UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Matematica

SECONDO WORKSHOP DI CRITTOGRAFIA "BUNNYTN" 2011

Lunedì 12 settembre 2011
Aula A108 Polo Ferrari
Facoltà di Scienze – Università di Trento

PROGRAMMA:

9:00 – 9:10	**Presentazione del workshop** *Prof. Massimiliano Sala,* Università di Trento.
9:10 – 9:40	**The Rabin scheme revisited** *Prof. Michele Elia,* Politecnico di Torino.
9:40 – 10:10	**Introduction to Quantum Cryptography** *Dott. Tommaso Gagliardoni,* Università di Perugia.
10:10 – 10:30	*Coffee break*
10:30 – 11:00	**Introduction to Hash Functions** *Dott. PHD Anna Rimoldi*, Université de la Méditerranée, Marsiglia.
11:00 – 11:20	**On the provable security of BEAR and LION schemes** *Dott. Matteo Piva*, Università di Trento.
11:20 – 11:40	**Elastic Block Cipher** *Dott. Emanuele Bellini*, Università di Trento.
11:40 – 12:00	*Coffee break*
12:00 – 12:30	**On the weights of affine-variety codes and some Hermitian codes** *Dott. Marco Pellegrini,* Università di Pisa.
12:30 – 13:00	**Introduction to Hyperelliptic Curve Cryptography** *Dott.ssa Stefania Vanzetti*, Università di Torino.

Titoli ed abstract del Workshop di Crittografia "BUNNYTN" – 12 settembre 2011

The Rabin scheme revised

Prof. Michele Elia, Politecnico di Torino.

Ore 9:10 – 9:40

The Rabin public-key cryptosystem is revisited with a focus on the problem of identifying the encrypted message unambiguously; both theoretical and practical solutions are given. The Rabin signature is also reconsidered and a deterministic padding mechanism is proposed.
All results concern scenarios where the primes involved are not limited to be Blum primes.

Introduction to Quantum Cryptography

Dott. Tommaso Gagliardoni, Università di Perugia.

Ore 9:40 – 10:10

Quantum Mechanics (QM) has revolutionized the way Physics looks at reality since the beginning of the last century.
Nevertheless, this theory seems to provide endless insights and applications. One of such interesting applications is Quantum Cryptography (QC). In QC the integrity or the confidentiality of the message is not given by allegedly hard-to-solve mathematical problems, but by physical laws directly, instead. QM tells us that, unlike in the classical case, it is not physically possible to copy quantum information. This fundamental and counterintuitive fact can be exploited in Quantum Key Exchange schemes in order to establish a secure channel between two parties in such a way that it would be impossible for an eavesdropper to intercept the session key without being noticed by the parties.
In this talk we will present the basic concepts of QM, along with one of the most well-known Quantum Key Exchange schemes and its practical implementations.

Introduction to Hash Functions

Dott. PHD Anna Rimoldi, Université de la Méditerranée, Marsiglia.

Ore 10:30 – 11:00

In this talk we discuss the role of Hash functions in Cryptography. We present several construction approaches, we summarize the main theoretical results and discuss some attacks.

On the provable security of BEAR and LION schemes

Dott. Matteo Piva, Università di Trento.

Ore 11:10 – 11:20

BEAR, LION and LIONESS are block ciphers presented by Biham and Anderson (1996), inspired by the famous Luby-Rackoff constructions of block ciphers from other cryptographic primitives (1988). The ciphers proposed by Biham and Anderson are based on one stream cipher and one hash function. Clearly, good properties of the primitives ensure good properties of the block cipher.
In particular, they are able to prove that their ciphers are immune to any efficient known-plaintext key-recovery attack that can use as input ONE plaintext-ciphertext pair. Our contribution is showing that they are actually immune to any efficient known-plaintext key-recovery attack that can use as input ANY number of plaintext-ciphertext pairs. We are able to get this improvement by using weaker hypotheses on the primitives.

Elastic Block Cipher

Dott. Emanuele Bellini, Università di Trento.

Ore 11:20 – 11:40

The need of encrypting different length messages with one unique cipher gave rise to the problem of constructing an elastic block cipher.
We'll briefly describe Bellare-Rogaway solution, and Patel-Ramzan-Sundaram's improvement; both solutions use a fixed length block cipher as a black box.
Yet, this extension are not efficient and furthermore they rely their security to the fact that the elastic cipher is indistinguishable from a pseudorandom permutation.
We'll then introduce an efficient elastic block cipher extension, due to Cook, which, under certain assumption on the key schedule, is provably secure against key recovery if the underlying block cipher is secure against the same attack.
Instead of the entire fixed length (say L) block cipher, Cook's uses its round function as a black box to construct the extension, and she obtains a cipher that can encrypt messages of variable length from L to 2L.
We also see a distinguisher that exploits a systematic use of the keyschedule when performing encryptions of different lengths. Finally we introduce an extension of Cook's idea which allows to encrypt messages of any length greater than L.

On the weights of affine-variety codes and some Hermitian codes

Dott. Marco Pellegrini, Università di Pisa.

Ore 12:00 – 12:30

For any affine-variety code we show how to construct an ideal whose solutions correspond to codewords with any assigned weight.
We use our ideal and a geometric characterization to determine the number of small-weight codewords for some families of Hermitian codes over any Fq.
In particular, we determine the number of minimum-weight code-words for all Hermitian codes with d not greater than q. For such codes we also count some other small-weight codewords.

Introduction to Hyperelliptic Curve Cryptography

Dott.ssa Stefania Vanzetti, Università di Torino.

Ore 12:30 – 13:00

The growth of interest around public key cryptography increases the need of finding new cryptosystems based on the difficulty of solving the discrete logarithm problem. The Jacobian of an hyperelliptic curve seems to be a good alternative to the group of points of an elliptic curve. In order to define this group, we introduce the concepts of hyperelliptic curve, divisor, Jacobian, show how to perform the sum between divisors and study the complexity of this operation.
Then we analyze some known attacks with particular attention to index calculus. Finally we try to understand what are the most suitable hyperelliptic curves to be used for our purposes.