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

Progress Report: January 1, 2001 – June 30, 2001

Shafi Goldwasser, Ronald L. Rivest, and Michael Sipser

Project Overview

Recent NTT-sponsored research has focussed on both introducing new cryptographic primitives and designing secure cryptographic protocols with repsect to existing definitions.

The emphasis of the research is on the development of novel frameworks and theoretical provably secure solutions to problems arising from applications.

Progress Through June 2001

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

1. RESETTABLY-SOUND CRYPTOGRAPHIC PROTOCOLS

Professor Goldwasser, together with Barak, Goldreich, and Lindell worked on Resettably-sound proofs and arguments. These concept was previously investigated by Reyzin and Micali in the public-key setting. These protocols maintain soundness even when the prover can reset the verifier to use the same random coins in repeated executions of the protocol. In the current work it is shown that resettably-sound zero-knowledge arguments for *NP* exist if collision-free hash functions exist. In contrast, resettably-sound zero-knowledge proofs are possible only for languages in P/poly.

Two applications of resettably-sound zero-knowledge arguments are presented. First, we construct resettable zero-knowledge arguments of knowledge for *NP*, using a natural relaxation of the definition of arguments (and proofs) of knowledge. We note that, under the standard definition of proof of knowledge, it is impossible to obtain resettable zero-knowledge arguments of knowledge for languages outside *BPP*. Second, we construct a constant-round resettable zero-knowledge argument for *NP* in the public-key model, under the assumption that collision-free hash functions exist. This improves upon the sub-exponential hardness assumption required by previous constructions.

We emphasize that our results use non-black-box zero-knowledge simulations. Indeed, we show that some of the results are *impossible* to achieve using black-box simulations. In particular, only languages in *BPP* have resettably-sound arguments that are zero-knowledge with respect to black-box simulation. [BGGL]

2. IDENTIFICATION SCHEMES IN PRESENCE of RESET ATTACKS.

Professor Goldwasser, worked on providing identification protocols that are secure even when the adversary can reset the internal state and/or randomization source of the user identifying itself, and when executed in an asynchronous environment like the Internet that gives the adversary concurrent access to instances of the user. These protocols are suitable for use by devices (like smartcards) which when under adversary control may not be able to reliably maintain their internal state between invocations. Several schemes, based on non-malleable encryption, signatures secure against chosen message attack, and proofs of knowledge, designed together with Bellare, Fischlin, and Micali appeared in *Eurocrypt 2001* [BFGM] .

3. RING SIGNATURES

Professor Rivest together with Shamir and Tauman introduce the notion of a *ring signature*: a digital signature that specifies a set of possible signers, such that the verifier can't tell which member actually produced the signature. Unlike group signatures, ring signatures have no group managers, no setup procedures, and no coordination: any user can sign on behalf of any set to which he belongs, and he can choose a new set for each message without getting the consent or assistance of the other members. The only requirement is that each possible signer is already using some public key signature scheme, such as RSA. Ring signatures provide an elegant way to leak authoritative secrets in an anonymous way, to implement designated-verifier signature schemes which can authenticate emails without undesired side effects, and to solve other problems in multiparty computations. Rivest et. al. proposed a ring signature scheme which is provably secure in the random oracle model, provides unconditional anonymity, and is exceptionally efficient: adding each ring member increases the cost of signing or verifying by a single modular multiplication and a single symmetric encryption.

4. IDENTITY ESCROW SCHEMES AND ANONYMOUS CREDENTIAL SYSTEMS

An identity escrow scheme allows a member of a group to prove membership in this group without revealing any extra information. At the same time, in case of abise, his identity can still be discovered. Such a scheme allows anonymous access control. Recently Anna Lysyanskaya put forward the notion of an identity escrow scheme with appointed verifiers. Such a scheme allows the user to only convince the appointed verifier(s) if his membership; but no unauthorized verifier can become convinced of the user's membership even if the user fully cooperates, unless the user is completely under his control. We provide a formal definition of this new notion and give an efficient construction of an identity escrow scheme with appointed verifiers provably secure under common number-theoretic assumptions in the public-key model. Our framework and techniques easily translate to the setting of an anonymous credential system. [CL]

5. THRESHOLD CRYPTOGRAPHY

Threshold cryptosystems and signatures schemes provide ways to distribute trust throughout a group and increase the availability of cryptographic systems. Although the adversary is allowed to corrupt up to one half of the servers, the goal is to sustain the security of the underlying functionality. A standard approach in designing these protocols is to base them upon existing single-party systems having

the desired properties.

The best practical yet provably secure signature schemes known (Cramer-Shoup'99) rely upon the inversion of a prime number modulo a secret value. Recently [LP] we improved the distributed modular inversion protocol of Catalano, Gennaro and Halevi to make it secure against an adaptive adversary, thereby enabling threshold signature schemes with stronger security properties than any previous result.

As a tool, we also developed an adaptively-secure, erasure-free threshold version of the Paillier cryptosystem.

6. ACCOUNTABLE-SUBGROUP MULTISIGNATURES

Leo Reyzin together with Silvio Micali, and Kazuo Ohta worked on Accountable-Subgroup Multisignatures will appear in *8th ACM Conference on Computer and Communications Security, 2001* [MOR].

Formal models and security proofs are especially important for multisignatures: in contrast to threshold signatures, no precise definitions were ever provided for such schemes, and some proposals were subsequently broken.

In the above mentioned paper, a variant of multi-signature schemes is formalized and implemented. The variant is called Accountable-Subgroup Multisignatures (ASM). In essence, ASM schemes enable any subgroup, S, of a given group, G, of potential signers, to sign efficiently a message M so that the signature provably reveals the identities of the signers in S to any verifier.

The proof of security of the implementation relies on random oracles and the hardness of the Discrete Log Problem.

7. MUTUALLY-INDEPENDENT COMMITMENTS

Leo Reyzin together with Moses Liskov, Anna Lysyanskaya, Silvio Micali, and Adam Smith studied the two-party commitment problem, where two players have secret values they wish to commit to each other. Traditional commitment schemes cannot be used here because they do not guarantee independence of the committed values. Here three increasingly strong definitions of independence in this setting and give practical protocols for each are presented . The work is related to work in non-malleable cryptography. However, the two-party commitment problem can be solved much more efficiently than by using non-malleability techniques.

John Hertzog is exploring ways to reconcile the fields of formal logic based security and computational cryptography. The computation cryptographic world can be thought of as an outgrowth of complexity theory, with its emphasis on reducibility and computability. Formal logic based security is an extension on formal verification methods, with emphasis on abstraction and state-space exploration. Both field have their advantages, and recent work has shown that the two fields are not as different as they seemed.

Sofya Raskhodnikova has been working on the problem of testing monotonicity on partially ordered sets. Given oracle access to a function on an arbitrary partially ordered set, the goal is to determine whether the function is monotone or is far from monotone, i. e. needs to be changed in many places to become monotone. This problem turns out to be equivalent (in terms of the number of queries required for testing) to the problem of testing whether a 2CNF formula is satisfied or is far from being satisfied. We describe some classes of POsets that are testable

with a constant number of queries. We give a lower bound of *log(N)* where *N* is the number of points in the domain of the function for the special case of testing monotonicity on the hypercube investigated in previous papers. The lower bound matches the known upper bound. For the general problem, we give an algorithm that requires *O(\sqrt(N))* queries and prove a matching lower bound (up to logarithmic terms). The lower bound construction is of independent interest. It gives a construction of dense graphs whose edge set can be partitioned into a nearly linear number of induced matching of linear size. This gives an alternative to the widely used Rusza-Szemeredi construction of dense graphs whose edge set can be partitioned into a linear number of induced matchings of nearly linear size.

Research Plan for the Next Six Months

1. Professor Goldwasser plans to explore whether current lower bounds (and impossibilities) in cryptography in the black-box model can be overcome using the new non black-box techniques invented 2001.

2. Compare the relative strength of the RSA intractability assumption and the strong-RSA assumption.

3. Professor Rivest plans to continue investigating technologies for voting. He is currently organizing (together with David Chaum) a specialized workshop on this topic (WOTE '01) which Kazuo Ohta (formerly of NTT) Tatsuaki Okamoto (currently at NTT) will attend. This workshop will be attended by many of the key researchers in the field. It is likely that this research will result in new directions for research in voting technologies, which we would then plan to pursue with the support of NTT.

4. Extend the framework and results of identity escrow to electronic voting. In electronic voting, it is desirable that the user, even when fully cooperating, is unable to convince the mafia that he has voted in a certain way. Similar to our identity escrow setting, there are two adversaries here: the voter (whose behavior may be adversarial since he is communicating with the mafia) and the mafia. This problem has found a number of heuristic solutions, but a formal approach has not been considered.

5. Improve threshold signature schemes. For example, recently, a non-interactive signature scheme was proposed by Shoup. However, its security can only be proved for a static adversary and in the random oracle model. An interesting question to explore is how close to it one can come if these are relaxed. This can lead both to more efficient constructions and to lower bounds.

References:

[BGGL] Boaz Barak, Oded Goldreich, Shafi Goldwasser and Yehuda Lindel. "Resettably-Sound Zero-Knowledge and its Applications, 42nd Annual Symposium on Foundations of Computer Science, Las Vegas, Nevada October 14-17, 2001. To appear.

[BFGM] Mihir Bellare, Marc Fischlin, Shafi Goldwasser, Silvio Micali. "Identification Protocols Secure Against Reset Attacks." In Advances in Cryptology - Eurocrypt 2001 Proceedings, Lecture Notes in Computer Science volume 2045, B. Pfitzmann, ed., Springer-Verlag, 2001.

[CL] Jan Camenisch, Anna Lysyanskaya. "An Identity Escrow Scheme with Appointed Verifiers." To appear in Crypto 2001.

[LP] Anna Lysyanskaya, Christopher Peikert. "Adaptive Security in the Threshold Setting: From Cryptosystems to Signature Schemes." Manuscript, Asiacrypt 2001. To appear.

[MOR] Silvio Micali, Kazuo Ohta, and Leonid Reyzin. "Accountable-Subgroup Multisignatures." To appear in 8th ACM Conference on Computer and Communications Security, 2001.
http://theory.lcs.mit.edu/~cis/pubs/reyzin/multisig.ps

Other Related Work:

[AR] Michel Abdalla and Leonid Reyzin. A New Forward-Secure Digital Signature Scheme. Advances in Cryptology -- Asiacrypt 2000, Taksuaki Okamoto, editor, Lecture Notes in Computer Science, volume 1976, Springer-Verlag, 2000. http://theory.lcs.mit.edu/~cis/pubs/reyzin/forwardsig.ps.

[MR] Silvio Micali and Leonid Reyzin. "Min-Round Resettable Zero Knowledge in the Public Key Model." In Advances in Cryptology - Eurocrypt 2001 Proceedings, Lecture Notes in Computer Science volume 2045, B. Pfitzmann, ed., Springer-Verlag, 2001. http://theory.lcs.mit.edu/~cis/pubs/reyzin/min-round-rzk.ps.

[MR] Silvio Micali and Leonid Reyzin. "Soundness in the Public Key Model." To appear in Crypto 2001.
http://theory.lcs.mit.edu/~cis/pubs/reyzin/soundness.ps.