# Some Guidelines for Non-repudiation Protocols

Panagiotis Louridas
38 Domboli St.
116 36 Athens
Greece
louridas@acm.org

## ABSTRACT

Non-repudiation protocols aim at preventing parties in a communication from falsely denying having taken part in that communication; for example, a non-repudiation protocol for digital certified mail should ensure that neither the sender can deny sending the message, nor the receiver can deny receiving it. We identify some guidelines for non-repudiation protocols. The guidelines are derived by examining a series of non-repudiation protocols that descend from a single ancestor.

## Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*security and protection (e.g., firewalls)*; K.4.4 [**Computers and Society**]: Electronic Commerce—*security*; K.5.m [**Legal Aspects of Computing**]: Miscellaneous; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

## General Terms

Legal Aspects, Security, Verification

## Keywords

Non-repudiation, Fair Exchange, Formal Verification

## 1. INTRODUCTION

When public key cryptography was first presented, it was pointed out that its techniques "also protect against the *threat of dispute*. That is, a message may be sent but later repudiated by either the transmitter or the receiver. Or, it may be alleged by either party that a message was sent when in fact none was" [21]. When the first practical implementation of public key cryptography was presented, it was observed that the capability to produce unforgeable digital signatures offers a step beyond privacy and authentication: "the recipient can convince a 'judge' that the signer sent the message" [28].

This is but an instance of a more general problem, that of *non-repudiation*: a party that has taken part in a communication should not be able to falsely deny the truth or validity of the communication or its parts. Unforgeable digital signatures are part of the solution; however, the problem is complicated when non-repudiation is, additionally, required to be *fair*.

Intuitively, a protocol is fair if it does not allow a party to gain an undue advantage. A simple exchange of signed items is not fair: it does not guard against threat of disputes, unless the signed items are exchanged simultaneously; otherwise the first recipient may never send her own item. Simultaneity, however, is hard to achieve when the parties do not interact face to face.

If fairness is ensured completely within the system specified by the protocol it is *strong*; if fairness is ensured within the system but with the proviso that additional assumptions about the participating parties are made it is *eventually strong*; and if fairness is ensured by external means it is *weak* [24]. Strong fairness ensures that it is never the case that only one party gets what she expects from the other. Weak fairness ensures that it is possible for a slighted party to prove her case to a judge (e.g., there is all the necessary evidence for the slighted party to convince the judge to strike down on the miscreant). In eventual strong fairness, recourse to external means is avoided at the cost of extra assumptions, such as that the parties follow a certain behaviour (e.g., eventually cooperate).

A number of non-repudiation protocols purporting to be fair, in general, have been proposed. In § 2 we introduce the main ideas. Then, in § 3, we list some guidelines to the practitioner who wants to implement and deploy a fair non-repudiation protocol. The guidelines are illustrated by way of a family of such protocols, descendants of a single ancestor. Some conclusions are offered in § 4.

The present paper follows previous work presenting informal guidelines for the design of cryptographic protocols [35, 5, 1]. It differs from the existing corpus in two ways: it deals specifically with non-repudiation (although its findings may be of wider interest); and it dons two hats: that of the protocol designer, and that of the implementer, as it is mindful of the ramifications of putting a protocol to practice.

As an aside, the author had no part in the development