Confidential QUBO solver

Mariano Caruso[1,2,3,4(✉)], Daniel Escanez-Exposito[5], Pino Caballero-Gil[5], and Carlos Kuchkovsky[4]

[1] UGR, Granada, Spain.
mcaruso@ugr.es
[2] FIDESOL, Granada, Spain.
[3] UNIR, Logroño, Spain.
[4] QCentroid, Bilbao, Spain.
[5] CryptULL–ULL, Tenerife, Spain.

Abstract. Quadratic Unconstrained Binary Optimization (QUBO) is widespread and solvable via classical or quantum computing. However, outsourcing these computations online exposes sensitive data to potential breaches. We introduce a novel encryption scheme that seamlessly integrates with any solver or hardware platform, ensuring data security without compromising performance. A robust python implementation delivers promising results, marking a significant step forward in secure optimization for both classical and quantum environments.

Keywords: QUBO problems, secure optimization, cryptographic solution, transfer principle, quantum computing, hardware agnostic.

1 Introduction

Quadratic Unconstrained Binary Optimization (QUBO) is crucial in combinatorial optimization across disciplines like cryptography, economics, physics, and machine learning [1–8]. It models problems such as max-cut, graph coloring, and clustering [9–11, 13], with applications in quantum computing via Ising models and quantum annealing [14–16]. As NP-hard [17], QUBO demands efficient and secure solving methods.

Online solvers risk exposing sensitive data. This work proposes an encryption scheme enabling secure external solving without revealing original data. Unlike standard homomorphic encryption [18–20], our approach meets the specific needs of QUBO.

We define the set of natural indices $I_n := \{1, \dots, n\}$ and the binary space $\{0,1\}^n$. A function $f(\boldsymbol{x}) = \sum_{(i,j)\in I_n^2} \mathtt{Q}_{ij}\, x_i x_j$ is defined using a matrix $\mathbf{Q} \in \mathbb{R}^{n\times n}$. Since adding a constant does not change the optimal solution, the typical QUBO problem is to find

$$\underset{\boldsymbol{x}\in\{0,1\}^n}{\mathtt{arg\,min}}\, f(\boldsymbol{x}),$$

where the objective function f can be expressed compactly as $f(\boldsymbol{x}) = \boldsymbol{x} \cdot \mathtt{Q}\,\boldsymbol{x}$. When solving such problems with cloud solvers, transmitting the matrix $\mathbf{Q}$ in clear text risks exposing sensitive information.

2 Transfer principle

The encrypted objects are denoted with a prime, so the encrypted objective function is $f'(\boldsymbol{x}') = \boldsymbol{x}' \cdot \mathtt{Q}' \boldsymbol{x}'$. Define a mapping T from the original optimization problem to an encrypted version $f'(\boldsymbol{x}') := f(T(\boldsymbol{x}'))$. This allows a user to send an encrypted `QUBO` problem to an external solver without exposing sensitive data (the matrix $\mathtt{Q}$). The transformation T defines a new optimization problem in such a way that its resolution in the encrypted domain can be carried out without revealing information about the original optimization problem and without requiring key exchange. In this context, we could mention some similarities with homomorphic encryption. Note that T will not be a homomorphism in all cases, as it will not preserve the operations of addition $\oplus$ or product $\odot$ in $\{0,1\}^n$. With a transformation T satisfying $\boldsymbol{x} = T(\boldsymbol{x}')$, we establish a relation between the original matrix $\mathtt{Q}$ and its encrypted counterpart $\mathtt{Q}'$. Matching the quadratic forms in the expressions for f and f' yields a closed-form relation through an encryption function: $\mathtt{Q}' = \mathcal{E}(\boldsymbol{k}_T, \mathtt{Q})$ or $\mathtt{Q}' = \mathcal{E}_{\boldsymbol{k}_T}(\mathtt{Q})$ [21]. The matrix of the original `QUBO` problem is encrypted and sent to the $\mathtt{QUBO-solver}$. The solution returned, $\boldsymbol{x}'_*$, is then decrypted locally, and the solution to the original problem is obtained via $\boldsymbol{x}_* = T(\boldsymbol{x}'_*)$. In order to construct T there are two ingredients: diffusion via permutations and confusion via substitutions, and the encrypted matrix $\mathtt{Q}'$ is obtained from $\mathcal{E}_{\boldsymbol{P}}$ and $\mathcal{E}_{\boldsymbol{k}}$, respectively.

3 Conclusions

This work addresses the security challenges in the online resolution of unconstrained binary quadratic optimization problems. By employing cryptographic methods, we establish a framework for securely solving these problems using both classical and quantum computing. This approach protects the problem's sensitive information during resolution and encourages the adoption of advanced techniques in online environments, promoting further development in quantum computing and data security.

A complete implementation of these proposals has been developed in `python`. The proposed cryptographic solution is independent of the optimization method, so it does not depend on how the `QUBO` problem is solved. It supports exact methods, classical or quantum annealing, as well as heuristic approaches such as simulated annealing and genetic algorithms, making it hardware agnostic.

Acknowledgments. We thank `FIDESOL`, `UGR`, and `QCentroid` for the support and recall also the anonymous readers for their constructive criticism of this work. This research has been partially supported by the project `ECO-20241014`: `QUORUM` funded by Ministerio de Ciencia, Innovación y Universidades, through `CDTI` and PID2022-138933OB-I00: `ATQUE` funded by `MCIN/AEI/10.13039/501100011033/FEDER,EU`.

References

1. Burek, Elżbieta, et al. "Algebraic attacks on block ciphers using quantum annealing." IEEE Transactions on Emerging Topics in Computing vol. 10, 2 pp. 678-689 (2022).
2. Phab, Luca, Stéphane Louise, and Renaud Sirdey. "First attempts at cryptanalyzing a (toy) block cipher by means of quantum optimization approaches" Journal of Computational Science 69 (2023): 102004.
3. Orús, R., Mugel, S., Lizaso, E.: "Quantum computing for finance: Overview and prospects", *Reviews in Physics*, vol. 4, pp. 100028, 2019.
4. Hong, S. W., et al.: "Market graph clustering via qubo and digital annealing", *Journal of Risk and Financial Management*, vol. 14, n. 1, pp. 34, 2021.
5. Neukart, F., et al.: "Traffic flow optimization using a quantum annealer", *Frontiers in ICT*, vol. 4, pp. 29 (2017).
6. Li, R. Y., et al.: "Quantum annealing versus classical machine learning applied to a simplified computational biology problem", *NPJ quantum information*, vol. 4, n. 1, pp. 14 (2018).
7. R. Novak, "Quantum Algorithms in Electromagnetic Propagation Modelling for Telecommunications", *IEEE Access* (2023).
8. Streif, M., Neukart, F., Leib, M.: "Solving quantum chemistry problems with a d-wave quantum annealer", *Quantum Technology and Optimization Problems: First International Workshop, Springer International Publishing*, vol, 11413, pp. 111-122 (2019).
9. Rehfeldt, D., Koch, T., Shinano, Y.: "Faster exact solution of sparse MaxCut and QUBO problems", *Mathematical Programming Computation*, vol. 15, n. 3, pp. 445-470 (2023).
10. Tabi, Z., et al.: "Quantum optimization for the graph coloring problem with space-efficient embedding", *2020 IEEE international conference on quantum computing and engineering (QCE)*, pp. 56-62 (2020).
11. Mniszewski, S. M.: "Graph partitioning as quadratic unconstrained binary optimization (QUBO) on spiking neuromorphic hardware", *Proceedings of the International Conference on Neuromorphic Systems*, pp. 1-5 (2019).
12. Date, P., Potok, T."Adiabatic quantum linear regression", *Scientific reports*, vol. 11, n. 1, pp. 21905 (2021).
13. Date, P., Arthur, D., Pusey-Nazzaro, L.: "QUBO formulations for training machine learning models", *Scientific reports*, vol. 11, n. 1, pp. 10029 (2021).
14. Brush, S. G.: "History of the Lenz-Ising model", *Reviews of modern physics*, vol. 39, n. 4, pp. 883 (1967).
15. Albash, T., Lidar, D. A.: "Adiabatic quantum computation", *Reviews of Modern Physics*, vol. 90, n. 1, pp. 015002 (2018).
16. P. Hauke, et al: "Perspectives of quantum annealing: Methods and implementations", *Reports on Progress in Physics*, vol. 83, n. 5, pp. 054401 (2020).
17. F. Barahona, *On the computational complexity of Ising spin glass models*, J. Phys. A: Math. Gen. 15 3241 (1982).
18. Paillier, P. "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes". Advances in Cryptology — EUROCRYPT '99. Lecture Notes in Computer Science. Vol. 1592. Springer. pp. 223–238 (1999).
19. ElGamal, T. "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms". IEEE Transactions on Information Theory. 31 (4): 469–472 (1985).

20. Goldwasser, S, Micali, S. “Probabilistic encryption & how to play mental poker keeping secret all partial information”. Proceedings of the fourteenth annual ACM symposium on Theory of computing - STOC ’82. pp. 365–377 (1982).
21. Boneh, D. and Shoup, V., “A Graduate Course in Applied Cryptography”, Applied Cryptography Group - University Stanford (2020).