FIELDS

ABSTRACTS 1.2

Invited Speakers

ADI AKAVIA
IAS

Solving Hidden Number Problem with One Bit Oracle and Advice

In the Hidden Number Problem (HNP), for p a prime and g a generator of Z_p^*, the goal is to find a hidden number s in Z_p^*, when given p, g and oracle access to the function $P_{s,k}(a) = MSB_k(sg^amodp)$ (for $MSB_k(x)$ denoting the k most significant bits in a binary representation of x). A non-uniform algorithm for HNP is given also a short advice string depending only of p and g (and not depending on the hidden number s). The algorithm is efficient if its running time and advice string are polynomial in log p.

DANIEL J. BERNSTEIN
University of Illinois at Chicago

High-speed cryptography

Protecting Internet communication against espionage and sabotage means using a shared secret key to authenticate and encrypt each message, and using public-key cryptography to share a secret key in the first place. Busy servers need all of this cryptography to be fast enough to handle not only regular loads but also denial-of-service attacks. This talk will explain ”batch binary Edwards” and other recent advances in cryptographic software speed.

REINIER BROKER
Microsoft Research

Constructing cryptographic curves with complex multiplication

Over the last 20 years, various algorithms have been developed to count the number of points on elliptic and hyperelliptic curves over finite fields. In this talk we consider the inverse problem of constructing curves of prescribed order over finite fields. The difficulty of this problem depends on its exact wording. We give an overview of the current state-of-the-art in curve construction and indicate what the open problems are.

CRAIG GENTRY
IBM

Fully Homomorphic Encryption Using Ideal Lattices

In this talk, I will describe a fully homomorphic encryption scheme, i.e., a scheme that allows one to evaluate circuits over encrypted data, even without being able to decrypt. I will also go over some applications, such as encrypted search-engine queries, searching through encrypted data, and cloud computing.

ROBERT GRANGER
Claude Shannon Institute, Dublin City University

Faster Modular Arithmetic for ECC

We propose a modular multiplication algorithm for a large family of integers we refer to as cyclotomic primes, that is competitive with the fastest, highly specialised and highly optimised modular multiplication methods, for bitlengths relevant to Elliptic Curve Cryptography. Coauthors: Andrew Moss, University of Bristol

ANTOINE JOUX
Universit de Versailles

Looking back at lattice-based cryptanalysis

In this talk, we revisit the use of lattice reduction as a cryptanalytic tool. We start from older attacks which used lattice reduction in a straightforward manner and work our way until we reached Coppersmith's small root algorithm, its variants and its numerous applications.

TANJA LANGE
Technische Universiteit Eindhoven

Pairings on Edwards curves

Since their introduction to cryptography by Bernstein and Lange, Edwards curves have received a lot of attention because of their very fast group law. The group law in affine form was introduced by Edwards in along with a description of the curve and several proofs of the group law. Remarkably none of the proofs provided a geometric interpretation of the group law while for elliptic curves in Weierstrass form the explanation via the chord-and-tangent method is the standard.

It was mostly for this lack of a geometric group law that Edwareds curves were considered unsuitable for pairing computations and indeed all attempts to develop explicit formulas for pairing computations led to worse performance than on Weierstrass curves.

In this talk I will report on recent work with Arene, Naehrig, and Ritzenthaler in which we developed a geometirc interpretation of the group law on twisted Edwards curves and derived explicit formulas for pairing computations that are competitive with those on Weierstrass curves. Coauthors: Christophe Arene, Michael Naehrig, Christophe Ritzenthaler

FRANCOIS MORAIN
Ecole polytechnique and University of Waterloo

Advances on the CM method for elliptic curves

The complex multiplication method (CM method) builds an algebraic curve over a given finite field GF(q) and having an easily computable cardinality. Used at first for elliptic curves, this method is one of the building blocks of the ECPP algorithm that proves the primality of large integers, and it appeared interesting for other applications, the most recent of which being the construction of pairing friendly curves. The aim of the talk is to recall the method, give some applications, and survey recent advances on several parts of the method, due to various authors, concentrating on elliptic curves. This includes class invariant computations, and the potential use of the Montgomery/Edwards parametrization of elliptic curves.

KENNY PATERSON
Royal Holloway, University of London

Non-Interactive Key Distribution and Identity-Based Encryption: A Retrospective Perspective

In this talk, we will investigate the relationships between identity-based non-interactive key distribution and identity-based encryption, providing a retrospective perspective on these distinct, but closely related, cryptographic primitives. We will also provide constructions for these primitives that make use of trapdoor discrete log groups and investigate the concrete schemes that result in two different computational settings. This talk represents joint work with Sriramkrishnan Srinivasan.

ERIC SCHOST
The University of Western Ontario

Fast arithmetics in Artin-Schreier towers over finite fields

An *Artin-Schreier tower* over the finite field F_p is a tower of field extensions generated by polynomials of the form $X^p - X - \alpha$. Following Cantor and Couveignes, we give algorithms with quasi-linear time complexity for arithmetic operations in such towers. As an application, we present an implementation of Couveignes' algorithm for computing isogenies between elliptic curves using the p-torsion. Coauthor: Luca De Feo

KATHERINE STANGE
Harvard University

The Elliptic Curve Discrete Logarithm Problem and Equivalent Hard Problems for Elliptic Divisibility Sequences

The division polynomials of an elliptic curve satisfy a recurrence relation. Evaluated at a given point on a given elliptic curve, both defined over a field K, the sequence of division polynomials becomes a sequence in K. Such a recurrence sequence is called an elliptic divisibility sequence.

We define three hard problems in the theory of elliptic divisibility sequences (EDS Association, EDS Residue and EDS Discrete Log), each of which is solvable in sub-exponential time if and only if the elliptic curve discrete logarithm problem is solvable in sub-exponential time.

We also relate the problem of EDS Association to the Tate pairing and the MOV, Frey-Rueck and Shipsey EDS attacks on the elliptic curve discrete logarithm problem in the cases where these apply.

This is joint work with Kristin Lauter performed at Microsoft Research.

RAINER STEINWANDT
Florida Atlantic University

Speeding up algebraic attacks: Multiple Right Hand Sides in hardware?

Algebraic attacks have become an established tool for analyzing symmetric ciphers. Complementing techniques building on Groebner bases and SAT-solvers, Raddum and Semaev proposed an approach known as MRHS to solve systems of polynomial equations over GF(2). This talk discusses a possible design of a special purpose architecture to implement MRHS. According to a preliminary analysis, such a device could enable significant performance gains over a software implementation, and when aiming at algebraic attacks against a realistic block cipher, such a hardware implementation seems an interesting option. Coauthors: Willi Geiselmann and Kenneth R. Matheis

ANDREW V. SUTHERLAND
MIT

Powered by Volcanoes: Three New Algorithms

The past year has seen dramatic improvement in the algorithms to compute three objects that have applications in elliptic curve cryptography: class polynomials, modular polynomials, and endomorphism rings. I will give a brief overview of each, focusing on their common component: isogeny volcanoes. When applied to large examples, these algorithms are orders of magnitude faster than the best methods available a year ago. Several practical examples will be presented to support this claim.

EDLYN TESKE
University of Waterloo

On Pairing-Friendly Elliptic Curves

Elliptic curves with small embedding degree and large prime-order subgroup are key ingredients for implementing pairing-based cryptographic systems. Such “pairing-friendly” curves are rare and thus require specific constructions. We present the framework developed with David Freeman and Mike Scott, that encompasses all of the constructions currently existing in the literature, and will touch on a few other selected topics on pairing-friendly elliptic curves.

Contributed Talks

PETER BIRKNER
Eindhoven University of Technology

Edwards Curves and the ECM Factorisation Method

The ECM method, introduced about 20 years ago by Lenstra, is one of the best algorithms for factoring integers. This method employs elliptic curves, usually in Montgomery form, to find a factor of a given integer. The recently introduced Edwards and Twisted Edwards curves offer very efficient arithmetic and can improve the speed of the ECM algorithm. We give a brief overview of the ECM method and Edwards curves, and show how to construct Edwards curves that are suitable for ECM, that is, Edwards curves with large torsion subgroup and positive rank over Q. Coauthors: Daniel J. Bernstein, Tanja Lange, Christiane Peters

SANJIT CHATTERJEE
University of Waterloo

Reusing Static Keys in Key Agreement Protocols

Contrary to conventional cryptographic wisdom, the NIST SP 800-56A standard explicitly allows the use of a static key pair in more than one of the key establishment protocols described in the standard. In this talk we give examples of key establishment protocols that are individually secure, but which are insecure when static key pairs are reused in two of the protocols. We also propose an enhancement of the extended Canetti-Krawczyk security model and definition for the situation where static public keys are reused in two or more key agreement protocols.

Coauthors: Alfred Menezes and Berkant Ustaoglu

FELIX FONTEIN
University of Calgary

A Concise Interpretation of the Infrastructure of a Global Field

The infrastructure has been used for a long time to speed up computation of fundamental units in global fields. Besides from that, the infrastructure was also proposed as mathematical object for use in Cryptography, first by J. Buchmann and H. C. Williams in 1990 in the case of real quadratic number fields. Since then, several proposals have been made for infrastructure based cryptosystems, based on both real quadratic number fields and real hyperelliptic function fields. All these cryptosystems are based of the hardness of computing distances in infrastructures.

In the function field case, a relation between the infrastructure and the divisor class group has been shown up by A. Stein in 1997 for elliptic function fields and by H.-G. Rck and S. Paulus in 1999 for hyperelliptic function fields. This relation essentially shows that distance computation in the infrastructure is equivalent to the Discrete Logarithm Problem in the divisor class group.

We extend this relation to all global fields, by relating the infrastructure to the (Arakelov) divisor class group. Our result extends the above named relations in the case of real quadratic fields, and is also compatible with R. Schoof's interpretation of the infrastructure in context of Arakelov divisor theory.

KORAY KARABINA
University of Waterloo

Factor-4 and 6 compression of cyclotomic subgroups

Bilinear pairings derived from supersingular elliptic curves of embedding degrees 4 and 6 over finite fields of characteristic two and three, respectively, have been used to implement pairing-based cryptographic protocols. The pairing values lie in certain prime-order subgroups of certain cyclotomic subgroups. It was previously known how to compress the pairing values over characteristic two fields by a factor of 2, and the pairing values over characteristic three fields by a factor of 6. We show how the pairing values over characteristic two fields can be compressed by a factor of 4. Moreover, we present and compare several algorithms for performing exponentiation in the prime-order subgroups using the compressed representations. In particular, in the case where the base is fixed, we gain a 59

ATEFEH MASHATAN
The Security and Cryptography Laboratory (LASEC), EPFL Swiss Federal Institute of Technology

Recent Designs for Message Recognition Protocols

There has been many recent proposals in designing protocols for constrained devices located in constrained environments, e.g. devices with limited computational power or memory in an ad hoc pervasive network. One problem of interest is designing message recognition protocols (MRPs), where the aim of the protocol is to enable a receiver to verify if a message is sent from the same sender from some previous communications. Several authors have proposed MRPs using a hash chaining technique.

In this talk, we will discuss the disadvantages of using a hash chain in an MRP designed for devices with low computational power and low memory. Moreover, when using a hash chain, one must consider security assumptions that are much stronger than standard assumptions. Further, we propose a new MRP suitable for devices in ad hoc networks which does not make use of hash chains. This new design uses random passwords that are being refreshed in each session, as opposed to precomputed elements of a hash chain. This new proposal relaxes the memory requirement and simplifies the security assumptions. Finally, we provide another MRP which provides explicit reconfirmation so that the sender knows weather or not the receiver has actually accepted the sent information. This is the first time the notion of explicit reconfirmation is looked it in the context of message recognitions. Coauthors: Douglas R. Stinson

NICOLAS MELONI
University of Waterloo

Elliptic curve point scalar multiplication combining double bases and Yao’s algorithm

In this work we propose to take one step back in the use of double base number systems for elliptic curve point scalar multiplication. Using a modified version of Yaos algorithm, we go back from the popular double base chain representation to a more general double base system.

We analyze the efficiency of our new method using different bases and optimal parameters. In particular, we propose for the first time a binary/Zeckendorf representation for integers, providing interesting results. Finally, we provide a comprehensive comparison to state-of-the-art methods, including a large variety of curve shapes and latest point addition formulae speed-ups. Coauthors: M. Anwar Hasan