Research Review Seminar for NSERC Strategic Project Grant Collaborated with RIM

University of Waterloo
February 25, 2010

Organizers: Guang Gong
Anwar Hasan

Projects under Review:

a) Multi-functional Modular Authenticators for Security in Ad Hoc Networks, 2007-2009 (extended to April 2010)

b) Platform Security and Content Protection, 2009-2011

A Collection of the Abstracts of Presented Talks

1. Selective DFT Attacks on Stream Ciphers and the Spectral Immunity of Boolean Functions

Honggang Hu

In this talk, we present two kinds of new attacks on stream ciphers based on linear feedback shift registers (LFSR): selective discrete Fourier transform (DFT) attacks and fast selective DFT attacks. Although these new attacks are closely related to algebraic attacks and fast algebraic attacks, respectively, they work for the case when the known attacks fail, i.e., when the Boolean functions employed are well-designed for meeting cryptographic requirements. The fast selective DFT attack is more efficient than known methods for the case when the number of observed consecutive bits of a filtering sequence is less than the linear complexity of the sequence. In general speaking, algebraic attacks can be considered as attacks in the time domain, while (fast) selective DFT attacks are the attacks launched in the DFT frequency domain. The remarkable phenomenon is that with such an attack launched in the frequency domain, the number of unknowns in the system of linear equations is invariant. However, in the algebraic attacks or fast algebraic attacks, this number is changed at different time instances. Thus, by utilizing the natural representation imposed by the underlying LFSRs, the analysis in terms of DFT spectra is more efficient and has more flexibility than algebraic attacks and fast algebraic attacks. Consequently, the selective DFT attack imposes a new criterion for the design of cryptographic strong Boolean functions. As an analogue to the algebraic immunity of a Boolean function, the new criterion is referred to as the spectral immunity of a Boolean function. One example of Boolean function with large algebraic immunity but low spectral immunity is provided.

Joint work with Guang Gong, Sondre Rønjom, and Tor Helleseth.

2. An Adaptive Idle-Wait Countermeasure Against Timing Attacks on Public-Key Cryptosystems

Carlos Moreno

Successful timing attacks against public-key cryptosystems have been demonstrated in many forms, suggesting the use of a technique known as *blinding* as countermeasure to these attacks.

Though somewhat overlooked and not well studied in existing literature, an alternative countermeasure has been considered, consisting of idle-wait to make the decryption time independent of the data. In this work, we propose and implement an optimized form of this countermeasure, making the idle-wait *adaptive*, with the goal of minimizing the performance penalty. We present both analytical and experimental results of simulations designed to evaluate our method's performance and effectiveness, and compare it against alternative countermeasures.

Joint work with Anwar Hasan.

3. Compressing Pairing Values

Koray Karabina

Bilinear pairings derived from supersingular elliptic curves of embedding degrees 4 and 6 over finite fields of characteristic two and three, and derived from supersingular hyperelliptic curves of embedding degrees 12 over finite fields of characteristic two have been used to implement pairing-based cryptographic protocols. The pairing values lie in certain prime-order subgroups of certain cyclotomic subgroups. We show how the pairing values over characteristic two and three fields can be compressed by a factor of 4 and 6, respectively. Our compression and decompression functions can be computed at a negligible cost and hence they can be nicely incorporated into a wide range of pairing-based cryptographic applications that require exponentiation or product of pairings.

Joint work with Alfred Menezes.

4. Adaptive Recovery for Transient Errors in Elliptic Curve Scalar Multiplication

Abdulaziz Alkhoraidly

Attacks exploiting various classes of faults to weaken cryptosystems and learn secret data have been proposed and shown to be practical. As such, efficient detection and recovery of errors have a growing importance in the design of cryptosystems. We address the problem of transient faults in elliptic curve scalar multiplication implementations. In particular, we propose the use of frequent validation during the scalar multiplication with an adaptive block size to achieve efficient and reliable error recovery. In our approach, the scalar multiplication is divided into blocks of iterations and efficient error detection schemes are used frequently to detect errors at the end of each block. Moreover, block sizes are modified in run-time based on the occurrence or absence of errors. This reduces the recomputation overhead and the loss due to errors by limiting the propagation of corrupted data. In addition, it doesn't require setting the optimal block size prior to the computation. Our analysis illustrates that these modifications enable considerably more efficient and reliable structures relative to known error recovery designs.

Joint work with Anwar Hasan.

5. Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices

Xinxin Fan

Due to the tight cost and constrained resources of high-volume consumer devices such as RFID tags, smart cards and wireless sensor nodes, it is desirable to employ lightweight and specialized cryptographic primitives for many security applications. Motivated by the design of the well-known Enigma machine, we present a novel ultra-lightweight cryptographic algorithm, referred to as Hummingbird, for resource-constrained devices in this talk. Hummingbird can provide the designed security with small block size and is resistant to the most common attacks such as linear and differential cryptanalysis. Furthermore, we also present efficient software implementation of Hummingbird on the 8-bit microcontroller ATmega128L from Atmel and the 16-bit microcontroller MSP430 from Texas Instruments, respectively. Our experimental results show that after a system initialization phase Hummingbird can achieve up to 148 and 4.7 times larger throughput for a size-optimized and a speed-optimized implementations, respectively, when compared to the state-of-the-art ultra-lightweight block cipher PRESENT on the similar platforms.

Joint work with Daniel Engels, Honggang Hu, Guang Gong, and Eric Smith.

6. Merging Precomputation and Scalar Multiplication Using Large-Digit Representation

Nicolas Méloni

Scalar Multiplication is the key operation of most elliptic curve based cryptosystems. It consists of computing $nP = P + ... + P$, where n is an integer and P a point on the curve. To perform this operation efficiently, many different methods have been proposed. However, they are all based on the same pattern: a precomputation stage where the first multiples of P $(3P, 5P,$etc) are computed and a multiplication stage where those points are used in a double-and-add scheme. In this work, we proposed to merged those two stages by generalizing the usual scalar recoding methods.

Joint work with Anwar Hasan.

7. Implementation of the Compression Function for Selected SHA-3 Candidates on FPGA

Ashkan H. Namin

Implementation of the main building block (compression function) for five different SHA-3 candidates on reconfigurable hardware is presented. The five candidates, namely Blue Midnight Wish, Luffa, Skein, Shabal, and Blake have been considered since they present faster software implementation results compared to the rest of the SHA-3 proposals. The results allow an easy comparison for hardware performance of the candidates.

Joint work with Anwar Hasan.

8. On the (In)Security of a Pairing-Based Group Signature Protocol

Sanjit Chatterjee

Recent time has witnessed a near exponential volume of research to find novel cryptographic applications from bilinear pairing. Some of the protocols are already available as commercial products and are being standardized. Even though such protocols invariably come with a proof of security, a bit of caution may not be completely out of place. In this talk we will take a close look at the security aspects of the well-known Boneh-Shacham group signature scheme.

Joint work with Darrel Hankerson and Alfred Menezes.

9. Cloud Computing Security and Privacy Concerns

Anuchart Tassanaviboon

Cloud computing is a new computing paradigm based on the concept of changing from computing resource investment to pay-per-use services like other utilities, e.g., electricity and hydro, in order to convert from capital expenditure to operation cost. Therefore, this computing paradigm is evolved, disseminated and adopted into IT communities rapidly. However, because of the variety of technologies in the cloud, its definitions, characteristics, services, layers, and architectures are divergent and confusing. This encourages discussion and consolidation to achieve consistent ideas about the cloud computing. Meanwhile, more and more individual and organization are placed in clouds; there is an increasing in concerns about the security and privacy in cloud computing environment. Consequently, we comprehensively discuss about possible threats and attacks in this environment to determine essential security requirements. Additionally, we also emphasize on factors to assess cloud provider because the security and privacy in clouds rely on their trustworthiness. Finally we summarized the definitions, characteristics, models, security and privacy requirements, and assessment factors for the cloud computing.

Joint work with Guang Gong.

10. Randomly Directed Exploration: An Efficient Node Clone Detection Protocol in Wireless Sensor Networks

Zhijun Li

Node clone attack, that is, the attempt by an adversary to add one or more nodes to the network by cloning captured nodes, imposes a severe threat to wireless sensor networks. In this talk, we present an innovative randomly directed exploration protocol to detect the node clone. Each node need only know its neighbors information, and then collaborates to forward claiming messages, trying to find out clone. No any specific routing protocols or infrastructures are demanded in the proposed protocol. Therefore, it is highly practical in the general sensor network applications. In addition, the memory requirement of the protocol is almost optimal. Furthermore, the protocol consumes relatively low communication overload, which is not inferior to any previous schemes. The simulation results show that the protocol can achieve high detection probability. Overall, the proposed protocol outweighs previous approaches in terms of practicability and performance.

Joint work with Guang Gong.