Efficient Secure Multiparty Computation

Marie Elisabeth Gaup Moe
PhD Student
Centre for Quantifiable Quality of Service in Communication Systems
Norwegian University of Science and Technology
Trondheim, Norway
marieeli@q2s.ntnu.no

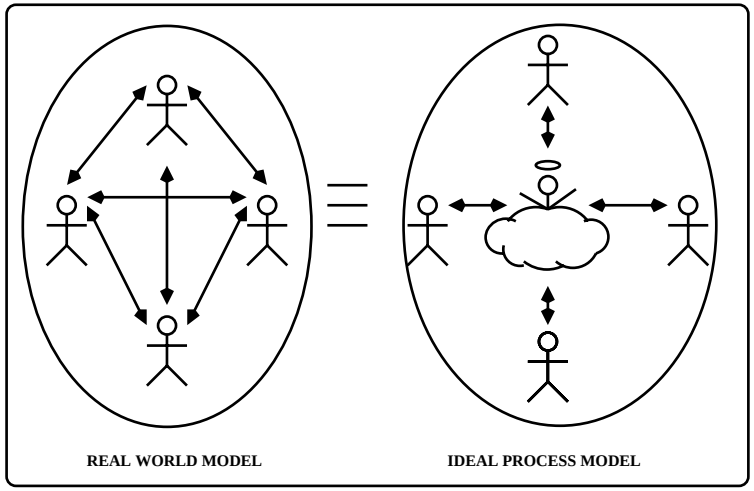
Outline

- Introduction to Protocol Security
- Secure Multiparty Computation
- Efficient Protocols

Introduction to Protocol Security

- One wants to prove that running a secure protocol is "just as good" as carrying out an idealized computational process where security is guaranteed
- Comparing the protocol execution in a real life model to an *ideal process* that captures the functionality of the protocol
- A protocol *emulates* the ideal process if the distribution of the output of an adversary attacking the protocol in the real world model is indistinguishable from the output distribution of an adversary in the ideal process model

Protocol Security Illustration



Multiparty Protocols continued

- Multiparty protocols can be applied to many cases where distributed cryptographic services are needed, like key distribution, contract signing, electronic elections, auctions and transactions

- It is not an easy task to realize complex protocols in a secure manner, one promising approach is to build secure protocols on top of each other in a theoretical framework of *universal composability*

Secure Multiparty Computation

- When realizing a distributed cryptographic service in a dynamic network many of the problems encountered can be reduced to the problem of performing a *secure multiparty computation*

- Several parties wish to compute a function with their own local inputs without revealing any information about their inputs to each other

- At the same time they should be able to trust that the output of the function is correct even though some of the parties and the communication channels may be corrupted

Secure Multiparty Computation continued

- In the mid 1980´s Yao constructed a protocol for two-party secure computation based on *garbled circuits* (uses private key encryption) and *oblivious transfer* (based on factoring problem)

- This protocol is provable secure against semi-honest adversaries (passive but curious) and is a constant-round protocol

- Goldreich et al. extended the protocol to multiparty and malicious (active) adversarial cases

Secure Multiparty Computation continued

- Protocols that are provably secure in this setting relies on authenticated channels (a public key infrastructure)
- The function f is assumed to be represented by an arithmetic circuit over a finite *field*
- The garbled circuit construction does not efficiently scale over large fields

Efficient Protocols

- *Randomizing polynomials* is a technique that increases the round-efficiency of secure computation protocols (Ishai and Kushilevitz FOCS 2000)
- This technique together with using branching programs instead of arithmetic circuits allows for multiparty computation over *rings* (result by Cramer et al. Eurocrypt 2003)
- Relaxation of the security model is another approach for making more efficient protocols

References

- R. Canetti, Security and Composition of Multi-party Cryptographic Protocols. Journal of Cryptology, vol.3, no.1, pp. 143-202, 2000

- R. Canetti, Universally Composable Security: A New Paradigm for Cryptographic Protocols, http://eprint.iacr.org/2000/067, 2005

- J. B. Nielsen, On Protocol Security in the Cryptographic Model. PhD dissertation, BRICS University of Aarhus, 2003

- R. Cramer, I. Damgård and J. B. Nielsen, Multiparty Computation from Threshold Homomorphic Encryption. Advances in Cryptology - EuroCrypt 2001, LNCS 2045:280-300, 2001

References

- A. C. Yao, How to Generate and Exchange Secrets, Proc. of 27th FOCS, 1986
- O. Goldreich, S. Micali and A. Wigderson, How to Play Any Mental Game, Proc. of 19th STOC, 1987
- Y. Ishai and E. Kushilevitz, Randomizing Polynomials: A New Representation with Applications to Round-Efficient Secure Computation, FOCS 2000
- R. Cramer, S. Fehr, Y. Ishai and E. Kushilevitz, Efficient Multi-Party Computation over Rings, Eurocrypt 2003