quantum communication cryptography

Abstract

We introduce a protocol to generate a secret encryption key shared between one sender and multiple receivers of the sender's choosing; this is known as conference key agreement (CKA). The participants — sender and designated receivers — are connected via a larger network, yet their roles in the protocol are not revealed to anyone but the sender, giving us a notion of anonymity and thus anonymous CKA or ACKA[1].

Notification

Input. Alice's choice of m receivers.
Goal. The m receivers get notified.

For agent $i = 1, \ldots, n$:

1. All agents $j \in \{1, \ldots, n\}$ do the following.
   (a) When j corresponds to Alice (j_a), and i is not a receiver, she chooses n random bits $\{r^i_{j,k}\}^n_{k=1}$ such that $\bigoplus^n_{k=1} r^i_{j,k} = 0$. If i is a receiver, she chooses n random bits such that $\bigoplus^n_{k=1} r^i_{j,k} = 1$. She sends bit $r^i_{j,k}$ to agent k.
   (b) When $j \neq j_a$, the agent chooses n random bits $\{r^i_{j,k}\}^n_{k=1}$ such that $\bigoplus^n_{k=1} r^i_{j,k} = 0$ and sends bit $r^i_{j,k}$ to agent k.
2. All agents $k \in \{1, \ldots, n\}$ receive $\{r^i_{j,k}\}^n_{j=1}$, compute $z^i_k = \bigoplus^n_{j=1} r^i_{j,k}$ and send it to agent i.
3. Agent i takes the received $\{z^i_k\}^n_{k=1}$ to compute $z^i = \bigoplus^n_{k=1} z^i_k$; if $z^i = 1$ they are thereby notified to be a designated receiver.

1

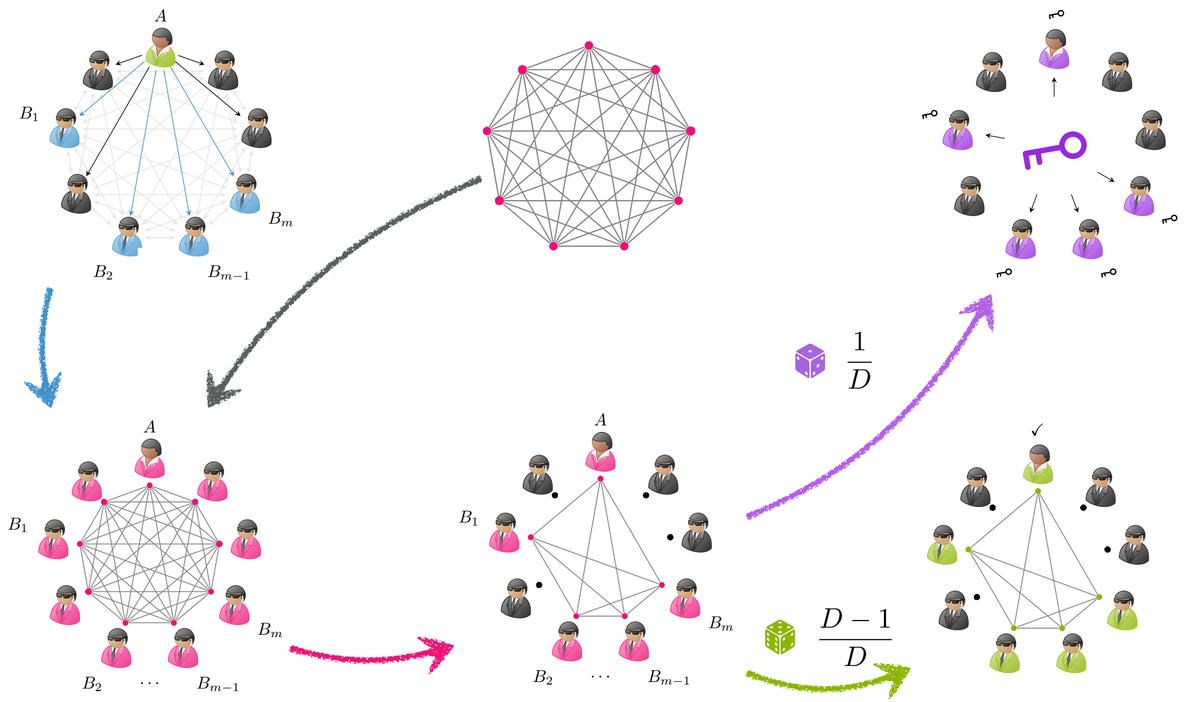
Anonymous Multiparty Entanglement

Input. A shared GHZ_n state; Alice knowing the identities of the non-participants $\bar{\mathbf{P}}$.
Goal. A GHZ_{m+1} state shared between $\mathbf{P}$.

1. Alice and the Bobs each draw a random bit. Everyone else measures in the X-basis, yielding a measurement outcome bit x_i for $i \in \bar{\mathbf{P}}$.
2. All parties broadcast their bits in a random order or, if possible, simultaneously.
3. Alice applies a Z gate if the parity of the non-participating parties' bits is odd.

2

AQIS 2021



Anonymous Conference Key Agreement

To realize ACKA, we make use of multipartite entangled quantum resources known as GHZ states distributed between all n parties in the network. These GHZ states contain intrinsic nonclassical correlations, which we can exploit to generate a shared key between only the $m < n$ participants.
We start with a classical "notification" protocol[2] that enables the sender to notify several receivers of its intention to establish a secret key with them. We then explain how to generate anonymous entanglement between only the participants from the shared GHZ states, how the sender can anonymously verify this process[3], and how an anonymous secret key is finally created.
All of the above subprotocols are combined into a single ACKA protocol where the participant roles are protected against an adversary who may corrupt one receiver or multiple nonparticipating parties in the network; the security of the key is preserved except for the trivial case where a participant is corrupted. We prove the anonymity of the participants on an information-theoretic level[1].

Anonymous Key Generation

Input. Alice as initiator; parameters L and D.
Goal. Anonymous generation of secret key between $\mathbf{P}$.

1. Alice notifies the m Bobs by running the `Notification` protocol.
2. The source generates and shares L GHZ states.
3. The parties run the `AME` protocol on them.
4. For each of the L states, the parties ask a public source of randomness to broadcast a bit b such that $\Pr[b = 1] = \frac{1}{D}$.
   `Verification` **round:** If $b = 0$, Alice runs the `Verification` protocol on the $(m + 1)$-partite state. The remaining parties announce random values.
   `KeyGen` **round:** If $b = 1$, Alice and the Bobs Z-measure to obtain a shared secret bit.
5. If Alice accepts all `Verification` rounds, she anonymously validates the protocol.

4

Verification

Input. A shared state between $|\mathbf{P}| = m + 1$ parties.
Goal. Verification or rejection of the shared state as a GHZ_{m+1} state by Alice.

1. Every B_i draws a random bit b_i and measures in the X- or Y-basis if it equals 0 or 1 respectively, obtaining a measurement outcome o_i.
2. Everyone broadcasts (b_i, o_i), including Alice, who chooses her bits (b_0, o_0) at random.
3. Alice resets her bit such that $\sum^m_{i=0} b_i = 0 \pmod 2$. She measures in the X- or Y-basis if her bit equals 0 or 1 respectively, thereby also resetting o_0.
4. If and only if $\frac{1}{2}\sum_i b_i + \sum^m_{i=0} o_i = 0 \pmod 2$, Alice accepts the state.

3