Bridging Protocol Security and Game Theory

Oana Ciobotaru

Saarland University
ociobotaru@cs.uni-saarland.de

Abstract. Over the years, various security notions have been proposed and analyzed in the classical cryptographic model. Even though the study of implication relations among security notions has been very prolific, important open problems remain. For example, for a decade it was not known [4] whether the notions of specialized simulator universally composable security and 1-bit specialized simulator universally composable security are equivalent or not. Another open problem [3] is finding strong security notions equivalent with appropriately defined game-theoretic notions. In this work, we give an answer to each of these open problems.

Keywords: rational cryptography; game theory; security models; universal composability

1 Introduction

1.1 Problem Statement and Motivation

Protocol security is important to have, however it is neither easy to define, nor to accomplish. Traditionally, cryptographic protocols are designed to achieve security properties in a "black and white" adversarial model which assumes protocol participants to be either completely honest or arbitrarily malicious. Security properties achieved in this classical model can provide strong guaranties, however, often enough they lead to protocols that are highly complex, very inefficient, and in some cases, even provably impossible to design.

Rational cryptography has recently emerged as a very promising alternative to the inflexible classical cryptographic model. Intuitively, the main goals for rational cryptography are formalizing suitable models, defining security notions and efficiently implementing protocols that fulfill these notions in the realistic scenarios which assume protocol participants to have well defined and rather selfish intentions and goals. Example scenarios where participants can be expected to behave selfishly rather than arbitrarily malicious include: auctions, file sharing, secret sharing and secure function evaluation. In contrast to the classical cryptographic model, rational cryptography draws inspiration from game theory and models protocol participants as rational players that try to maximize their benefit and, thus, deviate from the protocol only if they gain an advantage by doing so. If no rational player has any incentive to deviate from a given protocol, then in game theoretic terms such a protocol is called an equilibrium.

The research established in the field of rational cryptography shows that methods and notions from game theory can be successfully used in cryptography and vice versa. Thus, a natural question can be raised: To which extent are notions from game theory and cryptography related or, equivalently, which is the intrinsic connection between the two fields?

1.2 Background and Related Work

Finding an answer for this question represents the main motivation which triggered my work [2] on equivalence relations between security notions and game theoretic notions. The only previous research study concerned with such equivalence relations [3] is centered around the "power of costly computation". Intuitively, the meaning of costly computation is that rational players interested in running a protocol might be deterred from following it as it was designed if the cost of computation (e.g., number of steps needed to be performed, the size of memory used, etc.) is higher than a threshold they have decided upon. The main result shown by Halpern and Pass [3] is that when rational players prefer to avoid costly computations, then the game theoretic notion of strong universal implementation is equivalent to the cryptographic notion of weak precise secure computation.

Intuitively, the notion of strong universal implementation is fulfilled by a rational protocol with respect to a trusted mediator and a class of games if for each game in this class and each time when the truthful reporting by the rational parties of their correct input to the mediator is an equilibrium, then following the rational protocol is also an equilibrium. The cryptographic notion of weak precise secure computation is related to the notion of stand-alone security. Both security notions are defined by comparing the output of a real world execution of the protocol and its adversary with the output of an ideal world execution of an ideal functionality (i.e., a trusted entity which performs all protocol tasks securely) and an ideal adversary (also called simulator) which is trying to emulate any attack occurring in the real world. The entity that should try to distinguish between the output of the two worlds is called a distinguisher. The difference between stand-alone security and weak precise secure computation can be intuitively viewed as a difference in the order of quantifiers. More precisely, in the case of stand-alone security, the simulator depends only on the real world adversary, while the notion of weak precise secure computation is defined such that the simulator depends on the real world adversary, the distinguisher and the input distribution received by the participants in either of the two worlds. Hence, even though it is very insightful, the equivalence result between strong universal implementation and weak precise secure computation obtained by Halpern and Pass [3] leaves an open question whether one can derive similar equivalence relations, but for stronger security notions, i.e., where the simulator depends on fewer entities.

2 Approach and Uniqueness

In my work [2] I give a positive answer to this open question. First, I discard the cost of computation from the definition of strong universal implementation and I call this new game theoretic notion game universal implementation. Next, I define the notion of weak stand-alone security which is related to the notion of stand-alone security in the following respect: The ideal world simulator depends on the real world adversary and on the distinguisher. Finally, I show that game universal implementation and weak stand-alone security are equivalent. Thus, I am able to answer positively the open question from [3] regarding the existence of game-theoretic definitions that are equivalent to cryptographic security notions for which the ideal world simulator does not depend on both the distinguisher and the input distribution.

3 Additional Contributions and Results

Additionally, in my work [2], I investigate the effects of deriving "weak" security concepts from the existing security notions, similarly to the definition of weak stand-alone security from stand-alone security. This leads me to study the equivalence relations among various existing security notions and the newly derived notions. My main result in this area is a separation result between two variants of the universal composability (UC) security definition: 1-bit specialized simulator UC security and specialized simulator UC security. Indeed, UC security [1] is a very strong security notion but it is also equally hard to implement in practice. Thus, sometimes, it may suffice for a protocol to achieve one of the less stringent variants of UC security. Intuitively, the notion of specialized simulator UC security is also defined by comparing the output of the execution in the real world and in the ideal world. However, in contrast to stand-alone security for example, in the definition of specialized simulator UC security there exists an additional entity called the environment. Formally, the environment is modeling the composability properties of a security notion. Intuitively, the environment represents any other protocols, network adversaries or even copies of the original protocol which one may find in a real world as well as in an ideal world execution, besides the participants described in the simplistic stand-alone model. Indeed, the environment is allowed to give and collect arbitrarily many times the inputs and respectively the outputs from the participants that it is interacting with. In the end, the environment outputs its view of its interactions. If the output of the environment is always only one bit, then we obtain the notion of 1-bit specialized simulator UC security.

The separation result described above is interesting for two reasons. First, the nature of the implication relation between 1-bit specialized simulator UC security and specialized simulator UC security was left as open research for almost a decade [4]. Second, the separation result comes in contrast with the well known equivalence result between 1-bit UC security and UC security [1].

References

1. Canetti, R.: Universally composable security: A new paradigm for cryptographic protocols. In: 42nd IEEE symposium on Foundations of Computer Science (FOCS '01). pp. 136–145. IEEE Computer Society (2001)
2. Ciobotaru, O.: On the (non-)equivalence of UC security notions. In: 6th International Conference on Provable Security (ProvSec'12). pp. 104–124. Springer (2012)
3. Halpern, J.Y., Pass, R.: Game theory with costly computation: Formulation and application to protocol security. In: Innovations in Computer Science (ICS'10). pp. 120–142. Tsinghua University Press (2010)
4. Lindell, Y.: General composition and universal composability in secure multi-party computation. In: 44th Symposium on Foundations of Computer Science (FOCS'03). pp. 394–403. IEEE Computer Society (2003)