

# Classical and Quantum Anonymous Communication

Anne Broadbent

with Gilles Brassard, Joseph Fitzsimons, Sébastien Gambs and Alain Tapp

Presented at the C&O@40 research conference June 18-23, 2007, University of Waterloo

## Abstract

We present the first protocols for the anonymous transmission of both classical and quantum messages that are information-theoretically secure against an active adversary, without any assumption on the number of corrupt participants. The anonymity of the sender and receiver is perfectly preserved, and the privacy of the message is protected except with exponentially small probability. A single corrupt participant can cause the protocol to abort, but in the case of the quantum protocol, the state can only be destroyed with exponentially small probability: if the protocol succeeds, the state is transferred to the receiver and otherwise it remains in the hands of the sender (provided the receiver is honest). We also present information-theoretically secure protocols for **veto**, **collision detection** and **notification**.

Please see [1, 2] for full versions of the results presented here.

## Model

Our protocols involve  $n$  participants who have access to a broadcast channel and pairwise private channels. Our quantum protocol also assumes pairwise private authenticated quantum channels. We make no assumption on the number of honest participants (otherwise, we could use a general-purpose classical or quantum multi-party protocol [3, 4]). We use a security parameter  $s$ . The complexity of protocols is polynomial in  $n$ ,  $s$ , and the input length.

## Parity

We present David Chaum's dining cryptographers protocol, which is secure only against a passive adversary. In further sections, we build on the **parity** protocol to implement new functionalities that are secure against an active adversary.

**Input:**  $x_i \in \{0, 1\}$

**Output:**  $y_i = x_1 \oplus x_2 \oplus \dots \oplus x_n$

**Achieved functionality:**

- 1) (Correctness) The output is the same as in the ideal functionality (against passive adversary).
- 2) (Privacy) No adversary can learn more than the output of the ideal functionality.

Each participant  $i$  does the following:

1. Select at random an  $n$ -bit string  $r_i = r_i^1 r_i^2 \dots r_i^n$  with Hamming weight of parity  $x_i$ .
2. Send  $r_i^j$  to participant  $j$  using the private channel; keep bit  $r_i^i$  to yourself.
3. Compute  $z_i$ , the parity of the sum of all the bits received, including  $r_i^i$ .
4. Use the broadcast channel to announce  $z_i$ .
5. After the broadcast is finished, compute  $y_i = \bigoplus_{k=1}^n z_k$ . This is the outcome of the protocol.

## Veto

**Input:**  $x_i \in \{0, 1\}$

**Output:**  $y_i = x_1 \vee x_2 \vee \dots \vee x_n$

**Achieved functionality:**

- 1) (Reliability) No participant can make the protocol abort.
- 2) (Correctness) If all participants have input  $x_i = 0$ , then the protocol achieves the ideal functionality with probability 1. If there exists a participant with input  $x_i = 1$  then the protocol is correct with probability at least  $1 - 2^{-s}$ .
- 3) (Privacy) The most an adversary can learn is the information that it could have learned by assigning to all corrupt participants the input 0. Additionally, this information is revealed, even to a passive adversary, with probability at least  $1 - 2^{-s}$ .

The  $n$  participants agree on  $n$  orderings such that each ordering has a different last participant. **result**  $\leftarrow 0$

For each ordering,

Repeat  $s$  times:

1. Each participant  $i$  sets the value of  $p_i$  in the following way: if  $x_i = 0$  then  $p_i = 0$ ; otherwise,  $p_i = 1$  with probability  $\frac{1}{2}$  and  $p_i = 0$  with complementary probability.
2. The participants execute the **parity** protocol with inputs  $p_1, p_2, \dots, p_n$ , with the participants broadcasting according to the current ordering (if any participant refuses to broadcast, set the value **result**  $\leftarrow 1$ ). If the outcome of **parity** is 1, then set **result**  $\leftarrow 1$ .

Output the value **result**.

## Collision Detection

**Input:**  $x_i \in \{0, 1, 2\}$

**Output:** let  $r = \sum_{i=1}^n x_i$  then  $y_i = \min\{r, 2\}$

**Achieved Functionality:**

- 1) (Reliability) No participant can make the protocol abort.
- 2) (Correctness) The output of the protocol equals the output of the ideal functionality (except with exponentially small probability).
- 3) (Privacy) An adversary cannot learn more than it could have learned by assigning to all corrupt participants the input 0 in the ideal functionality.

**Veto A**

All participants perform the **veto** protocol with inputs  $\min\{x_i, 1\}$ .

**Veto B**

If the outcome of **veto A** is 0, skip this step. Otherwise, each participant with input 1 in **veto A** will set  $b_i = 1$  if he detected in **veto A** that another participant had input 1, or if  $x_i = 2$ . All other participants set  $b_i = 0$ . Then all participants perform a second **veto** protocol with inputs  $b_i$ .

**Output:**  $y_i = \begin{cases} 0 & \text{if the outcome of veto A is 0} \\ 1 & \text{if the outcome of veto A is 1 and the outcome of veto B is 0} \\ 2 & \text{if the outcome of veto A is 1 and the outcome of veto B is 1} \end{cases}$

## Notification

**Input:**  $\forall j \neq i, x_j^i \in \{0, 1\}$

**Output:**  $y_i = \bigvee_{j \neq i} x_j^i$

**Achieved Functionality:**

- 1) (Correctness) If the protocol does not abort then the output of the protocol equals the output of the ideal functionality (except with exponentially small probability).
- 2) (Privacy) The privacy is the same as in the ideal functionality.

For each participant  $i$ :

Participant  $i$  sets  $y_i \leftarrow 0$ .

Repeat  $s$  times:

1. Each participant  $j \neq i$  sets the value of  $p_j$  in the following way: if  $x_j^i = 0$  then  $p_j = 0$ ; otherwise,  $p_j = 1$  with probability  $\frac{1}{2}$  and  $p_j = 0$  with complementary probability. Let  $p_i = 0$ .
2. The participants execute the **parity** protocol with inputs  $p_1, p_2, \dots, p_n$ , with the exception that participant  $i$  does not broadcast his value (if any participant refuses to broadcast, abort).
3. Participant  $i$  computes the outcome of **parity**, and if it is 1,  $y_i \leftarrow 1$ .

## Anonymous Message Transmission

**Input:**  $x_i = \perp$  or  $x_i = (r, w)$  where  $r \in \{1, \dots, n\}$  and  $w \in \{0, 1\}^m$

**Output:** If  $|\{x_i \mid x_i \neq \perp\}| = 0$  then  $y_i = \text{NO TRANSMISSION}$  and if  $|\{x_i \mid x_i \neq \perp\}| > 1$  then  $y_i = \text{COLLISION}$ . Otherwise let  $S$  be such that  $x_S = (r, w)$  then all  $y_i = \perp$  except  $y_r = w$ .

**Achieved Functionality:**

- 1) (Correctness) The output equals the output of the ideal functionality (except with exponentially small probability). A single participant can make the protocol produce the output COLLISION.
- 2) (Privacy) The anonymity of the sender and receiver are perfect. If the protocol succeeds, except with exponentially small probability, participant  $r$  is the only participant who knows  $w$ .

**1. Multiple Sender Detection:** The participants execute the **collision detection** protocol; participants who have input  $x_i = \perp$  use input 0 while all others use input 1. If the outcome of **collision detection** is 1, continue, otherwise output NO TRANSMISSION if the output is 0 and COLLISION if the output is 2.

**2. Receiver Notification:** Let the sender  $S$  be the unique participant with  $x_S \neq \perp$ . The participants execute the **notification** protocol, with  $S$  using input  $x_S^r = 1$  and  $x_S^j = 0$  otherwise. All other participants use the input bits 0. Let  $R$  be the participant who computes as output  $y_R = 1$ . If the **notification** protocol fails, abort.

**3. Anonymous Message Transmission:**  $S$  computes  $w' = F(w)$ , (where  $(F, G)$  is a probabilistic encoding and decoding scheme[5] such that any combination of bit flips will be detected, except with exponentially small probability). The participants execute  $m+2(\log(m)+s)$  rounds of the **parity** protocol, with participants using the following inputs:  $S$  uses as input the bits of  $w'$ ;  $R$  uses as input the bits of a random  $m$ -bit string,  $r$  and all other players use 0 as input for each round. Let  $d$  be the output of the rounds of **parity**.  $R$  computes  $w'' = d \oplus r$  and  $y = G(w'')$ . A **veto** is performed: all players input 0 except  $R$  who inputs 1 if  $y = \perp$  and 0 otherwise.

If the outcome of **veto** is 1, the protocol aborts. Otherwise,  $R$  sets his output to  $y$ .

## Quantum Anonymous Message Transmission

**Input:**  $x_i = \perp$  or  $x_i = (r, |\psi\rangle)$  where  $r \in \{1, \dots, n\}$  and  $|\psi\rangle$  is an  $m$ -qubit message.

**Output:** If  $|\{x_i \mid x_i \neq \perp\}| = 0$  then  $y_i = \text{NO TRANSMISSION}$  and if  $|\{x_i \mid x_i \neq \perp\}| > 1$  then  $y_i = \text{COLLISION}$ . Otherwise let  $S$  be such that  $x_S = (r, |\psi\rangle)$  then all  $y_i = \perp$  except  $y_r = |\psi\rangle$ .

**Achieved Functionality:**

- 1) (Correctness) The output equals the output of the ideal functionality (except with exponentially small probability). A single participant can make the protocol produce the output COLLISION.
- 2) (Privacy) The anonymity of the sender and receiver are perfect. If the protocol succeeds, except with exponentially small probability, participant  $r$  is the only participant who has  $|\psi\rangle$ .

**1. Multiple Sender Detection:** The **collision detection** protocol is used to determine if one and only one participant wants to be the sender. If not, output NO TRANSMISSION or COLLISION, accordingly.

**2. Entanglement Distribution:** One arbitrarily designated participant creates  $2m+s$  instances of the state  $|+\rangle_n$  and sends one qubit of each instance to each participant, keeping one qubit of each instance for himself.

**3. Entanglement Verification:** For each of the  $2m+s$  instances, each participant makes  $n-1$  copies of his qubit by applying a control-not with it as the source and a qubit initialized to  $|0\rangle$  as the target. One such copy is sent to every other participant. Each participant *verifies* that all the  $n$  qubits in his possession are in the subspace spanned by  $\{|0^n\rangle, |1^n\rangle\}$ . Each participant broadcasts the outcome of the previous step. If any outcome is negative, the protocol aborts. Each participant *resets*  $n-1$  of his qubits to  $|0\rangle$  by performing  $n-1$  control-not operations. These qubits are discarded and the one remaining is back to the state distributed at step 2. The state shared among the honest participants is now *invariant under permutation*.

**4. Receiver Notification:** The participants execute the **notification** protocol in which only  $S$  notifies a single  $R$ .

**5. Anonymous Entanglement Generation**

For each of the  $2m+s$  instances, all participants except  $S$  and  $R$  measure in the Hadamard basis the qubit that remains from step 3. Each participant broadcasts the result of his measurement ( $S$  and  $R$  broadcast two random dummy bits).  $S$  computes the parity of all the bits received during the previous step (except his own and that of  $R$ ). If the parity is odd,  $S$  applies  $P$ , the conditional phase change, to his remaining qubit (the two qubits shared by  $S$  and  $R$  are now in Bell state  $|\Phi^+\rangle$ ).

**6. Perfect Anonymous Entanglement:**  $S$  creates  $2m$  instances of Bell state  $|\Phi^+\rangle$ . He keeps the first qubit of each pair; let  $\rho$  be the rest of the pairs.  $S$  creates a random classical key  $k$  of length  $4m+2s+1$ , and computes  $\rho' = \text{authenticate}(\rho, k)$  (this is a quantum authentication code[6]).  $S$  performs a teleportation measurement on  $\rho'$  using the anonymous  $|\Phi^+\rangle$  states generated during steps 2–5.  $S$  uses the anonymous message transmission protocol to send  $k$  and the teleportation bits to  $R$ .  $R$  completes the teleportation and computes  $\rho = \text{decode}(\rho', k)$ . If the decoding is successful,  $S$  and  $R$  share perfect anonymous entanglement (they share  $2m$  instances of  $|\Phi^+\rangle$ ). A **veto** is executed: all players input 0 except  $R$ , who inputs 1 if the authentication failed and 0 otherwise. If the outcome is 1, the protocol aborts.

**7. Fail-Safe Teleportation:**  $S$  teleports the state  $|\psi\rangle$  to  $R$  using the first  $m$  pairs generated in the previous step. The teleportation bits are anonymously transmitted to  $R$ . If the communication succeeds,  $R$  terminates the teleportation. A **veto** is performed: all players input 0 except  $R$ , who inputs 1 if the communication of the teleportation bits failed. If the outcome is 0, the protocol succeeds. Otherwise,  $S$  and  $R$  do the following:  $R$  performs a teleportation measurement using the remaining perfect anonymous entanglement to teleport back to  $S$  the quantum state resulting from the partially failed above teleportation. All participants broadcast  $2m$  random bits, except  $R$  who broadcasts the teleportation bits from above. The protocol continues even if one of the participants refuses to broadcast.  $S$  reconstructs  $|\psi\rangle$  from his own teleportation bits from above and  $R$ 's teleportation bits received from the broadcast. The protocol aborts.

## References

- [1] BROADBENT, A., and TAPP, A. "Information-theoretic security without an honest majority", preprint available at <http://arxiv.org/abs/0706.2010>.
- [2] BRASSARD, G., BROADBENT, A., FITZSIMONS, J., GAMBS, S. and TAPP, A. "Anonymous quantum communication", preprint available at <http://arxiv.org/abs/0706.2010>.
- [3] T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In *Proceedings of the twenty-first annual ACM Symposium on Theory of Computing (STOC)*, pages 73–85, 1989.
- [4] M. Ben-Or, C. Crépeau, D. Gottesman, A. Hassidim, and A. Smith. Secure multiparty quantum computation with (only) a strict honest majority. In *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2006)*, pages 249–260, 2006.
- [5] R. Cramer, S. Fehr, and C. Padró. Combinatorial codes for detection of algebraic manipulation and their applications. Manuscript, 2007.
- [6] H. Barnum, C. Crépeau, D. Gottesman, A. Smith, and A. Tapp. Authentication of quantum messages. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS02)*, page 449, 2002.