

Cryptography with Guardian Angels: Bringing Civilization to Pirates – Abstract

Gildas Avoine
gildas.avoine@epfl.ch

Swiss Federal Institute of Technology (EPFL),
Lausanne, Switzerland

Extended abstract available at <http://lasecwww.epfl.ch>

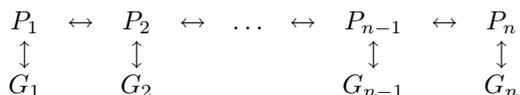
Serge Vaudenay
serge.vaudenay@epfl.ch

In contrast with traditional cryptographic protocols in which parties can have access to common third parties, and where at least one of them is assumed to be honest, we propose here a new model which is relevant for networks of communication devices with security modules. We then focus on the problem of fair exchange in this model. We propose a probabilistic protocol which provides arbitrarily low unfairness (involving a complexity cost).

I. Pirates and Guardian Angels Model

In classical mobile networks, the communication scheme is made of both devices P_i and providers; the latter may have put security modules G_i in their devices. G_i 's can only communicate with their own P_i , and P_i 's can only communicate with both their security module and their provider.

In future network like self-organized mobile networks, the communication chain looks as follows and providers are no longer involved.



Here we may assume that all users try to optimize their benefit and are potential pirates, and thus security modules serve as Guardian Angels in order to enforce community rules. Since users can modify the behavior of their devices, we can consider a user and a device as a same entity, a Pirate.

For practical considerations, we assume that guardians are tamper-resistant, simple and limited devices, and that they can only communicate with their own device P . Smart cards are examples of guardian angels. Guardians are set up by a given provider who may define his own community bylaw. This setting may lead to some interesting business models.

In this model, confidentiality, integrity, and authenticity are addressed in a classical way. A specific problem is the insurance of receipt: how to certify that a message was well transmitted and received? Here we address this problem in context of fair exchange problem.

II. Fair Exchange Protocol

The proposed protocol is a probabilistic fair exchange protocol between two entities P_i and P_{i+1} without trusted third party, which is in this way particularly relevant for self-organized networks. We recall first that an exchange protocol is fair if, at the end of the execution, either both parties have received the expected value v_i and v_{i+1} , or none of them have received any information about the other value.

In the pirates and angels model, we assume that G_i 's have a virtual private network (VPN) which protects confidentiality, integrity, authentication, and sequentiality of the exchanged messages. So, the only possible attack consists in aborting the protocol. During a first stage, G_i and G_{i+1} use this VPN in order to exchange the expected values v_i and v_{i+1} .

The remaining stage is a simple synchronization problem: G_i and G_{i+1} need to decide in a synchronous way that the exchange succeeded in order to disclose the exchanged value to their devices. In this synchronization protocol, the guardians, in turn, send a message through the VPN. This message can be a termination signal or some dummy random value. To do this, they flip a coin with probability p to issue a termination signal. The pirates P_i and P_{i+1} are assumed to be unable to distinguish the signal from a random value. Then, guardians consider that the protocol succeeds when they have both received and sent the termination signal. Since pirates are assumed to get no information in the messages, they cannot decide to stop depending on the protocol view. Hence they must decide to stop at some level no matter what the communication are.

An analysis of our synchronization protocol yields to the following theorems:

Theorem 1: Let C be the number of messages exchanged between G_i and G_{i+1} . If p is the termination probability, we have $E(C) = \frac{3}{p} - 1$ when P_i and P_{i+1} are honest.

Theorem 2 : If p is the termination probability and p_a the highest probability of unfairness over all possible misbehavior of pirates, we have $\frac{p}{4} \leq p_a \leq \frac{p}{4(1-p)}$.

The proofs of these theorems are available in the extended abstract, as well as variants and extensions.

ACKNOWLEDGMENTS

The work presented in this paper was supported (in part) by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center supported by the Swiss National Science Foundation under grant number 5005-67322.