Secure Communication in Broadcast Channels: The Answer to Franklin and Wright's Question*

Yongge Wang[1] and Yvo Desmedt[1,2]

[1] Department of EE & CS, University of Wisconsin – Milwaukee,
P.O. Box 784, WI 53201 Milwaukee, USA,
{wang,desmedt}@cs.uwm.edu
[2] The Center of Cryptography, Computer and Network Security
CEAS, University of Wisconsin – Milwaukee, and
Dept. of Mathematics, Royal Holloway, University of London, UK

Abstract. Problems of secure communication and computation have been studied extensively in network models. Goldreich, Goldwasser, and Linial, Franklin and Yung, and Franklin and Wright have initiated the study of secure communication and secure computation in multi-recipient (broadcast) models. A "broadcast channel" (such as ethernet) enables one processor to send the same message—simultaneously and privately—to a fixed subset of processors. In their Eurocrypt '98 paper, Franklin and Wright have shown that if there are n broadcast lines between a sender and a receiver and there are at most t malicious (Byzantine style) processors, then the condition $n > t$ is necessary and sufficient for achieving efficient probabilisticly reliable and probabilisticly private communication. They also showed that if $n > \lceil 3t/2 \rceil$ then there is an efficient protocol to achieve probabilisticly reliable and perfectly private communication. And they left open the question whether there exists an efficient protocol to achieve probabilisticly reliable and perfectly private communication when $\lceil 3t/2 \rceil \geq n > t$. In this paper, by using a different authentication scheme, we will answer this question affirmatively and study related problems.

Keywords: Network security, Privacy, Perfect secrecy, Reliability.

1 Introduction

If two parties are connected by a private and authenticated channel, then secure communication between them is guaranteed. However, in most cases, many parties are only indirectly connected, as elements of an incomplete network of private and authenticated channels. In other words they need to use intermediate or internal nodes. Achieving participants cooperation in the presence of faults is

* Research supported by DARPA F30602-97-1-0205. However the views and conclusions contained in this paper are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Defense Advance Research Projects Agency (DARPA), the Air Force, of the US Government.

J. Stern (Ed.): EUROCRYPT'99, LNCS 1592, pp. 446–458, 1999.
© Springer-Verlag Berlin Heidelberg 1999

a major problem in distributed networks. The interplay of network connectivity and secure communication have been studied extensively (see, e.g., [1,4,6,7,12]). For example, Dolev [6] and Dolev et al. [7] showed that, in the case of t Byzantine faults, reliable communication is achievable only if the systems's network is $2k+1$ connected. Hadzilacos [12] has shown that even in the absence of malicious failures connectivity $t+1$ is required to achieve reliable communication in the presence of t faulty participants.

Goldreich, Goldwasser, and Linial [11], Franklin and Yung [9], and Franklin and Wright [8] have initiated the study of secure communication and secure computation in *multi-recipient (broadcast)* models. A "broadcast channel" (such as ethernet) enables one participant to send the same message—simultaneously and privately—to a fixed subset of participants. Franklin and Yung [9] have given a necessary and sufficient condition for individuals to exchange private messages in broadcast models in the presence of passive adversaries (passive gossipers). For the case of active Byzantine adversaries, many results have been presented by Franklin and Wright [8]. Note that Goldreich, Goldwasser, and Linial [11] have also studied the fault-tolerant computation in the public broadcast model in the presence of active Byzantine adversaries.

There are many examples of broadcast channels. A simple example is a local area network like an Ethernet bus or a token ring. Another example is a shared cryptographic key. By publishing an encrypted message, a participant initiates a broadcast to the subset of participants that is able to decrypt it.

We will abstract away the concrete network structures and consider multicast graphs. Specifically, a multicast graph is just a graph $G(V, E)$. A vertex $A \in V$ is called a neighbor of another vertex $B \in V$ if there there is an edge $(A, B) \in E$. In a multicast graph, we assume that any message sent by a node A will be received identically by all its neighbors, whether or not A is faulty, and all parties outside of A's neighbor learn nothing about the content of the message. The neighbor networks have been studied by Franklin and Yung in [9]. They have also studied the more general notion of hypergraphs, which we do not need.

As Franklin and Wright [8] have pointed out, unlike the simple channel model, it is not possible to directly apply protocols over multicast lines to disjoint paths in a general multicast graph, since disjoint paths may have common neighbors. Franklin and Wright have shown that in certain cases the change from simple channel to broadcast channel hurts the adversary more than it helps, because the adversary suffers from the restriction that an incorrect transmission from a faulty processor will always be received identically by all of its neighbors.

It was shown [8] that if there are n broadcast lines (that is, n paths with disjoint neighborhoods) between a sender and a receiver and there are at most t malicious (Byzantine style) processors, then the condition $n > t$ is necessary and sufficient for achieving efficient probabilisticly reliable and probabilisticly private communication. They also showed that there is an efficient protocol to achieve probabilisticly reliable and perfectly private communication when $n > \lceil 3t/2 \rceil$, and there is an exponential bit complexity protocol for achieving probabilisticly reliable and perfectly private communication when $\lceil 3t/2 \rceil \geq n > t$. However,

they left open the question whether there exists an efficient protocol to achieve probabilisticly reliable and perfectly private communication when $\lceil 3t/2 \rceil \geq n > t$. In this paper, by using a different authentication scheme, we will answer this question affirmatively and study related problems. We will also show that it is **NP**-complete to decide whether a multicast graph has n disjoint broadcast lines (that is, n paths with disjoint neighborhoods).

Note that, similar as in Franklin and Wright [8], we will only consider the scenario when the underlying graph is known to all nodes. For the scenario that the graph is unknown, the protocols may be completely different, see Burmester, Desmedt, and Kabatianski [2].

2 Models

Throughout this paper, n denotes the number of multicast lines and t denotes the number of faults under the control of the adversary. We write $|S|$ to denote the number of elements in the set S. We write $x \in_R S$ to indicate that x is chosen with respect to the uniform distribution on S. Let $\mathbf{F}$ be a finite field, and let $a, b, M \in \mathbf{F}$. We define $\text{auth}(M, a, b) = aM + b$ (following [10,13,14]). In this paper, we will also use a multiple authentication scheme. That is, for $a, b, c, d, M \in \mathbf{F}$, let $\text{bauth}(M, a, b, c, d) = aM^3 + bM^2 + cM + d$. Note that the main advantage of the function bauth() is that each authentication key (a, b, c, d) can be used to authenticate three different messages M_0, M_1, and M_2 without revealing any information of the authentication key. While for the function auth() each authentication key (a, b) can only be used to authenticate one message (that is, it is a kind of one-time pad) (see Simmons [15]). Note that den Boer [5] used similar polynomials to construct one-time authentication schemes.

Theorem 1. *Let (a, b, c, d) be chosen uniformly from $\mathbf{F}^4$, $M_i \in \mathbf{F}$ for $i = 0, 1, 2$, and $s_i = \text{bauth}(M_i, a, b, c, d)$ for $i = 0, 1, 2$ be the authentication code of M_i respectively. Then, for any $a_0, b_0, c_0, d_0 \in \mathbf{F}$,*

$$\Pr[a{=}a_0|view_0] = \Pr[b{=}b_0|view_0] = \Pr[c{=}c_0|view_0] = \Pr[d{=}d_0|view_0] = \frac{1}{|\mathbf{F}|}$$

where $view_0 = (M_0, s_0, M_1, s_1, M_2, s_2)$

Proof. By the condition, we have the following three equations with four unknowns:

$$\begin{aligned} M_0^3 a + M_0^2 b + M_0 c + d &= s_0 \\ M_1^3 a + M_1^2 b + M_1 c + d &= s_1 \\ M_2^3 a + M_2^2 b + M_2 c + d &= s_2. \end{aligned}$$

Since the coefficient matrix of the above equations is a so-called Vandermonde matrix, no value of a can be ruled out. That is, every a is equally likely given the values $(M_0, s_0, M_1, s_1, M_2, s_2)$. (A similar argument applies for b, or c or d.) This completes the proof of the theorem. □

Following Franklin and Wright [8], we consider multicast as our only communication primitive. A message that is multicast by any node in a multicast neighbor network is received by all its neighbors with privacy (that is, non-neighbors learn nothing about what was sent) and authentication (that is, neighbors are guaranteed to receive the value that was multicast and to know which neighbor multicast it). In our models, we assume that all nodes in the multicast graph know the complete protocol specification and the complete structure of the multicast graph. In a message transmission protocol, the sender A starts with a message M^A drawn from a message space $\mathcal{M}$ with respect to a certain probability distribution. At the end of the protocol, the receiver B outputs a message M^B. We consider a synchronous system in which messages are sent via multicast in rounds. During each round of the protocol, each node receives any messages that were multicast by its neighbors at the end of the previous round, flips coins and perform local computations, and then possibly multicast a message. We will also assume that the message space $\mathcal{M}$ is a representable subset of the finite field $\mathbf{F}$.

Generally there are two kinds of adversaries. A passive adversary (or gossiper adversary) is an adversary who can only observe the traffics through t internal nodes. An active adversary (or Byzantine adversary) is an adversary with unlimited computational power who can control t internal nodes. That is, an active adversary will not only listen to the traffics through the controlled nodes, but also control the message sent by those controlled nodes. Both kinds of adversaries are assumed to know the complete protocol specification, message space, and the complete structure of the multicast graph. At the start of the protocol, the adversary chooses the t faulty nodes. A passive adversary can view the behavior (coin flips, computations, message received) of all the faulty nodes. An active adversary can view all the behavior of the faulty nodes and, in addition, control the message that they multicast. We allow for the strongest adversary. (An alternative interpretation is that t nodes are collaborating adversaries.)

For any execution of the protocol, let *adv* be the adversary's view of the entire protocol. We write $adv(M, r)$ to denote the adversary's view when $M^A = M$ and when the sequence of coin flips used by the adversary is r.

Definition 2. *(see Franklin and Wright [8])*

1. *A message transmission protocol is* δ-reliable *if, with probability at least* $1-\delta$, *B terminates with $M^B = M^A$. The probability is over the choices of M^A and the coin flips of all nodes.*
2. *A message transmission protocol is* ε-private *if, for every two messages M_0, M_1 and every r, $\sum_c |\Pr[adv(M_0, r) = c] - \Pr[adv(M_1, r) = c]| \leq 2\varepsilon$. The probabilities are taken over the coin flips of the honest parties, and the sum is over all possible values of the adversary's view.*
3. *A message transmission protocol is* perfectly private *if it is* 0-private.
4. *A message transmission protocol is* (ε, δ)-secure *if it is ε-private and δ-reliable.*

5. *An (ε, δ)-secure message transmission protocol is* efficient *if its round complexity and bit complexity are polynomial in the size of the network,* $\log \frac{1}{\varepsilon}$ *(if* $\varepsilon > 0$*) and* $\log \frac{1}{\delta}$ *(if* $\delta > 0$*).*

3 Background: Reliable Communication over Neighbor Networks

In this section, we review Franklin and Wright's Eurocrypt '98 protocols for reliable communication over multicast lines. The reader familiar with these protocols can skip this section. For two vertices A and B in a multicast graph $G(V, E)$, we say that A and B are connected by n neighborhood (except A and B) disjoint *lines* if there are n lines $p_1, \ldots, p_n \subseteq V$ with the following properties:

- For each $j \leq n$, the j-th line p_j is a sequence of $m_j + 2$ nodes $A = X_{0,j}$, $X_{1,j}, \ldots, X_{m+1,j} = B$ where $X_{i,j}$ is a neighbor of $X_{i+1,j}$.
- For each i_1, i_2, j_1, and j_2 with $j_1 \neq j_2$, the only possible common neighbors of X_{i_1,j_1} and X_{i_2,j_2} are A and B.

If there is no ambiguity we drop the "except A and B."

Without loss of generality, in this section we assume that party A (the message transmitter) and party B (the message recipient) are connected by n neighborhood disjoint *lines*, and we assume that $m_1 = m_2 = \ldots = m_n$.

Basic Propagation Protocol (Franklin and Wright [8]) In this protocol, A tries to propagate a value s^A to B.

- In round 1, A multicast s^A.
- In round ρ for $2 \leq \rho \leq m + 1$, each $X_{\rho-1,j} (1 \leq j \leq n)$ expects to receive a single element from $X_{\rho-2,j}$. Let $u_{\rho-1,j}$ be this value if a value was in fact received, or a publicly known default element otherwise. At the end of round ρ, $X_{\rho-1,j}$ multicast $u_{\rho-1,j}$.
- In round $m + 2$, B receives a single element from each $X_{m,j}$, or substitutes the default element. Let s_j^B be the value received or substituted on line j.

From now on when a party substitutes the default element, we just say that the party substitutes.

Full Distribution Protocol (Franklin and Wright [8]) In this protocol, each internal node $X_{i,j}$ tries to transmit an element $s_{i,j}$ to both A and B.

- In round 1, each $X_{i,j} (1 \leq i \leq m, 1 \leq j \leq n)$ multicast $s_{i,j}$ to (in particular) $X_{i-1,j}$ and $X_{i+1,j}$.
- In round ρ for $2 \leq \rho \leq m + 1$:
  - For $1 \leq j \leq n$ and $\rho \leq i \leq m$, each $X_{i,j}$ expects to be the intended recipient of an element from $X_{i-1,j}$ (initiated by $X_{i-\rho+1,j}$). Let $u_{i,j}$ be the received value or a default value if none is received.

- For $1 \leq j \leq n$ and $1 \leq i \leq m - \rho + 1$, $X_{i,j}$ expects to be the intended recipient of an element from $X_{i+1,j}$ (initiated by $X_{i+\rho-1,j}$). Let $v_{i,j}$ be the received or default value.
- For $1 \leq j \leq n$, B expects to be the intended recipient on the j-th line of a single element (initiated by $X_{m-\rho+2,j}$). Let $s^B_{m-\rho+2,j}$ be the received or default value.
- For $1 \leq j \leq n$, A expects to be the intended recipient on the j-th line of a single element (initiated by $X_{\rho-1,j}$). Let $s^A_{\rho-1,j}$ be the received or default value.
- $X_{i,j}$ multicasts $u_{i,j}$ to $X_{i+1,j}$ if $\rho \leq i \leq m$, and $v_{i,j}$ to $X_{i-1,j}$ if $1 \leq i \leq m - \rho + 1$.

Fact 3. *(Franklin and Wright [8]) If there are no faults on the j-th line, then $s^A_{i,j} = s^B_{i,j}$ for all $1 \leq i \leq m$. Further, if $X_{i,j}$ is the only fault on the j-th line, then $s^A_{i,j} = s^B_{i,j}$.*

Reliable Transmission Protocol (Franklin and Wright [8]) In this protocol, A tries to reliably transmit a message M^A to B.

- The nodes on all the n lines execute an instance of the Full Distribution Protocol, which takes place during rounds 1 through $m+1$. The element that $X_{i,j}$ initiates is $(a_{i,j}, b_{i,j})$ which is randomly chosen from $\mathbf{F}^2$. Let $(a^A_{i,j}, b^A_{i,j})$ and $(a^B_{i,j}, b^B_{i,j})$ be the values that A and B receive or substitute as the element initiated by $X_{i,j}$.
- The nodes on all the n lines execute an instance of the Basic Propagation Protocol from A to B, which takes place during rounds $m+2$ through $2m+3$. The element that A initiates is $\{(i, j, M^A, \text{auth}(M^A, a^A_{i,j}, b^A_{i,j})) : 1 \leq i \leq m, 1 \leq j \leq n\}$. In round $2m+3$, B receives or substitutes $\{(i, j, M^B_{i,j,k}, u^B_{i,j,k}) : 1 \leq i \leq m, 1 \leq j \leq n\}$ on the k-th line, $1 \leq k \leq n$.
- Let $r_k(M) = \{j : \exists i(M = M^B_{i,j,k} \& u^B_{i,j,k} = \text{auth}(M^B_{i,j,k}, a^B_{i,j}, b^B_{i,j}))\}$. B outputs M^B that maximizes $\max_k |r_k(M^B)|$.

Theorem 4. *(Franklin and Wright [8]) If $\delta > 0$, $n > t$, and $|\mathbf{F}| > mn^2/\delta$, then the Reliable Transmission Protocol is an efficient δ-reliable message transmission protocol.*

4 Reliable and Private Communication over Neighbor Networks

4.1 Survey of Franklin-Wright's Results

As in the previous section, we assume that party A (the message transmitter) and party B (the message recipient) are connected by n neighborhood disjoint *lines*. Franklin and Wright showed the following results regarding to privacy in broadcast networks:

1. If $n > t$, $\delta > 0$ and $\varepsilon > 0$, then there is an efficient (ε, δ)-secure message transmission protocol between A and B.
2. If $n > \lceil 3t/2 \rceil$ and $\delta > 0$, then there is an efficient $(0, \delta)$-secure message transmission protocol between A and B, that is, a δ-reliable and perfect private message transmission protocol.
3. If $t < n \leq \lceil 3t/2 \rceil$ and $\delta > 0$, then there is an exponential bit complexity $(0, \delta)$-secure message transmission protocol between A and B.

4.2 The Franklin-Wright's Open Problem

They left open the question whether it is possible to efficiently achieve perfect privacy when $t < n \leq \lceil 3t/2 \rceil$. That is, does there exist a polynomial time $(0, \delta)$-secure message transmission protocol between A and B when $t < n \leq \lceil 3t/2 \rceil$? We give an affirmative answer to this question.

4.3 The Solution

Intuitively, our protocol proceeds as follows. First, using the Full Distribution Protocol from the preceding section, each internal node $X_{i,j}$ transmits a random authentication key $(a_{i,j}, b_{i,j}, c_{i,j}, d_{i,j}) \in_R \mathbf{F}^4$ to both A and B. Secondly, using the Basic Propagation Protocol, B transmits to A a random $r \in_R \mathbf{F}$ authenticated by the keys in $\{(a_{i,j}, b_{i,j}, c_{i,j}, d_{i,j}) : 1 \leq i \leq m, 1 \leq j \leq n\}$. Thirdly, for each $1 \leq j \leq n$, A decides whether A and B agree on at least one authentication key on the j-th line. Let

$$K^A = \{(i_j, j) : (a^A_{i_j,j}, b^A_{i_j,j}, c^A_{i_j,j}, d^A_{i_j,j}) \text{ is the first key agreed upon by } A \text{ and } B \text{ on the } j\text{-th line}\}.$$

Lastly, A encrypts the message M^A using the sum of the pads $a^A_{i_j,j}$ $((i_j, j) \in K^A)$ and, using the Basic Propagation Protocol, transmits to B the set K^A and the ciphertext authenticated by the keys in $\{(a^A_{i,j}, b^A_{i,j}, c^A_{i,j}, d^A_{i,j}) : 1 \leq i \leq m, 1 \leq j \leq n\}$. Lastly, B decrypts the message.

Perfectly Private Transmission Protocol

- The nodes on all the n lines execute an instance of the Full Distribution Protocol, which takes place during rounds 1 through $m + 1$. The element that $X_{i,j}$ initiates is $(a_{i,j}, b_{i,j}, c_{i,j}, d_{i,j})$ which is randomly chosen from $\mathbf{F}^4$. Let $(a^A_{i,j}, b^A_{i,j}, c^A_{i,j}, d^A_{i,j})$ and $(a^B_{i,j}, b^B_{i,j}, c^B_{i,j}, d^B_{i,j})$ be the values that A and B receive or substitute as the element initiated by $X_{i,j}$.
- The nodes on all the n lines execute an instance of the Basic Propagation Protocol from B to A, which takes place during rounds $m+2$ through $2m+3$. The element that B initiates is $\{(i, j, r^B, \text{bauth}(r^B, a^B_{i,j}, b^B_{i,j}, c^B_{i,j}, d^B_{i,j})) : 1 \leq i \leq m, 1 \leq j \leq n\}$, where $r^B \in_R \mathbf{F}$. In round $2m+3$, A receives or substitutes $\{(i, j, r^A_{i,j,k}, u^A_{i,j,k}) : 1 \leq i \leq m, 1 \leq j \leq n\}$ on the k-th line, $1 \leq k \leq n$.

- Let $r_k(r) = \{j : \exists i(r = r^A_{i,j,k} \& u^A_{i,j,k} = \text{bauth}(r^A_{i,j,k}, a^A_{i,j}, b^A_{i,j}, c^A_{i,j}, d^A_{i,j}))\}$, r^A be the message that maximizes $|r_{k^A}(r^A)| = \max_k |r_k(r^A)|$, and let $K^A = \{(i_j, j) : j \in r_{k^A}(r^A), \forall (0 < i < i_j)(u^A_{i,j,k^A} \neq \text{bauth}(r^A, a^A_{i,j}, b^A_{i,j}, c^A_{i,j}, d^A_{i,j}))\}$. A computes $z^A = M^A + \sum_{(i_j,j) \in K^A} a^A_{i_j,j}$.
- In rounds $2m + 4$ through $3m + 5$, the nodes on all the n lines execute an instance of the Basic Propagation Protocol from A to B. The element that A initiates is $\{(i, j, z^A, K^A, \text{bauth}(\langle z^A, K^A \rangle, a^A_{i,j}, b^A_{i,j}, c^A_{i,j}, d^A_{i,j})) : 1 \leq i \leq m, 1 \leq j \leq n\}$, where $\langle z^A, K^A \rangle$ denotes the concatenation of z^A and K^A (without loss of generality, we assume that prefix-free codes are used so that we can uniquely recover z^A and K^A from $\langle z^A, K^A \rangle$). In round $3m + 5$, B receives or substitutes $\{(i, j, z^B_{i,j,k}, K^B_{i,j,k}, u^B_{i,j,k}) : 1 \leq i \leq m, 1 \leq j \leq n\}$ on the k-th line, $1 \leq k \leq n$.
- $R_k(\langle z, K \rangle) = \{j : \exists i(\langle z, K \rangle = \langle z^B_{i,j,k}, K^B_{i,j,k} \rangle \ \& \ u^B_{i,j,k} = \text{bauth}(\langle z^B_{i,j,k}, K^B_{i,j,k} \rangle, a^B_{i,j}, b^B_{i,j}, c^B_{i,j}, d^B_{i,j}))\}$, and let $\langle z^B, K^B \rangle$ be the message that maximizes the following: $|R_{k^B}(\langle z^B, K^B \rangle)| = \max_k |R_k(\langle z^B, K^B \rangle)|$. B outputs $M^B = z^B - \sum_{(i_j,j) \in K^B} a^B_{i_j,j}$.

The Perfectly Private Transmission Protocol provides efficient $(0, \delta)$-secure message transmission provided that the field $\mathbf{F}$ used by bauth() satisfies $|\mathbf{F}| \geq \frac{2(3n+mn^2)}{\delta}$. Since reliable communication is not possible when $t \geq n$, this protocol provides matching upper and lower bounds for perfect privacy and probabilistic reliability.

Theorem 5. *If $\delta > 0$, $n > t$, and $|\mathbf{F}| > 2(3n + mn^2)/\delta$, then the Perfectly Private Transmission Protocol is an efficient $(0, \delta)$-secure message transmission protocol.*

Proof. Let w_0 denote the number of lines with no faults, w_1 the number with exactly one fault, and w_+ the number with two or more faults. Then since $n > t$, it follows that $w_0 > w_+$. By Fact 3, $|K^A| \geq w_0 + w_1 > w_+ + w_1$. Whence there is a $(i_{j^*}, j^*) \in K^A$ such that the j^*-th line is a non-faulty line, and $a^A_{i_{j^*},j^*} = a_{i_{j^*},j^*}$, $b^A_{i_{j^*},j^*} = b_{i_{j^*},j^*}$, $c^A_{i_{j^*},j^*} = c_{i_{j^*},j^*}$, and $d^A_{i_{j^*},j^*} = d_{i_{j^*},j^*}$. By Theorem 1, the adversary gets no information about $a^A_{i_{j^*},j^*}$ given the view adv_{M^A}, where adv_{M^A} consists of the following information:

1. $\{(i, j, r^B, \text{bauth}(r^B, a^B_{i,j}, b^B_{i,j}, c^B_{i,j}, d^B_{i,j})) : 1 \leq i \leq m, 1 \leq j \leq n\}$;
2. $\{(i, j, z^A, K^A, \text{bauth}(\langle z^A, K^A \rangle, a^A_{i,j}, b^A_{i,j}, c^A_{i,j}, d^A_{i,j})) : 1 \leq i \leq m, 1 \leq j \leq n\}$; and
3. at most one randomly guessed (by the adversary) correct authenticator of some random message.

It should be noted that the above item 3 in the adversary's view adv_{M^A} is important for the following reasons: with non zero probability the first transmission from B to A may fail (i.e. in rounds $m + 2$ through $2m + 3$). That is, the adversary may create a bogus $(r^B)'$ (which is different from r^B) and guess the value $\text{bauth}((r^B)', a^B_{i_{j^*},j^*}, b^B_{i_{j^*},j^*}, c^B_{i_{j^*},j^*}, d^B_{i_{j^*},j^*}))$ correctly. Then at the end

of round $2m+3$, A may choose $r^A = (r^B)'$. The consequence is that there may be an item $(i_{j'}, j') \in K^A$ such that

$$(a^A_{i_{j'},j'}, b^A_{i_{j'},j'}, c^A_{i_{j'},j'}, d^A_{i_{j'},j'}) \neq (a^B_{i_{j'},j'}, b^B_{i_{j'},j'}, c^B_{i_{j'},j'}, d^B_{i_{j'},j'}).$$

It is easy for the adversary to decide whether such kind of item exists in K^A. When such an item exists, the adversary knows that he has guessed a correct authenticator of the message $(r^B)'$.

Since $z^A = M^A + a^A_{i_{j^*},j^*} + \sum_{(i_j,j)\in K^A, j\neq j^*} a^A_{i_j,j}$, we have that every M^A is equally likely given adv_{M^A}. Since this is the only relevant information about M^A in adv, we have that $\Pr[adv(M_0, r) = c] = \Pr[adv(M_1, r) = c]$ for every pair of messages M_0 and M_1, adversary's coin flips r, and the possible view c. It follows that $\sum_c |\Pr[adv(M_0, r) = c] - \Pr[adv(M_1, r) = c]| = 0$.

We now prove reliability. Let

$$\begin{aligned} K^{AB} = \{(i_j, j) : \exists i((a^A_{i,j}, b^A_{i,j}, c^A_{i,j}, d^A_{i,j}) = (a^B_{i,j}, b^B_{i,j}, c^B_{i,j}, d^B_{i,j})) \text{ and} \\ \forall(0 < i < i_j)((a^A_{i,j}, b^A_{i,j}, c^A_{i,j}, d^A_{i,j}) \neq (a^B_{i,j}, b^B_{i,j}, c^B_{i,j}, d^B_{i,j}))\}. \end{aligned}$$

It follows from the use of bauth() that the probability that there exists a k and $r' \neq r^B$ with $r_k(r') > w_1 + w_+$ is less than or equal to the probability that at least one fault node guesses a correct authenticator of r', which is again less than $mn^2/|\mathbf{F}|$ (see Franklin and Wright [8]). That is, the first transmission from B to A (i.e. in rounds $m+2$ through $2m+3$) succeeds with the probability at least $1 - mn^2/|\mathbf{F}|$. Let FTR denote the event that the first transmission from B to A succeeds. Now assume that $r^A = r^B$ and $u^A_{i,j,k_A} = \text{bauth}(r^A, a^A_{i,j}, b^A_{i,j}, c^A_{i,j}, d^A_{i,j}))$. Then

$$a^B_{i,j}(r^B)^3 + b^B_{i,j}(r^B)^2 + c^B_{i,j}r^B + d^B_{i,j} = a^A_{i,j}(r^A)^3 + b^A_{i,j}(r^A)^2 + c^A_{i,j}r^A + d^A_{i,j}$$

which implies that r^B is a solution of the equation

$$(a^B_{i,j} - a^A_{i,j})(r^B)^3 + (b^B_{i,j} - b^A_{i,j})(r^B)^2 + (c^B_{i,j} - c^A_{i,j})r^B + (d^B_{i,j} - d^A_{i,j}) = 0 \quad (1)$$

Since $a^A_{i,j}$, $b^A_{i,j}$, $c^A_{i,j}$,$d^A_{i,j}$, $a^B_{i,j}$, $b^B_{i,j}$, $c^B_{i,j}$, and $d^B_{i,j}$ are fixed before the random choice of r^B, and the equation (1) has at most three solutions, it follows that for any fixed $(i_j, j) \in K^A$,

$$\Pr[(a^A_{i_j,j}, b^A_{i_j,j}, c^A_{i_j,j}, d^A_{i_j,j}) \neq (a^B_{i_j,j}, b^B_{i_j,j}, c^B_{i_j,j}, d^B_{i_j,j})|\text{FTR}] \leq 3/|\mathbf{F}|. \quad (2)$$

Then, by the relation (2),

$$\begin{aligned} &\Pr[K^A = K^{AB}|\text{FTR}] \\ &\geq 1 - \sum_{(i_j,j)\in K^A} \Pr[(a^A_{i_j,j}, b^A_{i_j,j}, c^A_{i_j,j}, d^A_{i_j,j}) \neq (a^B_{i_j,j}, b^B_{i_j,j}, c^B_{i_j,j}, d^B_{i_j,j})|\text{FTR}] \\ &\geq 1 - \frac{3n}{|\mathbf{F}|}. \end{aligned}$$

Whence we have

$$\begin{aligned}\Pr[K^A = K^{AB}] &= \Pr[K^A = K^{AB}|\mathrm{FTR}] \cdot \Pr[\mathrm{FTR}] \\ &\geq \left(1 - \frac{mn^2}{|\mathbf{F}|}\right)\left(1 - \frac{3n}{|\mathbf{F}|}\right) \\ &\geq 1 - \frac{3n + mn^2}{|\mathbf{F}|}.\end{aligned}$$

A similar analysis shows that the probability that $K^B \neq K^{AB}$ or $z^B \neq z^A$ is less than $\frac{3n+mn^2}{|\mathbf{F}|}$. Hence our protocol is reliable with the probability

$$\Pr[K^A = K^{AB}] \cdot \Pr[K^B = K^{AB}] \geq \left(1 - \frac{3n + mn^2}{|\mathbf{F}|}\right)^2 \geq 1 - \frac{2(3n + mn^2)}{|\mathbf{F}|}.$$

Since $|\mathbf{F}| > 2(3n + mn^2)/\delta$, it follows that $\Pr[M^B = M^A] > 1 - \delta$. □

Remark: Note that in rounds $2m+4$ through $3m+5$ of our Perfectly Private Transmission Protocol, the information K^A is transmitted explicitly. Indeed, this is not necessary. We can omit the transmission of K^A. Then at the end of round $3m+5$, using the same method that A used to compute the set K^A at the end of round $2m+3$, B can compute K^B (which equals to K^A with high probability). If K^A is not transmitted explicitly, then we can also use the authentication code $\mathrm{bauth}(M, a, b, c) = aM^2 + bM + c$ instead of $\mathrm{bauth}(M, a, b, c, d)$, since even the adversary guesses a correct authentication code on a random $(r^B)'$, he has no idea whether he has succeed. For this modification, the proof for the corresponding Theorem 5 remains the same.

5 Weak Connectivity

In a more general setting of multicast graph, there is a channel from each node to its neighbor nodes. We say that two nodes A and B of a multicast graph is *strongly t-connected* (which was implicitly introduced by Franklin and Wright [8]) if there are t neighborhoods (except A and B) disjoint paths connecting A and B. Franklin and Wright [8] have observed that the multicast lines protocol can be simulated on any strongly $t+1$-connected multicast graph. That is, if A and B are strongly $t+1$-connected, then our results in the previous section shows that $(0, \delta)$-secure message transmission between A and B are possible. In the following, we show that this condition is not necessary.

Franklin and Yung [9] define that two nodes A and B in a multicast graph $G(V, E)$ are *weakly t-connected* if for any set $V_1 \subseteq V \setminus \{A, B\}$ with $|V_1| < t$, the removal of $neighbor(V_1)$ and all incident edges from $G(V, E)$ does not disconnect A and B, where $neighbor(V_1) = V_1 \cup \{v \in V \mid \exists u \in V_1 : (u, v) \in E\} \setminus \{A, B\}$. Franklin and Yung [9] show that it is co**NP** hard to decide whether a given graph is weakly t-connected.

Let A and B be two nodes on a multicast graph $G(V, E)$ and $t < n$. We say that A and B are *weakly (n, t)-connected* if there are n vertex disjoint paths

$p_1, \ldots, p_n$ between A and B and, for any vertex set $T \subseteq (V \setminus \{A, B\})$ with $|T| \leq t$, there exists an i $(1 \leq i \leq n)$ such that all vertices on p_i have no neighbor in T. Obviously, if two vertices are weakly (n, t)-connected then they are weakly $t + 1$-connected.

Theorem 6. *If A and B are weakly (n, t)-connected for some $t < n$, then the Perfectly Private Transmission Protocol in the previous section is an efficient $(0, \delta)$-secure message transmission between A and B.*

Proof. It follows straightforward from the proof of Theorem 5. □

Franklin and Yung [9] show that, in the context of a t-passive adversary, weak $t + 1$-connectivity is necessary and sufficient for achieving private communications. Theorem 6 provides a sufficient condition for achieving perfect privacy and probabilistic reliability against a t-active adversary in a general multi-cast graph. It is an open question whether the condition in Theorem 6 is also necessary.

It is easily observed that strong $t + 1$-connectivity implies weak $(t + 1, t)$-connectivity. The following example shows that (n, t)-weak connectivity does not imply strong $t + 1$-connectivity.

Example 7. Let $G(V, E)$ be the graph defined by $V = \{A, B\} \cup \{v_{i,j} : i, j = 1, 2, 3\}$ and $E = \{(A, v_{i,1}) : i = 1, 2, 3\} \cup \{(v_{i,j}, v_{i,j+1} : i = 1, 2, 3; j = 1, 2\} \cup \{(v_{i,3}, B) : 1 = 1, 2, 3\} \cup \{(v_{1,1}, v_{2,1}), (v_{2,2}, v_{3,2}), (v_{3,3}, v_{1,3})\}$. Then it is straightforward to show that A and B are weakly $(3, 1)$-connected but not strongly 2-connected in G.

Theorem 6 shows that, for at most one malicious node, efficient $(0, \delta)$-secure message transmission between A and B is possible in the multicast graph defined in Example 7. Note that this multicast graph is only strongly 1-connected, and so Franklin-Wright's results have no bearing on this example.

Similarly, for any $n > 2$ the following example gives a graph G and two vertices A and B such that A and B are weakly $(n, 1)$-connected but not weakly 3-connected.

Example 8. Let $G(V, E)$ be the graph defined by $V = \{A, B\} \cup \{v_{i,j} : i = 1, \ldots n; j = 1, 2\}$ and $E = \{(A, v_{i,1}) : i = 1, \ldots, n\} \cup \{(v_{i,1}, v_{i,2} : i = 1, \ldots, n\} \cup \{(v_{i,2}, B) : 1 = 1, \ldots, n\} \cup \{(v_{1,2}, v_{i,2}) : i = 2, \ldots, \lfloor \frac{n}{2} \rfloor\} \cup \{(v_{\lfloor \frac{n}{2} \rfloor + 1, 2}, v_{i,2}) : i = \lfloor \frac{n}{2} \rfloor + 2, \ldots, n\}$. Then it is straightforward to show that A and B are weakly $(n, 1)$-connected but not weakly 3-connected in G.

Then Theorem 6 shows that, for at most one malicious node, efficient $(0, \delta)$-secure message transmission between A and B is possible in the graph G defined in Example 8. The result by Franklin and Yung [9] shows that secure message transmission between A and B is impossible in this graph when there are two malicious nodes. However, if $n > 2t+1$ and we use non-broadcast channels, then secure message transmission is possible between A and B against t malicious nodes (see, e.g., Dolev, Dwork, Waarts, and Yung [7]). It follows that in certain

cases broadcast *helps* adversaries "more", which contrasts with Franklin and Wright's result [8] that in certain cases broadcast *hurts* adversaries "more".

We close our paper by showing that it is **NP**-hard to decide whether a given multicast graph is strongly k-connected.

Theorem 9. *It is* **NP***-complete to decide whether a given multicast graph is strongly k-connected.*

Proof. It is clear that the specified problem is in **NP**. Whence it suffices to reduce the following **NP**-complete problem IS (Independent Set) to our problem. A similar (but not identical) reduction for a different problem has appeared in Burmester, Desmedt, and Wang [3]. The independent set problem is:

Instance: A graph $G(V, E)$ and a number k.
Question: Does there exist a node set $V_1 \subseteq V$ of size k such that any two nodes in V_1 are not connected by an edge in E?

The input $G(V_G, E_G)$, to IS, consists of a set of vertices $V_G = \{v_1, \ldots, v_n\}$ and a set of edges E_G. In the following we construct a multicast graph $f(G) = MG(V; E)$ and two nodes $A, B \in V$ such that there is an independent set of size k in G if and only if A and B are strongly k-connected.

Let $V = \{A, B\} \cup \{u_{i,j} : i, j = 1, \ldots n\} \cup \{u_i : i = 1, \ldots, n\}$, and E be the set of the following edges.

1. For each pair $i, j = 1, \ldots, n$, there is an edge $(A, u_{i,j}) \in E$.
2. For each pair $i, j = 1, \ldots, n$: if there is exists an edge $(v_i, v_j) \in E_G$, then there are four edges $(u_{i,j}, u_i)$, $(u_{i,j}, u_j)$, $(u_{j,i}, u_i)$, and $(u_{j,i}, u_j)$ in E.
3. For each i, there is an edge $(u_i, B) \in E$.

It is clear that two paths P_1 and P_2 connecting A and B which go through u_i and u_j respectively are node disjoint and have no common neighborhoods (except A and B) if and only if there is no edge (v_i, v_j) in E_G. Hence there is an independent set of size k in G if and only if A and B are strongly k-connected. □

Similarly, we can define the corresponding problem for weak (n, t)-connectivity as follows:

Instance: A graph $G(V, E)$ and two number $n > k$.
Question: Is G weakly (n, t)-connected?

Using a reduction from the **NP**-complete problem "Vertex Cover", a similar argument as in the proof of Theorem 9 can be used to show that the above problem is co**NP**-hard (the details are omitted). Indeed, it is straightforward to show that the above problem belongs to Σ_2^p (that is, the second level of the polynomial time hierarchy). It remains open whether this problem is co**NP**-complete, or Σ_2^p-complete, or neither.

Acknowledgment

The authors thank Matt Franklin (Xerox) and Rebecca Wright (AT&T) for informing us, after the paper had been accepted, that Donald Beaver has found a different method to address the Franklin-Wright open problem.

References

1. M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computing. In: *Proc. ACM STOC, '88*, pages 1–10, ACM Press, 1988.
2. M. Burmester, Y. Desmedt, and G. Kabatianski. Trust and Security: A New Look at the Byzantine Generals Problem. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science* **38**, pages 75–83, American Mathematical Society, 1998.
3. M. Burmester, Y. Desmedt, and Y. Wang. Using approximation hardness to achieve dependable computation. In: *Proc. of the Second International Conference on Randomization and Approximation Techniques in Computer Science*, LNCS 1518, pages 172–186, Springer Verlag, 1998.
4. D. Chaum, C. Crepeau, and I. Damgard. Multiparty unconditional secure protocols. In: *Proc. ACM STOC, '88*, pages 11–19, ACM Press, 1988.
5. B. den Boer. A simple and key-economical unconditional authentication scheme. *Journal of Computer Security*, **2**:65–71, 1993.
6. D. Dolev. The Byzantine generals strike again. *J. of Algorithms*, **3**:14–30, 1982.
7. D. Dolev, C. Dwork, O. Waarts, and M. Yung. Perfectly secure message transmission. *J. of the ACM*, **40**(1):17–47, 1993.
8. M. Franklin and N. Wright. Secure communication in minimal connectivity models. In: *Advances in Cryptology, Proc. of Euro Crypt '98*, LNCS 1403, pages 346–360, Springer Verlag, 1998.
9. M. Franklin and M. Yung. Secure hypergraphs: privacy from partial broadcast. In: *Proc. ACM STOC, '95*, pages 36–44, ACM Press, 1995.
10. E. Gilbert, F. MacWilliams, and N. Sloane. Codes which detect deception. *The BELL System Technical Journal*, **53**(3):405–424, 1974.
11. O. Goldreich, S. Goldwasser, and N. Linial. Fault-tolerant computation in the full information model. *SIAM J. Comput.* **27**(2):506–544, 1998.
12. V. Hadzilacos. *Issues of Fault Tolerance in Concurrent Computations*. PhD thesis, Harvard University, Cambridge, MA, 1984.
13. T. Rabin. Robust sharing of secrets when the dealer is honest or faulty. *J. of the ACM*, **41**(6):1089–1109, 1994.
14. T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In: *Proc. ACM STOC, '89*, pages 73–85, ACM Press, 1989.
15. G. J. Simmons. A survey of information authentication. In: *Contemporay Cryptology, The Science of Information Integrity*, pages 379–419. IEEE Press, 1992.