QUANTUM INTERNET ALLIANCE

ANONYMITY IN QUANTUM NETWORK PROTOCOLS

QCC

TU berlin

Co-Funded by the European Union

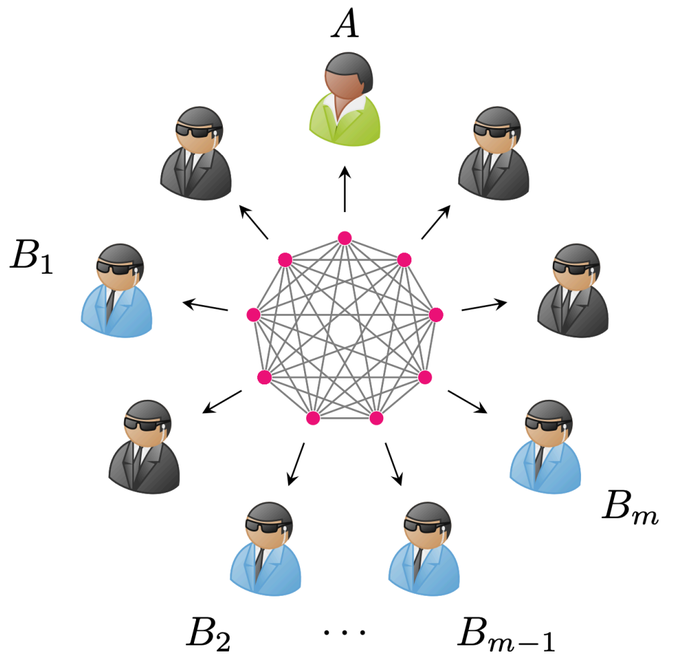
Fit into QIA’s bigger picture

- **Application domains**, User domains and use-cases
- **Identity protection**

Quantum Networks

A quantum network $N = \{1,2,\ldots,n\}$

- The ‘participants':
  - A *sender:* Alice A
  - Multiple *receivers:* Bobs B_j
- The 'non-participants'
  - Everyone else



QUANTUM INTERNET ALLIANCE
QUANTUM FLAGSHIP
Co-Funded by the European Union

Anonymity?

~~The identity of participants is unknown~~

The identity of participants remains “as unknown as it was”

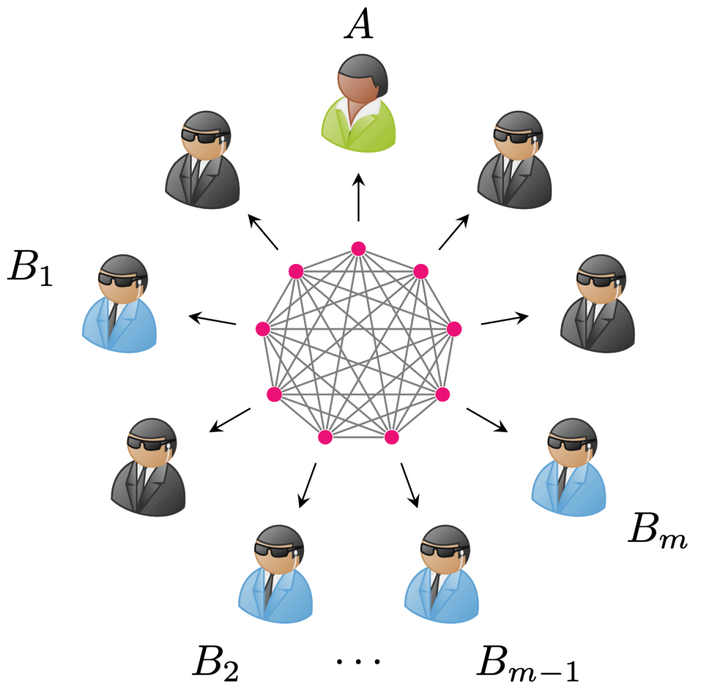
- To *the non-participants*: ***weak*** **anonymity**
- To *everyone**: ***strong*** **anonymity**
  - Alice chooses all identities
  - Variants

QUANTUM INTERNET ALLIANCE
QUANTUM FLAGSHIP
Co-Funded by the European Union

ANONYMOUS SECRET MESSAGING

Anonymous secret messaging

1. Alice picks the Bobs
2. Alice and the Bobs anonymously generate key k
3. Alice encrypts her message $s \rightarrow c = s \oplus k$
4. Alice anonymously broadcasts c
5. Bobs decrypt $c \rightarrow c \oplus k = m \oplus k \oplus k = m$



QUANTUM INTERNET ALLIANCE
QUANTUM FLAGSHIP
Co-Funded by the European Union

GHZ states

$$|0\ldots0\rangle_N + |1\ldots1\rangle_N$$

- Measure in Z
  - Correlated key
- Measure in X_n
  - ‘GHZ’ on remaining parties
- Measure **all qubits** in X
  - The *parity* of all outcomes is fixed

$$\left(|0\ldots0\rangle_{N-1} \pm |1\ldots1\rangle_{N-1}\right) \otimes |\pm\rangle_n$$

(GHZ is stabilizer)

Anonymous secret messaging

1. Alice picks the Bobs
2. Alice and the Bobs anonymously generate key k
3. Alice encrypts her message $s \rightarrow c = s \oplus k$
4. Alice anonymously broadcasts c
5. Bobs decrypt $c \rightarrow c \oplus k = m \oplus k \oplus k = m$

QUANTUM INTERNET ALLIANCE
QUANTUM FLAGSHIP
Co-Funded by the European Union

BROADCASTING

Broadcasting

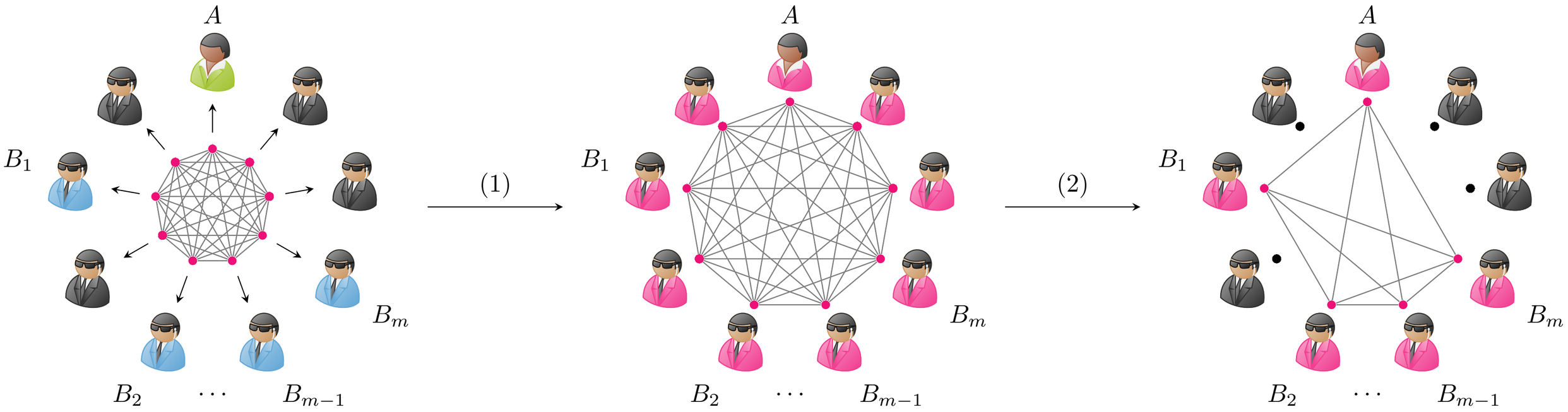
Protocol for Alice to send message b

1. Share GHZ state over entire network N $\quad |0\ldots0\rangle + (-1)^0 |1\ldots1\rangle$
2. Alice applies Z_a if $b = 1$ $\quad |0\ldots0\rangle + (-1)^{b_a} |1\ldots1\rangle$
3. Everyone measures X_i, obtain m_i, announce
4. Now $b = \bigoplus m_i$

QUANTUM INTERNET ALLIANCE
QUANTUM FLAGSHIP
Co-Funded by the European Union

KEY AGREEMENT

What we want



Verification

- **Bobs** select random X and Y measurements
- **Alice** completes a stabilizer element
- **Parity** is fixed

- **Repeating** gives exponentially small cheat probability

Contribution to QIA and future steps

- **Application domain**
- Crystallise a ***Use case*** instead
- Invitation to tomorrow morning

Links

- Anonymous Tranmissions:
  - Christandl, Wehner (2005). Quantum Anonymous Transmissions. https://doi.org/10.1007/11593447_12
- Anonymous conference key agreement:
  - Hahn, de Jong, Pappa (2020). Anonymous Quantum Conference Key Agreement. https://doi.org/10.1103/PRXQuantum.1.020325
  - Grasselli, Murta et al. (2022). Secure anonymous conferencing in quantum networks. https://doi.org/10.1103/PRXQuantum.3.040306
  - de Jong, Hahn et al. (2020). Anonymous conference key agreement in linear quantum networks. https://arxiv.org/abs/2205.09169
- Experimental work:
  - Thalacker et al. (2021). Anonymous and secret communication in quantum networks. https://doi.org/10.1088/1367-2630/ac1808
  - Rückle et al. (2022). Experimental anonymous conference key agreement using linear cluster states. https://arxiv.org/abs/2207.09487

THANK YOU!

Jarn de Jong, dejong@tu-berlin.de

QUANTUM INTERNET ALLIANCE

QUANTUM FLAGSHIP

Co-Funded by the European Union

A first approach

(Bad) Protocol for Alice and Bobs to agree on key k

1. Share GHZ state over entire network N $\quad |0\ldots0\rangle_N + (-1)^0 |1\ldots1\rangle_N$
2. All non-participants j measure X_j $\quad |0\ldots0\rangle_P + (-1)^\alpha |1\ldots1\rangle_P$
3. All participants j measure Z_j, obtain k_j
4. All participants agree on $k = k_j$

What happens when non-participants deviate?

QUANTUM INTERNET ALLIANCE
QUANTUM FLAGSHIP
Co-Funded by the European Union

A better protocol

Protocol for Alice and Bobs to agree on key k

1. Share GHZ state over entire network N
2. All non-participants j measure X_j
3. Network asks public random source for random b

4a. (Key generation)

Participants measure Z and obtain key k

4b. (Verification)

Participants run verification round

} Repeat ad inf.

QUANTUM INTERNET ALLIANCE

QUANTUM FLAGSHIP

Co-Funded by the European Union

Verification

(Supposedly) the state is: $\left(|0\ldots0\rangle_P + (-1)^{\alpha}|1\ldots1\rangle_P\right) \otimes |garb\rangle_{NP}$

1. All Bobs pick random b_j, measure X_j or Y_j

2a. All Bobs announce b_j and outcome o_j

2b. Others announce random b_j and o_j

3. Alice resets $b_a = \oplus_{Bobs}\, b_j$, measures X_j or Y_j

4. Alice accepts iff $o_a \oplus \alpha = \oplus_{Bobs}\, o_j$

Important points

1. Timing issues
2. Initial GHZ state is not checked
3. Dephasing of GHZ results in failed verification