Absolutely Secure Message Transmission Using a Key Sharing Graph

M1303 Yoshihiro INDO  Nishizeki Lab.

July 30, 2012

Abstract

Assume that there are players and an eavesdropper Eve of unlimited computational power and that several pairs of players have shared secret keys beforehand. In a key sharing graph, each vertex corresponds to a player, and each edge corresponds to a secret key shared by the two players corresponding to the ends of the edge. Given a key sharing graph, a player wishes to send a message to another player so that the eavesdropper Eve and any other player can get no information on the message. In this thesis, we first give a necessary and sufficient condition on a key sharing graph for the existence of such a unicast protocol. We then extend the condition to the case where a multiple number of players other than the sender and receiver passively collude. We finally give a sufficient condition for the existence of a secure multicast protocol.

1 Summary

Achieving secure communication has been one of the most important problems in information technology. There are a lot of works on secure message transmissions. Many conventional models assume a communication network consisting of various channels: private communication channels, partial broadcast channels [2], multicast channels and neighbor network channels [1]. In contrast, our model assumes that every communication is done through a public network and may be overheard by anyone, but assumes that several pairs of players have shared secret keys beforehand as in [3, 4]. Under such a model we deal with a secure message transmission using a public network and secret keys shared by several pairs of players. More precisely, we consider the following situation.

There are \( n \geq 2 \) players \( p_1, p_2, \ldots, p_n \) and an eavesdropper Eve of unlimited computational power, and several pairs of players have already shared secret keys. For simplicity, a message and all secret keys are assumed to be one-bit numbers, although our results can be easily generalized to the case where a message and all keys are \( \ell \)-bit numbers for a positive number \( \ell \). Let \( G \) be a graph, called a key sharing graph [3, 4], in which each vertex represents a player \( p_i, 1 \leq i \leq n \), and each edge \( p_ip_j \) joining vertices \( p_i \) and \( p_j \) represents a secret key \( k_{ij} \in \{0, 1\} \) shared by players \( p_i \) and \( p_j \), as illustrated in Fig. 1. A secret key \( k_{ij} \) is known only to players \( p_i \) and \( p_j \). All players and Eve know the shape of graph \( G \). Every communication (conversation) between players through a public network can be overheard by any player and Eve. Since Eve has an unlimited computational power, one cannot use any cryptographic protocol based on the computational hardness assumption such as the RSA public key cryptosystem. All players can generate random numbers (flip coins), and are “honest,” that is, follow a specified protocol and do not “lie.”

![Figure 1: An example of key sharing graph G.](image)

Under such a situation, if \( G \) is a connected graph, that is, \( G \) has a spanning tree as drawn by thick lines in Fig. 1, then any player, say \( p_1 \), can send a one-bit message to all the other players so that the eavesdropper Eve can get no information on the message. Clearly, this can be done, within \( n - 1 \) communication rounds, by the “flooding protocol”, which floods the message from \( p_1 \) to the other players by using the secret keys on a spanning tree. This can also be done with exactly one communication round [4].
In this thesis we first consider a unicast protocol by which a player, say $p_1$, sends a message $m$ to a designated player, say $p_2$, so that Eve and any player other than $p_1$ and $p_2$ cannot get any information on $m$. We prove that there is such a unicast protocol if and only if $G$ has either an edge $p_1p_2$ joining vertices $p_1$ and $p_2$ or a path of either $p_1$ and $p_2$, having no common vertices except $p_1$ and $p_2$. This result immediately implies that such a secure message transmission can be done between every pair of players if and only if $G$ is a 2-connected graph.

We then extend the result to the case where a multiple number of players other than $p_1$ and $p_2$ passively collude. More precisely, we showed that a player $p_1$ can send a message $m$ to another player $p_2$ absolutely securely against a $c$-collusive attack if and only if the key sharing graph $G$ has either an edge joining $p_1$ and $p_2$ or a set of $c + 1$ internally disjoint paths between $p_1$ and $p_2$. This result implies that every player can send a message to any other player absolutely securely against a $c$-collusive attack if and only if the key sharing graph $G$ is $(c + 1)$-connected.

We finally give a sufficient condition for the existence of a multicast protocol by which a player $p_1$ can send a message to a multiple number of designated players, say $p_2, p_3, \ldots, p_q$, so that Eve and any other player get no information on the message.

Let $V$ be the set of all players, that is, $V = \{p_1, p_2, \ldots, p_n\}$. Let $Q = \{p_1, p_2, \ldots, p_q\}$. For a subset $Q^*$ of $Q$ with $|Q^*| = q^* \geq 2$, we define a graph $F(Q^*)$, as follows. Let $t$ be a positive integer, and let $T_1, T_2, \ldots, T_t$ be $t$ trees such that

(a) each tree $T_i$, $1 \leq i \leq t$, contains all the vertices in $Q^*$ and possibly some other vertices in $V$;
(b) any vertex $p_\ell \in V - Q$ is not contained in at least one of the $t$ trees $T_1, T_2, \ldots, T_t$; and
(c) $T_1, T_2, \ldots, T_t$ are pairwise edge-disjoint.

Then $F(Q^*)$ is the union of these $t$ trees $T_1, T_2, \ldots, T_t$. We now define a graph $\hat{F}$ in terms of graphs $F(Q^*)$. Let $s$ be a positive integer, and let $Q_1, Q_2, \ldots, Q_s$ be subsets of $Q$ satisfying the following (a)–(c):

(a) $Q = Q_1 \cup Q_2 \cup \cdots \cup Q_s$;
(b) $Q_1, Q_2, \ldots, Q_s$ are “connecting,” that is, for any indices $i$ and $j$, $1 \leq i < j \leq s$, there is a sequence $i_1, i_2, \ldots, i_k$ of indices such that $i_1 = i$, $i_k = j$, and $Q_{i_\ell} \cap Q_{i_{\ell+1}} \neq \emptyset$ for every $\ell$, $1 \leq \ell \leq k - 1$; and
(c) there exist pairwise edge-disjoint graphs $F(Q_1), F(Q_2), \ldots, F(Q_s)$.

Then let $\hat{F}$ be the union of graphs $F(Q_1), F(Q_2), \ldots, F(Q_s)$. Clearly $\hat{F}$ is a connected graph, which contains all vertices $p_1, p_2, \ldots, p_q$ and possibly some others. It should be noted that $F(Q_i)$ and $F(Q_j)$, $1 \leq i < j \leq s$, may share a common vertex $p_\ell \notin Q$.

We showed that a player $p_1$ can send a message $m$ to players $p_2, p_3, \ldots, p_q$ absolutely securely if the key sharing graph $G$ contains $\hat{F}$ as a subgraph.

2 Conclusions

For simplicity, we assumed that a message and all secret keys are 1-bit numbers. However, one can easily extend the results to the case where a message and all secret keys are $\ell$-bit numbers for any $\ell (\geq 1)$. In this case, $\oplus$ must be a bit-wise exclusive OR.

It is desirable to find a necessary and sufficient condition for the existence of a secure multicast protocol.

References


Publications