Constant Phase Bit Optimal Protocols for Perfectly Reliable and Secure Message Transmission

Arpita Patra[1], Ashish Choudhary[1,⋆], K. Srinathan[2], and C. Pandu Rangan[1,⋆⋆]

[1] Dept of Computer Science and Engineering
IIT Madras, Chennai India 600036
arpita@cse.iitm.ernet.in, ashishc@cse.iitm.ernet.in, rangan@iitm.ernet.in
[2] International Institute of Information Technology
Hyderabad India 500032
srinathan@iiit.ac.in

Abstract. In this paper, we study the problem of *perfectly reliable message transmission*(PRMT) and *perfectly secure message transmission*(PSMT) between a sender **S** and a receiver **R** in a synchronous network, where **S** and **R** are connected by n vertex disjoint paths called wires, each of which facilitates bidirectional communication. We assume that atmost t of these wires are under the control of adversary. We present two-phase-*bit optimal* PRMT protocol considering Byzantine adversary as well as mixed adversary. We also present a three phase PRMT protocol which reliably sends a message containing l field elements by overall communicating $O(l)$ field elements. This is a significant improvement over the PRMT protocol proposed in [10] to achieve the same task which takes $log(t)$ phases. We also present a three-phase-*bit-optimal* PSMT protocol which securely sends a message consisting of t field elements by communicating $O(t^2)$ field elements.

Keywords: Reliable and Secure Communication, Information Theoretic Security, Communication Efficiency.

1 Introduction

In the problem of *perfectly reliable message transmission* (PRMT), a sender **S** is connected to **R** in an unreliable network by n vertex disjoint paths called wires; **S** wishes to send a message m chosen from a finite field $\mathbb{F}$ reliably to **R**, in a guaranteed manner, inspite of the presence of several kinds of faults in the network. The problem of *perfectly secure message transmission*(PSMT) has an additional constraint that the adversary should get no information about m. The faults in

⋆ Work Supported by Project No. CSE/05-06/076/DITX/CPAN on Protocols for Secure Communication and Computation Sponsored by Department of Information Technology, Government of India.

⋆⋆ Work Supported by Microsoft Project No CSE0506075MICOCPAN on Foundation Research in Cryptography.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 221–235, 2006.

the network is modeled by an *adversary* who controls the actions of nodes in the network in a variety of ways. There are various network settings, fault models and computational models in which PRMT and PSMT problem has been studied extensively [3,2,4,13,12,5,7,11]. The PRMT and PSMT problems are very important primitives in various reliable and secure distributed protocols.

In this paper, we focus on undirected synchronous networks, where the adversary is an adaptive threshold Byzantine adversary having infinite computing power. In the past, PRMT and PSMT had been studied extensively in this setting [3,13,15,10,1]. The problem of PRMT and PSMT in this setting was first posed in [3]. In [3], it is proved that for t Byzantine faults, a two phase or three phase protocol exists iff there exists atleast $2t+1$ vertex disjoint paths between **S** and **R**. However, the protocols of [3] involve lot of communication overhead. These protocols were improved significantly in [13]. However, the protocols of both [3] and [13] consider the problem of sending only one field element reliably and securely. So, in order to send a message consisting more than one field elements, we have to parallely execute these protocols for individual field elements, which will result in a huge communication overhead. This problem was first addressed in [15], where the authors attempted to give optimal PRMT and PSMT protocols to send messages containing more than one field element. In [15], the authors proved a lower bound of $\Omega(\frac{nl}{n-2t})$ field elements to be communicated to send a message containing l field elements reliably(securely) by using any two phase PRMT(PSMT) protocol. In view of this lower bound, any two phase PRMT(PSMT)protocol, which achieves this bound to send a message containing l field elements, reliably(securely) is called bit optimal two phase PRMT(PSMT) protocol. In [15], the authors claimed a two phase secure and reliable protocol to achieve this bound. However, in [1], the protocol of [15] has been proved to be unreliable. In [1], a two phase optimal PSMT(also PRMT) protocol has been proposed to send a message of size $O(t)$ securely and reliably by communicating overall $O(t^2)$ field elements. However, the protocol performs local computation(computation by **S** and **R**) which is not polynomial in n. Thus there doesnot exist any two phase polynomial time bit optimal PRMT protocol. In this paper, we propose a two phase bit optimal PRMT protocol, which performs local computation which is polynomial in n. We also show how to extend this protocol to incorporate additional faults of type omission and failstop.

In [10], a $log(t)$ phase protocol has been proposed to reliably send a message m of sufficiently large length l ($l = \Omega(nlog^2n)$, by communicating overall $O(l)$ field elements. In this paper, we significantly improve the above result by proposing a three phase protocol that reliably sends a message of size $l(l = \Omega(t^2))$ by communicating $O(l)$ field elements. Thus we can achieve reliability for free! We also propose a three phase PSMT protocol, that securely sends a message of size $O(t)$ by communicating overall $O(t^2)$ field elements. Though, the same task can be done by using the two phase protocol of [1], as mentioned earlier, their protocol involve huge amount of local computation, which is not polynomial in n. However, the three phase protocol proposed in this paper involves only polynomial time computation.