Quantum enhanced Secure Multiparty computation

A. D'Urbano[1], M. Oliveira[2,3,4], L. S. Barbosa[2,4]
[1]University of Salento, [2]Universidade do Minho, [3]International Iberian Nanotechnology Laboratory, [4]INESC TEC

26th International Workshop on Algebraic Development Techniques 2022

Outline

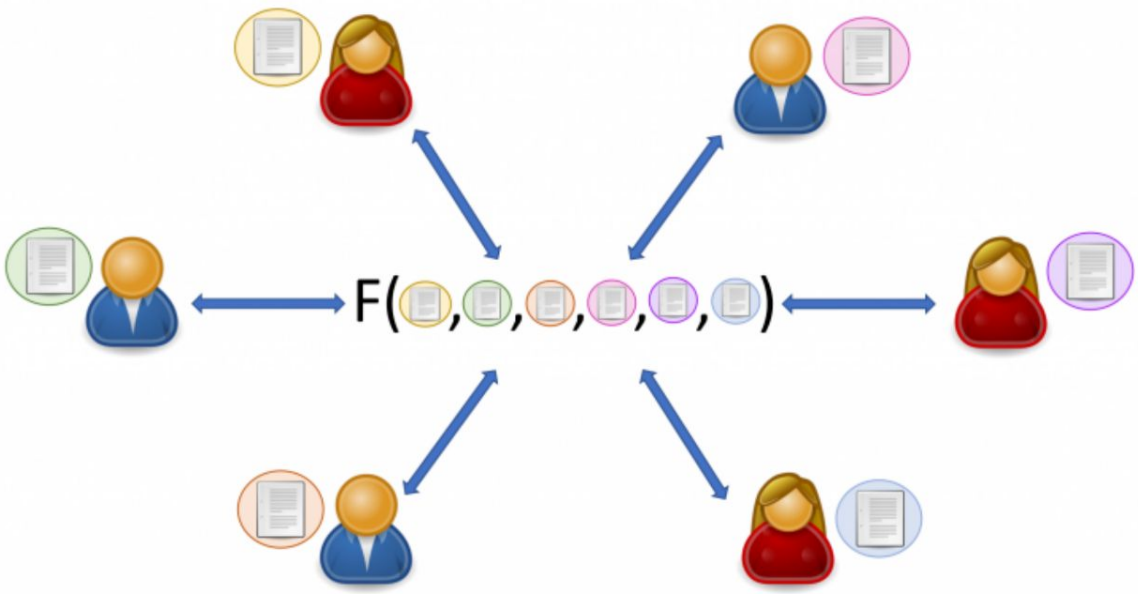
- General concepts
- Quantum-enhanced protocol
- Techniques
- Triplewise AND
- Conclusions

Outline

- General concepts
- Quantum-enhanced protocol
- Techniques
- Triplewise AND
- Conclusions

SMPC

Secure multi-party computation, SMPC, allows to compute *securely* a function using inputs from all clients involved in the protocol.



Yao's Millionaires' problem

Bruce Wayne and Tony Stark are interested in knowing who's richer without revealing their capital.[1]

[1] A. Yao, "Protocols for secure computations" in 2013 IEEE 54th Annual Symposium on Foundations of Computer Science, null, 1982 pp. 160-164. doi: 10.1109/SFCS.1982.88 https://doi.ieeecomputersociety.org/10.1109/SFCS.1982.88

Quantum-enhanced SMPC

We investigate the usage of quantum techniques in SMPC.

- In the context analysed, the parties has limited computational power.
- The computational quantum model utilised is $NMQC_{\oplus}$.

$NMQC_{\oplus}$

Non-adaptive measurement-based quantum computation with linear side-processing: $NMQC_{\oplus}$.

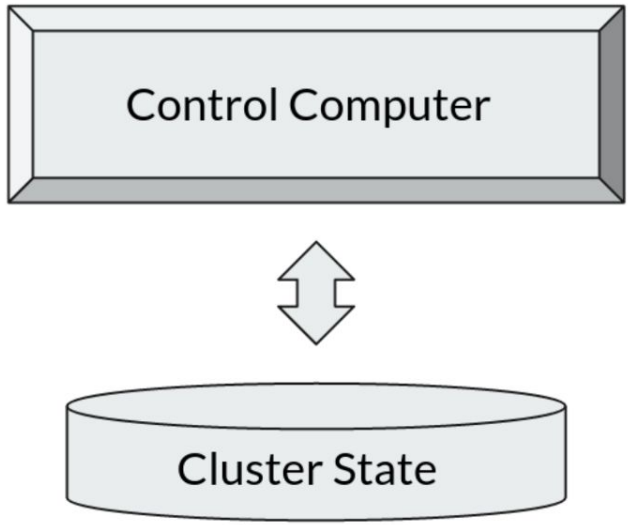


Figure: Schema of MQC, Measerement-based quantum computation.

Outline

- General concepts
- Quantum-enhanced protocol
- Techniques
- Triplewise AND
- Conclusions

NAND construction

Quantum correlation have intrinsic computational power[2]. An example is the construction of nand gate from linear computation and a 3-qubit GHZ state.

$$\sigma_a \otimes \sigma_b \otimes \sigma_{a \oplus b} \left|\psi\right\rangle = (-1)^{NAND(a,b)} \left|\psi\right\rangle$$

[2] Anders, Janet and Browne, Dan E., "Computational Power of Correlations" in Phys. Rev. Lett., volume 102, 2009, doi: 10.1103/PhysRevLett.102.050502 https://link.aps.org/doi/10.1103/PhysRevLett.102.050502

Other functions?

- Using NANDs to compute a general Boolean function can becomes too cumbersome.
- Can we apply similar techniques to compute other functions?
- For cryptographic reasons we are interested in symmetric Boolean functions.

Triplewise AND

We will build upon the protocol known in literature to compute the non-linear function Pairwise AND:[3]

$$f(x_1, \ldots, x_n) = \bigoplus_{i=1}^{n-1} x_i \left(\bigoplus_{j=i+1}^{n} x_j \right)$$

The goal is to find a protocol to compute the Triplewise AND:

$$f_3(x) = \bigoplus_{1 \leq i < j < k \leq n} x_i x_j x_k$$

[3] M. Clementi, A. Pappa, A. Eckstein, I. A. Walmsley, E. Kashefi, and S. Barz. Classical multiparty computation using quantum resources., 96(6):62317, 2017. https://link.aps.org/doi/10.1103/PhysRevA.96.062317

Outline

- General concepts
- Quantum-enhanced protocol
- Techniques
- Triplewise AND
- Conclusions

Periodic Fourier representation

To find an algorithm[4] to compute a function f in the $NMQC_{\oplus}$ model, instead of the usual Fourier representation:

$$f(x) = \sum_{S \subseteq [n]} \widehat{f}(S) \prod_{i \in S} x_i$$

it can be used the *periodic Fourier representation*:

$$f(x) = \cos\left(\pi \sum_{S \subseteq [n]} \phi_S \prod_{i \in S} x_i\right)$$

[4] R. Mori. Periodic Fourier representation of Boolean functions, 2018. https://doi.org/10.48550/arxiv.1803.09947

Measurements assignments

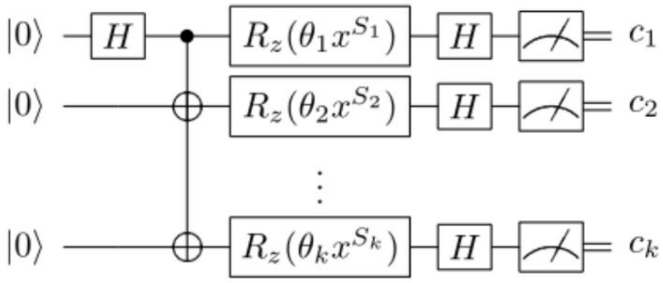
Let k be the *sparsity* of the f, then the resource state needed to perform the computation is:

$$\left|\psi^k_{GHZ}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle^{\oplus k} + \left|1\right\rangle^{\oplus k}\right)$$

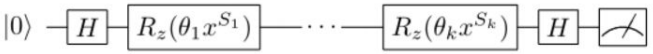
And the computation:

$$\left\langle\psi^k_{GHZ}\right| \bigoplus_i M_i \left|\psi^k_{GHZ}\right\rangle = \cos\left(poly_f(x;\phi_S)\right) = (-1)^{f(x)}$$

Equivalence GHZ-single qubit

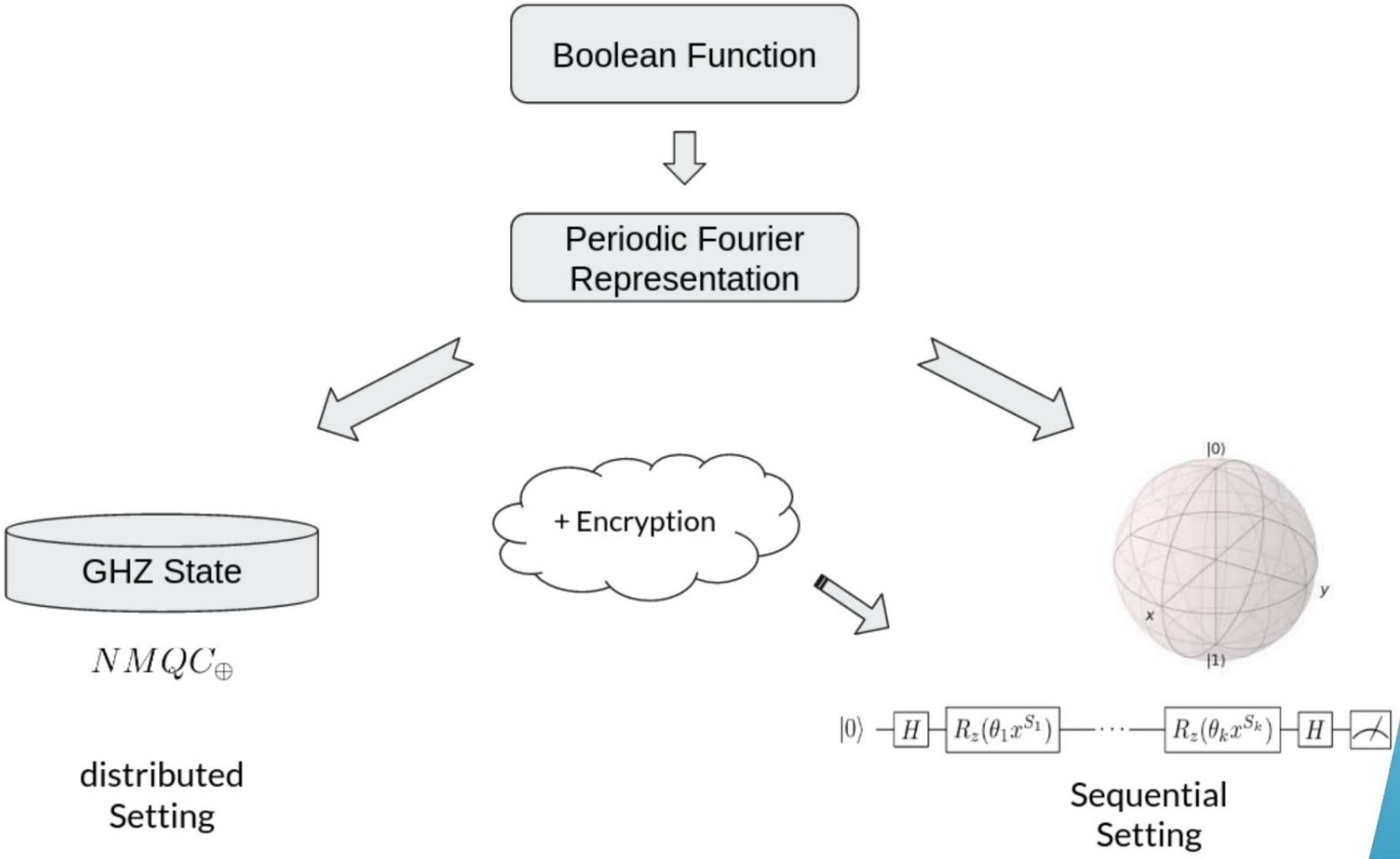


GHZ state with non-adaptive qubit measurements, $x^S := \prod_{i \in S} x_i$



Single-qubit configuration.

Distributed vs sequential



Outline

- General concepts
- Quantum-enhanced protocol
- Techniques
- Triplewise AND
- Conclusions

Setting

We can now specify the multiparty problem's setting.
n *clients* want the triplewise AND of their data.
In addition:

- a *server* will be included in the protocol;
- clients want to keep secret their data;
- the server should not know the output of the camputation.

Limitations

- All parties are restricted to only linear classical operations;
- All parties can apply 1-qubit z-rotations;
- The server can apply 1-qubit Hadamard Gate and create 1-qubit in state $|0\rangle$;
- Clients have access to a source of randomness.

Poly

The *sparse* polynomial equivalent to the triplewise AND function is:

$$P(x) = \frac{\pi}{4}\Big((n-2)*\bigoplus_{i=1}^{n} x_i + \sum_{i=1}^{n} x_i - \sum_{i=1}^{n}\Big((\bigoplus_{j=1}^{n} x_j)\oplus x_i\Big)\Big)$$

In a sequential setting, it will generate $2n+1$ quantum operations. Note that the $parity$ is required to be known.

Classical Subroutine

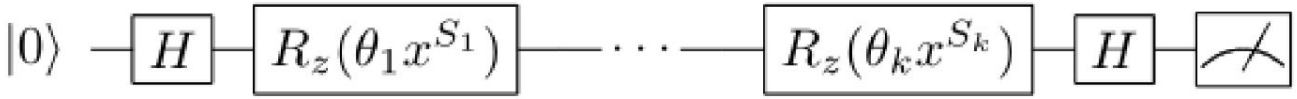
The classical algorithm used in the pairwise AND protocol[3] can be used.

1. each client divide its bit in n bits: $x_i = \bigoplus_j x_{i,j}$;
2. $x_{i,j}$ is sent to client j which compute $p_j = \bigoplus_i x_{i,j}$;
3. clients share p_j and the parity is: $p = \bigoplus_j p_j$

Each client must know the parity before the protocol's execution: this algorithm is run as initialisation step.

[3] M. Clementi, A. Pappa, A. Eckstein, I. A. Walmsley, E. Kashefi, and S. Barz. Classical multiparty computation using quantum resources., 96(6):62317, 2017. https://link.aps.org/doi/10.1103/PhysRevA.96.062317

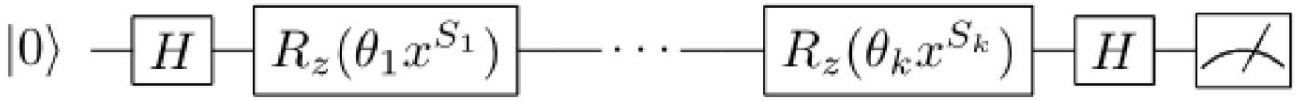
Qubit manipulation



Initial server operations:

1. creation of 1-qubit in $|0\rangle$;
2. application of Hadamard Gate;
3. sending the qubit to the first client.

Qubit manipulation

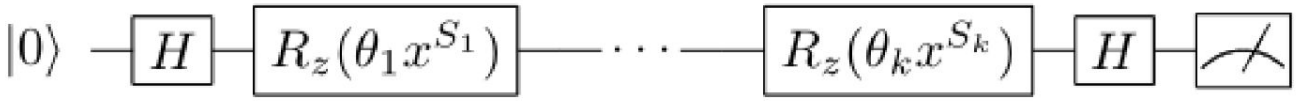


$$P(x) = \frac{\pi}{4}\left((n-2)*\bigoplus_{i=1}^{n} x_i + \sum_{i=1}^{n} x_i - \sum_{i=1}^{n}\left((\bigoplus_{j=1}^{n} x_j) \oplus x_i\right)\right)$$

Each client $\mathcal{C}_i$, upon receiving the qubit, will apply:

1. $R_z(\frac{\pi}{4}x_i)$;
2. $R_z(-\frac{\pi}{4}s_i)$ where $s_i = p \oplus x_i$;

Qubit manipulation



Final server operations:

1. application of $R_z(\frac{\pi(n-2)}{4}p)$;
2. application of Hadamard Gate;
3. measurement of the qubit;
4. broadcasting the result.

Security

- Each client apply:

$$R_z(\pi r_i)$$

- The server will measure:

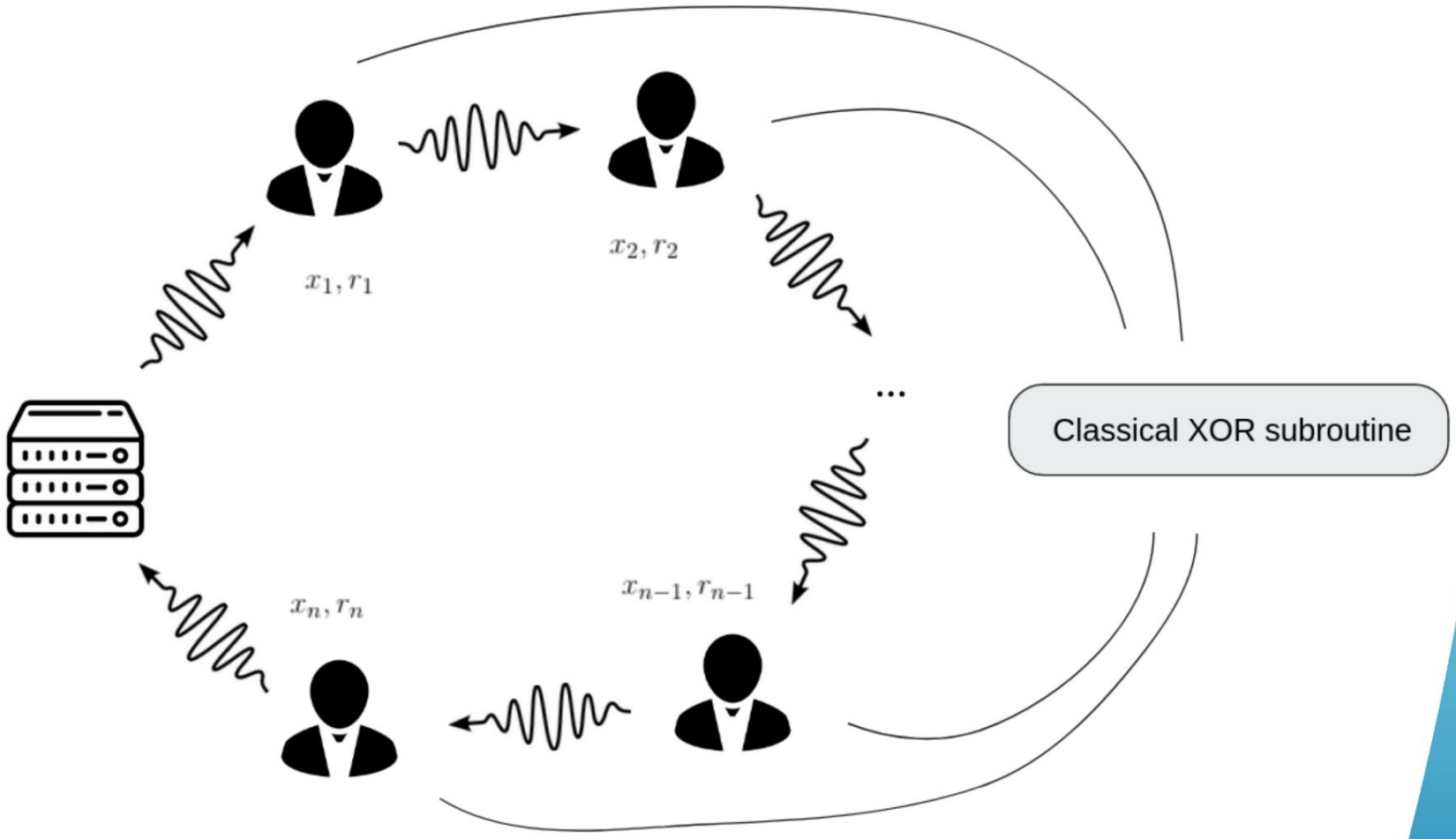
$$M = f(x) \oplus R$$

with $R = \bigoplus_i r_i$, computable with the *classical subroutine*.

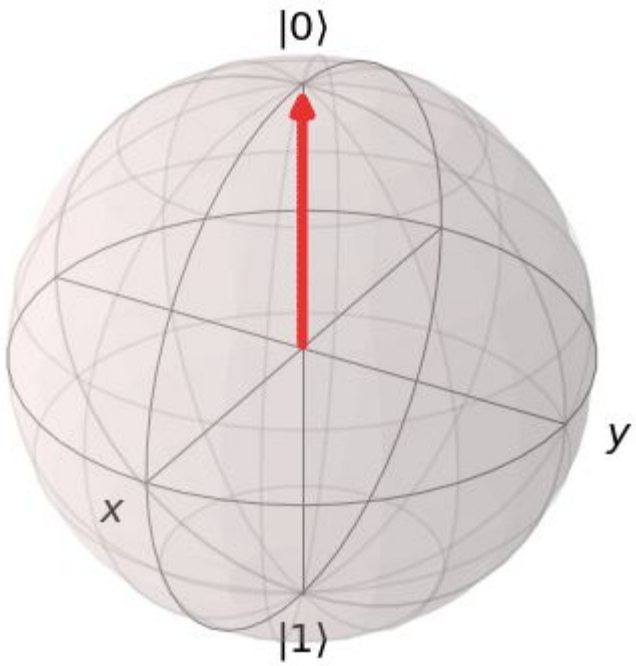
- Clients will recover the unencrypted result:

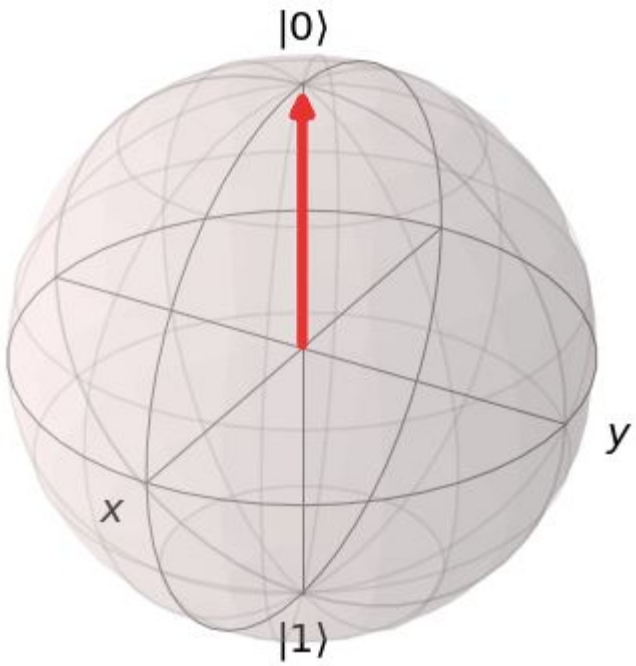
$$f(x) = M \oplus R$$

Schema



Simulation





Outline

- General concepts
- Quantum-enhanced protocol
- Techniques
- Triplewise AND
- Conclusions

Observations

- This protocol is a quantum enhanced SMPC toy model.
- The protocol could be simplified by exploiting:

$$C_n^3 = C_n^2 \wedge XOR_n$$

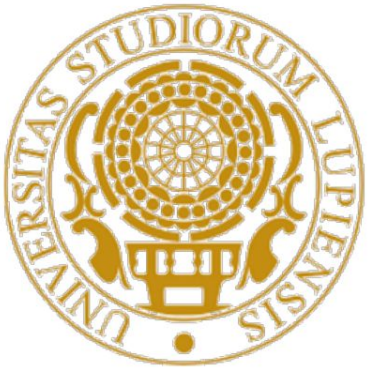
- The first non trivial case is the complete symmetric Boolean function of order 4: C_n^4

Towards higher orders

The polynomial found for C_n^4 is:

$$P_4(x) = \frac{\pi}{8}\Bigg((n-3)\Big(\sum_{i=1}^{n} x_i - \bigoplus_{j=1}^{n} x_j\Big) + \\ + \sum_{i=1}^{n}\Big(\big(\bigoplus_{j=1}^{n} x_j\big) \oplus x_i\Big) - \Big(\sum_{i<j} x_i \oplus x_j\Big)\Bigg)$$

The same technique utilised to craft the presented protocol can be applied with C_n^4.



Universidade do Minho

Thank you very much!