Annual Research Review Seminar for NSERC Strategic Project Grant Collaborated with RIM

University of Waterloo
December 3, 2008

Organizers: Guang Gong
Anwar Hasan
Herb Little

A Collection of Abstracts of Presented Talks

1. On Practicality of Identity-Based Batch Verification

Xinxin Fan

As we move into the ear of pervasive computing, where computers and various mobile devices with embedded processors are everywhere and constantly communicate with their environments, there are going to be a host of devices exchanging messages with each other, e.g., Mobile Ad Hoc Networks (MANETs), Wireless Sensor Networks (WSNs), Vehicular Ad Hoc Networks (VANETs), etc. For these systems to work properly, system designers are facing the problem on how to efficiently authenticate messages. Any cryptographic solutions should meet the following requirements simultaneously: (1) cryptographic overhead remain low, and yet (2) a large number of messages from many different signers can be verified very quickly. Traditional public key infrastructure (PKI) based authentication mechanisms are hard to meet the stringent time requirement in pervasive computing environment since an receiver need to verify both certificates and messages from many senders. Although researchers also have developed efficient hash chain based message authentication technique which uses time-delayed key release so that the necessary verification keys are delivered after the authenticated messages arrive, this approach requires loose clock synchronization between the sender and receivers and does not provide other desirable features such as non-repudiation of messages (for the purpose of identifying malicious users).

In this work, we consider the batch verification of an identity-based signature (IBS) scheme based on Elliptic Curve Discrete Logarithm Problem (ECDLP), so called BNN-IBS scheme, proposed by Bellare et. al. in 2004. With the BNN-IBS scheme, the use of certificates is eliminated and a successful signature verification shows the receiver two things at the same time: (1) the signature

has been created by the sender using his/her private key which is behind his ID; and (2) his/her ID is certified by a trusted third party (TTP), and it is the result of the TTP?s certification of his/her ID that has enabled the sender to create the signature. We also implement the BNN-IBS scheme and its batch verification using a Koblitz curve defined over $GF(2^{163})$.

2. Exotic Number Systems for ECC

Nicolas Mloni

In this talk, we will deal with efficient implementation of Elliptic Curve Cryptography using some "exotic" number systems. The Residue number system will be used to represent field elements and to perform field multiplications. We will also introduce the Zeckendorf representation and the euclidean addition chains, that will be used to perform the point scalar multiplication.

3. MIMO and LDPC Based Schemes for Physical Layer Security in Wireless Networks

Hong Wen

Compared with wireline networks, wireless networks lack a physical boundary due to the broadcasting nature of wireless transmissions. The wireless security has become a critical concern in the physical layer. Physical-layer security techniques, which are based on the shannon secrecy model are effective in resolving the boundary, efficiency and link reliability issues. The built-in security of the physical-layer is defined as the physical-layer transmissions which guarantee low probability of interception (LPI) based on transmission properties such as modulations, signals and channels, without resorting to source data encryption. No secret keys are required before transmissions. In this presentation, we will introduce our recent works about a cross layer MIMO based security scheme and a LDPC based perfect secrecy system. In the first scheme, the physical-layer can utilize upper-layer encryption techniques for security, while physical-layer security techniques can also assist the security design in the upper-layer. In the second scheme, we use the feedback to hide the information stream in the additional noise impairing the adversary by using the random sequence that only be known between the legitimate partner. No secret key is preshared, we can approach the perfect secrecy.

4. Error Detection and Recovery in EC Scalar Multiplication

Abdulaziz Alkhoraidly

Faults can corrupt data in storage, in transient, or during a computation. Like other digital systems, cryptosystems are vulnerable to natural and artificial

faults. However, the effects of faults on cryptosystems far suppress the corruption of data. Attacks that exploit various classes of faults to learn secret data have been proposed and shown to be practical. As such, efficient detection and recovery of errors resulting from faults have a growing importance in the design of cryptosystems. We review existing error detection and recovery schemes for elliptic curve scalar multiplication and give a brief evaluation. Then, we propose the use of frequent validation and checkpointing during the scalar multiplication for more efficient error detection and recovery. In our approach, the scalar multiplication iterations are grouped into blocks and simple, efficient error detection schemes are used to detect errors early, which significantly limits the propagation of corrupted data. Moreover, we use the same error detection schemes to achieve efficient error recovery without requiring complete time and hardware redundancy. Our analysis illustrates that these modifications enable considerably more efficient and reliable structures relative to known error detection and recovery designs.

5. On the Security of Pseudorandom Sequences Generated via the Additive Order

Honggang Hu

The additive order is related to the counter-mode encryption (CTR mode encryption) of block ciphers. CTR mode encryption turns a block cipher into a stream cipher. The next keystream block is generated by encrypting successive values of a "counter". The additive order is also related to some Golay complementary sequences which can be used in orthogonal frequency-division multiplexing (OFDM) applications. For example, a well-known construction found by Davis and Jedwab in 1999 uses the additive order. Compared with the conventional order in sequence generation, the behavior of the sequences from the additive order is much different. Suppose that a sequence generated via the conventional order has good pseudorandom properties. However, the sequence generated by the same function via the additive order may not have good pseudorandom properties. We present a simple example to show this phenomena. Moreover, some general conditions are given under which such sequences generated via the additive order have maximal period and low autocorrelation. Based on some numerical data, a conjecture is proposed.

6. Two Bitwise-Operation-Based Entity Authentication Protocols

Zhijun Li

The surprisingly simple and elegant HB+ entity authentication protocol, presented by Juel and Weis at Crypto 2005, is very suitable for low-cost pervasive computing devices, such as RFID tags and sensor nodes. However, despite an gentle security proof under its limited attack model, HB+ is vulnerable to

a GRS man-in-the-middle attack that allows an adversary to recover the secret authentication key. In this talk, we present two HB+ variants: HB-RR protocol and HB-CM protocol, using the techniques of random rotation and circulant matrix encoding respectively. We develop a mathematica model of rotational equivalence class to analyze proposed protocols. Then we prove that the two protocols remain the same security level in the model of HB+, with additional trivial requirement. Furthermore, HB-RR and HB-CM can resist general man-in-the-middle attacks, including the original GRS attack. Meanwhile, HB-CM achieves much better communication performance.