LINEAR ENTANGLEMENT SUFFICES FOR f-ROUTING

KEVIN BOGNER
COSIC, KU Leuven, Belgium
kevin.bogner@kuleuven.be

Abstract. In f-routing, Alice receives an n-bit string x and an unknown qubit, and Bob receives an n-bit string y. They share a state prepared in advance and exchange one simultaneous message each. The party selected by the Boolean function $f(x, y)$ must then recover the unknown qubit without further communication. To perform f-routing successfully, Alice and Bob need to share entanglement that scales with n for some functions f, but the lower and upper bounds for the entanglement are not tight. This paper shows that $2n + 2$ shared EPR pairs suffice for every function f. The best previous bound that holds for all functions is a shared state of $2^{O(\sqrt{n \log n})}$ qubits. The new strategy moves the cost from the shared state to the messages: Alice sends an exponentially long message of $2^{n+1} + 1$ qubits, while Bob sends only classical bits. When the messages are counted towards the resources as well, the previous strategy remains the cheapest known. The result also limits lower bounds that count only the shared state: they cannot exceed a linear number of EPR pairs. The result is formalized in Lean.

1. Introduction

Position verification [CGMO14] aims to certify where a prover is located using only timed messages. In a routing protocol [KMS11, BFSS13], two verifiers send the prover two n-bit strings x and y together with an unknown qubit, and the prover must return the qubit to the verifier selected by a Boolean function $f(x, y)$. Two colluding attackers stand between the claimed position and the verifiers, one on each side. The attacker who intercepts the qubit must send her message before the other string reaches her, so she does not yet know $f(x, y)$. She cannot keep the qubit and also forward a copy, because an unknown quantum state cannot be copied [WZ82]. Attackers who share enough entanglement in advance can still break every protocol of this kind [BCF$^+$14, BK11]. The protocol is therefore secure only against attackers with limited entanglement, and the question is how much an attack needs [BFSS13].

The attackers' task is called f-routing [BFSS13, ABM$^+$24]. Alice, the attacker who intercepts the qubit Q, receives $x \in \{0, 1\}^n$, while Bob receives $y \in \{0, 1\}^n$. Beforehand, they share an entangled state. They exchange one simultaneous message each and then recover Q locally, Alice when $f(x, y) = 0$ and Bob when $f(x, y) = 1$. These two possibilities are the routing cases. A strategy for f-routing is a shared state together with the operations that Alice and Bob apply. Section 2 defines the task precisely.

How much entanglement f-routing needs is known only in part. For upper bounds, a garden-hose strategy routes every function with a number of EPR pairs that is exponential in n [BFSS13]. A strategy built from conditional disclosure of secrets [LVW17] reduces the required shared state to $2^{O(\sqrt{n \log n})}$ qubits [ABM$^+$24], which is subexponential in n and the best bound known for all functions [May26]. For lower bounds, a line of work counts only the shared state and places no limit on the messages or the local operations. For explicit functions, these bounds are linear in n when recovery is perfect in one of the two routing cases [ACM25, HM26], and logarithmic when both cases may have error [Bog26]. These lower bounds leave open whether some functions need more than linearly many EPR pairs.

1.1. Every function routes with $2n + 2$ EPR pairs.

This paper shows that no function needs more than linearly many EPR pairs when the messages are not limited. The price is an exponentially long quantum message from Alice. The following theorem states both facts in the model of Section 2.

Theorem 1 (Linear entanglement)**.** *Let $n \geq 1$ and let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be any Boolean function. There is a strategy for f-routing with the following three properties.*

(1) *The shared state is $2n + 2$ EPR pairs.*
(2) *On every input pair (x, y), the selected party recovers the qubit perfectly: Alice if $f(x, y) = 0$, and Bob if $f(x, y) = 1$.*
(3) *Alice sends $2^{n+1} + 1$ qubits and $3n + 2$ classical bits, and Bob sends $3n + 2$ classical bits.*

In words, $2n + 2$ EPR pairs route the qubit perfectly for every Boolean function, at the price of a message from Alice that is exponentially long. The shared state is the same for all functions, and only the local operations depend on f. For inner product, equality, greater-than and disjointness, perfect recovery needs $\Omega(n)$ EPR pairs [ACM25, HM26]. Linear upper bounds were already known for these four functions [BFSS13, ACM25], and Theorem 1 shows that no other function needs more.

Theorem 1 also limits what lower bounds can show. A lower bound that counts only the shared state must hold for the strategy of Theorem 1, so it cannot exceed $2n + 2$ EPR pairs. In particular, a robust lower bound, one that allows error in both routing cases, can grow at most linearly in n. Whether such a bound can grow faster than logarithmically remains open [May26, Bog26].

1.2. **The cost moves from the shared state to the messages.** The strategy of Theorem 1 trades shared entanglement for long messages. Alice's message contains two registers of 2^n qubits each, and she keeps two more registers of the same size. Theorem 1 does not limit lower bounds that count every qubit Alice and Bob hold, including their messages. For a random function, these bounds show that linearly many qubits are needed [BCS22, EFS25]. The strategy of [ABM$^+$24] sends only $2^{O(\sqrt{n \log n})}$ qubits, so it remains the cheapest known for all functions when the messages are counted as well. Theorem 1 thus shows that a security proof against attackers with $2n + 2$ or more EPR pairs must also limit another resource, such as their communication. Whether linear entanglement can be combined with messages of subexponential length is open. For a related task with a referee, Gur, Huang and Tang [GHT26] use $O(n)$ pre-shared entangled qubits, but their protocol also shares random unitaries that their count leaves free, so their result does not give Theorem 1.

1.3. **The idea: a key that stays in superposition.** The strategy encrypts the unknown qubit with two key bits and lets $f(x, y)$ decide who can decrypt it, similar to the strategy of [ABM$^+$24]. Alice prepares an EPR pair herself. On the qubit and one half of this pair, she performs quantum teleportation [BBC$^+$93] without the measurement: she applies only its unitary part. The two bits that the measurement would produce, the key bits, therefore stay in superposition in two of her qubits. The other half of the pair, which she sends to Bob, carries the qubit encrypted with the key bits. If Bob learns both key bits, he decrypts and holds the qubit. If instead no system other than this encrypted half depends on the key bits, Alice inverts her unitary. She then holds the qubit again, and the half with Bob is one half of an unused EPR pair.

The strategy therefore has to disclose each key bit to Bob when $f(x, y) = 1$ and to hide it from him when $f(x, y) = 0$. The strategy of [ABM$^+$24] discloses the key with a classical protocol for conditional disclosure of secrets [LVW17]. Such a protocol hides the key with randomness that Alice and Bob share in advance, and this randomness makes the shared state of that strategy large. The new strategy uses a quantum message instead, in which Alice hides the key with entanglement that she prepares alone. For each key bit, she prepares a maximally entangled state of two registers, each with 2^n qubits, one for every n-bit string. She sends one register to Bob and keeps the other. The strategy turns this state into the one obtained by applying $(X \pm V)/\sqrt{2}$ to the register sent to Bob, where the sign carries the key bit. Here X is the Pauli operator that flips one of the 2^n qubits of this register, and V is a product of Pauli Z operators chosen such that X and V commute when $f(x, y) = 1$ and anticommute when $f(x, y) = 0$. If the two operators commute, the two signs give Bob orthogonal states, so he reads the key bit. If they anticommute, both signs give Bob the maximally mixed state, and Alice removes the

dependence on the key bit by acting on the register she kept. So Alice is able to recover the unknown qubit.

Alice applies X and V, but the right pair depends on both inputs. The input x selects the qubits on which V has a factor Z, and y shifts this pattern relative to the qubit that X flips. Alice does not have y when she acts. The shared EPR pairs supply the shift. A measurement by Bob that depends on y leaves Alice's halves of $n+1$ EPR pairs in a superposition of two basis states, $|0, a\rangle$ and $|1, a+y\rangle$, each labelled by a bit and an n-bit string, where $a+y$ is the bitwise sum modulo 2. Alice applies X to the qubit for the string a on the first and V shifted by $a+y$ on the second, and then measures her halves in a basis that hides which of the two she applied. Each key bit uses $n+1$ EPR pairs, which gives $2n+2$ in total.

2. Routing model

This section defines f-routing and perfect recovery in the model of [May26, BHM$^+$26, Bog26]. Fix a Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Before any input arrives, Alice and Bob share a quantum state. Alice then receives $x \in \{0,1\}^n$ and a qubit Q, while Bob receives $y \in \{0,1\}^n$. The shared state does not depend on x, y or the state of Q. Figure 1 shows a strategy for f-routing, which consists of the shared state and the operations of Alice and Bob. Before the message exchange, Alice, who knows only x, applies a quantum operation to Q and her part of the shared state, and Bob, who knows only y, applies one to his part. Each party keeps a part of the result and sends the rest to the other party. The two messages are sent simultaneously, so neither party has the other's message when it produces its own. After the exchange, no further communication takes place. If $f(x,y) = 0$, Alice has to recover the qubit Q, and if $f(x,y) = 1$, Bob has to recover the qubit Q. Recovery is perfect on the input pair (x,y) when the selected party ends with the qubit in its original state. If the qubit was entangled with another system, the joint state of the recovered qubit and this system must be the original one as well. Only the shared state counts as a cost in this model. The operations are arbitrary, and the messages may be quantum and of any length.

3. The strategy

This section describes the strategy of Theorem 1, and Section 4 proves that it recovers the qubit. Section 3.1 fixes the notation. Section 3.2 recalls how teleportation encrypts the unknown qubit with a key that stays in superposition. Section 3.3 defines the operators that Alice applies

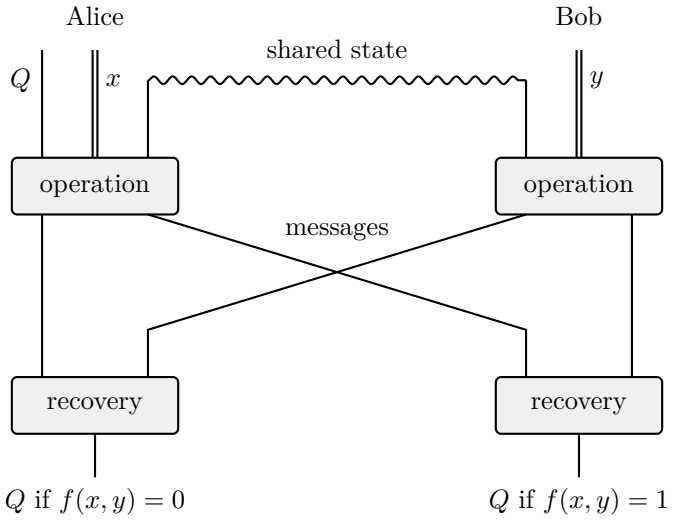


Figure 1. A strategy for f-routing, with time running downward. Double lines denote classical inputs, and the wavy line denotes the shared state. Alice recovers the qubit when $f(x,y) = 0$, and Bob recovers it when $f(x,y) = 1$.

to her registers and shows that $f(x, y)$ decides whether they commute. Section 3.4 lists the steps of the strategy.

3.1. **Notation.** Strings in $\{0,1\}^n$ are added bitwise modulo 2, and $\ell \cdot y = \ell_1 y_1 + \cdots + \ell_n y_n$ modulo 2 is the inner product of two strings. We write $N = 2^n$ for the number of strings. The Pauli operators are $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ and $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$. An EPR pair is the two-qubit state $|\Phi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. For a register W of dimension D with basis states $|w\rangle$ and a second register W' of the same dimension, the maximally entangled state is

$$|\Omega\rangle_{WW'} = \frac{1}{\sqrt{D}} \sum_w |w\rangle_W |w\rangle_{W'}. \tag{1}$$

3.2. **Teleportation without measurement.** Alice encrypts the unknown qubit Q by teleporting it without measuring. For a pair of bits $k = (k_1, k_2)$, let $P_k = X^{k_1} Z^{k_2}$. Alice prepares an EPR pair $|\Phi\rangle_{TC}$ of her own. The four states $|\Phi_k\rangle = (I \otimes P_k)|\Phi\rangle$ form the Bell basis of two qubits, and for every state $|\psi\rangle$ of Q [BBC+93],

$$|\psi\rangle_Q \otimes |\Phi\rangle_{TC} = \frac{1}{2} \sum_{k \in \{0,1\}^2} |\Phi_k\rangle_{QT} \otimes P_k |\psi\rangle_C. \tag{2}$$

In teleportation, Alice measures QT in the Bell basis, and her outcome k tells the holder of C which operator P_k to remove. In the strategy of Theorem 1, she does not measure QT. She applies the *Bell-basis change*, the unitary $\sum_k |k\rangle\langle\Phi_k|$ on QT that maps each Bell state $|\Phi_k\rangle$ to the basis state $|k\rangle = |k_1\rangle|k_2\rangle$. We call the two qubits after this unitary the *key qubits* K_1 and K_2, because they hold the key bits k_1 and k_2. By the teleportation identity (2), the state is then

$$\frac{1}{2} \sum_{k \in \{0,1\}^2} |k_1\rangle_{K_1} |k_2\rangle_{K_2} \otimes P_k |\psi\rangle_C. \tag{3}$$

The qubit C carries $|\psi\rangle$ encrypted by P_k, and the key k is in superposition. Two facts follow. First, a party that holds C and learns k recovers $|\psi\rangle$ by applying $P_k^\dagger$. Second, as long as the state has the form (3), Alice recovers $|\psi\rangle$ in Q by inverting the Bell-basis change on $K_1 K_2$, wherever C is.

3.3. **Operators that commute according to f.** For each key qubit, Alice uses two *work registers* W and W' of $N = 2^n$ qubits each. She later sends W to Bob, which makes her message exponentially long. The qubits of each work register are indexed by the strings $c \in \{0,1\}^n$, and we call c the address of its qubit. We write X_c and Z_c for the Pauli operators X and Z on the qubit with address c, in W or in W'. For Alice's input x and a string $b \in \{0,1\}^n$, let

$$V_{x,b} = \prod_{c \,:\, f(x, b+c) = 0} Z_c. \tag{4}$$

The operator $V_{x,b}$ has a factor Z_c wherever the row $f(x, \cdot)$ of the function, shifted by b, is zero. Both X_a and $V_{x,b}$ are real symmetric matrices that square to the identity. The next lemma shows that X_a and $V_{x,a+y}$ anticommute when $f(x, y) = 0$ and commute when $f(x, y) = 1$, for every address a.

Lemma 2 (Commutation)**.** *For all $x, y, a \in \{0,1\}^n$,*

$$X_a V_{x,a+y} = \begin{cases} -V_{x,a+y} X_a, & f(x,y) = 0, \\ V_{x,a+y} X_a, & f(x,y) = 1. \end{cases} \tag{5}$$

Proof. The operator X_a anticommutes with Z_a and commutes with Z_c for every $c \neq a$. By the definition (4) of $V_{x,a+y}$, this product contains the factor Z_a when $f(x, (a+y)+a) = 0$, and not otherwise. Since $(a+y)+a = y$, the two operators anticommute when $f(x, y) = 0$ and commute when $f(x, y) = 1$. □

3.4. **The steps of the strategy.** The strategy treats each key qubit in its own block. Block $i \in \{1,2\}$ consists of the key qubit K_i, two shared registers L_i and R_i, and the work registers W_i and W_i'. Alice holds L_i and Bob holds R_i, and each of these two registers has $n+1$ qubits. A basis state $|r,j\rangle$ of such a register has a label (r,j) that consists of a bit r and a string $j \in \{0,1\}^n$. The registers L_i and R_i share $n+1$ EPR pairs,

$$|\Phi\rangle_{L_iR_i}^{\otimes(n+1)} = \frac{1}{\sqrt{2N}} \sum_{r\in\{0,1\}} \sum_{j\in\{0,1\}^n} |r,j\rangle_{L_i} |r,j\rangle_{R_i}. \tag{6}$$

The strategy uses two orthonormal bases of a register of $n+1$ qubits. Bob measures in the basis

$$|\beta_{a,u}^y\rangle = \frac{|0,a\rangle + (-1)^u |1,a+y\rangle}{\sqrt{2}}, \qquad a \in \{0,1\}^n,\ u \in \{0,1\}, \tag{7}$$

which depends on his input y. Each vector is a superposition of two labels whose strings differ by y, and these $2N$ vectors form an orthonormal basis. Alice measures in the Hadamard basis

$$|h_{s,\ell}\rangle = \frac{1}{\sqrt{2N}} \sum_{r\in\{0,1\}} \sum_{j\in\{0,1\}^n} (-1)^{sr+\ell\cdot j} |r,j\rangle, \qquad s \in \{0,1\},\ \ell \in \{0,1\}^n. \tag{8}$$

Each vector of the Hadamard basis has an overlap of absolute value $1/\sqrt{2N}$ with every basis state $|r,j\rangle$. Alice's outcome therefore reveals nothing about the label, and the measurement leaves only signs that both parties can compute after the exchange.

Strategy 1. The shared state is the block state (6) for $i=1$ and $i=2$, which is $2n+2$ EPR pairs.

Bob before the exchange. Bob holds y. For each block i, he measures R_i in the basis (7) and obtains an outcome (a_i, u_i). He sends y and both outcomes to Alice and keeps a copy.

Alice before the exchange. Alice holds x and the qubit Q.

(1) She prepares an EPR pair $|\Phi\rangle_{TC}$ and applies the Bell-basis change of Section 3.2 to QT, which gives the key qubits K_1 and K_2.

(2) For each block i, she prepares the work registers W_iW_i' in the maximally entangled state $|\Omega\rangle$ of (1). She then applies a unitary G_x to $K_iL_iW_i$. On a key qubit that holds the bit z and a register L_i in the state $|r,j\rangle$, this unitary applies X_j to W_i if $r=0$, and $(-1)^z V_{x,j}$ if $r=1$:

$$G_x\,|z\rangle_{K_i}|r,j\rangle_{L_i}|\varphi\rangle_{W_i} = \begin{cases} |z\rangle|0,j\rangle \otimes X_j|\varphi\rangle, & r=0, \\ |z\rangle|1,j\rangle \otimes (-1)^z V_{x,j}|\varphi\rangle, & r=1. \end{cases} \tag{9}$$

She measures L_i in the Hadamard basis (8) and obtains an outcome (s_i, ℓ_i).

(3) She sends the qubit C, the registers W_1 and W_2 of $N=2^n$ qubits each, her input x and both outcomes to Bob. She keeps K_1, K_2, W_1', W_2' and a copy of x and of her outcomes.

Recovery. Both parties now know x, y and all outcomes. For each block i and each bit z, let

$$t_i = u_i + s_i + \ell_i \cdot y \bmod 2, \qquad M_{i,z} = \frac{X_{a_i} + (-1)^{z+t_i} V_{x,a_i+y}}{\sqrt{2}}. \tag{10}$$

- If $f(x,y)=0$, Alice recovers. For each block i, she applies $M_{i,z}$ to W_i' controlled by the key qubit K_i, that is, the unitary $\sum_z |z\rangle\langle z|_{K_i} \otimes M_{i,z}$ on K_iW_i'. She then inverts the Bell-basis change on K_1K_2, which returns the qubit Q.
- If $f(x,y)=1$, Bob recovers. For each block i, he measures the observable $X_{a_i}V_{x,a_i+y}$ on W_i, whose eigenvalues are 1 and -1. He writes his outcome as $(-1)^{e_i}$ and sets $k_i = e_i + t_i$ modulo 2. He applies $P_k^\dagger$ with $k=(k_1,k_2)$ to C and outputs C as the recovered qubit Q.

Lemma 3 below shows that the steps before the exchange leave W_iW_i' in the state $(M_{i,z}\otimes I)|\Omega\rangle$ when the key qubit K_i holds the bit z. Up to the known bit t_i, the key bit z is thus the sign between X_{a_i} and V_{x,a_i+y}. Alice's recovery uses that $M_{i,z}$ is unitary when $f(x,y)=0$, and Bob's recovery uses that $X_{a_i}V_{x,a_i+y}$ is an observable when $f(x,y)=1$. Section 4 proves both facts and shows that Bob's bit k_i equals the key bit. In the model of Section 2, Alice's message consists of C, W_1, W_2 and her classical message, and everything that Bob keeps or sends is classical.

4. Proof of Theorem 1

This section proves that Strategy 1 has the three properties of Theorem 1. Section 4.1 computes the state of one block after the exchange. Section 4.2 uses this state to show that Alice recovers the qubit when $f(x,y)=0$ and Bob when $f(x,y)=1$, and counts the resources.

4.1. One block after the exchange.

We consider the registers K_i, L_i, R_i, W_i and W_i' of one block, for one value z of the key qubit, and drop the index i. Each of the work registers W and W' has dimension $D=2^N$.

Lemma 3 (One block)**.** *Fix the inputs x and y, a bit z, an outcome (a,u) of Bob and an outcome (s,ℓ) of Alice. Then*

$$\left(\langle h_{s,\ell}|_L \otimes \langle \beta^y_{a,u}|_R\right) G_x \, |z\rangle_K |\Phi\rangle_{LR}^{\otimes(n+1)} |\Omega\rangle_{WW'} = \frac{(-1)^{\ell\cdot a}}{2N} \, |z\rangle_K \otimes (M_z \otimes I)|\Omega\rangle_{WW'}, \tag{11}$$

where

$$M_z = \frac{X_a + (-1)^{z+t} V_{x,a+y}}{\sqrt{2}} \qquad \text{and} \qquad t = u + s + \ell\cdot y \bmod 2. \tag{12}$$

The vector $(M_z \otimes I)|\Omega\rangle$ has norm one.

The left-hand side of (11) is the state of the block after both measurements, not normalized. On the right-hand side, the prefactor has absolute value $1/(2N)$ for every outcome and does not depend on z, and the vector after it has norm one. Every outcome is therefore equally likely for $z=0$ and $z=1$. The outcomes thus reveal nothing about the key bit, and a superposition of its two values survives. The key bit appears only in the sign between X_a and $V_{x,a+y}$ in the state of the work registers.

Proof. We compute the state of the block after both measurements, which is the left-hand side of (11), in three steps: Bob's measurement, Alice's unitary G_x and Alice's measurement. Bob's measurement acts on R alone, so it commutes with Alice's operations and we apply it first.

First, Bob's outcome (a,u) leaves L in the state that R was projected on. The vector $|\beta^y_{a,u}\rangle$ of Bob's basis (7) has real coefficients, so

$$\begin{aligned}\left(I_L \otimes \langle \beta^y_{a,u}|_R\right)|\Phi\rangle_{LR}^{\otimes(n+1)} &= \frac{1}{\sqrt{2N}} \sum_{r,j} \langle \beta^y_{a,u}|r,j\rangle \, |r,j\rangle_L \\ &= \frac{1}{\sqrt{2N}} \cdot \frac{|0,a\rangle_L + (-1)^u |1,a+y\rangle_L}{\sqrt{2}}.\end{aligned}$$

Second, by its definition (9), the unitary G_x applies X_a to W in the first term and $(-1)^z V_{x,a+y}$ in the second term. This gives

$$\frac{1}{\sqrt{2N}} \, |z\rangle_K \otimes \frac{|0,a\rangle_L \otimes (X_a \otimes I)|\Omega\rangle + (-1)^{u+z} |1,a+y\rangle_L \otimes (V_{x,a+y} \otimes I)|\Omega\rangle}{\sqrt{2}}.$$

Third, Alice's outcome (s,ℓ) projects L on the vector $|h_{s,\ell}\rangle$ of the Hadamard basis (8). Its overlaps with the two labels are

$$\langle h_{s,\ell}|0,a\rangle = \frac{(-1)^{\ell\cdot a}}{\sqrt{2N}}, \qquad \langle h_{s,\ell}|1,a+y\rangle = \frac{(-1)^{s+\ell\cdot a+\ell\cdot y}}{\sqrt{2N}}.$$

The projection therefore gives

$$\frac{(-1)^{\ell\cdot a}}{2N} \, |z\rangle_K \otimes \frac{\left(X_a + (-1)^{z+u+s+\ell\cdot y} V_{x,a+y}\right) \otimes I}{\sqrt{2}} \, |\Omega\rangle.$$

Since $t = u+s+\ell\cdot y$ modulo 2, the operator in front of $|\Omega\rangle$ is $M_z \otimes I$, so this expression is the right-hand side of (11).

It remains to compute the norm. Write $V = V_{x,a+y}$ and $\sigma = (-1)^{z+t}$. The matrix M_z is real, so the squared norm of $(M_z \otimes I)|\Omega\rangle$ is $\mathrm{Tr}(M_z^{\mathsf{T}} M_z)/D$. Since X_a and V are symmetric and square to the identity,

$$\begin{aligned} M_z^{\mathsf{T}} M_z &= \tfrac{1}{2}\,(X_a + \sigma V)(X_a + \sigma V) \\ &= \tfrac{1}{2}\,\big(X_a^2 + V^2 + \sigma(X_a V + V X_a)\big) \\ &= I + \tfrac{\sigma}{2}\,(X_a V + V X_a). \end{aligned}$$

The matrix V is diagonal and X_a maps every basis state to a different one, so $X_a V$ and $V X_a$ have zero diagonal. Hence $\mathrm{Tr}(M_z^{\mathsf{T}} M_z) = D$, and the norm is one. □

4.2. **The two recoveries.**

Proof of Theorem 1. We first take the qubit Q in a pure state $|\psi\rangle$. We combine the two blocks, and then show that Alice recovers $|\psi\rangle$ when $f(x,y) = 0$ and Bob when $f(x,y) = 1$. The part on perfect recovery extends both routing cases to a qubit that is entangled with another system, and the last part counts the EPR pairs and the messages.

Both blocks together. After step (1), the key qubits and C are in the encrypted state (3). All later operations are linear, and those of block i act only on K_i, L_i, R_i, W_i and W_i'. We therefore apply Lemma 3 to block i with $z = k_i$, in each term k of (3). Every term gets the same prefactor, of absolute value $1/(2N)^2$. For fixed outcomes of the four measurements, the normalized state after the exchange is therefore, up to a sign,

$$\frac{1}{2} \sum_{k \in \{0,1\}^2} |k_1\rangle_{K_1} |k_2\rangle_{K_2} \otimes P_k |\psi\rangle_C \otimes (M_{1,k_1} \otimes I)|\Omega\rangle_{W_1 W_1'} \otimes (M_{2,k_2} \otimes I)|\Omega\rangle_{W_2 W_2'}, \tag{13}$$

with the matrices $M_{i,z}$ of (10). The vector (13) has norm one because every vector $(M_{i,z} \otimes I)|\Omega\rangle$ has norm one by Lemma 3. It differs from the encrypted state (3) only in the work registers, which now depend on the key.

Alice recovers when $f(x,y) = 0$. We show that Alice's operations return each pair of work registers to $|\Omega\rangle$, which removes the dependence on the key. The proof of Lemma 3 showed that $M_{i,z}^{\mathsf{T}} M_{i,z} = I + \frac{\sigma}{2}(X_{a_i} V + V X_{a_i})$, with $V = V_{x,a_i+y}$ and $\sigma = (-1)^{z+t_i}$. The second term vanishes because the two operators anticommute by Lemma 2, so $M_{i,z}^{\mathsf{T}} M_{i,z} = I$. The matrix $M_{i,z}$ is real and symmetric, so it is unitary and $M_{i,z}^2 = I$. Alice applies $M_{i,z}$ to W_i'. An operator on one half of the maximally entangled state can be moved to the other half as its transpose, $(I \otimes M)|\Omega\rangle = (M^{\mathsf{T}} \otimes I)|\Omega\rangle$ for every matrix M written in the basis of (1). Hence

$$\begin{aligned} (I \otimes M_{i,z})(M_{i,z} \otimes I)|\Omega\rangle &= (M_{i,z} \otimes I)(I \otimes M_{i,z})|\Omega\rangle \\ &= (M_{i,z} \otimes I)(M_{i,z}^{\mathsf{T}} \otimes I)|\Omega\rangle \\ &= (M_{i,z}^2 \otimes I)|\Omega\rangle \\ &= |\Omega\rangle. \end{aligned}$$

Alice applies this operation controlled by the key qubit K_i, so in each term of (13) it acts with $z = k_i$. The state becomes

$$\Big(\frac{1}{2} \sum_{k \in \{0,1\}^2} |k_1\rangle_{K_1} |k_2\rangle_{K_2} \otimes P_k |\psi\rangle_C\Big) \otimes |\Omega\rangle_{W_1 W_1'} \otimes |\Omega\rangle_{W_2 W_2'}.$$

The first factor is the encrypted state (3). Inverting the Bell-basis change on $K_1 K_2$ turns it into $|\psi\rangle_Q \otimes |\Phi\rangle_{TC}$ by the teleportation identity (2), so Alice holds $|\psi\rangle$ in Q.

Bob recovers when $f(x,y) = 1$. We show that Bob's measurement finds the key bit k_i with certainty in every term of (13). By Lemma 2, the operators X_{a_i} and V_{x,a_i+y} commute. Their product $S_i = X_{a_i} V_{x,a_i+y}$ is then a real symmetric matrix with $S_i^2 = I$, so it is an observable

with eigenvalues 1 and -1. Write $V = V_{x,a_i+y}$ and $\sigma = (-1)^{z+t_i}$. Then

$$\begin{aligned} S_i\,(X_{a_i} + \sigma V) &= X_{a_i} V X_{a_i} + \sigma X_{a_i} V V \\ &= V X_{a_i} X_{a_i} + \sigma X_{a_i} \\ &= V + \sigma X_{a_i} \\ &= \sigma\,(X_{a_i} + \sigma V), \end{aligned}$$

where the second line uses that X_{a_i} and V commute and that $V^2 = I$, and the last line uses $\sigma^2 = 1$. Hence $S_i M_{i,z} = (-1)^{z+t_i} M_{i,z}$, and $(M_{i,z} \otimes I)|\Omega\rangle$ is an eigenvector of S_i on W_i with eigenvalue $(-1)^{z+t_i}$. In the term k of (13), Bob's measurement of S_i therefore gives the outcome $(-1)^{k_i+t_i}$ with certainty and leaves the term unchanged. The four terms give four different pairs of outcomes, so the two measurements select one term k, each with probability $1/4$, and the bits that Bob computes from his outcomes are the key bits of this term. His correction $P_k^\dagger$ maps $P_k|\psi\rangle$ to $|\psi\rangle$, and the state becomes

$$|\psi\rangle_C \otimes |k_1\rangle_{K_1} |k_2\rangle_{K_2} \otimes (M_{1,k_1} \otimes I)|\Omega\rangle_{W_1 W_1'} \otimes (M_{2,k_2} \otimes I)|\Omega\rangle_{W_2 W_2'},$$

so Bob holds $|\psi\rangle$ in C.

Perfect recovery. In both routing cases and for all outcomes, the final state is $|\psi\rangle$ in the recovered qubit, in tensor product with a state of the other registers that does not depend on $|\psi\rangle$. Every operation of the strategy is linear and does not depend on $|\psi\rangle$ either. The same calculation therefore applies to a qubit Q that is entangled with another system, and the strategy returns the joint state of this system and the qubit unchanged. Hence recovery is perfect on every input pair (x, y), which is the second property of Theorem 1.

Resources. The shared state is the block state (6) for two blocks, which is $2(n+1) = 2n+2$ EPR pairs. The EPR pair TC and the work registers are prepared by Alice alone and are not part of the shared state. Alice sends the qubit C and the registers W_1 and W_2 of $N = 2^n$ qubits each, in total $2^{n+1}+1$ qubits. She also sends x and two outcomes (s_i, ℓ_i), which are $n + 2(n+1) = 3n+2$ bits. Bob sends y and two outcomes (a_i, u_i), which are $3n+2$ bits. □

5. Conclusion

This paper showed that $2n+2$ shared EPR pairs suffice to route a qubit perfectly for every Boolean function, so a lower bound that counts only the shared state can grow at most linearly in n. The price is an exponentially long quantum message from Alice. Two problems remain open. First, is there a function for which routing with constant error in both routing cases needs $\Omega(n)$ EPR pairs when the messages are not limited? By Theorem 1, such a bound would be optimal. Second, can the messages be shorter? The strategy sends $2^{n+1}+1$ qubits, and it is open whether every function has a strategy with $O(n)$ EPR pairs and messages of subexponential length.

Lean formalization

A Lean formalization proves Theorem 1, using only Lean's three standard axioms. The code is available at `https://github.com/kevinbogner/linear-routing-lean`.

Disclosure of AI use

The strategy was found by GPT-6.2 Sol (OpenAI) in a research session directed by the author, and the same model wrote the Lean formalization. Claude Fable 5.2 (Anthropic) checked the strategy by independent derivation and numerical simulation, drafted the text and reviewed the formal statement. The author takes responsibility for the paper's content.

References

[ABM+24] R. Allerstorfer, H. Buhrman, A. May, F. Speelman, and P. Verduyn Lunel, *Relating non-local quantum computation to information theoretic cryptography*, Quantum **8** (2024), 1387.

[ACM25] V. R. Asadi, E. Culf, and A. May, *Rank lower bounds on non-local quantum computation*, in *16th Innovations in Theoretical Computer Science Conference*, LIPIcs **325** (2025), 11:1–11:18.

[BBC+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels*, Physical Review Letters **70** (1993), 1895–1899.

[BCF+14] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, *Position-based quantum cryptography: impossibility and constructions*, SIAM Journal on Computing **43** (2014), 150–178.

[BCS22] A. Bluhm, M. Christandl, and F. Speelman, *A single-qubit position verification protocol that is secure against multi-qubit attacks*, Nature Physics **18** (2022), 623–626.

[BFSS13] H. Buhrman, S. Fehr, C. Schaffner, and F. Speelman, *The garden-hose model*, in *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science*, ACM (2013), 145–158.

[BHM+26] A. Bluhm, S. Höfer, A. May, M. Stasiuk, P. Verduyn Lunel, and H. Yuen, *A complexity theory for non-local quantum computation*, Quantum **10** (2026), 2152.

[BK11] S. Beigi and R. König, *Simplified instantaneous non-local quantum computation with applications to position-based cryptography*, New Journal of Physics **13** (2011), 093036.

[Bog26] K. Bogner, *Robust logarithmic entanglement lower bound for f-routing*, arXiv:2608.05775v3, 2026.

[CGMO14] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, *Position-based cryptography*, SIAM Journal on Computing **43** (2014), 1291–1341.

[EFS25] L. Escolà-Farràs and F. Speelman, *Quantum position verification in one shot: parallel repetition of the f-BB84 and f-routing protocols*, arXiv:2503.09544, 2025.

[GHT26] T. Gur, M. M.-Y. Huang, and E.-C. Tang, *Quantum encodings, private messages, and communication complexity*, arXiv:2609.17690v1, 2026.

[HM26] A. Hasegawa and R. Mataraarachchi, *New lower bounds for CDS and f-routing*, arXiv:2609.24291v2, 2026.

[KMS11] A. Kent, W. J. Munro, and T. P. Spiller, *Quantum tagging: authenticating location via quantum information and relativistic signaling constraints*, Physical Review A **84** (2011), 012326.

[LVW17] T. Liu, V. Vaikuntanathan, and H. Wee, *Conditional disclosure of secrets via non-linear reconstruction*, in *Advances in Cryptology – CRYPTO 2017*, Lecture Notes in Computer Science, Springer (2017), 758–790.

[May26] A. May, *Entanglement cost in non-local quantum computation*, arXiv:2605.02840v4, 2026.

[WZ82] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned*, Nature **299** (1982), 802–803.