mathsf{NP}$ (see [4]); on the other hand, if they do not exist, then most cryptographic protocols and pseudo-random generators are not secure since their security is based on the hardness of several one-way function candidates.

In Algorithmic Information Theory the central notion is Kolmogorov complexity, $\mathsf{K}(x)$, proposed in [5], [7] and [3], that measures the information contained in a string x by means of the length of its shortest description. The computational hardness is easily encoded in this information measure by considering its time-bounded version, $\mathsf{K}^t(x)$, where the restriction is that the program describing it must run within time $t(|x|)$.

Here, we are interested in the connection between Kolmogorov complexity and the study of one-way functions, a line of work first considered in [8] and [2]. In these works, the authors provided a characterization of strong and weak one-way functions based on the expected value of $\mathsf{K}_f^{t \log t}(x|f(x), r, n)$. Furthermore, based on the difference between $\mathsf{K}_f^t(x|n)$ and $\mathsf{K}_f^t(x|f(x), n)$ they propose an individual approach characterization to one-way functions. We show that the expected value approach cannot be used to fully characterize the class of strong one-way functions. Moreover, we provide a sufficient condition under which Kolmogorov one-way functions (as defined in [2]) are weak one-way functions.

Pursuing the idea of having a full classification of classes of one-way functions using Kolmogorov based measures, we give alternative characterizations of one-way functions based on time-bounded Kolmogorov complexity. We define several classes of functions, namely Kolmogorov strong and weak one-way functions and show that these are equivalent to the usual notions of strong and weak one-way functions.

Joint work with João Rasga, Dep. Matemática, Instituto Superior Técnico, U Lisboa, Portugal and CMAF-CIO, U Lisboa, Portugal and André Souto at Dep. Matemática, Instituto Superior Técnico, U Lisboa, Portugal and SQIG at Instituto de Telecomunicações.

References

1. F. Casal, J. Rasga and A. Souto. Kolmogorov One-way Functions Revisited *Submitted for publication.*
2. L. Antunes, A. Matos, A. Pinto, A. Souto, and A. Teixeira. One-way functions using algorithmic and classical information theories. *Theory of Computing Systems*, 52(1):162–178, 2013.
3. G. Chaitin. On the length of programs for computing finite binary sequences. *Journal of ACM*, 13(4):547–569, 1966.
4. O. Goldreich. *Foundations of Cryptography.* Cambridge University Press, 2001.
5. A. Kolmogorov. Three approaches to the quantitative definition of information. *Problems of information transmission*, 1(1):1–7, 1965.
6. J. Rompel. One-way functions are necessary and sufficient for secure signatures. In *Proceedings of Symp. on Theory of Computing '90*, pages 387–394. ACM, 1990.
7. R. Solomonoff. A formal theory of inductive inference, part I. *Information and Control*, 7(1):1–22, 1964.
8. A. Souto, A. Pinto and A. Teixeira, A. One-way functions using Kolmogorov complexity. In *Proceedings of CiE 2010*, Açores, Portugal, 2010.

Dos Primórdios da Criptografia em Portugal

António Lázaro

A criptografia histórica em Portugal, de João Pedro Ribeiro a Nuno Valdez dos Santos. Um dos mais antigos testemunhos da utilização da linguagem criptográfica nos confins da Europa Ocidental: huma carta em data de 20 de Junho de 1498, escrita a ElRei em cifra. Leitura e algumas considerações em torno desse documento, designadamente em torno das características da linguagem criptográfica utilizada, comparativamente ao que podemos observar, na mesma época, noutros estados europeus. Problemas e projetos no domínio dos estudos da criptografia histórica em Portugal

Criptografia Quântica

Paulo Mateus

É do conhecimento que privacidade perfeitamente segura é impossível utilizando criptografia clássica e quântica. Recentemente surgiram algumas ideias de utilizar resultados relativistas para obter protocolos de segurança perfeitos. Nesta apresentação discutimos estas impossibilidade bem como as perspectivas que se abrem quando se utiliza relatividade para obter privacidade. Note-se que algumas destas ideias estão a ser implementadas em laboratório e podem ser estendidas à utilização massiva usando fibra ótica e relógios sincronizados.

Symbolic Probabilistic Analysis of Side-Channel Information*

Guilherme Ramos and Carlos Caleiro
SQIG-Instituto Telecomunicações
Dep. Mathematics, Instituto Superior Técnico
Universidade de Lisboa, Portugal

Abstract

We propose and explore a framework for the symbolic static analysis of side-channel attacks. Our approach is built on top of a probabilistic model for studying off-line guessing attacks to security protocols, which already took into account algebraic and probabilistic mathematical properties of cryptography. In our extension, we further consider side-channel information concerning observable physical properties of the implementations of cryptographic primitives. Overall, the framework encompasses a probabilistic symbolic attacker, more powerful than conventional Dolev-Yao attackers, and able to capture and quantify attacks that also explore side-channel weaknesses. We illustrate the power of our framework with several meaningful examples, semi-automated by our (in development) prototype analyzer.

*The authors acknowledge the support from PEst-OE/EEI/LA0008/2013 and UID/ EEA/50008/2013. The first author further acknowledge the support from the DP-PMI and Fundação para a Ciência e a Tecnologia (Portugal), namely through scholarship SFRH/BD/52242/2013.

Quantum bit-string oblivious transfer protocols

André Souto

In this talk we will take a tour on oblivious transfer protocols as building blocks for cryptographic applications and present a proposal of an oblivious transfer protocol using quantum phenomena. We also provide proofs of its security.