Criptografía para problemas QUBO

Mariano Caruso*
Fundación I+D del Software Libre, FIDESOL
mcaruso@fidesol.org
Universidad Internacional de La Rioja, UNIR
mariano.caruso@unir.net

Daniel Escanez-Exposito
Universidad de La Laguna
Tenerife, Spain
jescanez@ull.edu.es

Pino Caballero-Gil
Universidad de La Laguna
Tenerife, Spain
pcaballe@ull.edu.es

Carlos Kuchkovsky
QCentroid
Bilbao, Spain
carlos@qcentroid.xyz

***Resumen*—Los problemas cuadráticos sin restricciones de optimización binaria (QUBO) son ubicuos y pueden ser resueltos vía computación clásica o cuántica. Su resolución vía internet conlleva una posible exposición de la información codificada en dicho problema de optimización. Este artículo propone la resolución de problemas QUBO de forma segura mediante dos métodos criptográficos *agnósticos* al hardware utilizado.**

***Index Terms*—QUBO, optimización, computación cuántica, criptografía**

Tipo de contribución: *Investigación original*

I. Introducción

La programación cuadrática binaria sin restricciones, también conocida como optimización binaria cuadrática sin restricciones QUBO, es un desafío central en la optimización combinatoria con una amplia gama de aplicaciones en diversos campos: informática teórica, economía, física, aprendizaje automático [1]–[6]. En su formulación general, estos problemas son computacionalmente difíciles, perteneciente a la clase NP−hard. Su relevancia se extiende a muchos problemas clásicos de la informática teórica, tales como max-cut, coloración de grafos y partición de conjuntos [7]–[9]. En el ámbito del aprendizaje automático es posible mapear modelos de regresión, clasificación y clusterización a problemas tipo QUBO [10], [11]. Dada la estrecha relación entre estos últimos y los modelos tipo Ising [12], es posible atacar su resolución en el contexto de la computación cuántica adiabática [13] y mediante un proceso físico conocido como *quantum annealing* [14], lo que destaca su importancia en el desarrollo de algoritmos y aplicaciones cuánticas.

En el mundo de la optimización, los problemas cuadráticos sin restricciones de optimización binaria (QUBO) se han establecido en una enorme variedad de campos: En el ámbito de las finanzas [1], QUBO se aplica a la optimización de carteras, la gestión de riesgos y las estrategias de negociación algorítmica. Los modelos económicos [2] aprovechan este esquema para resolver problemas de asignación de recursos, equilibrio de mercado y minimización de costes. En el ámbito de las rutas y la logística [3], este ayuda a resolver problemas de rutas de vehículos, optimización de la ubicación de instalaciones y dilemas de gestión de la cadena de suministro. Más allá de estos ámbitos, QUBO trasciende las fronteras disciplinarias, siendo también de gran utilidad en áreas tan diversas como la biología computacional [4], las telecomunicaciones [5] o la sanidad [6].

Es por ello que la resolución de cualquiera de estos problemas plantea desafíos significativos, especialmente cuando se trata de equilibrar la eficiencia computacional con la seguridad de la información. Tanto la computación clásica como la cuántica ofrecen métodos para abordar estos problemas, pero su resolución a través de plataformas en línea genera dificultades vinculadas a la privacidad y la exposición de datos sensibles. Es decir, cuando se envía un problema a un resolutor en la nube de problemas tipo QUBO, los datos del mismo son compartidos con el servidor en cuestión, pudiendo ser consultados y alterados por los proveedores del servicio.

En esta encrucijada digital, emerge la necesidad apremiante de salvaguardar la confidencialidad de tales empresas intelectuales. En estas páginas, se propone un tratado sobre la seguridad en la resolución de QUBO, tejido con los hilos de la criptografía, que promete resguardar celosamente la integridad de la información.

En este artículo, exploraremos una solución que combina la potencia de los métodos criptográficos con la resolución de problemas QUBO, ofreciendo una forma segura y fiable al usuario de abordar estos desafíos. Para ello, se propone un sistema de cifrado del problema original de manera que el proveedor de hardware, en adelante $\texttt{QUBO}-\texttt{solver}$, opere con los datos cifrados y resuelva el problema sin exponer la información de los datos originales. Finalmente, será posible recuperar la solución de manera local por el usuario. El objetivo es dotar de una capa de seguridad del lado del usuario que pretenda resolver un problema de este tipo.

II. Definición y resolución de problemas QUBO

Comencemos por definir el conjunto de índices naturales $I_n := \{1, \cdots n\}$, luego consideremos el espacio de $n-$tuplas binarias $\texttt{B}=\{0,1\}^n$, una función $f : \texttt{B} \longrightarrow \mathbb{R}$ construida a partir de una matriz $\mathbf{Q}\in\mathbb{R}^{n\times n}$, cuyos elementos son Q_{ij}, un vector columna $\boldsymbol{p} \in \mathbb{R}^n$ cuyos elementos son p_i y un vector columna $\boldsymbol{x} \in \texttt{B}$ de componentes x_i, donde $(i,j) \in I_n^2$

$$f(\boldsymbol{x}) = \sum_{(i,j)\in I_n^2} Q_{ij}\, x_i\, x_j + \sum_{i\in I_n} p_i\, x_i \tag{1}$$

Dado que se pretende optimizar la función f, existe cierta arbitrariedad en la definición de f a menos de una constante real aditiva. En otras palabras, si $\boldsymbol{x}_*$ es un valor óptimo para $f(\boldsymbol{x})$ también lo será para $f(\boldsymbol{x}) + c$, $\forall c \in \mathbb{R}$.

El problema de optimización QUBO suele consisitir en la minimización de f, i.e. encontrar un vector binario $\boldsymbol{x}_* \in \texttt{B}$ tal que $f(\boldsymbol{x}_*) \leq f(\boldsymbol{x})$, $\forall \boldsymbol{x} \in \texttt{B}$,

$$\underset{\boldsymbol{x}\in\texttt{B}}{\texttt{argmin}}\, f(\boldsymbol{x}). \tag{2}$$

Haciendo uso de la identidad $x_i^2 = x_i$, $\forall i \in I_n$ es posible reescribir f de forma que su parte cuadrática contenga solo

productos $x_i x_j$ con $i \neq j$ y trasladar el término x_i^2 a la parte lineal de f

$$f(\boldsymbol{x}) = \sum_{\substack{(i,j)\in I_n^2 \\ i\neq j}} Q_{ij}\, x_i\, x_j + \sum_{i\in I_n} (Q_{ii} + p_i) x_i \tag{3}$$

Tomando en cuenta que $\sum_{i\in I_n} p_i x_i = \boldsymbol{p}\cdot\boldsymbol{x}$ se puede escribir también como $\boldsymbol{x}\cdot \mathtt{diag}(\boldsymbol{p})\boldsymbol{x}$, donde $\mathtt{diag}(\boldsymbol{p})$ representa la matriz que tiene en su diagonal principal las componentes de $\boldsymbol{p}$ y nulos el resto de sus elementos de matriz. Esto permite trasladar los términos lineales a la parte cuadrática de f para expresarla finalmente de forma compacta como

$$f(\boldsymbol{x}) = \boldsymbol{x}\cdot \mathtt{Q}\,\boldsymbol{x} \tag{4}$$

donde $\mathtt{Q} := \mathbf{Q} + \mathtt{diag}(\boldsymbol{p})$. Notar que la matriz $\mathtt{Q}$ contiene toda la información del problema QUBO a resolver.

En cuanto a la resolución del problema de optimización (2) con la función cuadrática dada por (4), podemos esquematizarla en la siguiente figura 1.

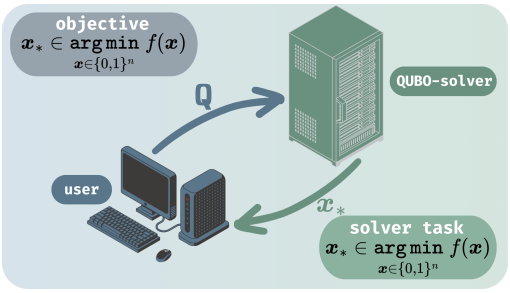

Figura 1: A partir de la definición de $f(\boldsymbol{x})$, la matriz $\mathtt{Q}$ es enviada vía internet al dispositivo $\mathtt{QUBO-solver}$ que minimiza a $f(\boldsymbol{x})$.

Se ha hecho mención a la ubicuidad de los problemas QUBO, en tanto multiplicidad y variedad de casos de uso, pero además hay un amplio grado de inclusión, en el sentido en que es posible encontrar problemas que no sean cuadráticos, con restricciones y que no sean en variable binaria y que igualmente pueden mapearse a la generosa categoría de problemas QUBO.

III. Principio de transferencia

En esta sección se hará referencia a una propuesta de resolución segura de (2), formularemos un principio que permita mapear (transferir) el problema de optimización original a otro equivalente en el dominio cifrado, resolverlo de manera segura y obtener la solución localmente.

En general, dada una función $f\colon \mathtt{X} \longrightarrow \mathbb{R}$ y un problema de optimización para $f(\boldsymbol{x})$, pretendemos construir otra función $g\colon \mathtt{Y} \longrightarrow \mathbb{R}$ que capture el problema de optimización original. Sea T una transformación de $\mathtt{Y}$ en $\mathtt{X}$, con la cual mapear el problema de optimización (2) de f en otro similar para otra función g, de forma tal que resolver el problema para g sea seguro y pueda obtenerse la solución del problema original usando T.

Definimos la función g según

$$g(\boldsymbol{y}) := f\big(T(\boldsymbol{y})\big), \tag{5}$$

es decir, la función g toma valores idénticos que los transformados por T de la función f. Esto garantiza una conexión entre los argumentos de f y g que las hacen óptimas. En el caso de optimización, minimizar o maximizar, similar al de (2), resulta que

$$\underset{\boldsymbol{x}\in\mathtt{X}}{\mathtt{arg\,opt}}\ f(\boldsymbol{x}) \xleftrightarrow{\ T\ } \underset{\boldsymbol{y}\in\mathtt{Y}}{\mathtt{arg\,opt}}\ g(\boldsymbol{y}), \tag{6}$$

donde $\mathtt{arg\,opt}$ abrevia la búsqueda del argumento que optimiza (maximiza o minimiza) a la función en cuestión. De manera que si al minimizar (maximizar) g se obtiene $\boldsymbol{y}_*$ entonces se sabrá que el mínimo (máximo) para f se obtendrá en $\boldsymbol{x}_*$ tal que $\boldsymbol{x}_* = T(\boldsymbol{y}_*)$.

En adelante, denotaremos por $\boldsymbol{x}'$ al vector binario y por $f'(\boldsymbol{x}')$ a la función objetivo que resultan de cifrar vía T al vector binario $\boldsymbol{x}$ y a la función objetivo $f(\boldsymbol{x})$, originales, denotado por $\boldsymbol{x} = T(\boldsymbol{x}')$.

Se propone que T sea una transformación caracterizada por una matriz que hace las veces de clave local generada para transformar (cifrar) el problema original de manera de enviarse de forma segura al $\mathtt{QUBO-solver}$.

También consideramos otra propuesta con un término aditivo para la transformación T, que mapea dos vectores $\boldsymbol{x}, \boldsymbol{x}' \in \{0,1\}^n$. En este caso el factor aditivo hace las veces de clave local generada para transformar (cifrar) el problema original de manera de enviarse de forma segura al $\mathtt{QUBO-solver}$. Repetimos el procedimiento de la sección anterior en tanto estudiar la forma que tendrá la matriz $\mathtt{Q}'$ que debe enviarse al $\mathtt{QUBO-solver}$.

IV. Conclusiones

El presente trabajo ofrece dos soluciones para abordar los desafíos de seguridad asociados con la resolución en línea de problemas cuadráticos sin restricciones de optimización binaria. Al proponer el uso de dos métodos criptográficos, se establece un marco confiable para la resolución segura de estos problemas, tanto a través de computación clásica como cuántica. Esta aproximación no solo garantiza la protección de la información del problema durante el proceso de resolución, sino que también promueve la adopción de técnicas avanzadas en un entorno en línea, fomentando así el desarrollo continuo en el campo de la computación cuántica y la seguridad de datos.

Se ha comentado que existe una estrecha relación entre los problemas QUBO y los modelos de Ising, y que estos últimos pueden ser tratados con computación cuántica. No obstante, cabe destacar que la transformación de protección de la información de los datos se ha aplicado solamente a nivel de variables binarias del problema QUBO. Esto se debe a que: **a.** se presupone que el canal de comunicación por el que se envía la información de la matriz $\mathtt{Q}$ es clásico y **b.** dar una capa de seguridad al usuario que garantice que el problema a resolver por $\mathtt{QUBO-solver}$ no será expuesto, independientemente de la naturaleza clásica o cuántica de tal proveedor. Sin embargo, podría pensarse en un esquema en el que las operaciones de cifrado y descifrado se apliquen a los estados cuánticos asociados al problema QUBO vía Ising. En este caso y para mantener válida la afirmación **b.** deben ser considerados, al menos, dos escenarios respecto a la naturaleza de la comunicación $\mathtt{usuario-solver}$: **1. canal cuántico** el usuario debería poder manipular y enviar/recibir la información de los estados cuánticos al/del proveedor **2. canal clásico** y el usuario manipule y envíe/reciba la información de

los estados cuánticos cifrada. Notar que este último escenario no parece ser práctico, pues se trata de un problema QUBO que se transforma a uno Ising, se le aplican operaciones de cifrado/descifrado y luego se vuelve a transformar para enviarse/recibirse al/del solver vía el canal clásico. Podría imaginarse que la propuesta de métodos para cifrar el problema Ising equivalente y conservar un canal clásico, tendrá sentido práctico si se quisiera implementar directamente en un proveedor de hardware cuántico. En ese caso, la solución de seguridad sería implementable fuera del entorno local del usuario. En resumen, el argumento de la protección de la información en formato cuántico se saldría fuera del contexto de este trabajo, pues pretendía ser agnóstico al hardware, sin presuponer siquiera su naturaleza.

Es posible que la solución general provenga de aplicar ambas propuestas de manera conjunta. Se encuentran en proceso la implementación en código y la aplicación de las técnicas de criptoanálisis adecuadas.

AGRADECIMIENTOS

La presente investigación fue realizada con el soporte en el contexto de la Red de Excelencia Contramedidas Inteligentes de Ciberseguirdad para la Red del Futuro (CICERO), CER-20231019, financiado por el Ministerio de Ciencia, Innovación y Universidades, a través de CDTI, el proyecto Q−CAYLE, European Union, Next Generation UE/MICIU/Plan de Recuperacion, Transformacion y esiliencia/Junta de Castilla y Leon y el proyecto PID2022-138933OB-I00: ATQUE financiado por MCIN/AEI/10.13039/501100011033/FEDER, EU.

REFERENCIAS

[1] Orús, R., Mugel, S., Lizaso, E.: “Quantum computing for finance: Overview and prospects”, *Reviews in Physics*, vol. 4, pp. 100028, 2019.
[2] 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.
[3] Neukart, F., et al.: “Traffic flow optimization using a quantum annealer”, *Frontiers in ICT*, vol. 4, pp. 29, 2017.
[4] 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.
[5] Novak, R.: “Quantum Algorithms in Electromagnetic Propagation Modelling for Telecommunications”, *IEEE Access*, 2023.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10] Date, P., Potok, T.:“Adiabatic quantum linear regression”, *Scientific reports*, vol. 11, n. 1, pp. 21905, 2021.
[11] Date, P., Arthur, D., Pusey-Nazzaro, L.: “QUBO formulations for training machine learning models”, *Scientific reports*, vol. 11, n. 1, pp. 10029, 2021.
[12] Brush, S. G.: “History of the Lenz-Ising model”, *Reviews of modern physics*, vol. 39, n. 4, pp. 883, 1967.
[13] Albash, T., Lidar, D. A.: “Adiabatic quantum computation”, *Reviews of Modern Physics*, vol. 90, n. 1, pp. 015002, 2018.
[14] Hauke, P., et al: “Perspectives of quantum annealing: Methods and implementations”, *Reports on Progress in Physics*, vol. 83, n. 5, pp. 054401, 2020.
[15] Horn, R. A., Johnson, C. R. “Matrix Analysis”, *Cambridge University Press*, ISBN: 0521386322, (1990).
[16] Birkhoff, G. “Three observations on linear algebra”, *Univ. Nac. Tacuman, Rev. Ser.* A, 5, 147-151 (1946).