Journal of ELECTRICAL ENGINEERING, VOL. 52, NO. 7-8, 2001, 244–247

EDUCATION AND RESEARCH IN CRYPTOGRAPHY AT THE DEPARTMENT OF MATHEMATICS FEI STU IN BRATISLAVA

Otokar Grošek — Ladislav Satko *

A new era in cryptology is broadly dated to mid seventieth. In the same time we count the most fruitful period of the Semigroup Theory Seminar whose leading person was Professor Š. Schwarz. His non-trivial contribution to the coding theory, number theory and finite fields is know all over the world. This was a very good basis for some of his graduate students and co-workers to be forwarded to study different problems arising from cryptology, especially from an algebraic point of view. In 1984 we started to teach a course "*Secret communication in computer networks*" for postgraduate study (PhD) at the former EF SVŠT as the first in former Czechoslovakia. This course was attended by many experts of the whole ČSSR for more than 4 years. In the same year O. Grošek wrote the first Lecture Notes for these students. In 1985 O. Grošek (EF SVŠT) and K. Nemoga (MÚ SAV) decided to establish a new seminar CRYPTO. It was established in 1986 in cooperation with other people, like P. Volauf from KM EF SVŠT, Š. Porubský, O. Štrauch, I. Žembery, M. Laššák and S. Jakubec from MÚ SAV, P. Farkaš from KTL EF SVŠT and J. Vyskoč from VS SAV. CRYPTO-seminar was attended by experts from MFF UK, MÚ SAV, KM EF SVŠT and other scientific institutions. We were mainly reading the journal CRYPTOLOGIA, published in Indiana, USA. In that time, for us, this was the only one available journal in the field. CRYPTO-seminar temporarily ended in November 1989. Since the same year we started a cooperation with one of the best known centers all over the world in that time, namely in Lincoln, Nebraska.

In 1990 we opened a course *Ciphering* for all students of MFF UK and FEI STU. The publishing house GRADA has published the first monograph of this area in Slovak in 1992: *Šifrovanie — metódy, algoritmy, prax*, written by O. Grošek and Š. Porubský. (As far as we know, before there was written in ČSR only one publication by Jaromír Lichtner *Šifrování: Úvod do kryptografie chemické, grafické, čtyřidceti šifrovými klíči*. Alojz Srdce Pub. 1939.) In February 1993 our seminar started to work again at the Department of Mathematics FEI STU under new circumstances. A great challenge for founders had also been an offer for cooperation from the former director of the Central Security Agency of the Ministry of Interior, Ing. Eduard Puffler. In the school year 1996/97 the seminar was not public because of specific tasks solved for MV SR.

In 1995 the course Ciphering for regular students began, and there were set off the first Bachelor's projects and Diploma Theses in this area. These projects include both practical and theoretical problems of cryptology. Since the same year we have had graduate students in the field of 25-11-9 Applied Informatics, and also (since 1997) 11-14-9 Applied Mathematics.

Cryptology is unquestionably counted as one of the most attractive theories in both Applied Mathematics and Computer Science. Hence it is not surprising that there is a very close cooperation between our Department of Mathematics and Department of Computer Science and Engineering.

Since 2000/01 at the Department of Mathematics, and in cooperation with the Department of Computer Science and Engineering, we have had the first Masters degree students in the field of Security of Information Technologies. All of these activities allowed FEI STU in Bratislava to be the leading institution in Slovakia in the area of Applied Informatics, including Computer Security. There is a large cooperation with governmental institutions, *eg* Ministry of Interior (7 finished technical reports), Ministry of Defense (1 finished technical report), and National Bank of Slovakia (7 realized special seminars). Some parts of research projects may belong to the area of Applied Informatics and comprise problems lying within the scope of different parts of computer science, cryptology, algebra, informatics, and other parts of discrete mathematics. Given areas are getting closer, emphasize each other, interlace. Clearly, the borderline problems emerged. It seems that combining the methods characteristic for particular areas should be the approach how to solve them, *ie* to take a look at the problems from different points of view. To be a part of a solution of real problems, beginning 1996 we participate in grants in computer science. From our Department, in all projects have participated O. Grošek and L. Satko. Gradually they were followed by

* Department of Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak Technical University, Ilkovičova 3, 812 19 Bratislava, Slovakia, E-mail: grosek@kmat.elf.stuba.sk, satko@kmat.elf.stuba.sk

ISSN 1335-3632

Š. Porubský, K. Nemoga, H. Lichardová, M. Adámyová-Šimovcová, M. Vojvoda and M. Greško.

Next we are introducing principal results of the research projects in the field of cryptology where we contributed.

Discrete structures in combinatorics and algebra (1991-96)

Principal Investigator: Doc. RNDr. Peter Horák, Dr.Sc., (since 1994 O. Grošek)
This research project belonged to the area of pure mathematics. There were mathematicians working in algebra, cryptology and combinatorics participating in it. The program covered a wide spectrum of problems. More specifically we were studying various generalizations of a notion of ideal in semigroups, and possibility of their utilization in coding theory, cryptology and formal languages. In this program we cooperated with several universities, *eg* University of Nebraska, Simon Fraser University, McMaster University, University of Hawai, Computer and Automation Institute in Budapest, University of Tel Aviv, Milton Keynees University. The notion of A-ideal has its impetus in three notions as the notion of difference sets on groups (Bruck), mild ideals (Putcha) and quasy-zero (Ries). This notion has also been used in papers concerned with formal languages and cryptology, namely for the so-called access structures. The main result was in description of such structures especially in the case when difference sets do not exist. Our contributions described also a possibility of using Walsh-Hadamard transform to characterize finite semigroups and groups as well as an application of these results in design of so called S-boxes. Another problem arising from cryptanalysis of Markov block ciphers was to show to what extent it is possible to reconstruct a Markov Chain with finitely many states from a given (observed) finite but sufficiently large part of a trajectory. Here, by a reconstruction we mean finding as many as possible transition probability matrices leading to an estimated final probability distribution. This problem was solved with respect to the quasi-norm $\max p_{ij}$ of transient matrices belonging to a primitive idempotent.

We presented our results at 23 international conferences, including "A SEMIGROUP MEETING".This was the name of an international conference held on May 29–31, 1994 on the occasion of 80 years of Professor Štefan Schwarz. The organizing and Program Committee (K.H. Hofmann, Š. Porubský, L.N. Shevrin, L. Satko and O. Grošek), decided to present to the participants of the conference an outline of branches of mathematics to which professor Schwarz has mainly contributed. Of course, results related to cryptology were included too.

Another event was a visit of the famous mathematician Paul Erdös from the Hungarian Academy of Sciences. During his stay, Sep. 23–29, 1994 he gave a lecture "Problems in Combinatorics and Number theory". At the same time P. Horák solved together with Erdös one of his colouring problems.

Intelligent support of software development (1996)

Principal Investigator: Prof. Ing. Pavol Návrat, PhD., (CSE Department)
Department of Mathematics joined this project in the last year of its duration only. Our contribution consisted of a study of DES-like cryptosystems, and a study of the so-called bent-like functions on quasi-groups, a very perspective construction which has been involved by us, and referred in the USA and Greece. We also started in giving special classes for extra talented students interested in the field, and getting on in projects of breaking practically DES and McEliece cryptosystems. Further, in designing an on-line cryptosystem based on IDEA and Blowfish as well as to design an applicable electronic cash model at least in a local network. Moreover we organized a Summer School on Cryptanalysis in Liptovský Mikuláš. There were presented current methods to break stream ciphers. The conference was organized in cooperation with MÚ SAV and Military Technical Institute in Liptovský Mikuláš. We presented our results at 6 international conferences.

Methods and tools for software systems development (1997-99)

Principal Investigator: Prof. RNDr. Ľudovít Molnár, Dr.Sc., (CSE Department)
Main goals in the area of Cryptology and Discrete Structures were to study methods of finding suitable Boolean functions for DES-like cryptosystems, algorithms for finding strong primes on the basis of Pockhlington lemma, acceptable by all short exponents up to 1024 bits, and Complexity Theory of RSG based on Luby-Rackoff lemma. We took advantage of a close cooperation with the Department of Mathematics, Institute of Chemical Technology, Prague, CZ; Computer Science Department, University of Nebraska, Lincoln, USA and Computer Science Department, De Montfort University, Milton Keynees, GB. During this project, members of the research team participated in domestic and international conferences with their own contributions.

We analyzed a collision attack, applied to the modified GOST algorithm, and proved that if non-bijective S-boxes are used in the algorithm, then it is feasible to break it when a weak key is in use.

Studying a specific random number generator we proved that the approach to this type of generators by U. Maurer is different to that of Luby-Rackoff, serving a new sight in classification of random sequences. We also focused on RSA algorithm and proved that approximately 3 % of randomly generated 512 bits long strong primes can be used with arbitrary short exponent, $s = 2^k + 1$, $0 < k < 1024$. By our experiments, all corresponding

decryption exponents are as large that it is impossible to use the attack based on the so-called continuous fractions. Another obtained result was how to find to a given message x RSA parameters such that this message would not be encrypted. Inspired by VanTilbourgh attack to McEliece cryptosystem we built up a simplest Markov model and found a new bound for complexity of it. Antal in his MSc Thesis showed how to break one linear randomized additive stream cipher. Finally, we described a class of semigroups completely characterized by the so-called traces of Walsh-Hadamard transform.

Studying stream ciphers we did cryptanalysis of one clock-controlled running key generator, and found explicit equations for this generator. Computer simulation has shown a large linear complexity and long period of the produced keystream sequence. The generator is resistant to fast correlation attacks but fails to a known plaintext attack.

We presented our results at 22 international conferences.

In September 1998 we started, in cooperation with the Ministry of Interior and the National Bank of Slovakia, special seminars for people working in financial e-banking and related areas. By the end of 2000 there were seven of them. The number of participants varies from 15 to 30, and during this period they got more than 1200 pages of lecture notes. Details are available on our web-page (http://www.elf.stuba.sk/Katedry/KM/crypto).

Methods and tools of information and knowledge discovery, representation, presentation and searching 2000-2002

Principal Investigator: Doc. Ing. Vladimír Vojtek, PhD.,

Targets of this project can be divided into several parts. On the basis of the so-called A-ideals we would like to design a new generation of S-boxes, a main nonlinear part of any iterated DES-like cryptosystem. Further, we are trying to distinguish S-boxes by new criteria, namely via all groups of order 16. Concretely, Pieprzyk suggested to study *mod* 16 linear behavior of DES S-boxes. Using our experience in the semigroup theory, translations and morphism of such structures we would like to study this kind of attack in general. Concerning stream ciphers, we will study several constructions of pseudorandom sequences with good non-linearity, difference parameters, correlation immunity and spectral properties. We would like to involve students to the theory via specialized seminars, semester projects and diploma theses. Following this we are heading them towards trying to repeat some successful attacks on DES-like cryptosystems using parallel programing and special sophisticated sorting algorithms. The expected contribution is of both theoretical and practical nature and will serve to the further development of cryptology. We are focusing on problems belonging nowadays to the centre of interest in the field.

Up to these days we presented our results at 17 international conferences. O. Grošek was an invited speaker at CITEDI-IPN, Tijuana, Mexico where he gave two lectures for graduate students, and at University Autonomia de Baja California in Ensenada, Mexico a plenary lecture.

Partial results are as follows:

- In S-box theory: It is well known that there does not exist a Boolean function $f\colon Z_2^n \to Z_2^m$ satisfying both basic cryptologic criteria, balancedness and perfect nonlinearity. For n even, $n \geq 2m$, a construction which so far closest to the target is due to Nyberg. In her construction she used slightly unbalanced functions, namely bent functions. These functions satisfy also a condition of the minimal mutual input/output information. We proved that if we use as a domain a quasigroup instead of the group Z_2^n one can construct functions which are at the same time balanced and perfectly nonlinear. Such functions have a completely flat difference table. By using techniques previously invented, we found a construction of perfectly non-linear bijective S-boxes. For the time being, our results are more theoretical than practical. They show that such a change of domain might bring new ideas to cryptography. Here we mention two possible applications. The first one is when a message $x \in S$ is scrambled by a function F to a bit string $F(x) \in Z_2^m$. Another example is a counter counting in some order elements of S. The arguments $x \in S$ are successive elements of S, possibly parametrized with a key, and the output sequence are blocks of bits, or their conversion to integers from the given range.
- We also studied Qu and Vanstone's results related to the security of Webb's public-key cryptosystem. We proved that their results could be simplified significantly. Besides, it is desirable to know how to construct all the factorizations of the Elementary Abelian p-group. This problem can be solved immediately from our constructive treatment.
- A survey article with an original approach to cryptographic algorithms as permutations on a finite set with a properly chosen algebraic structure was introduced too.
- There are well known design principles for block ciphers introduced by Lai. We analyzed two AES candidates, namely MARS and Serpent relative to the Lai's classification of the round functions. The aim was to decide if the Lai's classification is enough for classification of the round functions of MARS and Serpent. The result is that Serpent can be viewed as a generalization of the Type II (Lai's classification), and MARS provides a new type with respect Lai's classification.
- Additive stream cipher systems are based on a deterministic generation of a pseudorandom keystream sequences. A ciphertext is then produced as a modular addition of the plaintext and the keystream. For keystream sequences for additive synchronous stream ciphers there are some common cryptographic measures of their strength (unpredictability, randomness, *etc*). In our contribution we studied some properties of selected k-distributed sequences from the point of view of cryptology. A simple

construction of such a k-distributed binary sequence was given by Ford. The uniformity of the distribution of k-tuples follows from the construction of this sequence. This is an opposite approach to that one, used in T.W. Cusick, C. Ding, A. Renvall. Analysis using computer simulations shows that the Ford's sequence appears to have large linear complexity. There were observed some other weaknesses in the distribution of difference parameters. This work also shows that a usage of a pseudorandom sequence in cryptology must be considered in a more complex manner, *ie* statistical and special cryptographic properties should be studied together.

- In our research, we are also concentrated on cryptanalysis of Clock-Controlled Running Key Generators. One simple running key generator which combines the outputs of two asynchronously clocked LFSRs was analysed. The period of the keystream and several theorems concerning the number of runs in a ml-sequence has been proved. Results of applied statistical tests (FIPS 140-1, gap test, serial correlation test) were presented. Finally, a modification of the generator using substitution of FCSRs (feedback with carry shift registers) for LFSRs was studied too.
- Another part of our research was motivated by results on amplified weak-unpredictability obtained by concatenating the values of the function on several independent instances, due to O. Goldreich, N. Nisan, A. Wigderson. A slightly different approach to the design of a completely equidistributed pseudorandom sequence based on concatenation of k-distributed sequences was given by Knuth. We proposed a new construction of a completely equidistributed sequence based on concatenation of (almost k-distributed) ml-sequences. Next we study local properties of this sequence, namely concatenation of two ml-sequences. Our analysis, using exhaustive computer simulations, shows that the concatenation of two ml-sequences has large linear complexity and moderate "out-of-phase" autocorrelation function magnitudes. It appears that concatenation of ml-sequences may bring interesting design ideas in the field of keystream generators.

In June 2001, we organized an international conference TATRACRYPT '01. For details see the site:

http://www.elf.stuba.sk/Katedry/KM/crypto/Slovak/konf/index.html

A list of people working in the field beyond the borders is nearly endless. Thus, continuing in our CRYPTO seminar, organizing workshops participated by leading experts in the field, and ourselves participating in foreign conferences we would like to be both informed, and inform researchers about our recent results. Moreover, since there are many particular problems which might be solved by students, some particular results are gained also by semester and diploma projects. Up to these days 3 people finished their PhD theses, and 15 Master theses related to cryptology have been finished. Members of our CRYPTO group have published 41 scientific papers, and 23 other papers related to cryptology. At present we have 8 graduate students.

Received May 31, 2001

Otokar Grošek (Prof, RNDr, PhD), graduated at the Comenius University (1973), assigned to Professor Š. Schwarz as a graduate student (CSc-1978), (Prof-1998). He is working at the Department of Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava. Since 1983 he is working in cryptology.

Ladislav Satko (Doc, RNDr, PhD), graduated at the Comenius University (1962), assigned to Professor Š. Schwarz as a graduate student (CSc-1978), (Assoc Prof-1984). He is head of the Department of Mathematics, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava. Since 1983 he is working in cryptology.