Report on Indocrypt2010

Attendee: about 200 researchers from many countries (Japan, America, Canada, Germany, Belgium, Ireland, Turkey, etc.)

Time: December 12-15, 2010

Invited Talks on the Workshop:

Title: Lightweight Cryptography for RFID Systems

Speaker: Professor Guang Gong
Abstract: Radio frequency identification (RFID) is a technology for the automated identification of physical entities using radio frequency transmissions. In the past ten years, RFID systems have gained popularity in many applications, such as supply chain management, library systems, e-passports, contactless cards, identification systems, and human implantation. RFID is one of the most promising technologies in the field of ubiquitous and pervasive computing. Many new applications can be created by embedding an object with RFID tags. However, the rapid development of RFID systems raises serious privacy and security concerns that could prevent the benefits of RFID technology from being fully utilized. The tutorial covers three topics: a) Introduction to Security and Privacy of RFID Systems, b) Design of Lightweight Crypto primitives; c) Design of Authentication Protocols.

Title: Pairing Based Cryptography

Speaker: Professor Sanjit Chatterjee
Abstract: Bilinear pairing is now a well-accepted mathematical tool to build new cryptographic applications. This might appear a little paradoxical because not so long ago the same mathematical structure was considered as a main deterrent to the deployment of elliptic curve cryptography. The tutorial aims to trace the story of this changed perception in the crypto community. The narration is based on some novel construction of cryptographic protocols with an eye on the interplay of functionality, security and efficiency.

The Conference Presentations:
(1) Getting a Few things right and many things wrong
Speaker: Neal Koblitz

Content: Professor Neal Koblitz gives a very good presentation about the research on the cryptography. First, he illustrated the pitfalls of working in cryptography by giving a (far from exhaustive) survey of the many misjudgments he have made and erroneous beliefs he

has had over the course of 25 years working in this field. Then, Professor Neal Koblitz described a few of the embarrassing moments in the history of provable security, which is the name of an ambitious program that aims to transform cryptography into a science.

(2) Partial Key Exposure attack on RSA-Improvement for Limited lattice Dimensions
Speaker: Santanu Sarkar, Sourav Sen Gupta, and Subhamoy Maitra

Content: In this paper, the authors presented a variant of their method which provides better experimental results depending on practical lattice parameters and the values of d. We also propose a sublattice structure that improves the experimental results significantly for smaller decryption exponents.

(3) Towards Provable security of the unbalanced oil and vinegar signature scheme under direct attacks
Speaker: Stanislav Bulygin, Albrecht Petzoldt, and Johannes Buchmann

Content: In this paper, the authors show that solving systems coming from the public key of the Unbalanced oil and vinegar (UOV) signature scheme is on average at least as hard as solving a certain quadratic system with completely random quadratic part. The authors rely on the empirical fact that complexity of solving a non-linear polynomial system is determined by the homogeneous part of this system of the highest degree.

(4) Cyclicrainbow-A Multivariate Signature Scheme with a Partially Cyclic Public Key
Speaker: Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann

Content: In [PB10] Petzoldt et al. proposed a way how to reduce the public key size of the UOV scheme by a large factor. In this paper, we extend this idea to the Rainbow signature scheme of Ding and Schmidt [DS05]. By our construction it is possible to reduce the size of the public key by up to 62%.

(5) Combined Security Analysis of the One-and Three-Pass Unified Model Key Agreement Protocols
Speaker: Sanjit Chatterjee, Alfred Menezes, and Berkant Ustaoglu

Content: This paper revisit the security of the one-and three-pass UM protocols when static key pairs and reused. The authors propose a shared security model that incorporaes the individual security attributes of the two proticols. The authors then show, provided appropriate measures are taken, that the protocols are secure even when static key pairs are reused.

(6) Indifferentiability beyond the birthday bound for the xor of two public random permutations
Speaker: Avradip Mandal, Jacques Patarin, and Valerie Nachef

Content: This paper is to get the precise security results for this constructuon when the two permutations on n bits f and g are public. The authors first prove that f $\oplus$ g is indifferentiable from a random function on n bits when the attacker is limited with q queries. This bound can be called birthday bound. The author also prove that this bound can be improved to $q^3<<2^{2n}$.

(7) The characterization of Luby-Rachoff and Its optimum single-key Variants
Speaker: Mridul Nandi

Content: based on the former structure--Luby-Rackoff encryption structure, The author studies the long-standing open problem and (informally) prove the following: LR is secure if its *key-assigning* is not palindrome (i.e. the order of key indices is not same with its reverse order). The author also research the class of LR-variants where some of its round functions can be tweaked (our previous characterzation would bot work for the variants). The authors propose a single-key LR-variant SPRP, denoted by LRv, making only four invocations of the PRF. The author also show that a PRP-distinguishing attack on a wide class of single-key, LR-variants with three PRE-invocations.

(8) Versatile Pret a Voter: Handling Multiple Election Methods with a Unified Interface
Speaker: Zhe Xia, Chris Culmame, James Heather, Hugo Jonker, Peter Y. A. Ryan, Steve Schneider, and Sriramkrishnan Srinivasan

Content: This paper introduces a scheme which handles many of the popular election methods that are currently used around the world. The proposed method not only ensures privacy, receipt-freeness and end-to-end verifiability, but also keeps the voter interface simple and consistent between various election methods.

(9) Cryptographic hash function theory and practice
Speaker: Bart Preneel

Content: Professor Perneel introduces the situation of the development of the hash function. Until 2005, the amount of theoretical research and cryptanalysis invested in this topic was rather limited. From the hundred designs published before2005, about 80% was cryptanalyzed. The serious shortcomings have been identified in the theoretical foundations of existing designs. In response to the hash function crisis, a large number of papers have been published with theoretical results and novel designs. In November 2007, NIST announced the start of the SHA-3 competition. Professor Perneel presents a brief outline of the state of the art of hash function half-way the competition and attempt to identify open research issues.

(10) Cryptanalysis of Tav-128 hash function
Speaker: Ashish Kumar, Somitra Kumar Sanadhya, Praveen Gauravaram, Masoumeh Safkhani, Majid Naderi,

Content: Tav-128 is one 128-bit light weight hash function proposed by Peris-Lopez et al. for a low-cost RFID tag authentication protocol. Apart from some statistical tests for randomness by the designers themselves, Tav-128 has not undergone any other thorough security analysis. Based on these tests, the designers claimed that Tav-128 does not posses any trivial weaknesses. In this article, the author carry out the first third party security analysis of Tav-128 and show that this hash function is neither collision resistant nor second preimage resistant. The authors first show a practical collision on Tav-128. Then, the authors show a second preimage attack on Tav-128. Finally, the authors study the constituent functions of Tav-128 and show that the concatenation of nonlinear functions A and B produces a 64-bit permutation from 32-bit messages. This could be a useful light weight primitive for future RFID protocols.

(11) Near-collisions for the reduced round versions of some second round SHA-3 compression functions using hill climbing
Speaker: Meltem Sonmez Turan, Erdener Uyan

Content: A hash function is near-collision resistant, if it is hard to find two messages with hash values that differ in only a small number of bits. In this paper, the author use hill climbing methods to evaluate the near-collision resistance of some of the second round SHA-3 candidates.

(12) Speed up the wide-pipe: secure and fast hashing
Speaker: Mridul Nandi, Souradyuti Paul

Content: This paper proposes a new sequential mode of operation-the fast wide pipe or FWP for short-to hash messages of arbitrary length. The authors also compare the FWP with several other modes of operation.

(13) New Boomerang attacks on ARIA
Speaker: Ewan Fleischmann, Christian Forler, Michael Gorski, Stefan Lucks,

Content: In this paper, the author presents three new attacks of reduced round ARIA which shows some weaknesses of the cipher. Moreover, the proposed attacks have the lovest memory complexity compared to existing attacks on ARIA.

(14) Algebraic, AIDA/Cube and Side Channel Analysis of KATAN Family of block ciphers
Speaker: Gregory V. Bard, Nicolas T. Courtois, Jorge Nakahara Jr. Pouyan Sepehrdad, and Bingsheng Zhang

Content: This paper presents the first results on AIDA/cube, algebraic and side-channel attacks on variable number of rounds of all members of the KATAN family of block ciphers. The proposed cube attacks reach 60, 40, and 30 rounds of KATAN32, KATAN48

and KATAN64, respectively. In this algebraic attacks, the author use SAT solvers as a tool to solve the quadratic equations representation of all KATAN ciphers. The author introduces a novel pre-processing stage on the equations system before feeding it to the SAT solver.

(15) The Improbable differential attack: Cryptanalysis of reduced round CLEFIA
Speaker: Cihangir Tezcan

Content: In this paper, the author proposes a new statistical cryptanalytic technique that we call improbable differential cryptanalysis which uses a differential that is less probable when the correct key is used. The author provide data complexity estimates for this kind od attacks and also show a method to expand impossible differentials to improbable differentials.

(16) Greedy distinguishers and Nonrandomness detectors
Speaker: Paul Stankovski

Content: The author present the concept of greedy distinguishers and show how some simple observations and the well known greedy heuristic can be combined into a very powerful strategy (the Greedy bit set algorithm) for efficient and systematic construction of distinguishers and nonrandomness detectors. We show how this strategy can be applied to a large array of stream and block ciphers, and the author show that the proposed method outperforms every other method.

(17) Polynomial Multiplication over Binary Fields Using Charlier Polynomial Representation with Low Space Complexity
Speaker: Sedat Akleylek, Murat Cenk, and Ferruh Ozbudak

Content: In this paper, the author give a new way to represent certain finite fields $GF(2^n)$. This representation is based on Charlier polynomials. The authors show that multiplication in Charlier polynomial representation can be performed with subquadratic space complexity. One can obtain binomial or trinomial irreducible polynomials in Charlier polynomial representation which allows us faster modular reduction over binary fields when there is no desirable such low weight irreducible polynomial in other representations.

(18) Random Euclidean Addition Chain Generation and Its Application to Point Multiplication
Speaker: Fabien Herbaut, Pierre-Yvan Liardet, Nicolas Meloni, Yannick Teglia, and Pascal Veron

Content: This paper proposes to modify the key generation process using a small Euclidean addition chain c instead of a scalar k. This can allow to use a previous scheme, secure against side channel attacks, but whose efficiency relies on the computation of small chains computing the scalar. The authors propose two different ways to generate short Euclidean

addition chains and give a first theoretical analysis of the size and distribution of the obtained keys. The authors also propose a new scheme in the context of fixed base point scalar multiplication.

(19) Attack on a higher-order masking of the AES based on homographic functions
Speaker: Emmanuel Prouff, Thomas Roche

Content: In this context, the development of sound and practical countermeasures against attacks of arbitrary fixed order d is of crucial interest. Surprisingly, while many studies have been dedicated to the attacks, only a very few methods have been published that claim to provide security against d^{th}-order side channel attacks whatever the order d. Among them, the one proposed by Courtois and Goubin at ICISC2005 was especially interesting due to its great efficiency. In this paper, the author show that the method is however flawed and the author exhibit several higher-order attacks that can defeat the countermeasure for any value of d.

(20) Improved impossible differential cryptanalysis of 7-round AES-128
Speaker: Hamid Mala, Mohammad Dakhilalian, Vincent Rijmen, and Mahmoud Modarres-Hashemi

Content: Using a new 4-round impossible differential in AES that allows us to exploit the redundancy in the key schedule of AES-128 in a way more effective than previous work, the author present a new impossible differential attack on 7 rounds of this block cipher. By this attack, 7-round AES-128 is breakable with a data complexity of about 2^{106} chosen plaintexts and a time complexity equivalent to about 2^{110} encryption.

(21) Cryptanalysis of a perturbated white-box AES implementation
Speaker: Yoni De Mulder, Brecht Wyseur, and Bart Preneel

Content: In this paper, the authors present an algebraic analysis to recover equivalent keys from the implementation. The author show how the perturbations and system of random equations can be distinguished from the implementation, and how the linear input and output encodings can be eliminated.

(22) A Program Generator for Intel AES-NI Instructions
Speaker: Raymond Manley, David Gregg

Content: The authors present a program generator that creates optimized AES code automatically from a simple, annotated C version of the code. The author show how this generator can be used to rapidly create highly optimized versions of several AES modes. The resulting code generated has performance that is equal to, or up to 7% faster than the hand-tuned assembly libraries from Intel.

(23) ECC2K-130 on NVIDIA GPUs

Speaker: Daniel J. Bernstein, Hsieh-Chung Chen, Chen-Mou Cheng, Tanja Lange, Ruben Niederhagen, Peter Schwabe, and Bo-Yin Yang

Content: This paper explains how to optimize the ECC2K-130 computation for this unusual platform. The resulting GPU software performs more than 63 million iterations per second, including 320 million $F(2^{131})$ multiplications per second, on a $500 NVIDIA GTX 295 graphics card. The same techniques for finite-field arithmetic and elliptic-curve arithmetic can be reused in implementations of larger systems that are secure against similar attacks, making GPUs an interesting option as coprocessors when a busy Internet server has many elliptic-curve operations to perform in parallel.

(24) One byte per clock: A novel RC4 hardware
Speaker: Sourav Sen Gupta, Koushik Sinha, Subhamoy Maitra, and Bhabani P. Sinha

Content: In this paper, the authors take a fresh look at the hardware implementation of RC4 and propose a novel architecture which generates 1 key-stream byte per clock cycle. The strategy considers generation of two consecutive key-stream bytes by unwrapping the RC4 cycles. The same architecture is customized to perform the key scheduling algorithm at a rate of 1 round per clock.