Research in Cryptography, Information Security, and Algorithm Development
9807-12&26

Progress Report: January 1, 2002—June 30, 2002

Shafi Goldwasser, Ronald L. Rivest, Michael Sipser

Project Overview

The emphasis of the research, which is expressed in each one of our projects, is on the development of novel frameworks and theoretical provably secure solutions to problems arising from applications.

Progress Through June 2002

A. A SIGNATURE SCHEME FOR EFFICIENT PROTOCOLS
Anna Lysyanskaya, joint work with Dr. Jan Camenisch

Digital signature schemes are a fundamental cryptographic primitive, of use both in its own right, and as a building block in cryptographic protocol design. In this paper, we propose a practical and provably secure signature scheme and show protocols (1) for issuing a signature on a committed value (so the signer has no information about the signed value), and (2) for proving knowledge of a signature on a committed value. This signature scheme and corresponding protocols are a building block for the design of anonymity-enhancing cryptographic systems, such as electronic cash, group signatures, and anonymous credential systems. The security of our signature scheme and protocols relies on the Strong RSA assumption. These results are a generalization of the anonymous credential system of Camenisch and Lysyanskaya.

[CL02b] Jan Camenisch and Anna Lysyanskaya. "A Signature Scheme for Efficient Protocols." To appear in "Security of Communication Networks 2002."

B. ASYNCHRONOUS VERIFIABLE SECRET SHARING
Anna Lysyanskaya, joint work with Christian Cachin, Klaus Kursawe, and Reto Strobl (IBM Zurich)

Verifiable secret sharing is an important primitive in distributed cryptography. With the growing interest in the deployment of threshold cryptosystems in practice, the traditional assumption of a synchronous network has to be reconsidered and generalized to an asynchronous model. We propose practical verifiable secret-sharing protocol for asynchronous networks. The protocol creates a discrete logarithm-based sharing and uses only a quadratic number of messages in the number of participating servers. It yields the first asynchronous Byzantine agreement protocol in the standard model whose efficiency makes it suitable for use in practice.

[CKLS02] Christian Cachin, Klaus Kursawe, Anna Lysyanskaya and Reto Strobl. "Asynchronous verifiable secret sharing." Part of the paper "Asynchronous verifiable secret sharing and proactive cryptosystems." To appear in ACM-CCS 2002.

C. PROPERTY TESTING
Sofya Raskhodnikova

The field of property testing studies algorithms that distinguish, using a small number of queries, between inputs which satisfy a given property, and those that are "far" from satisfying the property. In this project, we investigated the problem of testing visual properties of two-dimensional images. The input to the problems consists of an image represented by a two-dimensional matrix M[1..n,1..n], where each entry is either 0 or 1; the 1 entry is interpreted as a "black" pixel, while the 0 entry is interpreted as a "white" pixel. For a given property (e.g., convexity), the goal of the algorithm is to distinguish between the following two cases, with large constant probability:

(1). The image satisfies the property.
(2). At least a constant (say _) fraction of pixels needs to be changed in order for the image to satisfy the property.

We showed that such algorithms exist for several interesting visual properties, including:

(1). Is the input object a half-space?
(2). Is the input object convex?
(3). Is the input object connected?

The number of queries performed by our algorithms is only polynomial in 1/_.

D. FINGERPRINTING
Christopher Peikert, Abhi Shelat, and Adam Smith.

Fingerprinting is a technique for protecting published data against unauthorized copying by making each copy unique. Such a fingerprint must satisfy several requirements to be useful; in particular, one must ensure that a small coalition of users who compare their copies cannot discover all marks. At the same time, the fingerprints must be fairly short, for efficiency reasons. See the previous Progress Report for more information about the background and formal specification of the problem.

We have investigated the relationship between the length of the fingerprints, and the size of coalition that the fingerprints can resist. In particular, we showed an improved lower bound on the length of collusion-secure fingerprinting codes. In this work, we improve the previously known Boneh-Shaw lower bound on the length of these codes by a factor of c, where c is the number of colluders. We go on to show that the Boneh-Shaw construction cannot be improved, and additionally, any scheme that fits into a fairly generic paradigm that we define cannot do much better than Boneh-Shaw.

[PSS'03] "Lower Bounds for Collusion-Secure Fingerprinting". By Chris Peikert, Abhi Shelat and Adam Smith.
To appear in Symposium on Discrete Algorithms, 2003.

E. ANALYSIS OF THE KHAZAD BLOCK CIPHER
Abhi Shelat

Khazad is one of the finalists in the NESSIE block cipher competition. This block cipher is a 64 bit block cipher with a 128 bit key and it employs the new wide-tail strategy to achieve security. Khazad is not a Feistel type cipher. Each round has three separate and invertible transformations: (1) an S-box 8x8 applied to each of the 8 bytes; (2) a linear diffusion function, which is derived from the generator matrix of an MDS code; (3) key addition. In the case of Khazad, both 1 and 2 are involutions (i.e., s(s(x))=x). Our analysis has focused on the algebraic properties of the cipher. We have a series of different algebraic representations for the S-box and the linear diffusion matrix for one round of the Khazad cipher.

This is an on-going project.