
Conferences

AMS Short Courses

Public-Key Cryptography

Baltimore, Maryland
January 13–14, 2003

This entry-level course is under the direction of Daniel B. Lieman, University of Georgia. It will survey both mathematical and practical considerations in modern cryptography. Topics will include basic cryptographic techniques and how they are used today, along with the limitations of those techniques, and some goals of current cryptographic research. The course will also incorporate a survey of some real-world attacks on widely used cryptographic protocols, as well as areas of current and future research.

No prior knowledge of finite fields or computational number theory is required or expected. The course will be self-contained and will include suggested undergraduate research projects.

Speakers (subject to change) include Daniel Bailey, Brown University; William D. Banks, University of Missouri, Columbia; Paul Garrett, University of Minnesota; Igor E. Shparlinski, Macquarie University; William Whyte, NTRU Cryptosystems, Inc.; and the organizer.

It is planned that lecture notes will be available to those who register for this course. Advance registration fees are \$80 for AMS/MAA members, \$110 for nonmembers, and \$35 for students/unemployed/emeritus; on-site registration fees are \$100 AMS/MAA members, \$130 for nonmembers, and \$50 for students/unemployed/emeritus. Registration and housing information can be found in this issue of the *Notices*; see the section “Registering in Advance and Hotel Accommodations” in the announcement for the meetings in Baltimore. The registration form is at the back of this issue.

1. Public-key and Symmetric-key Cryptography

This talk will cover the basic constructions of public-key and symmetric cryptography and will give some examples of basic encryption, decryption, signature and verification primitives. We will also cover the key ideas of “randomness” and probabilistic encryption, which are extremely important in subsequent security discussions.

2. Cryptography in the Real World Today

This lecture will survey how cryptography and cryptographic algorithms are used today and current proposals for next generation security architectures. Topics will

include SSL/TLS and the Internet (i.e., secure Web browsing—what that really means), WAP (and other next generation cell phone architectures, etc.), as well as the cryptographic needs of “new” devices (e.g., RFID tokens, like the Mobil Speedpass) and applications. We will also discuss the limitations of current cryptographic technologies and what new innovations are needed.

3. Towards Faster Cryptosystems, I

This talk will cover elliptic curve cryptography (briefly!), along with a comparison to older techniques such as RSA and Diffie-Hellman. This talk will cover mathematical techniques for speeding up some “classical” algorithms: for example, the use of optimal extension fields to speed up the Diffie-Hellman and elliptic curve cryptosystems.

4. Attacks, I

This talk will use mathematical techniques to show that being able to recover even a small amount of data is enough to crack some cryptosystems. The combination of techniques from exponential sums and lattice reduction has a number of cryptographic applications, helping to make rigorous several heuristic approaches. It provides a two-edged sword which can be used both to prove important security results and also to create powerful rigorously proved attacks.

5. Attacks, II

This talk will focus on more “cryptographic” attacks. We will introduce the notion of an oracle and discuss adaptive chosen ciphertext attacks, etc. We will consider some of the security properties (particularly with respect to randomness) that a “safe” cryptosystem must possess.

6. Towards Faster Cryptosystems, II

This final talk will survey some current research in mathematical cryptography today—including new cryptosystems based on lattices (NTRU), along with interesting research into cryptosystems based on the (conjectured) rarity of zeroes of sparse polynomials.