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

Progress Report: January 1, 2000—June 30, 2000

Shafi Goldwasser, Ronald L. Rivest and Mike Sipser

Project Overview

Recent NTT-sponsored research has focussed on both designing secure cryptographic protocols and showing their optimality by exhibiting impossibility of stronger cryptographic protocols in both multi-party(distributed) and two-party scenarios.

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

Progress Through June 2000

We highlight progress made during this period on several on going projects.

NOVEL COMMITMENT SCHEMES

In previous work, Professor Rivest has proposed a new scheme for achieving information-theoretically secure commitments when both parties are computationally unbounded. The value committed to by Alice is information-theoretically concealed from Bob (until revealed), but Alice can only change the value committed to with negligible probability. The scheme utilizes both a trusted third party and private channels between all pairs of parties to achieve this result (without some such extensions, the result was known to be unachievable).

More recently, Professor Rivest, in collaboration with NTT researcher Kazuo Ohta, has extended this result to handle the following concern. If the channel between Alice and Bob is not private, then a fourth party (Eve) might be able to forge a commitment from Alice, given the actual commitment Alice made. (In essence, this is a form of malleability of the commitment scheme.) Rivest and Ohta show how to make the previous commitment scheme secure against such an attack, using similar but more elaborate number-theoretic techniques.

ALL-OR-NOTHING TRANSFORM (AONT).

The All-Or-Nothing Transform (AONT), introduced by Rivest, and further investigated by Boyko and Canetti et al., is an invertible (randomized) transformation T which reveals ``no information'' about its input x even if almost all the bits of T(x) become known. It has many applications and can be defined in the perfect, statistical or computational settings.

Most recently, Yevgeniy Dodis, Amit Sahai (a graduate student supported by NTT funds) , and Adam Smith in a work titlled "An Optimal Lower Bound for Perfect All-Or-Nothing Transforms." consider the perfect setting, where T maps k bits to n bits such that learning any (n-l) bits of output still completely hides x. While the trivial bound on l is that l must be at least k, the best constructions of perfect AONT's were restricted to have l>n/2 (when n<2^k). In other words, one must miss at least half of the output in order not to learn anything about the input, even when the output size is exponentially long! They show that this, unfortunately, indeed has to be the case by establishing a tight lower bound on l. On the other hand, statistical AONT's offer almost the same security as perfect AONT's but can achieve l roughly equal to k, indicating an exponential separation between the perfect and the statistical settings. They show that this separation holds even in the more general setting where the adversary can adaptively choose which output bits to see one-bit-at-a-time. Therefore and despite their very attractive perfect security, perfect AONT's are of limited use in most situations.

THRESHOLD CRYPTOGRAPHY

Stas Jarecki (supported by NTT funds) and Anna Lysyanskaya significantly improved their results on adaptively secure threshold protocols in the erasure-free model. Adaptivity in threshold protocol implies resilience against a network adversary which chooses the players against which it wants to stage an attack *during* the run of the protocol. The erasure-free property of the protocol implies that we do not require the participating players to reliably erase their data, and hence the protocols can be implemented using standard servers running standard operating systems. Stas and Anna reduced the computation and communication costs of their adaptive erasure-free protocols by the factor linear in the security parameter. This improvement implies the first non-trivial multiparty computation protocol in the adaptive erasure-free model which has a communication and computation complexity comparable to the complexity of best non-adaptive protocols. Hence these protocols became viable for practical use, for example in an implementation of a key certification authority that is fault-tolerant against virus attacks.

This efficiency improvement is based on the identification of a novel property, called selective security, of an encryption procedure which is needed by the parties participating in the threshold protocol to communicate secretely. Selective security of an encryption scheme means that if a group of cleartexts is encrypted, and if the adversary asks to see the cleartexts of half of them, all information about the *remaining* cleartexts remains hidden. Surprisingly, standard encryption schemes are not known to be selectively secure.

ANONYMOUS SUBSCRIPTION PROTOCOLS

Zulfikat Ramzan (supported by NTT grant) and Matthias Ruhl focused on anonymous subscription protocols. Such protocols allow a legitimate user to subscribe to an electronic service, and then anonymously and unlinkably access the service. In addition to formally defining the problem, we put forth practical examples, and discussed the security features and properties needed in such protocols. One such property is is termination: access priveleges can be used only a fixed number of times or for a fixed period. We developed two practical schemes which are the first to have this property. The first scheme is based on blind digital signatures, and the second is based on a group signature scheme. The security analysis includes identifying a new (comptutationally) equivalent variant of the Decisional Diffie-Hellman assumption, which may be of independent interest. A paper describing these results has been submitted to ASIACRYPT 2000.

BLOCK CIPHER DESIGN

Leonid Reyzin and Zulfikar Ramzan (both supported by the NTT grant) have developed a new, more refined, model for studying the security of symmetric-key cryptographic primitives, such as block ciphers. This model accounts for the fact that many such primitives consist of iterating simpler primitives for a number of rounds, and may provide insight into the security of such designs. They showed that a block cipher remains secure even when its inner rounds are not secret. This work further improves our understanding of block-cipher security and may simplify the design of future block ciphers. The observation can be extended to other cryptographic primitives, such as MACs. The work will be published in Crypto 2000.

PROTOCOLS FOR CONCURRENT AND RESETTABLE SETTING

Goldwasser has been working on designing secure cryptographic identification protocols in an asynchronous environement where several concurrent versions of protocol may be running interleaved with each other. The work involves introducing new stronger definitions of security for identification protocols that address the threat introduced in a concurrent setting, and designing protocols which provaly satisfy these notions.

Research Plan for the Next Six Months

A resource which is heavily used in threshold cryptography is for the dedicated servers (simulating the trusted entity) to share in advance — in an off-line set-up stage — randomness to be used later during the on-line protocol. Unfortunately, even though the ability to share randomness in advance off-line enables proving strong cryptographic security properties, it does require secure storage of quite a bit of data. We plan to work on eliminating the need of shared randomness in a set-up stage and hopefully replacing it by pseudo-random generation on-line.

We will also work on important related open problems in general multi-party computation, such as secure multi-party computation that remains secure under concurrent composition (this has applications in secure electronic transactions) and more efficient erasure-free multi-party computation. Some of our threshold techniques described above may be applicable here. Finally, we plan to explore receipt-free multi-party computation, which has particular application to electronic voting.

We plan to continue exploring the theory of block cipher design. In a recent breakthrough, Reyzin, Rivest, and Ramzan were able to develop a simple necessary and sufficient condition for determining when a block cipher of a relatively general form is secure against adaptive chosen plaintext attacks. We hope to develop similar conditions for determining security against adaptive chosen plaintext and ciphertext attacks. The overall goal is to gain a more fundamental understanding of what makes block ciphers secure.

Moses Liskov (supported by the grant) and Silvio Micali are working on improving e-cash schemes in two ways: first, to deal with the inherent efficiency problem that arises due the necesity of using zero-knowledge techniques when e-coins are minted, and second, to more precisely define what it means for an e-cash scheme to be secure.