9th Central European Conference on Cryptography - Třebíč'09
June 23 -26, 2009

Searching a secure genus 2 curve with small parameters over a prime field

Pierrick Gaudry

Abstract: Genus 2 curve cryptosystems provide reasonable alternatives to elliptic curve cryptosystems. In the case where the base field is a prime field, pointing counting is still a complicated task. However this is essential if one wishes to get a curve with small parameters in order to speed up the group law. We will present recent advances in genus 2 point counting in large characteristic and report on an ongoing large scale computation that looks for a secure genus 2 curve with small parameters over the prime field with $2^{127} - 1$ elements.

Attacks on the filter generator and nonlinear combiner generator

Tor Helleseth

Abstract: The filter generator consists of a linear feedback shift register (LFSR) and a Boolean filtering function that combines some bits from the shift register to create a key stream. The nonlinear combination generator employs several (LFSRs) and a Boolean function that combines bit from all the registers to produce the key stream. A new attack on the filter generator has been described by Rønjom and Helleseth who also extended the attack to linear feedback shift registers over an extension field $GF(2^m)$. Some improvements of the attacks of the filter generator and applications to the nonlinear combiner generator have been further given by Rønjom, Gong, Helleseth and Hojsik. The purpose of this talk is to give an overview of these attacks and to discuss how to extend the attacks on the filter generator to the nonlinear combination generator.

Cryptographic Aspects of Real Hyperelliptic Curves

Mike Jacobson , Jr.

Abstract: The majority of work on hyperelliptic curve cryptography makes use of the so-called imaginary model of a hyperelliptic curve, in which the Jacobian, a finite abelian group, is used in a variety of protocols. The Mumford representation of divisors leads to a convenient representation of group elements with efficient arithmetic. The real model is in some sense more general than the imaginary model, as every imaginary hyperelliptic curve defined over a finite field with more than 5 elements is birationally equivalent to a real one over the same base field, whereas the converse is not true in general without extending the base field. However, the real model has not been as well-studied for cryptographic applications, because arithmetic in the Jacobian is thought to be more cumbersome and less efficient.

In this talk, I will give an overview of cryptographic applications using real hyperelliptic curves. The main theme behind this area is exploiting the so-called baby step operation in the infrastructure, which is faster than other general divisor operations. I will touch on the cryptographic protocols that have been proposed, recent improvements to arithmetic including cubing and explicit formulas for divisor arithmetic in genus 2, and advances in solving the infrastructure discrete logarithm problem, whose presumed intractability is the basis of security for the related cryptographic protocols.

m-sequences with good cross correlation for communications and cryptography

Alexander Kholosha

Abstract: In this talk, we outline the wide application area found for m-sequences in communications and cryptography and outline the properties of m-sequences that made them vital for these applications. Then we focus of families of m-sequences

with good cross-correlation properties. The recent problem for the study in this area was analyzing cross-correlation of m-sequences that have different length. This also brings us to the underlying equations over finite fields where one can find both open problems and elegant solutions.

Efficient Divisor Reduction on Hyperelliptic Curves

Renate Scheidler

Abstract: Hyperelliptic curve cryptography makes extensive use of scalar multiplication. Generally, this is accomplished by writing the scalar in some base m, with the digits belonging to some digit set S. Scalar multiplication is done by performing repeated m-tuplings plus subsequent reduction, followed by tuplings by the appropriate element in S plus subsequent reduction. For $m = 2$ and $S = 0, 1$, this is the standard double and add method; for $m = 2$ and $S = -1, 0, 1$, it is scalar multiplication using the non-adjacent form representation of the scalar.

However, in certain cases, larger values of m are desirable, especially if a fast m-tupling procedure is available. Examples include m = 3, or m could be (a power of) the characteristic of the base field. In these cases, a method for rapidly reducing a large divisor is required. This talk presents a highly efficient divisor reduction algorithm. The technique is based on a fast method for reducing ideals in quadratic number fields due to Sawilla et al. It consists of a simple application of the Euclidean algorithm to the Mumford basis coefficients of the input divisor, along with computing certain linear recurrences. No intermediate divisors are computed throughout the procedure; the Mumford representation of the final reduced divisor is recovered via simple formulas at the end.

This is joint work with Roberto Avanzi (Ruhr-Universitaet Bochum, Germany) and Michael Jacobson (University of Calgary).

Multiple side equations over finite fields

Igor Semaev

Abstract: Multiple side(MS) equations is a new type of equations over finite fields which may be solved with Agreeing-Gluing family of algorithms. They are natural generalization of sparse and multiple right hand side (MRHS) linear equations studied earlier by H.Raddum and this author. One multivariate equation $f(X) = 0$ in MS form is determined by a list of MRHS linear equations:

$$\begin{aligned} A_1X &= a_{1,1}, \ldots, a_{1,r}, \\ &\ldots, \\ A_tX &= a_{t,1}, \ldots, a_{t,s}, \end{aligned} \tag{1}$$

such that $X = x$ is a solution to $f(X) = 0$ if and only if it is a solution to at least one of the linear systems $A_iX = a_{i,j}$. In this talk we show that the equations from different ciphers get a more compact representation, e.g. for Trivium and AES. We also describe rules for operating multiple side equations and solve them in so doing.

We apply this new solving technique to random sparse Boolean equations, where each equation depends on a low number of variables. Any subset of Boolean vectors is representable as a union of its sub-cosets. Therefore any Boolean equation is described as a MS equation (1) via the above representation of its solutions, where for the sake of efficiency one finds a cover with minimal number of cosets. We find by experiments that earlier designed Gluing Algorithm becomes significantly faster when operating with sparse Boolean equations in form of (1).

Violating Key Separation: On Using One Secret Key for Two Purposes

Rainer Steinwandt

Abstract: The talk discusses scenarios where a signature scheme and an encryption scheme are used simultaneously. For the ordinary public key setting, a situation is considered where only a single public key pair is used, i.e., the secret key is used for both decrypting and signing messages, and the public key is used to encrypt messages and to verify signatures. Similarly, for an identity-based scenario, a set-up is considered where users have one secret key only, obtained from a single key generation center. This secret user key then is used to sign messages and to decrypt ciphertexts. The talk discusses security notions for such combined schemes and examples where strong provable security guarantees can be established.

This talk is based on joint work with María Isabel González Vasco and Florian Hess.