Book of Abstracts

WORKSHOP ON MATHEMATICAL CRYPTOLOGY

Editors:

Jaime Gutiérrez,

Álvar Ibeas

Santander (Spain), 29–30 June 2006

UC UNIVERSIDAD DE CANTABRIA

Index

Preface

The word cryptology stems from the Greek $\kappa\rho\upsilon\pi\tau\acute{o}\varsigma$, "hidden", and $\lambda\acute{o}\gamma o\varsigma$ "word". Cryptology is the science of secure communications and has traditionally dealt with the confidentiality of information, but innovation in using information produces new requirements for protection of that information. Cryptographic work has increased rapidly during the past three decades and so has the importance of applications. Topics as common as smart cards, cellular phones, internet purchases, pay per-view TV... are only partial features of this technological society in which we are all immersed. Cryptographic applications have to face great mathematical difficulties as far as design and implementation are concerned.

The purpose of this workshop is to present the most recent developments in mathematical cryptography. Topics include:

- Primality and Integer Factorization.
- Secure Encryption Schemes based on Group theory and Matroids.
- Gröbner Basis and Algebraic Cryptanalysis.
- Elliptic and Hyperelliptic curve cryptosystems.
- Lattices and lattice-based Cryptosystems.
- Pseudorandom Sequence Generators for Stream Ciphers.
- Public key cryptosystems based on Algebraic coding theory.
- Cryptographic Protocols and Information Security with mathematical emphasis.
- Quantum Cryptology.
- Optical Chaos Cryptography.

The program consists of 14 invited talks plus a thesis defense dissertation. We would like to express our sincere gratitude to all speakers.

We thank the Vicerrectorado de Investigación y Desarrollo, Facultad de Ciencias and Departamento de Matemáticas, Estadística y Computación of the University of Cantabria for their generous financial and logistic supports.

We write this short note in anticipation that the attendees of the Workshop on Mathematical Cryptology will find the experience scientifically rewarding and personally satisfying. May the historical and natural beauty of Cantabria be a setting conductive to stimulating interactions.

Jaime Gutierrez, Álvar Ibeas

The Probabilistic Theory of the Joint Linear Complexity of Multisequences

Harald Niederreiter

— Background on stream ciphers
— Linear and joint linear complexity
— The stochastic framework
— The LCP of single sequences
— The JLCP of multisequences
— Periodic (multi)sequences

Background on stream ciphers

Stream ciphers use pseudorandom keystreams for encryption and decryption. One of the main issues in the design and the analysis of keystreams is: how close is the keystream to a "truly random" sequence?

Fact: keystream generators mostly use linear feedback shift registers (LFSRs) as basic steps in their algorithm.

System-theoretic approach: to what extent can the keystream be simulated by short LFSRs?

In practice, the keystream is a sequence over $\mathbb{F}_2$, but in the theory we can consider sequences over any finite field $\mathbb{F}_q$.
There is a recent trend in stream ciphers towards *word-based* or *vectorized* stream ciphers.

Examples:

PANAMA, SOBER
DRAGON, NLS, SSS (ECRYPT stream cipher candidates)

In such stream ciphers, the keystreams are *multisequences*, i.e., parallel streams of finitely many sequences over $\mathbb{F}_q$. A multisequence consisting of m parallel streams of sequences $S_1, \ldots, S_m$ over $\mathbb{F}_q$ is denoted by

$$\mathbf{S} = (S_1, \ldots, S_m)$$

and called an m-fold multisequence over $\mathbb{F}_q$.

Linear and joint linear complexity

The basic definitions for the system-theoretic approach to the assessment of keystreams are the following.

Def. For a sequence S over $\mathbb{F}_q$ and $n \geq 1$, the *nth linear complexity* $L_n(S)$ is the length of the shortest LFSR that can generate the first n terms of S. We put $L_n(S) = 0$ if the first n terms of S are 0.

Def. The sequence $L_1(S), L_2(S), \ldots$ of nonnegative integers is called the *linear complexity profile* (LCP) of S.

Def. For an m-fold multisequence

$$\mathbf{S} = (S_1, \ldots, S_m)$$

over $\mathbb{F}_q$ and $n \geq 1$, the *nth joint linear complexity* $L_n^{(m)}(\mathbf{S})$ is the length of the shortest LFSR that can simultaneously generate the first n terms of each sequence S_j, $1 \leq j \leq m$. We put $L_n^{(m)}(\mathbf{S}) = 0$ if all these terms are 0.

Def. The sequence $L_1^{(m)}(\mathbf{S}), L_2^{(m)}(\mathbf{S}), \ldots$ of nonnegative integers is called the *joint linear complexity profile* (JLCP) of $\mathbf{S}$.

Note $0 \leq L_n^{(m)}(\mathbf{S}) \leq n$ and $L_n^{(m)}(\mathbf{S}) \leq L_{n+1}^{(m)}(\mathbf{S})$.

The stochastic framework

A fundamental question is: what is the behavior of the LCP (resp. JLCP) of "truly random" sequences (resp. multisequences) or of the overwhelming majority of sequences (resp. multisequences)? This behavior serves then as a yardstick in the design of keystreams.

We need a stochastic model such that:

(i) strings over $\mathbb{F}_q$ of the same length are equiprobable;

(ii) corresponding terms in the m streams making up an m-fold multisequence over $\mathbb{F}_q$ are statistically independent.

With such a stochastic model, "overwhelming majority" means "with probability 1". We can also talk about expected values of quantities such as $L_n^{(m)}(\mathbf{S})$.

Let $\mathbb{F}_q^m$ be the set of m-tuples of elements of $\mathbb{F}_q$ and let $(\mathbb{F}_q^m)^\infty$ be the sequence space over $\mathbb{F}_q^m$. Then $(\mathbb{F}_q^m)^\infty$ can be identified with the set of m-fold multisequences over $\mathbb{F}_q$.

Let $\mu_{q,m}$ be the probability measure on $\mathbb{F}_q^m$ which assigns the measure q^{-m} to each element of $\mathbb{F}_q^m$. Furthermore, let $\mu_{q,m}^\infty$ be the complete product measure on $(\mathbb{F}_q^m)^\infty$ induced by $\mu_{q,m}$.

Then $\mu_{q,m}^\infty$ is the probability measure on the set of m-fold multisequences over $\mathbb{F}_q$ which provides the desired stochastic framework.

Thus, "with probability 1" means that a statement holds on a set of $\mu_{q,m}^{\infty}$-measure 1.

The LCP of single sequences

A more or less satisfactory description of the LCP of random single sequences S over $\mathbb{F}_q$ was already given in the 1980s. In the following, the prime power q is arbitrary.

Th. 1 (Rueppel, Smeets). *The expected value E_n and the variance V_n of $L_n(S)$ satisfy*

$$\begin{aligned} E_n &= \frac{n}{2} + O(1) \quad as\ n \to \infty, \\ V_n &= O(1) \quad as\ n \to \infty. \end{aligned}$$

Th. 2 (H.N.). *With probability 1 we have*

$$\lim_{n\to\infty} \frac{L_n(S)}{n} = \frac{1}{2}.$$

Th. 3 (H.N.). *With probability 1 we have*

$$\begin{aligned} \liminf_{n\to\infty} \frac{L_n(S) - \frac{n}{2}}{\log_q n} &= -\frac{1}{2}, \\ \limsup_{n\to\infty} \frac{L_n(S) - \frac{n}{2}}{\log_q n} &= \frac{1}{2}. \end{aligned}$$

The JLCP of multisequences

Basic question for word-based stream ciphers: what is the behavior of $L_n^{(m)}(\mathbf{S})$ for arbitrary m? For $m = 1$ we have the results in the previous section.

Folklore conjecture from the late 1990s (Ding, Xing,...): $L_n^{(m)}(\mathbf{S})$ is roughly $\frac{mn}{m+1}$ for random m-fold multisequences $\mathbf{S}$ over $\mathbb{F}_q$.

Th. 4 (H.N. – Wang, 2005). *For any $m \geq 1$ we have with probability 1*

$$\lim_{n\to\infty} \frac{L_n^{(m)}(\mathbf{S})}{n} = \frac{m}{m+1}.$$

The proof requires tools from several areas:

- lattice basis reduction in function fields (Schmidt, 1991)
- multidim. Berlekamp-Massey algorithm (Wang – Zhu – Pei, 2004)
- probability theory

A crucial role in the proof of Th. 4 is played by information on the following counting function.

For $m \geq 1$, $n \geq 1$, $0 \leq L \leq n$, let

$N_n^{(m)}(L) = \#$ m-fold multisequences over $\mathbb{F}_q$ of length n with nth joint linear complexity equal to L.

Trivially $N_n^{(m)}(0) = 1$. For $m = 1$, $1 \le L \le n$, we have the classical formula

$$N_n^{(1)}(L) = (q-1)q^{\min(2L-1, 2n-2L)}.$$

For any $m \ge 1$ and $1 \le L \le n/2$, it was shown by H.N. (2003) that

$$N_n^{(m)}(L) = (q^m - 1)q^{(m+1)L-m}.$$

The case $m \ge 2$ and $n/2 < L \le n$ is much more difficult. It was solved recently by Wang – H.N. (online 2005).

For any $m \ge 1$ and $L \ge 1$, let $P(m; L)$ be the set of m-tuples $\mathbf{I} = (i_1, \dots, i_m) \in \mathbb{Z}^m$ with $i_1 \ge i_2 \ge \cdots \ge i_m \ge 0$ and $i_1 + \cdots + i_m = L$. Then the formula of Wang and H.N. says that for any $m \ge 1$ and $1 \le L \le n$ we have

$$N_n^{(m)}(L) = \sum_{\mathbf{I} \in P(m;L)} a(\mathbf{I}) q^{b(\mathbf{I}, n-L)},$$

where $a(\mathbf{I})$ and $b(\mathbf{I}, n-L)$ depend only on the indicated objects.

A consequence is:

$$N_n^{(m)}(L) \le C(q,m) L^m q^{2mn-(m+1)L}.$$

This bound is useful when L is close to n. Otherwise, we use the elementary bound

$$N_n^{(m)}(L) \le q^{(m+1)L}.$$

The following result refines Th. 4 and is a weak analog of Th. 3.

Th. 5 (H.N. – Wang, to appear). *For any $m \ge 1$ we have with probability 1*

$$\begin{aligned} \liminf_{n\to\infty} \frac{L_n^{(m)}(\mathbf{S}) - \frac{mn}{m+1}}{\log_q n} &\ge -\frac{1}{m+1}, \\ \limsup_{n\to\infty} \frac{L_n^{(m)}(\mathbf{S}) - \frac{mn}{m+1}}{\log_q n} &\le 1. \end{aligned}$$

In particular, with probability 1 we have

$$L_n^{(m)}(\mathbf{S}) = \frac{mn}{m+1} + O(\log n) \quad \text{as } n \to \infty.$$

Dai – Imamura – Yang (2005): sufficient condition for m-fold multisequence $\mathbf{S}$ over $\mathbb{F}_q$ to satisfy

$$\lim_{n\to\infty} \frac{L_n^{(m)}(\mathbf{S})}{n} = \frac{m}{m+1}.$$

For any $m \ge 1$ and $n \ge 1$, let $E_n^{(m)}$ be the expected value of $L_n^{(m)}(\mathbf{S})$. The following result is derived from Th. 4 and the dominated convergence theorem.

Th. 6 (H.N. – Wang, 2005). *For any $m \geq 1$ we have*

$$E_n^{(m)} = \frac{mn}{m+1} + o(n) \quad as\ n \to \infty.$$

Conjecture. For any $m \geq 1$ we have

$$E_n^{(m)} = \frac{mn}{m+1} + O(1) \quad \text{as } n \to \infty.$$

Known special cases:

- $m = 1$: Th. 1.
- $m = 2$: Wang – H.N. (online 2005), for $q = 2$ also Feng – Dai (2005).
- $m = 3$: H.N. – Wang (to appear).

Periodic (multi)sequences

Note that all keystreams used in practice in stream ciphers are periodic. Thus, this case has received a lot of attention.

For $N \geq 1$, a sequence $s_0, s_1, \ldots$ is called *N-periodic* if $s_{i+N} = s_i$ for all $i \geq 0$. Similarly for multisequences.

Def. The *joint linear complexity* $L^{(m)}(\mathbf{S})$ of a periodic m-fold multisequence $\mathbf{S}$ over $\mathbb{F}_q$ is defined by

$$L^{(m)}(\mathbf{S}) = \sup_{n \geq 1} L_n^{(m)}(\mathbf{S}).$$

Note: if $\mathbf{S}$ is N-periodic, then $L^{(m)}(\mathbf{S}) \leq N$.

For fixed $m \geq 1$ and $N \geq 1$, let $G_N^{(m)}$ be the expected value of $L^{(m)}(\mathbf{S})$ for N-periodic $\mathbf{S}$. Thus

$$G_N^{(m)} = \frac{1}{q^{mN}} \sum_{\mathbf{S}} L^{(m)}(\mathbf{S}),$$

where the sum is over all q^{mN} m-fold N-periodic multisequences $\mathbf{S}$ over $\mathbb{F}_q$.

Formulas for $m = 1$:
Rueppel (1986) for $q = 2$ and special N.
Dai – Yang (1991) for any q and N.
Meidl – H.N. (2002) for any q and N.

Formulas for $m \geq 2$:
Meidl – H.N. (2003) for any m, q, N.
Fu – H.N. – Su (2005) for any m, q, N.

The formulas for $m \geq 2$ are proved by using the generalized DFT for multisequences and cyclotomy.

Write $N = p^v w$, where the prime p is the characteristic of $\mathbb{F}_q$ and $\gcd(p, w) = 1$.

Th. 7 (Fu – H.N. – Su, 2005). *We have*

$$\begin{aligned} G_N^{(2)} &\geq N - O(\log\log(w+2)), \\ G_N^{(m)} &\geq N - O(1) \quad \textit{for } m \geq 3. \end{aligned}$$

Similarly, we can study the variance $W_N^{(m)}$ of $L^{(m)}(\mathbf{S})$ for N-periodic multisequences $\mathbf{S}$. Formulas for $W_N^{(m)}$:
$m = 1$: Dai – Yang (1991).
$m \geq 2$: Fu – H.N. – Su (2005).

Th. 8 (Fu – H.N. – Su, 2005). *We have*

$$\begin{aligned} W_N^{(2)} &= O(\log(w+1)\log\log(w+2)), \\ W_N^{(m)} &= O(1) \quad \text{for } m \geq 3. \end{aligned}$$

Harald Niederreiter Dep. Mathematics, National University of Singapore
nied@math.nus.edu.sg

Gröbner Bases and Cryptology: application to 2R-
Jean-Charles Faugère

Joint work with: **Ludovic Perret**

The full version of this paper will be presented at CRYPTO 2006

One-round schemes [Patarin, Goubin] are generalizations of C^*. The public key of these schemes are of the form

$$t \circ \psi \circ s$$

where t, s are two affine mappings over $GF(q)^n$, and $\psi : GF(q)^n \to GF(q)^n$ is a bijective mapping given by n multivariate polynomials of degree *two*.

The public key of Two-round schemes (2R) is the composition of two one-round schemes. The secret key of two-round schemes consists of:

- Three affine bijections r, s, $t : GF(q)^n \to GF(q)^n$
- Two applications $\phi, \psi : GF(q)^n \to GF(q)^n$, given by n quadratic polynomials.

The public key is given by n polynomials $p_1, \ldots, p_n$ of total degree 4 describing:

$$p = t \circ \psi \circ s \circ \phi \circ r$$

Following Patarin and Goubin, when *all* the polynomials are given, this scheme is called 2R scheme. If *only some* of them are given, it is called 2R-- scheme. In the following we denote by r the number of removed polynomials.

The 2R-- scheme permits to thwart an attack described at Crypto 99 (D.F. Ye, K.Y. Lam, Z.D. Dai.) against 2R schemes. Usually, the "minus variant" leads to a real strengthen of the schemes considered. We show here that this is actually not true for 2R schemes: we propose an efficient algorithm for decomposing 2R-- schemes using Gröbner basis computations; that is to say we are able to express $p_1, \ldots, p_{n-r}$ as the composition of two algebraic set of equations of degree 2. For instance, if we remove up to $r \leq \frac{n}{2}$ equations we are able to recover a decomposition in $O(n^{12})$. We provide experimental results illustrating the efficiency of our approach: we have been able to decompose 2R-- schemes for most of the challenges proposed by the designers in less than a handful of hours. We believe that our results renders the principle of two-round schemes, including 2R-- schemes, useless.

Jean-Charles Faugère	CNRS-UPMC-INRIA, LIP6/SALSA Jean-Charles.Faugere@lip6.fr
Ludovic Perret	UCL, Crypto Group, Microelectronic Laboratory ludovic.perret@uclouvain.be

Cryptanalysis of Non Linear Pseudorandom Number Generators

Domingo Gómez Pérez

Thesis dissertation : Universidad de Cantabria, June 2006.

"Random" numbers have many applications, among them decision making, numerical simulations for the Monte Carlo method, sampling, numerical analysis and testing computer chips for defects. Our main motivation is that of constructing secure cryptosystems in cryptology.

It is hard to imagine a well-designed cryptographic application that does not use random numbers. The fundamental objective of cryptography is to enable two people, usually referred to as Alice and Bob, to communicate over an insecure channel in such a way that an opponent, Oscar, cannot understand what is being said. Alice encrypts the plaintext, using a predetermined key, and sends the resulting ciphertext over the channel. Oscar, upon seeing the ciphertext in the channel by eavesdropping cannot determine what the plaintext was; but Bob,who knows the encryption key, can decrypt the ciphertext and reconstruct the plaintext.

The necessity of privacy has made people study techniques to cipher their messages. On the other hand, being able to understand encrypted messages gives a sensible advantage. This basically means that while keeping their messages secret, people have been trying decypher their neighbour's messages.

In this war between people who encrypt messages and attackers, who want to decrypt messages, there had been many partial victories for the latter group until this knowlegde was unified by Claude Shannon [14] in 1948. He set the foundations for cryptography, and thanks to that article, many ideas were proven, like the one about unconditional security, a measure that concerns the security of cryptosystems when there is no limit on the amount of computation that Oscar is allowed to do. This concept is very closely related to random numbers.

"Random" is a word that will appear very often in this thesis as well as in real life. Probably the most commonly encountered randomness requirement today is the user password. This is usually a simple character string. Obviously, if a password can be guessed, it does not provide security.

Many other requirements come from the cryptographic arena. Apart from ciphering text, cryptographic techniques can be used to provide a variety of services including confidentiality and authentication. Such services are keys, that are unknown to and unguessable by an adversary.

The frequency and volume of the requirement for random quantities differs greatly for different cryptographic systems. In many of them, random quantities are required when the key pair is generated, but thereafter any number of messages can be signed without any further need for randomness. Other algorithms, such as the public key Digital Signature Algorithm that has been proposed by the US National Institute of Standards and Technology (NIST), require random numbers in great quantities.

Presently, the lack of generally available facilities for generating such unpredictable numbers is an open wound in the design of cryptographic software. For the software developer who wants to build a key or password generation procedure that runs on a wide range of hardware, the only safe strategy so far has been to force the local installation to supply a suitable routine to generate random numbers.

It is important to keep in mind that the requirement is for data that an adversary would have a very low probability of guessing or determining. This will fail if pseudo-random data is used which only meets traditional statistical tests for randomness or which is based on limited range sources, such as clocks. Frequently such random quantities are determinable by an adversary searching through an embarrassingly small space of possibilities.

There exist ways to solve this problem in a deterministic fashion having a small quantity of random numbers, using the so called pseudorandom number generators. Normally, in this scheme, a true random number, called the seed, is taken and from it a sequence is generated. This is done applying a function which is the generator itself. A question arises; how is it possible to generate something that should be random using a deterministic function. The answer is given by Donald Knuth in the second book of "The art of programming" ([11]):

"All that can be said about a sequence of numbers is whether it appears random or not."

Pseudorandom number generators are faster than others methods, some of them, like the linear generator, are capable of generating a sequence of 1024 bits in 24×10^{-9} seconds. In contrast reading from a computer device takes more than a 10^{-6} seconds (1000 times faster, for more information read [15]).

To conclude this part of the preamble, we would like to insist on the point even accessing true random information does not mean that it is not unguesseable to the attacker.

One important mathematical concept to measure the random quality of a sequence of random numbers is its discrepancy, if this value is very high it will show us that, instead of distributing uniformly, the elements of the sequence are more likely to be in some intervals. In Chapter 3 of this dissertation we present bounds for non-linear multiple recursive congruential pseudorandom number generators.

A range of interesting mathematical problems arise in attempting to cryptanalysis pseudorandom number generators. Basically, there are two kinds of cryptanalysis problems: *reconstruction problems*, which attempt to reconstruct the parameters of the generator from some output of the generator, and *predicting problems*, which attempts to predict future output of the generator from some observed output.

In recent years, methods based on *lattice basis reduction* or juts *lattice reduction* or the so called LLL-technique (see [19]) have been used repeatedly for the cryptanalytic attack of various cryptosystems. Lattice reduction techniques seem inherently linear. The general idea of this technique is to relate our non linear problem to a lattice problem by building a lattice from the non linear equation, and translate our problem to finding a vector with smallest euclidean norm possible in the lattice, the so called Shortest Vector Problem SVP. In this thesis we apply this general linearization technique for predicting several nonlinear pseudorandom number generators.

Many very well-known and important cryptographic protocols are based on the assumption that factoring large composite integers is computationally difficult. The most famous one is RSA cryptosystem, which is currently used in a wide variety of products, platforms, and industries around the world. RSA is incorporated into all of the major protocols for secure Internet communications, including S/MIME and S/WAN.

We consider a number n which is product of two primes: p and q. We analyze the assumption that factoring is computationally difficult when the cryptanalyst has access to extra information.

In cryptographic applications, the cryptanalyst may have available additional information above and beyond the number n itself, see [18]. In practice, Alice or Bob (one of them) typically knows p and q already, and uses these factors implicitly and/or explicitly during her/his cryptographic computations. The results of these computations may become known

to the cryptanalyst, who thereby may find himself at an advantage compared to a pure factoring situation. The necessary information and timing measurements may be obtained by passively eavesdropping on an interactive protocol. The Chinese Remainder Theorem (CRT) is also often used to optimize RSA private key operations. With CRT, $y \bmod p$ and $y \bmod q$ are computed first (being y is the message to send). These initial modular reduction steps can be vulnerable to timing attacks. The simplest such attack is to choose values of y that are close to p or to q, and then use timing measurements to determine whether the guessed value is larger or smaller that the actual value of p and q.

So in practice, additional extra information may become available to the cryptanalyst, for one of the following reasons:

- loss of the equipment that generated p and q,
- explicit release of partial extra information as part of a protocol, for instance exchange of secret,
- timing measurements,
- routine usage of p and q to decrypt mail, sign messages, etc.,
- poor physical security to store and guard p and q,
- any other heuristic attack ...

Suppose that an attacker is able to find the high-order h bits of the smallest prime p, can we break the RSA cryptosystem?

We have to mention Coppersmith [4, 5] has obtained a strong result on this question. In Chapter 8 we apply the lattice reduction to study this problem.

Here is a brief synopsis of the nine chapters in this thesis.

Chapter 1 remains a relatively small introduction to pseudorandom number generators, some other concepts that will be used throughout the thesis, such as exponential sums and lattice, are also included. The most interesting problems in lattice theory will be introduced as well as methods to solve them. Fixed the dimiension, all the methods run in polynomial time and will be of great importance in our results.

Chapter 2 addresses two different problems, which are related. The first one is the following: given $f(x, y)$, an integer polynomial and two natural numbers Δ, Δ_1, find all solutions whose first component is bounded by Δ and the second one is bounded by Δ_1. The method of Coppersmith is explained together with the theoretical result. In the rest of the chapter we present original results for later use about bounds for the number of solutions of polynomials over finite rings and, the number of small solution of a special modular equation.

Chapter 3 contains an extension of a result in [10] of Niederreiter and Shparlinski, about discrepancy bounds for sequences of s-tuples generated by successive non-linear multiple recursive congruential pseudorandom number generators of higher orders. The key of this result is based on non-linear properties of the iterations of multivariate polynomials.

Chapter 4 deals with three theorems for the inversive congruential generator (ICG). The ICG is a sequence (u_n) of pseudorandom numbers defined by the relation $u_{n+1} \equiv au_n^{-1} + b \bmod p$ where a, b belong to the finite field with a prime number p of elements. We show that if sufficient number of the most significant bits of several consecutive values u_n of the ICG are given, one can recover the initial value u_0 (even in the case where the coefficients a

and b are not known). This suggests that for cryptographic applications, ICG should be used with great care. Our results are somewhat similar to those known for the linear congruential generator (LCG), $x_{n+1} \equiv ax_n + b \bmod p$, but apply only to much longer bit strings. This may suggest that ICG is cryptographically stronger and more useful than LCG.

Section 4.2 will deal with situations when the coefficients a, b and p are known to the attacker.

Section 4.3 talks about a new idea that will be applied when coefficients b and p are known.

Section 4.4 proves a similar theorem when the coefficients a, b are unknown, and in this case we achieve a higher level of security. In other words, we need more bits to be able to predicting the sequence. However, there is a drawback in this case, the method cannot be applied when the coefficients have special properties.

Chapter 5 applies the same ideas as the previous chapter for the quadratic congruential generator (QCG) and, in particular, for the celebrated Pollard generator.

There are two sections in this chapter. The first one applies the lattice reduction technique to the cases of quadratic generator in different situations. We also obtain a more precise result in the special case of the Pollard generator.

The theorems which talk about predicting the QCG in the first section only hold after excluding a small set of values of the coefficients/parameters defining the QCG. If this small set is not excluded, the algorithm for finding the secret information may fail. In the second section of this chapter, we can eliminated that small set using a new technique which makes use of two lattice reductions.

Chapter 6 is devoted to discussing the results of numerical tests and some heuristic approaches to the problem of predicting pseudorandom number generators studied in the previous two chapters. We briefly comment on the implementation and how it was done.

It is divided into two sections. In Section 6.1 we discuss the inverse and the quadratic congruential generator.

In Section 6.2 we discuss an implementation of these algorithms, why we have choosen some specific tools and something about the hardware used.

Chapter 7 contains an upper bound on the security of the polynomial generator when the modulo is prime and when it is not. In both cases, the coefficients of the polynomial are known. The result requires to exclude some special polynomial coefficients that make our method ineffective.

Chapter 8 studies the problem of factoring a natural number with high bits known. Our approach is inspired in algorithms presented in previous chapters. It is divided in three sections. We start by motivating the problem from the cryptography point of view, and commenting the state of the art. The chapter is structured as follows. In Section 8.2 we start with some preparatives in Subsection 8.2.1 and then we give a first approach in Subsection 8.2.2. In Subsection 8.2.3 we apply a second round lattice reduction and, we give vague idea of the algorithm for arbitrary number of rounds. Finally, Section 8.3 presents numerical results and time consumed of our implementation in C++ using the **NTL** (Number Theory Library) of the presented heuristic algorithm.

Chapter 9 is devoted to questions that are still open and future lines of investigation. Most of them fall in the field of pseudorandom number generators but there is also reference to RSA cryptosystem.

We would like to point out that some of the questions seem close to being solved after our research and the ideas that have led to it.

A significant part of the results in this dissertation are published in [9, 4, 3, 6, 7, 12, 5]

References

[1] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski : *Predicting the inversive generator*. Proc. IMA, Lectures Notes in Computer Science, Springer-Verlag, **N.2898**, 264-275, (2003).

[2] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski : *Predicting nonlinear pseudorandom number generators*. Mathematics and Computation, AMS, **N. 74**, 1471-1494, (2005).

[3] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski : *Reconstructing noisy polynomial evaluation in residue rings*. Journal of Algorithms. S 0196-6774(04)00115-4/FLA. Online www.elsevier.com/locate/jalgor

[4] D. Coppersmith, 'Factoring with a hint'. *IBM Research Report RC. 19905*, 1995.

[5] D. Coppersmith, 'Small solutions to polynomial equations, and low exponent RSA vulnerabilities', *J. Cryptology*, **10**, 1997, 233–260.

[6] D. Gomez, J. Gutierrez, A. Ibeas and D. Sevilla : *Prediciendo el generator cuadratico*. Avances en Criptologia y Seguridad de la Informacion. Diaz de Santos, ISBN 84-7978-650-7, 185-195 (2004).

[7] D. Gomez, J. Gutierrez and A. Ibeas : *Cryptanalysis of the Quadratic Generator*. Proc. INDOCRYPT'05, Lectures Notes in Computer Science, Springer-Verlag. **N.3797**, 118-129, (2005).

[8] D. Gomez, J. Gutierrez and A. Ibeas : *Attacking the RSA cryptosystem with partial information*. Proc. RECSI'06, to appear (2006).

[9] J. Gutiérrez and D. Gomez-Perez: ' Iterations of Multivariate Polynomials and Discrepancy of Pseudorandom Numbers' . Proc. AAECC, ÝLectures Notes in Computer Science, Springer-Verlag, **N. 2227**, 194-204, (2001).

[10] F. Griffin, H. Niederreiter and I. Shparlinski, 'On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders', *Proc. the 13th Symp. on Appl. Algebra, Algebraic Algorithms, and Error-Correcting Codes, Hawaii, 1999*, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **1719** , 1999, 87–93.

[11] D. E. Knuth, 'The art of Computer Programming', *Addison-Wesley series in Computer Science and Information Processing*, **Vol 2**.

[12] Paul C. Kocher, 'Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems'. *Proc. CRYPTO-96, Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1109**, 1996, 104-113.

[13] A. K. Lenstra, H. W. Lenstra and L. Lovász, 'Factoring polynomials with rational coefficients', *Mathematische Annalen*, **261**, 1982, 515–534.

[14] C. E. Shannon, 'A mathematical theory of communication'*Bell System Technical Journal*, **27**, 1948, 379–423 and 623–656.

[15] Silberschatz et all, 'Operating Systems', Springer-Verlag, Chicago, 1982.

Domingo Gómez Pérez Dep. Matemáticas, Estadística y Computación, Univ. Cantabria
gomezd@unican.es

On the equation $\tau(\lambda(n)) = \omega(n) + k$

Francesco Pappalardi

Let τ denote the 'number of divisors' function, let λ denote the Charmichael function and let ω denote the 'number of prime divisors' function. We investigate some properties of the positive integers n that satisfy the equation $\tau(\lambda(n)) = \omega(n) + k$ providing a complete description for the solutions when $k = 0, 1, 2$, and give some properties of the solutions in the other cases.

This is a joint project with A. Glibichuk and F. Luca.

Francesco Pappalardi Università degli Studi, Roma III
pappa@mat.uniroma3.it

An application of verifiable randomness: subliminal-free EC-DSA

M^a Isabel González Vasco

Joint work with: **Jens M. Bohli, Rainer Steinwandt**

Cryptographic schemes can also be used for purposes they have not been designed for. In particular, this "misuse" can be carried over if participants involved in a certain scheme, instead of choosing certain values uniformly at random (as specified by the scheme´s specification), select them according to a biased distribution. One (extensively investigated) example of this is the use of subliminal channels in signature schemes: assume two prisoners are allowed to exchange signed messages, while their communication is monitored by a warden. Then, the prisoners may want to exchange a secret message hidden in the signature of a "harmless" cover message. Verifiable random functions are well explored tools aiming at preventing malicious behaviours in this fashion, but are unfortunately not suited for all situations that may arise. We comment on the above issues, present a new notion for signature schemes (being subliminal free with proof) and propose a subliminal-free version of the signature scheme EC-DSA, which is suitable for scenarios with high security needs.

Jens-Matthias Bohli	Fakultät für Informatik, Universität Karlsruhe bohli@ira.uka.de
M^a Isabel González Vasco	Universidad Rey Juan Carlos, Madrid mariaisabel.vasco@urjc.es
Rainer Steinwandt	Dep. Math Sciences, Florida Atlantic University rsteinwa@fau.edu

Cryptographic Tools in Electronic Cash

Llorenç Huguet Rotger, Magdalena Payeras Capellà

Joint work with: **Josep Lluís Ferrer Gomila**

Digital or Electronic cash are a kind of electronic money in which money is included in pieces of digital information called coins. Digital coins are strings of bits that can be transferred through networks. Digital cash try to simulate Physical cash and its features: security, privacy, off-line payment and transferability.

Physical cash is secure: physical coins cannot be easily counterfeited or duplicated. Privacy is guarantied when physical cash is used; transactions aren't recorded and users can transfer coins without identification, they can remain anonymous to everybody including the other part involved in the transaction.

For digital cash some of the features of the physical cash are difficult to achieve due to its digital nature. While physical cash cannot be duplicated, digital coins (digital information) can be copied and potentially reused. Digital cash systems must include security systems that avoid the fraudulent reutilization of coins.

A solution for the reutilization problem is the inclusion in the payment stage of an on-line verification of the coin. This way, a user never accepts a coin before checking its validity through an on-line connection with a trusted third party (TTP), usually the bank, which checks if the coin was used before. In this case, the payment is rejected. These systems are called on-line. This solution isn't desirable because is in conflict with one of the desirable features described above: off-line payments. Other solutions are the identification of the payer in off-line payment (but this solution doesn't achieve the desired anonymity) and the use of hardware devices (tamper resistant devices). Moreover, a collusion of a merchant and the bank should not be able to trace payments (untraceability property). Some schemes are anonymous, but the identities of users can be revealed by a collusion of parties.

The solution adopted in some anonymous off-line proposals is to include in payments some information about the payer. These systems allow double spending in the payment stage and detect it later during the deposit of the coin. If the payer uses the coin only once, the included identifying information is useless but if the coin is reused, the information revealed in two payments can be used to identify the double-spender. The main advantage of the off-line systems is that only the customer and the merchant are involved in the payment stage. Anonymity and off-line payment can be accomplished.

There are two techniques that allow the identification of double-spenders, one is called cut & choose, and is used by Chaum in his electronic cash system, and the other is called single-term and is used in Brand's payment system. Both techniques use cryptography to reveal the identity of double-spenders.

Together with the basic properties, recent protocols achieve some additional properties. Recent applications of E-commerce have been challenging the existing electronic payment systems with special requirements. Some of these applications, like information purchases in online e-commerce or microcommerce, require special features that most payment systems cannot satisfy. The micropayments are electronic payment systems suitable for the requirements of payments of low value. Micropayments are useful in payments for web visualisation, download of shareware or musical files, access to press articles, use of search engines or databases... Conventional electronic payment systems are not alternative for micropayments due to their costs of storage, communication and computation.

We have presented protocols useful in case of micropayments and payments of high quantities (payments with specific requirements, like anonymity revocation in case of payments of high amounts). Moreover we have presented an anonymous transferable system.

Recently we have worked in the incorporation of atomicity to payment systems with identification of double-spenders. With these properties the payment systems can be used in electronic purchase protocols, achieving the fair exchange between the coin and the purchased item.

Magdalena Payeras Capellà	Dep. Mat. Informàtica, Universitat de les Illes Balears mpayeras@uib.es
Llorenç Huguet Rotger	Dep. Mat. Informàtica, Universitat de les Illes Balears l.huguet@uib.es
Josep Lluís Ferrer Gomila	Dep. Mat. Informàtica, Universitat de les Illes Balears dmijfg@clust.uib.es

Chaos-based optical communications
Luis Pesquera González

Chaotic signals have been proposed as broadband information carriers with the potential of providing a high level of robustness and privacy in data transmission. Encryption is achieved by encoding at the physical layer, providing full compatibility to conventional software encryption techniques. In chaotic communication systems messages are embedded within a chaotic carrier in the emitter, and recovered after transmission by a receiver upon synchronization with the emitter. The receiver architecture can be viewed as performing a nonlinear filtering process, intended to generate locally a message-free chaotic signal, which is then used for subtraction from the encoded transmitted signal. Optical systems provide simple ways of generating very high-dimensional chaotic carriers that offer a substantial security level, and also the possibility of very high transmission rates. Generation of chaotic signals with high dimension and high information entropy can be achieved in diode lasers by means of delayed feedback. However, smart attacks can recover the message when a nonlinear optoelectronic feedback architecture is used. We show that chaotic cryptosystems based on optoelectronic feedback with one and two delays can be broken. A digital message is extracted for two different configurations by reconstructing the nonlinear dynamics with modular neural networks.

Luis Pesquera González Instituto de Física de Cantabria, CSIC-Universidad de Cantabria
luis.pesquera@unican.es

Huge Group Structure of Elliptic Curves over Finite Fields

Igor E. Shparlinski

Introduction

Notation

$\mathbb{F}_q$ = finite field of q elements.

An elliptic curve $\mathbb{E}$ is given by a *Weierstraß equation* over $\mathbb{F}_q$ or $\mathbb{Q}$

$$y^2 = x^3 + Ax + B$$

(if $\gcd(q, 6) = 1$).

Main Facts

- Hasse–Weil bound: $|\#\mathbb{E}(\mathbb{F}_q) - q - 1| \le 2q^{1/2}$
- $\mathbb{E}(\mathbb{F}_q)$ is an Abelian group, with a special "point at infinity" $\mathcal{O}$ as the neutral element.

Some Questions

- What are possible group structures which can be represented by elliptic curves?
- Is it typical for $\mathbb{E}$ to be have a large exponent $\mathfrak{e}_q(\mathbb{E})$ (=the size of the largest cyclic subgroup of $\mathbb{E}(\mathbb{F}_q)$)?
- How often a "random" curve $\mathbb{E}$ is cyclic?
- What is a typical arithmetic structure of $\#\mathbb{E}(\mathbb{F}_q)$?
- How many $N \in [q - 2q^{1/2} + 1, q + 2q^{1/2} + 1]$ are taken as cardinalities $\#\mathbb{E}(\mathbb{F}_q)$?

Typically we consider "statistical" results in the following situations:

- The field $\mathbb{F}_q$ is fixed, the curve $\mathbb{E}$ runs through all elliptic curves over $\mathbb{F}_q$ (or over some natural classes of curves).
- The field $\mathbb{F}_q$ and the curve $\mathbb{E}$ are both fixed, we consider $\mathbb{E}(\mathbb{F}_{q^n})$ in the extension fields
- The curve $\mathbb{E}$ is defined over $\mathbb{Q}$ (and fixed). We consider reductions $\mathbb{E}(\mathbb{F}_p)$ modulo consecutive primes p

Remark: They are described in the increasing order of hardness.

Group Structure of $\mathbb{E}(\mathbb{F}_q)$ and Arithmetic Properties of $\#\mathbb{E}(\mathbb{F}_q)$

... are closely related. E.g. the question about the size of $\gcd(\#\mathbb{E}(\mathbb{F}_q), q - 1)$ appears very frequently.

Some Motivation

The following questions are of mathematical interest and also have various cryptographic applications.

Florian Hess, Tanja Lange, Joe Silverman, I.S., **1999–2004**::

Bounds on the discrepancy of many pseudorandom number generators on elliptic curves are nontrivial only if the exponent

$$\mathbf{e}_q(\mathbb{E}) \geq q^{1/2+\varepsilon}.$$

Complex Multiplication

If $\mathbb{E}$ is an elliptic curve over an algebraic number field, $\mathbb{K}$ then endomorphism ring $\mathrm{End}_{\mathbb{K}}(\mathbb{E})$ of $\mathbb{E}$ over $\mathbb{K}$, contains a copy of the integers corresponding to the morphisms $x \mapsto nx$ for each $n \in \mathbb{Z}$. If $\mathrm{End}_{\mathbb{K}}(\mathbb{E})$ is strictly bigger than $\mathbb{Z}$, we say $\mathbb{E}$ has *complex multiplication* (CM) for in that case, it is a classical result that the ring is isomorphic to an order in an imaginary quadratic field. Otherwise, we say $\mathbb{E}$ is a non-CM curve.

Many of the questions about elliptic curves fall naturally into these two categories, the CM case and the non-CM case.

Typically, the CM case is the easier since there is an additional structure.

Group Structure of $\mathbb{E}(\mathbb{F}_q)$

Classical Results

$\mathbb{E}(\mathbb{F}_q)$ is

- either cyclic
- or isomorphic to a product of two cyclic groups $\mathbb{Z}/M \times \mathbb{Z}/L$ with $L|M = \mathbf{e}_q(\mathbb{E})$.

Max Deuring, **1941**:

All values $N \in [q - 2q^{1/2} + 1, q + 2q^{1/2} + 1]$, except for a small number of explicitly described exceptions, are taken as cardinalities $\#\mathbb{E}(\mathbb{F}_q)$ (for $q = p$ there is no exception).

More Precise Results

Michael Tsfasman; Filipe Voloch; Hans-George Rück, **1988**:

Roughly speaking, with only few fully described exceptions, for any L and M with

$$L \mid \gcd(M, q - 1)$$

and such that LM can be realised as a cardinality of an elliptic curve over $\mathbb{F}_q$, there is also $\mathbb{E}$ for which

$$\mathbb{E}(\mathbb{F}_q) \cong \mathbb{Z}/L\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}.$$

Hendrik Lenstra, **1987**:

- For any $N \in [p - 2p^{1/2} + 1, p + 2p^{1/2} + 1]$, the probability that $\#\mathbb{E}(\mathbb{F}_p) = N$ for a random curve $\mathbb{E}$ is $O\left(p^{-1/2} \log p (\log\log p)^2\right)$.
- For any, but at most two values, in the *half interval* $N \in [p - p^{1/2} + 1, p + p^{1/2} + 1]$, the probability that $\#\mathbb{E}(\mathbb{F}_p) = N$ for a random curve $\mathbb{E}$ is at least $cp^{-1/2}(\log p)^{-1}$ for an absolute constant $c > 0$.

  Under the **ERH**, there are no exceptions and the bound becomes $cp^{-1/2}(\log\log p)^{-1}$.

Note: About q^2 Weierstraß equations, about $4q^{1/2}$ possible values for N.

Exponent $\mathbf{e}_q(\mathbb{E})$

Clearly

- if $\mathbb{E}(\mathbb{F}_q)$ is cyclic, then $\mathbf{e}_q(\mathbb{E}) = \#\mathbb{E}(\mathbb{F}_q) \sim q$ — as good as it gets;
- if $\mathbb{E}(\mathbb{F}_q)$ is isomorphic to a product of two cyclic groups $\mathbb{Z}/M \times \mathbb{Z}/L$ with $L|M$, then

$$\mathbf{e}_q(\mathbb{E}) = M \geq \#\mathbb{E}(\mathbb{F}_q)^{1/2} \sim q^{1/2}$$

  ... falls below the threshold $q^{1/2+\varepsilon}$.

Better Bounds?

Rene Schoof, **1991**:

If $\mathbb{E}$ (defined over $\mathbb{Q}$) has no complex multiplication then

- for all primes

$$\mathbf{e}_p(\mathbb{E}) \gg p^{1/2} \frac{\log p}{\log \log p}$$

  ... still below the threshold $p^{1/2+\varepsilon}$.

- under the **ERH**, for infinitely many primes,

$$\mathbf{e}_p(\mathbb{E}) \ll p^{7/8} \log p.$$

If $\mathbb{E} : y^2 = x^3 - x$ then $\mathbb{E}$ has complex multiplication over $\mathbb{Z}[i]$. On the other hand, $\mathbf{e}_p(\mathbb{E}) = k \sim p^{1/2}$ for every prime p of the form $p = k^2 + 1$.

Bill Duke, **2003**:

For almost all primes p and **all** curves $\mathbb{E}$ over $\mathbb{F}_p$

$$\mathbf{e}_p(\mathbb{E}) \geq p^{3/4-\varepsilon}$$

... comfortably above the $p^{1/2+\varepsilon}$ threshold!!

Kevin Ford and I.S., **2005**:

- The above bound is tight.
- A similar bound for Jacobians of curves of genus $g \geq 2$.

Even Better Bounds?

The bounds on the discrepancy of many sequences from elliptic curves attain their full strength when $\mathbf{e}_p(\mathbb{E})$ is of order close to q.

Question: Is it typical for $\mathbf{e}_q(\mathbb{E})$ to be close to q?

Bill Duke, **2003**:

For any curve $\mathbb{E}$ (defined over $\mathbb{Q}$) and almost all primes p

$$\mathbf{e}_p(\mathbb{E}) \geq p^{1-\varepsilon}$$

unconditionally if E has complex multiplication and under the **ERH**, otherwise.

I.S., **2003**:

For any prime p and almost all curves $\mathbb{E}$ (defined over $\mathbb{F}_p$)

$$\mathbf{e}_p(\mathbb{E}) \geq p^{1-\varepsilon}.$$

Florian Luca and I.S., **2004**:

Let $\mathbb{E}$ be an ordinary curve defined over $\mathbb{F}_q$. Then

- for almost all integers n,
$$\mathbf{e}_{q^n}(\mathbb{E}) \geq q^{n-2n(\log n)^{-1/6}}.$$
- for all integers n,
$$\mathbf{e}_{q^n}(\mathbb{E}) \geq q^{n/2+c(q)n/\log n}$$

The proofs are based of some deep facts of the theory of Diophantine Approximations

- Subspace Theorem;
- Lower bounds of linear forms of p-adic logarithms;
- Upper bounds on the number of zeros of linear recurrence sequences.

Essentially the proof of the first bound follows the ideas of *P. Corvaja and U. Zannier,* **2004**.

It also gives a subexponential upper bound on
$$d(q^n) = \gcd(\#\mathbb{E}(\mathbb{F}_{q^n}), q^n - 1)$$
which also appears in the estimate of the complexity of the structure finding algorithm of *Victor Miller,* **1984-2004**.

Florian Luca, James McKee and I.S., **2004**:

Let $\mathbb{E}$ be an ordinary curve defined over $\mathbb{F}_q$. Then for infinitely many integers n,
$$\mathbf{e}_{q^n}(\mathbb{E}) \ll q^n \exp\left(-n^{c/\log\log n}\right).$$
for some $c > 0$ depending only on q.

The proof is based on:

- studying the degree $d(r)$ of the extension of $\mathbb{F}_q$ generated by points of r-torsion groups (i.e. groups of points P on $\mathbb{E}$ in the algebraic closure $\overline{\mathbb{F}}_q$ with $rP = \mathcal{O}$) for distinct primes r;
- a modification of a result of Adleman–Pomerance–Rumely (1983) on constructing integers n which have exponentially many divisors of the form $r - 1$, where r is prime.

How do we proceed?
Combine the following facts:

- *Weil Pairing:* If $\mathbb{E}(\mathbb{F}_q) \cong \mathbb{Z}/M \times \mathbb{Z}/L$ with $L|M$, then $L|q-1$.
- *Hendrik Lenstra,* **1987**: For any N, the probability that $\#\mathbb{E}(\mathbb{F}_q) = N$ for a random curve $\mathbb{E}$ is $O\left(q^{-1/2}\log q(\log\log q)^2\right)$.

  Thus all values of $N \in [q - 2q^{1/2}, q + 2q^{1/2}]$ are taken about the same number of times.

The question about $e_q(\mathbb{E})$ is now reduced to studying how often $N \in [q - 2q^{1/2} + 1, q + 2q^{1/2} + 1]$ has a large common divisor with $q - 1$.

Is Cyclicity Typical?

- Fix the field — Vary the curve:

  Sergei Vlăduţ, **1999**:
  At least 75% of elliptic curves over $\mathbb{F}_q$ are cyclic, but **not** 100%.
- Fix the curve over $\mathbb{F}_q$: — Vary the extension: *Sergei Vlăduţ,* **1999**:
  Over every finite there is a curve $\mathbb{E}$ such that $\mathbb{E}(\mathbb{F}_{q^n})$ is cyclic for a positive proportion of n.

- Fix the curve over $\mathbb{Q}$: — Vary the prime:

  Related to the **Lang–Trotter Conjecture!**

  Alina Cojocaru, Ram Murty, Bill Duke, **2001-2006**: (a series of results)

  - under the **ERH** the set of primes for which $\mathbb{E}(\mathbb{F}_p)$ is cyclic is of positive density (depending on $\mathbb{E}$);
  - the smallest prime for which $\mathbb{E}(\mathbb{F}_p)$ is cyclic is not too large.

Finding the Group Structure

Victor Miller, **1984-2004**:
There is a probabilistic algorithm which runs in time $(\log q)^{O(1)}$ + time to factor

$$d(q) = \gcd(\#\mathbb{E}(\mathbb{F}_q), q-1)$$

John Friedlander, Carl Pomerance and I.S., **2005**:
Typically $d(q)$ is easy to factor: the expected time is $(\log q)^{1+o(1)}$.

David Kohel and I.S., **2001**:
Deterministic algorithm which runs in time $q^{1/2+o(1)}$ (in fact it produces a set of generators).

The result is based on the extension of *Bombieri's bound* of exponential sums

$$\sum_{P \in \mathcal{H}} \exp\left(2\pi\sqrt{-1}\mathrm{Tr}\left(f(P)\right)/p\right) = O(q^{1/2})$$

for any subgroup $\mathcal{H} \in \mathbb{E}(\mathbb{F}_q)$ and any function f which is not constant on $\mathbb{E}$.

Arithmetic Structure of $\#\mathbb{E}(\mathbb{F}_q)$

Primality

The Holy Grail is to prove at least one out of the following claims (also very important for elliptic curve cryptography):

- For every q, there are sufficiently many curves $\mathbb{E}$ over $\mathbb{F}_q$, such that $\#\mathbb{E}(\mathbb{F}_q)$ is prime;
- for a curve $\mathbb{E}$ over $\mathbb{F}_q$, $\#\mathbb{E}(\mathbb{F}_{q^n})/\#\mathbb{E}(\mathbb{F}_q)$ is prime for infinitely many integers n;
- for a curve $\mathbb{E}$ over $\mathbb{Q}$, $\#\mathbb{E}(\mathbb{F}_p)$ is prime for infinitely many primes p.

Out of reach!

One of the obstacles is the lack of the results about primes in short intervals.

Large and Small Prime Divisors of $\#\mathbb{E}(\mathbb{F}_q)$

Question: What if we ask for curves such that $\#\mathbb{E}(\mathbb{F}_q)$ does not have a large prime divisor?

Hendrik Lenstra, **1987**: For the rigorous analysis of the *elliptic curve factorisation* we need to show that there are sufficiently many curves over $\mathbb{F}_p$ for which $\#\mathbb{E}(\mathbb{F}_p)$ is smooth. — Still unknown!

Hendrik Lenstra, Jonathan Pila and Carl Pomerance, **1993**:
The current knowledge is enough to analyze rigorously the hyperelliptic smoothness test (larger intervals...).

Question: What if we only ask for curves such that $\#\mathbb{E}(\mathbb{F}_q)$ has a large prime divisor?

Glyn Harman, **2005**:
There is a positive proportion of integers n in the middle part of the Hasse–Weil interval $n \in [q+1-q^{1/2}, q+1+q^{1/2}]$ with the largest prime divisor $P(n) \geq n^{0.74}$

Number of Prime Divisors

Kumar Murty and Ram Murty, **1984**:
Under the **ERH**, for any non-CM elliptic curve $\mathbb{E}$ over $\mathbb{Q}$, one has an analogue of the *Turán–Kubilius* inequality:

$$\sum_{p \le x} \left(\omega\left(N_{\mathbb{E}}(p)\right) - \log\log p\right)^2 = O(\pi(x)\log\log x)$$

where, as usual, $\pi(x) = \#\{p \le x\}$.

Yu-Ru Liu, **2004**:
For CM curves, a similar result is obtained unconditionally.

Jörn Steuding and Annegret Weng, **2005**:
There are at least $C(\mathbb{E})x/(\log x)^2$ primes $p \le x$ such that

- $\Omega(N_{\mathbb{E}}(p)) \le 8$, if $\mathbb{E}$ is a non-CM curve,
- $\omega(N_{\mathbb{E}}(p)) \le 5$, if $\mathbb{E}$ is a non-CM curve,
- $\Omega(N_{\mathbb{E}}(p)) \le 3$, if $\mathbb{E}$ is a CM curve.

CM Discriminants

For a curve $\mathbb{E}$ defined over $\mathbb{F}_p$ we put $t = \#E(\mathbb{F}_p) - p - 1$ and write

$$t^2 - 4p = -r^2 s$$

where s is squarefree. Then either $-s$ or $-4s$ is the discriminant of the endomorphism ring of $\mathbb{E}$, or CM discriminant.

Florian Luca and I.S., **2004**:

- The discriminant is usually large for a "random" curve;
- All curves modulo p define $2p^{1/2} + O(p^{1/3})$ distinct discriminants.

In particular, the last bound is based on an improvement of a result of Cutter–Granville–Tucker.

Cryptographic Applications

Embedding Degree and MOV Attack

Alfred Menezes, Tatsuaki Okamoto and Scott Vanstone, **1993**:
MOV constructs an embedding of a fixed cyclic subgroup of order L of $\mathbb{E}(\mathbb{F}_p)$ into the multiplicative group $\mathbb{F}_{p^k}^*$ provided $L | p^k - 1$.

Number Field Sieve: **discrete logarithm** in $\mathbb{F}_{p^k}^*$ can be found in time $\mathcal{L}_{p^k}\left(1/3, (64/9)^{1/3}\right)$ where, as usual,

$$\mathcal{L}_m(\alpha, \beta) = \exp\left((\beta + o(1))(\log m)^{\alpha}(\log\log m)^{1-\alpha}\right).$$

The smallest k with

$$\#\mathbb{E}(\mathbb{F}_p) | p^k - 1$$

is called the **embedding degree**.

If the embedding degree of $\mathbb{E}(\mathbb{F}_p) = o\left((\log p)^2\right)$ then the **discrete logarithm** on $\mathbb{E}(\mathbb{F}_p)$ can be solved in subexponential time $p^{o(1)}$.

R. Balasubramanian and N. Koblitz, **1998**:
For *almost all primes* p and almost all elliptic curves over $\mathbb{F}_p$ of *prime cardinality* the embedding degree is large.

E.g. for a "random" prime $p \in [x/2, x]$ and a random curve modulo p,

$$\Pr\{\text{embedding degree} \le (\log p)^2\} \le x^{-1+o(1)}.$$

Florian Luca and I.S., **2004**:
For *all* primes p and almost all elliptic curves over $\mathbb{F}_p$ of *prime cardinality* the embedding degree is large:

Let $\log K = O(\log_2 p)$. For a randomly chosen curve

$$\Pr\{\text{embedding degree} \le K\} \le p^{-1/(4\kappa+6)+o(1)},$$

where

$$\kappa = \frac{\log K}{\log_2 p}.$$

For $K = (\log p)^2$ the RHS is $p^{-1/14+o(1)}$.

The proof is based on

- studying $N \in [p+1-2p^{1/2}, p+1+2p^{1/2}]$ with $N | p^k - 1$, for some $k \le K$;
- Lenstra's bound on the number of curves with $\mathbb{E}(\mathbb{F}_p) = N$.

For $H \ge h \ge 1$ and $K \ge 1$, we let $N(p, K, H, h)$ be the number of integers $N \in [H - h, H + h]$ with $N \mid (p^k - 1)$ for some $k \le K$.

For $\log H \asymp \log h \asymp \log p$ and $\log K = O(\log_2 p)$,

$$N(p, K, H, h) \le h^{1-1/(2\kappa+3)+o(1)},$$

where

$$\kappa = \frac{\log K}{\log_2 p}.$$

Also, similar results about the probability that

- $P(\#\mathbb{E}(\mathbb{F}_p)) | p^k - 1$ for $k \le K$;
- $\#\mathbb{E}(\mathbb{F}_p) | \prod_{k=1}^{K} (p^k - 1)$.

Scarcity of Pairing Friendly Fields

For several other cryptographic applications of the *Tate or Weil pairing* on elliptic one need elliptic curves $\mathbb{E}$ with **small** embedding degree.

Supersingular curves gave $\mathbb{E}(\mathbb{F}_q) = q + 1$ thus are natural candidates. However, one can also suspect that supersingular curves have some cryptographic weaknesses and thus ask for constructions generating *ordinary curves*.

Let

$$\Phi_k(X) = \prod_{\substack{j=0 \\ \gcd(j,k)=1}}^{k} (X - \exp(2\pi\sqrt{-1}j/k))$$

be the kth *cyclotomic polynomial*.

Typically, such constructions work into two steps:

Step 1 Choose a prime ℓ, integers $k \ge 2$ and t, and a prime power q such that

$$\begin{aligned} |t| &\le 2q^{1/2}, \qquad t \ne 0, 1, 2, \\ \ell &\mid q + 1 - t, \qquad \ell \mid \Phi_k(q). \end{aligned} \tag{1}$$

Step 2 Construct an elliptic curve $\mathbb{E}$ over $\mathbb{F}_q$ with $\#\mathbb{E}(\mathbb{F}_q) = q + 1 - t$.

k should be reasonable small (e.g., $k = 2, 3, 4, 6$), while the ratio $\log \ell / \log q$ should be as large as possible, preferably close to 1.

Unfortunately, there is no efficient algorithm for Step 2, except for the case when the $t^2 - 4q$ has a very small square-free part; that is, when

$$t^2 - 4q = -r^2 s \tag{2}$$

with some integers r and s, where s is a small square-free positive integer. In this case either $-s$ or $-4s$ is the fundamental discriminant of the CM field of $\mathbb{E}$.

Let $Q_k(x, y, z)$ the number of prime powers $q \le x$ for which there exist prime $\ell \ge y$ and t satisfying (1) and (2) with a square-free $s \le z$.

Florian Luca and I.S., **2005**:
For any fixed k and real $x,\ y$ and z the following bound holds

$$Q_k(x, y, z) \le x^{3/2+o(1)} y^{-1} z$$

as $x \to \infty$.

In particular, if $z = x^{o(1)}$, which is the only practically interesting case anyway, we see that unless $y \le x^{1/2}$ there are very few finite fields suitable for pairing based cryptography.

In other words, unless the common request of the primality of the cardinality of the curve is relaxed to the request for this cardinality to have a large prime divisor (e.g., a prime divisor ℓ with $\log \ell / \log q \ge 1/2$), the suitable fields are very rare.

Heuristic on MNT curves

Atsuko Miyaji, Masaki Nakabayashi and Shunzou Takano, **2001**:
MNT algorithm to produce elliptic curves satisfying the condition (1) with $k = 3, 4, 6$, and the condition (2) for a given value of s.

Florian Luca and I.S., **2005**:
Heuristic estimates on the number of elliptic curves which can be produced by **MNT**.

It seems that they produce only finitely many suitable curves (still this can be enough for practical needs of elliptic curve cryptography).

Our arguments are based on a combination of the following observations:

- **MNT** gives a parametric family of curves whose parameter runs through a solution of a *Pell equation* $u^2 - 3sv^2 = -8$ (for $k = 6$, and similar for $k = 3, 4$).
- Consecutive solutions (u_j, v_j) of a Pell equation grow exponentially, as at least s^{cj} and most probably as $e^{cs^{1/2}j}$ for some constant $c > 0$.
- The probability of a random integer n to be prime is $1/\log n$.
- MNT curves should satisfy two independent primality conditions (on the field size and on the cardinality of the curve).

Therefore, the expected total number of **MNT** curves for every s is bounded, by the order of magnitude, by

$$\sum_{j=1}^{\infty} \frac{1}{(\log s^{cj})^2} \ll \frac{1}{\log s} \sum_{j=1}^{\infty} \frac{1}{j^2} \ll \frac{1}{\log s}.$$

or even by

$$\sum_{j=1}^{\infty} \frac{1}{(\log e^{cs^{1/2}j})^2} \ll \frac{1}{s^{1/2}} \sum_{j=1}^{\infty} \frac{1}{j^2} \ll \frac{1}{s^{1/2}}.$$

Probably the total number of all **MNT** curves of prime cardinalities (over all finite fields) and of bounded CM discriminant, is bounded by an absolute constant.

Apparently the number of all **MNT** curves of prime cardinalities with CM discriminant up to z, is at most $z^{1/2+o(1)}$.

Similar heuristic shows that **MNT** produces sufficiently many curves whose cardinality has a large prime divisor.

Generating Pseudorandom Points on Elliptic Curves

Fix a point $G \in \mathbb{E}(\mathbb{F}_p)$ of order t

- EC Linear Congruential Generator, **EC-LCG**:

  For the "initial value" $U_0 \in \mathbb{E}(\mathbb{F}_q)$, consider the sequence:

  $$U_k = G \oplus U_{k-1} = kG \oplus U_0, \qquad k = 1, 2, \ldots .$$

  Introduced and studied by:

  Sean Hallgren, **1994**: **EC-LCG**

  Also by
  Gong, Berson, Stinson, **2001**:
  Beelen, Doumen, **2002**:
  El Mahassni, Hess, I.S., **2001-2003**:

- EC Power Generator, **EC-PG**:

  For an integer $e \geq 2$, consider the sequence (with $W_0 = G$),

  $$W_k = eW_{k-1} = e^k G, \qquad k = 1, 2, \ldots,$$

  Introduced and studied by:

  Tanja Lange, I.S., **2003**:

- EC Naor-Reingold Generator, **EC-NRG**:

  Given an integer vector $\mathbf{a} = (a_1, \ldots a_k)$, consider the sequence:

  $$F_{\mathbf{a}}(n) = a_1^{\nu_1} \ldots a_k^{\nu_k} G, \qquad n = 1, 2, \ldots,$$

  where $n = \nu_1 \ldots \nu_k$ is the bit representation of n, $0 \leq n \leq 2^k - 1$.

  Introduced and studied by:

  Bill Banks, Frances Griffin, Daniel Lieman, Joe Silverman, I.S., **1999-2001**:

  Example: Let $G \in \mathbb{E}(\mathbb{F}_p)$ be of order $t = 19$, $k = 4$ and $\mathbf{a} = (2, 5, 3, 4)$. Then,

  $$\begin{aligned}
  F_{\mathbf{a}}(0) &= 2^0 5^0 3^0 4^0 G = G, \\
  F_{\mathbf{a}}(1) &= 2^0 5^0 3^0 4^1 G = 4G, \\
  F_{\mathbf{a}}(2) &= 2^0 5^0 3^1 4^0 G = 3G, \\
  F_{\mathbf{a}}(3) &= 2^0 5^0 3^1 4^1 G = 12G, \\
  \ldots & \quad \ldots \\
  F_{\mathbf{a}}(11) &= 2^1 5^0 3^1 4^1 G = 24G = 5G, \\
  \ldots & \quad \ldots \\
  F_{\mathbf{a}}(15) &= 2^1 5^1 3^1 4^1 G = 120G = 6G,
  \end{aligned}$$

They all have analogues in the group $\mathbb{F}_q^*$

Florian Hess, Tanja Lange, I.S., **2001–2004**:

Theorem:
If G is of order $t \geq p^{1/2+\varepsilon}$ then

EC-LCG, **EC-PG**, **EC-NRG**

are reasonably well distributed

Conjecture:
The above sequences are very well distributed

Proof ingredients:

- Bounds of exponential sums

  David Kohel, I.S., **2000**:

  $$\sum_{P \in \mathcal{H}} \exp\left(2\pi i f(P)/p\right) = O(p^{1/2})$$

  for any subgroup $\mathcal{H} \in \mathbb{E}(\mathbb{F}_p)$ and any function f which is not constant on $\mathbb{E}$.

- Results about not vanishing some functions over $\mathbb{E}$

Igor E. Shparlinski Center for Advanced Comptuing, Macquarie University
igor@comp.mq.edu.au

On secret sharing schemes, matroids, and polymatroids

Carles Padró Laimón

One of the main open problems in secret sharing is the characterization of the access structures of ideal secret sharing schemes. As a consequence of the results by Brickell and Davenport, every one of those access structures is related in a certain way to a unique matroid.

Matroid ports are combinatorial objects that are almost equivalent to matroid-related access structures. They were introduced in 1964 by Lehman and a forbidden minor characterization was given by Seymour in 1976. These and other subsequent works on that topic have not been noticed until now by the researchers interested on secret sharing.

By combining those results with some techniques in secret sharing, we obtain new characterizations of matroid-related access structures. As a consequence, we generalize the result by Brickell and Davenport by proving that, if the information rate of a secret sharing scheme is greater than 2/3, then its access structure is matroid-related. This generalizes several results that were obtained for particular families of access structures.

In addition, we study the use of polymatroids for obtaining upper bounds on the optimal information rate of access structures. We prove that all the bounds that are obtained by this technique for an access structure apply also to the dual structure.

Finally, we present lower bounds on the optimal information rate of the access structures that are related to two matroids that are not secret sharing representable: the Vamos matroid and the non-Desargues matroid.

Carles Padró Laimón Dep. Mat. Aplicada IV, Universitat Politècnica de Catalunya
cpadro@ma4.upc.edu

Character Sums and Nonlinear Recurrence Sequences

Simon R. Blackburn

This talk is based on recent joint work with Igor Shparlinski.

Let R be a finite ring (with a multiplicative identity) of cardinality m. Let $(a_n)_{n=0}^{\infty}$ be a sequence over R. Suppose (a_n) satisfies a non-linear recurrence of order d. We aim to show how to prove an upper bound on a certain character sum associated with (a_n); this bound can be used to prove results on the autocorrelation of the sequence, and on the distribution of windows of fixed length (less than d) in the sequence. Our bounds are non-trivial only when the period of the sequence is close to m^d (a situation that arises, for example, when we are studying de Bruijn sequences). In contrast to a typical situation where d is regarded as being fixed, our results allow d to grow but m to remain bounded.

Simon R. Blackburn Dep. Pure Mathematics, Royal Holloway, Univ. London
s.blackburn@rhul.ac.uk

Large prime variation of the lattice sieve

Gagan Garg

The number field sieve (NFS) is asymptotically the fastest known algorithm for factoring integers [1]. There are primarily two ways in which NFS can be implemented: line sieve and lattice sieve. Lattice sieve was proposed by Pollard in 1991 [2]. It is known to be better than the line sieve. A preliminary analysis of the lattice sieve was done by Pollard in this introductory paper. He showed that the work done using the lattice sieve is less than that in the line sieve; but we still get most of the solutions that would have been generated by the line sieve. Thus, lattice sieve takes less time to produce a majority of the relations. However, Pollard did not analyze the large prime variations of the lattice sieve.

In most of the present day implementations of the NFS, we allow for 2 to 3 large primes. Hence, it is important to study the large prime variant of this problem. In our analysis, we also consider the 4 large prime variant to handle larger RSA challenge numbers.

We present a rigorous analysis of the total number of integers sieved (work done) in the lattice sieve. More importantly, we analyze the number of partial solutions obtained when using the large prime variations.

We divide the factor base into two parts:

$$S : \text{the small primes: } p \leq B_0$$

$$M : \text{the medium primes: } B_0 < p \leq B_1$$

We also have

$$L : \text{the large primes: } B_1 < p \leq B_2$$

Let x be a typical auxiliary integer that is obtained from the NFS *i.e.* $x(a,b) = a - mb$ for the rational sieve and $x(a,b) = norm(a - \alpha b)$ for the algebraic sieve, where a and b are sieve parameters and α is a complex root of the NFS polynomial. Define $r := \log B_0 / \log x$, $s := \log B_1 / \log x$ and $t := \log B_2 / \log x$.

Our results are as follows:

(i) The work done using the lattice sieve divided by the work done using the line sieve is

$$\frac{\log\log {B_1}^2 - \log\log {B_0}^2}{2\log\log B_1}$$

(ii) The fraction of full relations obtained when using the lattice sieve is

$$1 - \frac{\rho(1/r)}{\rho(1/s)} \quad \text{where} \quad \rho \text{ is the Dickman function}$$

(iii) The fraction of partial relations obtained when allowing k large primes in the lattice sieve is

$$1 - \frac{J_k(r,s,t)}{J_k(s,s,t)} \quad \text{where} \quad J_k(r,s,t) := \frac{1}{k!}\int_s^t\int_s^t\cdots\int_s^t \rho\left(\frac{1-\sum_{i=1}^k \lambda_k}{r}\right)\frac{d\lambda_1}{\lambda_1}\frac{d\lambda_2}{\lambda_2}\cdots\frac{d\lambda_k}{\lambda_k}$$

We also estimate this integral numerically for $k = 1, 2, 3, 4$. We display a table that compares the estimates with actual sieving results. We display another table that shows the fraction of the work done and the fraction of solutions (full as well as partial) obtained as a function of B_0 and B_1.

References

[1] A. K. Lenstra and H. W. Lenstra Jr. (eds.), *The development of the number field sieve*, Lecture notes in Math. vol. 1554, Springer-Verlag, Berlin and Heidelberg, 1993.

[2] J. M. Pollard, *The lattice sieve*, in [1], pp. 4-10.

Gagan Garg Indian Institute of Sciences, Bangalore
gagan@csa.iisc.ernet.in

Differential Codes

Antonio Campillo López

AG-codes are constructed by evaluating rational functions which are defined in neigbourhoods of some fixed set of rational points over finite fields. Behaviour and applications of such codes depend not only on the vector subpace of considered functions, but, mainly, on the geometry of the considered rational points. The talk shows properties an applications of AG-codes obtained by evaluting at singular points of ordinary differential equations on algebraic varieties over finite fields.

Antonio Campillo López Dep. Álgebra, Geom. y Topología, Universidad de Valladolid
campillo@agt.uva.es

An Heuristic Algorithm for Finding Small Roots of Multivariate Polynomials over the Integers

Jaime Gutiérrez Gutiérrez

Joint work with: **Domingo Gómez and Álvar Ibeas**

In 1996, Coppersmith [8, 9, 10] introduced two rigorous lattice-based methods for finding small roots of polynomials: one for univariate modular and another one for bivariate integer polynomial equations. One of the main results is:

Theorem 1 (Theorem 2-[8]) *Let $p(\varepsilon_1, \varepsilon_2)$ be an irreducible polynomial in two variables over $\mathbb{Z}$, of maximum degree δ in each variable separately. Let Δ_1, Δ_2 be bounds on the desired solutions x_0, y_0. Define $p^*(\varepsilon_1, \varepsilon_2) = p(\varepsilon_1\Delta_1, \varepsilon_2\Delta_2)$ and let W be the absolute value of the largest coefficient of $p^*(\varepsilon_1, \varepsilon_2)$. If*

$$\Delta_1\Delta_2 \leq W^{2/(3\delta)-\varepsilon}2^{-14\delta/3},$$

then in polynomial time in $(\log W, \delta, 1/\varepsilon)$ we can find all integer pairs (x_0, y_0) with $p(x_0, y_0) = 0$ bounded by $|x_0| \leq \Delta_1, |y_0| \leq \Delta_2$.

The complicated proof of this important result is based on *lattice basis reduction*, with the so called LLL-technique (see [19]).

Lattice reduction techniques seem inherently linear. The general idea of this technique is to translate our non linear problem to finding a short vector in a lattice built from the nonlinear equation. Then, the so-called Shortest Vector Problem and Closest Vector Problem in lattices play a major role.

In recent years, these techniques have been used repeatedly for the cryptanalytic attack of various cryptosystems. Coppersmith's algorithm has many applications in cryptology: cryptanalysis of RSA with small public exponent when some part of the message is known, polynomial time factorization of $N = pq$ with high bits known and polynomial time factorization of $N = p^r q$ for large r; several papers have been published on different applications of those results in cryptology, see for instance [17, 6, 11, 15, 13, 18]. The paper [8] also proposed heuristic multivariate extensions for both approaches. The goal in this kind of method is to maximize the bounds up to which roots of the polynomials can be computed in polynomial time.

In this talk we present a method to compute small roots of a system of multivariate polynomial equations with integer coefficients simpler than other known algorithms for bivariate polynomials. Our heuristic algorithm is based on the same idea used for predicting nonlinear pseudorandom numbers, see [3, 4, 5, 12]. Despite we are not able to provide bounds to which common roots of the polynomials can be computed, we have implemented in C++ our approach showing that it works relatively well in practice.

The Algorithm

Let $f_1, \ldots, f_m$ be polynomials in the variables $x_1, \ldots, x_n$ with integer coefficients. Suppose that the associated polynomial system of equations has an unknown common zero

$(\varepsilon_1, \ldots, \varepsilon_n) \in \mathbb{Z}^n$ such that each component ε_i is bounded by some known integer bound $\Delta_i \in \mathbb{Z}$, that is, $|\varepsilon_i| \leq \Delta_i$, $i = 1, \ldots n$ and

$$\begin{aligned} f_1(\varepsilon_1, \ldots, \varepsilon_n) &= 0, \\ f_2(\varepsilon_1, \ldots, \varepsilon_n) &= 0, \\ &\vdots \\ f_m(\varepsilon_1, \ldots, \varepsilon_n) &= 0. \end{aligned} \tag{3}$$

Our main task is to design an efficient algorithm for computing the common zero $(\varepsilon_1, \ldots, \varepsilon_n) \in \mathbb{Z}^n$.

Basically, the algorithm is divided into several linearization steps.

First iteration: We construct a certain lattice $\mathcal{L}$. It depends on the Equation (3). We also show that a certain vector $\mathbf{E}$ directly related to missing information about $(\varepsilon_1, \ldots, \varepsilon_n)$ is a very short vector in the set $\mathbf{t} + \mathcal{L}$, where $\mathbf{t}$ depends on the bounds Δ_i and the coefficients of the polynomials f_i. A short vector $\mathbf{F}$ in $\mathbf{t} + \mathcal{L}$ is found; see [16, 1] for appropriate algorithms. If $\mathbf{F} = \mathbf{E}$ then the unknowns are discovered in this linearization step.

Second and more iterations: If $\mathbf{E} \neq \mathbf{F}$, then we express $\mathbf{E} - \mathbf{F}$ as a linear combination of a reduced basis of the lattice $\mathcal{L}$ with small unknown coefficients obtaining some new equations with new bounds. Then, we apply the previous technique to the lattice associated to that new equations and with these new bounds.

This process can be repeated as many times as desired in order to obtain better results.

References

[1] L. Babai, "On Lovasz Lattice Reduction and the Nearest Lattice Point Problem", *Combinatorica*, **6**, 1986, 1–6.

[2] T. Becker, V. Weispfenning, "Groebner bases. A computational approach to commutative algebra". In cooperation with Heinz Kredel. Graduate Texts in Mathematics, **141**. Springer-Verlag, New York, 1993.

[3] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, "Predicting nonlinear pseudorandom number generators", *Math. Computation*, **74** (2005), 1471–1494.

[4] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, "Predicting the inversive generator", *Proc. Coding and Cryptography, IMA-03*, LNCS **2898**, Springer-Verlag, Berlin 2003, 264–275.

[5] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, "Reconstructing noisy polynomial evaluation in residue rings", *Journal of Algorithms*. In press, S0196-6774(04)- 00115-4/FLA AID:1388. Available online.

[6] J. Bloemer, A. May, "A tool kit for Finding small roots of Bivariate Polynomial over the Integers", *Advances in Cryptology-Crypto 2003*, LNCS **2729**, Springer Verlag, 2003, 27–43.

[7] J.W.S. Cassels, "An Introduction to the Geometry of Numbers". Springer-Verlag, New York, 1971.

[8] D. Coppersmith: "Small solutions to polynomial equations and low exponent RSA vulnerabilities". *J. Cryptology* **10 (4)**, 1997, 233–260.

[9] D. Coppersmith: "Finding a Small Root of a Bivariate Integer Equations; Factoring with High Bits Known". U. Maurer (Ed), *Proc. EUROCRYPT-96*, LNCS **1070**, Springer-Verlag, Berlin 1996, 155–156.

[10] D. Coppersmith: "Factoring with a hint". *IBM Research Report RC. 1995*, January 16, 1995.

[11] J-S Coron, "Finding small roots of Bivariate Integer Polynomial Equations Revisted", *Proc. Advances in Cryptology- Eurocrypt'04*, LNCS **3027**, Springer Verlag, 2004, 492–505.

[12] D. Gomez-Perez, J. Gutierrez and A. Ibeas, "Cryptanalysis of the Quadratic generator", *Proceedings in Cryptology-INDOCRYPT 2005*, LNCS **3797**, Springer Verlag, Berlin 2005, 118–129.

[13] D. Gomez-Perez, J. Gutierrez and A. Ibeas, "Efficient Factoring Based on Extra Information", Preprint, University of Cantabria, Spain 2006. A preliminary version in Proc. Spanish Conference on Cryptography, RECSI-2006, Barcelona, September 2006.

[14] J.W.S. Gruber and C.G. Lekkerkerker, "Geometry of Numbers". North-Holland, 1987.

[15] N.A. Howgrave-Grahm, "Finding small roots of univariate revisted", *Proc. Cryptography and Coding*, LNCS **1355**, Springer Verlag, 1997, 131–142.

[16] R. Kannan, "Minkowski's convex body theorem and integer programming", *Math. Oper. Res.*, **12** (1987), 415–440.

[17] A. May, "Computing the RSA Secret Key is Deterministic Polynomial Time Equivalent to Factoring", *In Advances in Cryptology (Crypto 2004)*, LNCS **3152**, Springer Verlag, 2004, 213–219.

[18] Paul C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems". *Proc. CRYPTO-96*, LNCS **1109**, Springer-Verlag, Berlin 1996, 104–113.

[19] A. K. Lenstra, H. W. Lenstra and L. Lovász, "Factoring polynomials with rational coefficients", *Mathematische Annalen*, **261** (1982), 515–534.

[20] P.Q. Nguyen and J. Stern, "Lattice reduction in cryptology: An update", in: W. Bosma (Ed), *Proc. ANTS-IV*, LNCS **1838**, Springer-Verlag, Berlin 2000, 85–112.

[21] V. Shoup, "Number theory **C++** library (NTL)", version 5.3.1, available at `http://www.shoup.net/ntl/`.

[22] R. L. Rivest and A. Shamir: "Efficient factoring based on partial information". *Advances in Cryptology, Proc. EUROCRYPT-85*, LNCS **219**, Springer-Verlag, Berlin 1986, 31–34.

Domingo Gómez Pérez	Dep. Matemáticas, Estadística y Computación, Univ. Cantabria gomezd@unican.es
Jaime Gutiérrez Gutiérrez	Dep. Matemáticas, Estadística y Computación, Univ. Cantabria jaime.gutierrez@unican.es
Álvar Ibeas Martín	Dep. Matemáticas, Estadística y Computación, Univ. Cantabria alvar.ibeas@unican.es

Gröbner Bases and Cayley Digraphs
Álvar Ibeas Martín

Joint work with: **Domingo Gómez, Jaime Gutiérrez**

Cayley digraphs are usefull representations of the structure of a group. A simple particular case is formed by circulant graphs: the Cayley digraph of cyclic groups. This kind of graphs have been widely studied beacuase of their applications to computer networks.

In the case of an abelian group, the paths in a Cayley digraph can be identified to monomials. Then, one can build a certain monomial ideal which is a Minimum Distance Diagram of the graph. This is the initial ideal of a binomial ideal, and so, it can be computed using Gröbner Bases.

With that Minimum Distance Diagram, represented for instance by a system of generators, we can solve some problems on the graph:

- Routing Problem: finding a path among two vertices with minimum length.
- Diameter: compute the largest distance between pairs of vertices.
- Average Minimum Distance: compute the average distance.

References

[1] J.C. Bermond, F. Comellas, D.F. Hsu: "Distributed loop computer networks: a survey". J. Parallel and Distributed Computing, **24**, 2-10, 1995.

[2] D. Gómez, J. Gutiérrez, A. Ibeas: "Cayley digraphs of finite cyclic groups and monomial ideals". Preprint, 2005.

[3] E. Miller, B. Sturmfels: "Monomial Ideal and Planar Graphs". Proc. AAECC-13, LNCS **1719**, 19-28, 1999.

Domingo Gómez Pérez	Dep. Matemáticas, Estadística y Computación, Univ. Cantabria gomezd@unican.es
Jaime Gutiérrez Gutiérrez	Dep. Matemáticas, Estadística y Computación, Univ. Cantabria jaime.gutierrez@unican.es
Álvar Ibeas Martín	Dep. Matemáticas, Estadística y Computación, Univ. Cantabria alvar.ibeas@unican.es

3-Loop Networks can have arbitrarily many Minimum Distance Diagrams

Pilar Sabariego Arenas

Joint work with: **Francisco Santos**

Multi-loop networks were proposed by Wong and Coppersmith for organizing multi-module memory services [4].

The double-loop networks have been widely studied with the aid of the diagrams called *L-shapes*. It is well known that an *L-shape* for a double-loop network is a minimum distance diagram, MDD, which is a two-dimensional array that gives the shortest paths form one node to every other node. These diagrams are a strong tool in proving many properties for the double-loop networks, for example: for computing the diameter or the average minimal distance of the corresponding graphs.

By contrast, the MDD for a triple-loop network does not have a uniform nice shape like the *L-shapes* in dimension two, and this fact has made difficult the study of the properties of the triple-loop networks. For example, [1] proposed the study of a particular type of tiles that they called *hyper-L tiles* , but it was shown in [2] that these exist only for very special parameters of the network..

In this talk, building up on the relations between MDD's and monomial ideals shown in [3], we show that there exist three-loop networks with an arbitrarily big number of associated "coherent" MDD's, so finding a characterization of the MDD's for a three-loop network is going to be difficult. Here, we call an MDD coherent if it is indeed the diagram related to a monomial ideal. Equivalently, that if the shortest path from v_1 to v_2 in the MDD passes through a third vertex v_3, then the two subpaths induced are the shortest paths that the diagram gives from v_1 to v_3 and from v_3 to v_2.

References

[1] F. Aguiló, M.A. Fiol, C. García, Triple-loop networks with small transmission delay. *Discrete Math.* ***167/168*** (1997) 3–16.

[2] C. Chen, F.K. Hwang, J.S. Lee, S.J. Shih, The existence of hyper-L triple-loop networks. *Discrete Math.* ***268*** (2003) 287–291.

[3] D. Gómez, J. Gutierrez, A. Ibeas, Cayley Digraphs of Finite Cyclic Groups and Monomial Ideals *Preprint*. University of Cantabria (2006).

[4] C.K. Wong, D. Coppersmith, A combinatorial problem related to multimodule organizations. *J. Assoc. Comput. Mach.* ***21*** (1974) 392–402.

Pilar Sabriego Arenas Dep. Matemáticas, Estadística y Computación, Univ. Cantabria
pilar.sabariego@unican.es

Francisco Santos Leal Dep. Matemáticas, Estadística y Computación, Univ. Cantabria
santosf@unican.es

Quantum cryptology

Emilio Santos Corchero

In quantum theory the states of physical systems are represented by rays in a Hilbert space and the evolution by a unitary transformation of the space. On the other hand it is assumed that measurements produce an unpredictable change in the measured system. These properties may be used to devise procedures to transmit a key (a sequence of numbers 0 and 1) so that whenever between the sender and the receiver there is an eavesdropper, the receiver is able to detect its existence, so rejecting the key. There are several protocols for secure quantum key distribution using weak light signals (photons), some of them tested already experimentally. Specially simple is BB84, which will be studied in some detail.

Emilio Santos Corchero Dep. Física Moderna, Universidad de Cantabria
emilio.santos@unican.es

List of attendants

Mar Bezanilla	Universidad de Cantabria	mar.bezanilla@alumnos.unican.es
Simon R. Blackburn	Royal Holloway, London	s.blackburn@rhul.ac.uk
Cruz E. Borges	Universidad de Cantabria	cruz.borges@alumnos.unican.es
Antonio Campillo	Universidad de Valladolid	campillo@agt.uva.es
Jean-Charles Faugère	CNRS-INRIA, Paris	jean-charles.faugere@lip6.fr
Carlos Fernández	Universidad Complutense de Madrid	cafernan@mat.ucm.es
Gagan Garg	Indian Insititute of Science, Bangalore	gagan@csa.iisc.ernet.in
Domingo Gómez	Universidad de Cantabria	gomezd@unican.es
M^a Isabel González	Universidad Rey Juan Carlos, Madrid	mariaisabel.vasco@urjc.es
Jaime Gutiérrez	Universidad de Cantabria	jaime.gutierrez@unican.es
Llorenç Huguet	Universitat de les Illes Balears	l.huguet@uib.es
Álvar Ibeas	Universidad de Cantabria	alvar.ibeas@unican.es
Harald Niederreiter	National University of Singapore	nied@math.nus.edu.sg
Carles Padró	Universitat Politècnica de Catalunya	cpadro@ma4.upc.edu
Francesco Pappalardi	Università degli Studi Roma III	pappa@mat.uniroma3.it
Magdalena Payeras	Universitat de les Illes Balears	mpayeras@uib.es
Luis Pesquera	CSIC - Universidad de Cantabria	luis.pesquera@unican.es
Pilar Sabariego	Universidad de Cantabria	pilar.sabariego@unican.es
Emilio Santos	Universidad de Cantabria	emilio.santos@unican.es
Francisco Santos	Universidad de Cantabria	santosf@unican.es
Igor Shparlinski	Macquarie University, Sydney	igor@comp.mq.edu.au
Jorge Villar	Universitat Politècnica de Catalunya	jvillar@ma4.upc.edu
Bartosz Źrałek	Polish Academy of Sciences	b.zralek@impan.gov.pl