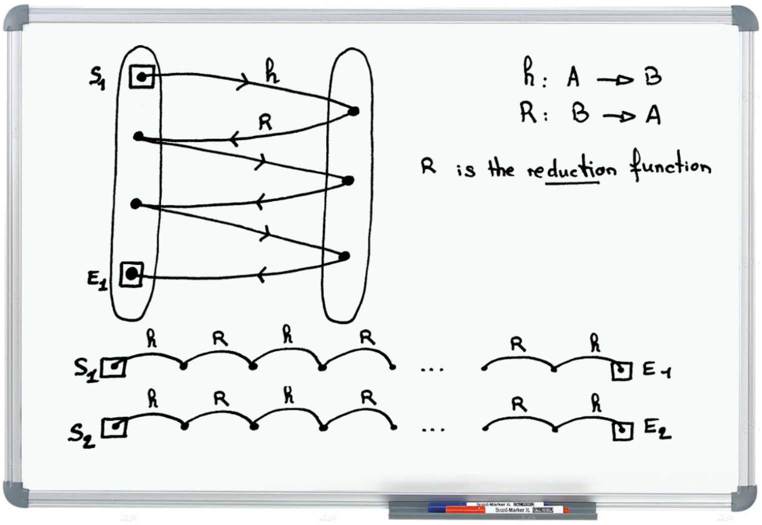
Improving the Precomputation of Cryptanalytic Time-Memory Trade-Offs Using a Distributed Architecture

Keywords: Cryptography, Time-Memory Trade-Off, Password Cracking, Algorithmics, Probability

Goal: Modify the precomputation procedure of rainbow tables in order to make it compliant with a distributed architecture.



Level	Master in Computer Science or Maths
Academic Year	2018/19
Location	IRISA Rennes, France (www.irisa.fr)
Domain	Security and Cryptography
Supervisor	Gildas Avoine (www.avoine.net)
Required Skills	C Programming, Algorithmics, Probabilities
Theory/Practice	Theory: 60%, Practice: 40%

Topic: Many cryptanalytic problems can be solved in theory using an exhaustive search in the key space, but are still hard to solve in practice because each new instance of the problem requires restarting the process from scratch. Such a problem is for example the cracking of passwords [3].

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, a time-memory trade-off can solve it with T units of time and M units of memory. In the methods we are looking at, T is proportional to N^2/M^2 and a typical setting is $T = M = N^{2/3}$ [1]

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. 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.

Research on TMTO mainly focuses on the storage of the points. However, a practical bottleneck is also the precomputation phase, which is time-expensive, typically 200 times more expansive than an exhaustive search. One may think that distributing this phase fix the issue. Unfortunately not. This phase is hardly distributable. In this internship, our aim will be to improve the precomputation procedure to be able to distributed this phase on large-scale clusters.

During this internship, the student will:

- Review the literature related to TMTO.
- Implement the cryptanalytic time-memory trade-off (TMTO) technique.
- Make a model of a distributed precomputatuion procedure.
- Perform experiments in order to instanciate this model and identify the optimal parameters.
- Possibly, improve the precomputation procedure to make it faster.
- Implement a distributed precomputation phase in a large-scale cluster.

Laboratory: IRISA (*Institut de Recherche en Informatique et Systèmes Aléatoires*), founded in 1975, is a mixed research centre for IT, image, signal processing, and robotics, located in Rennes, France. The institute hosts 800 researchers belonging to 41 teams, and is funded by 7 entities, namely CNRS, ENS Rennes, Inria, INSA Rennes, Institut-Mines-Télécom, Supélec, Université de Bretagne Sud (UBS), and Université de Rennes 1. (www.irisa.fr)

Advisor: Gildas Avoine is a professor of Information Security and Cryptography at INSA Rennes in France. His research activities take place at IRISA, in Rennes (France), in the research group "Embedded Security and Cryptography" (EMSEC). Previously, he was a researcher at the MIT (USA) in the CSAIL, and at the EPFL (Switzerland) in the LASEC, where he obtained a PhD degree in cryptography. Gildas Avoine's main research area is information security, which he addressed with a cryptographic approach. His topics of interest include privacy models, lightweight authentication, distance bounding protocols, cryptanalytic time-memory trade-offs, and forensics.

Contact:
Gildas Avoine (gildas.avoine@irisa.fr, www.avoine.net)
IRISA Rennes, Campus universitaire de Beaulieu (www.irisa.fr)
263 Avenue du Général Leclerc – CS 74205
F-35042 RENNES Cedex

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. Ophcrack password cracker: http://ophcrack.sourceforge.net/, Last Access: September 2014.