PhD Thesis Proposal

Distributed Cryptanalytic Time-Memory Trade-Offs

Contact: Gildas AVOINE (`gildas.avoine@irisa.fr`)

IRISA, Rennes, France

Application deadline: April 18th, 2019

The research group EMSEC from the research institute IRISA in France has an open PhD thesis position in the field of cryptography and algorithms, starting in September 2019. The candidate is expected to:

- Have followed a master program in computer science;
- Be strongly interested in both theoretical and applied aspects of computer science;
- Be fluent in English.

Keywords

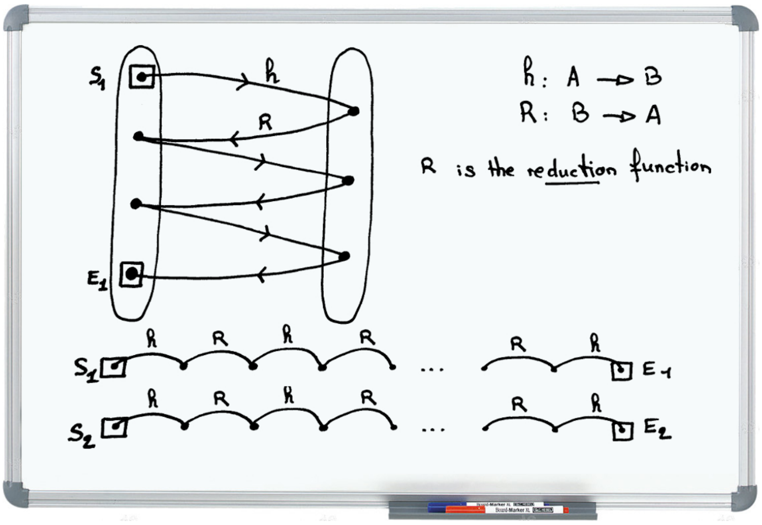
Security, Cryptography, Time-Memory Trade-Off, Password Cracking, Algorithmics, Probability, Distributed Computing.

Context

Many cryptanalytic problems can be solved using an exhaustive search in the key space, but each new instance of the problem requires restarting this expensive process from scratch. The basic idea of a cryptanalytic time-memory trade-off (TMTO) is to carry out an exhaustive search once for all such that following instances of the problem become easier to solve. Thus, if there are N possible solutions to a given problem, and M units of memory are allocated for the attack, then a time-memory trade-off can solve the problem with T units of time where T is proportional to N^2/M^2, instead of $T = N$ with an exhaustive seach [1, 3]. TMTOs are used to perform chosen plaintext attacks when N is reasonably sized. TMTOs are for example available in any security expert's toolbox to crack passwords [4], especially when the attack must be done in a short time, e.g., during legal investigations. The power of TMTOs is much broader than this use case, though.

Background

The cryptanalytic time-memory trade-off has been introduced in 1980 by Hellman [2] and applied to DES. Given a plaintext P and a ciphertext C, the problem consists in recovering the key K such that $C = E_K(P)$, where E is an encryption function assumed to follow the behavior of a random function. Encrypting P under all possible keys and storing each corresponding ciphertext allows for immediate cryptanalysis but needs N elements of memory. The idea of a trade-off is to use chains of keys, which is done using a reduction function R that generates a key from a ciphertext. Using E and R, chains of alternating ciphertexts and keys can thus be generated. The key point is that only the first and the last element of each chain are stored. This process is called the precomputation phase and it is done well in advance before the attack. Then, during the attack itself, in order to retrieve K, a chain is generated from C. If at some point it yields a stored end of chain, then the entire chain is regenerated from its starting point. However, finding a matching end of chain does not necessarily imply that the key will be found in the regenerated chain. There exist situations where the chain that has been generated from C merges with a chain that is stored in the memory that does not contain K. This situation is called a false alarm and is very costly.



Research Issue

Currently, it is hard to perform a TMTO when N is large, let's say when $N > 2^{48}$ because the precomputation phase is quite long. Unfortunately, distributing the precomputation phase over several computers, e.g., on a 5'000-core cluster, is not as efficient as one may expect. For example, while someone may expect a 5'000 speed-up factor with the above-mentioned cluster, it will not be higher than 100 with the current techniques used for the precomputations. The reason is that all the processes must exchange messages all along the precomputation phase in order to discard duplicated values as early as possible. The objective of this thesis is to find a solution to make a distributed precomputation phase as efficient as possible, given the optimal bound is reached when the communication overhead is nul. Note this case never occurs because there is a communication overhead even when considering a single processing unit because the computed values must be temporarily stored in a cache memory. In this thesis, it will be important to consider both the computation and the communication parameters in order to suit the algorithm used for the precomputation phase to the considered processing units (CPU, GPU, FPGA) and memories (RAM, SSD, etc.).

References

[1] Gildas Avoine, Pascal Junod, and Philippe Oechslin. Time-memory trade-offs: False alarm detection using checkpoints. In *Progress in Cryptology – Indocrypt 2005*, volume 3797 of *Lecture Notes in Computer Science*, pages 183–196, Bangalore, India, December 2005. Cryptology Research Society of India, Springer-Verlag.

[2] Martin Hellman. A cryptanalytic time-memory trade off. *IEEE Transactions on Information Theory*, IT-26(4):401–406, July 1980.

[3] Philippe Oechslin. Making a faster cryptanalytic time-memory trade-off. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO'03*, volume 2729 of *Lecture Notes in Computer Science*, pages 617–630, Santa Barbara, California, USA, August 2003. IACR, Springer-Verlag.

[4] Philippe Oechslin. http://ophcrack.sourceforge.net/, Last Access: April 2019.

Research Institute

IRISA (*Institut de Recherche en Informatique et Systèmes Aléatoires*), founded in 1975, is a research center for IT, image, signal processing, and robotics, located in Rennes, France. The institute hosts 800 researchers distributed in 40 research groups, and is funded by 7 entities, namely CNRS, ENS Rennes, Inria, INSA Rennes, Institut-Mines-Télécom, CentraleSupélec, Université de Bretagne Sud (UBS), and Université de Rennes 1. IRISA so "forms a research cluster for excellence within the ICTS, with scientific priorities that include bioinformatics, system security, new software architecture (many-cores, cloud computing), and virtual reality". IRISA is well-known for its research activities in computer security and cryptography (more than 100 researchers work full-time on this topic) and many neighboring companies are actively involved in this field. Rennes is located in the West part of France, about 45 minutes by car from the sea, and a fast train connects Rennes to Paris in less than 1h30.

Research Group

Embedded Security and Cryptography (EMSEC) is a research group within the IRISA computer science institute located in Rennes, France. EMSEC was created in February 2016 and is headed by Prof. Gildas Avoine and Prof. Pierre-Alain Fouque. The group hosts more than 35 researchers, including 8 permanent members. EMSEC's activities are organized along three axes: cryptography, formal methods, and system security.

Link: `https://www.irisa.fr/emsec`

Contact and Applications

Applications should contain a curriculum vitæ (including the grades obtained so far during the Master), and a motivation letter explaining why you are excited by this PhD thesis proposal. Applications should be sent by email to Gildas Avoine (`gildas.avoine@irisa.fr`).