COMPUTER RESEARCH AND MODELING
2026 VOL. 18 NO. 5 P. e1129–e1159
DOI: 10.20537/2076-7633-2026-18-5-1129-1159

Ки&М

MODELS IN PHYSICS AND TECHNOLOGY

UDC: 681.5.015

A comprehensive review of common QUBO solvers in the cybersecurity domain. Advantages and disadvantages

K. Yu. Khubiev[1,a], Ya. A. Kholodov[1,b], A. S. Petrenko[2,c]

[1]Sirius University of Science and Technology,
1 Olimpiyskiy ave., Sirius, Sirius Federal Territory, Krasnodar region, 354340, Russia
[2]St. Petersburg Federal Research Center of the Russian Academy of Science,
39 14th Line V.O., St. Petersburg, 199178, Russia

E-mail: [a] kasymkhankhubievnis@gmail.com, [b] holodov.ya@talantiuspeh.ru, [c] a.petrenko1999@rambler.ru

Received 02.04.2026, after completion — 21.07.2026.
Accepted for publication 02.10.2026.

Quadratic Unconstrained Binary Optimization (QUBO) provides a common modeling framework for combinatorial optimization problems arising in cybersecurity. This review analyzes how cryptanalytic constraints, anomaly-detection objectives, network-defense tasks and cyber-risk models can be encoded as QUBO or equivalent Ising formulations. We compare three classes of solvers used in the literature: physical quantum annealers, hybrid quantum-classical workflows and quantum-inspired classical heuristics such as simulated annealing and simulated bifurcation. Particular attention is paid to the gap between formal QUBO expressiveness and practical solvability on current hardware, including embedding overhead, limited connectivity, noise and scaling constraints. The reviewed studies are grouped by application domain and assessed in terms of model size, solution quality, runtime indicators and reproducibility of computational settings. We show that QUBO is already useful as a unifying language for cybersecurity optimization, while near-term practical advantages are most plausible in hybrid and quantum-inspired settings rather than in fully quantum implementations. The review concludes by outlining open problems in QUBO construction, decomposition, sparsification and benchmarking for cybersecurity applications.

Keywords: cybersecurity, quantum annealing, quantum computation, QUBO

Citation: *Computer Research and Modeling*, 2026, vol. 18, no. 5, pp. e1129–e1159.

This work was obtained with the financial support of the project “Technologies for countering previously unknown quantum cyber threats”, implemented within the framework of the state program of the “Sirius” Federal Territory “Scientific and technological development of the ‘Sirius’ Federal Territory” (Agreement No. 23-03 dated September 27, 2024).

© 2026 Kasymkhan Yu. Khubiev, Yaroslav A. Kholodov, Alexey S. Petrenko
This work is licensed under the Creative Commons Attribution-NoDerivs 3.0 Unported License.
To view a copy of this license, visit http://creativecommons.org/licenses/by-nd/3.0/
or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

КОМПЬЮТЕРНЫЕ ИССЛЕДОВАНИЯ
И МОДЕЛИРОВАНИЕ 2026 Т. 18 № 5 С. e1129–e1159
DOI: 10.20537/2076-7633-2026-18-5-1129-1159

Ки&М

МОДЕЛИ В ФИЗИКЕ И ТЕХНОЛОГИИ

УДК: 681.5.015

Анализ применимости QUBO-алгоритмов в области информационной безопасности. Достоинства и недостатки

К. Ю. Хубиев[1,a], Я. А. Холодов[1,b], А. С. Петренко[2,c]

[1]Научно-технологический университет «Сириус»,
Россия, 354340, Краснодарский край, Федеральная территория «Сириус», пгт Сириус,
проспект Олимпийский, д. 1
[2]Санкт-Петербургский федеральный исследовательский центр Российской академии наук,
Россия, 199178, г. Санкт-Петербург, 14-я линия В.О., д. 39

E-mail: [a] kasymkhankhubievnis@gmail.com, [b] holodov.ya@talantiuspeh.ru, [c] a.petrenko1999@rambler.ru

Получено 02.04.2026, после доработки — 21.07.2026.
Принято к публикации 02.10.2026.

Квадратичная неограниченная бинарная оптимизация (*QUBO*) зарекомендовала себя в качестве эффективного инструмента для решения NP-трудных задач в области информационной безопасности. В QUBO-формулировке задача описывается в виде квадратичной функции бинарных переменных, минимум которой соответствует оптимальному решению. Такая запись учитывает линейные (индивидуальное влияние) и квадратичные (парные взаимодействия) зависимости. Особенно примечательно, что QUBO-алгоритмы можно имплементировать в квантовые вычислительные устройства на основе отжига, например *D-Wave*, которые позволяют найти собственное состояние гамильтониана соответствующей модели Изинга посредством квантовых или гибридных алгоритмов. При этом решение QUBO-задачи можно получить и на полностью классической архитектуре. Такие алгоритмы называют квантово вдохновленными, потому что они имитируют физические явления. Примером таких квантово вдохновленных алгоритмов являются симулированный отжиг (Simulated Annealing, SA) и симулированные бифуркации (Simulated Bifurcation, SB). За последние 5–7 лет большое количество работ было посвящено применению QUBO-формулировки для разнообразных задач информационной безопасности, начиная от взлома ключей безопасности до детекции атак, с целью доказать эффективность новых вычислительных парадигм. В данном исследовании мы анализируем эти работы, сгруппировав их по области применения и выделяя архитектурные подходы (квантовая, гибридная, классическая) в каждом сценарии. Мы уделяем внимание тому, как задача была переформулирована в QUBO-постановку или модель Изинга, анализируем ключевые стратегии решения и полученные результаты на оптимальность, масштабируемость, сложность. Мы выделяем основные преимущества и недостатки каждой QUBO-постановки в контексте информационной безопасности и в заключение обсуждаем актуальные задачи и перспективные направления для исследований.

Ключевые слова: информационная безопасность, квантовый отжиг, квантовые вычисления, QUBO

Работа выполнена при финансовой поддержке проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение № 23-03 от 27.09.2024 г.).

© 2026 Касымхан Юсуфович Хубиев, Ярослав Александрович Холодов, Алексей Сергеевич Петренко
Статья доступна по лицензии Creative Commons Attribution-NoDerivs 3.0 Unported License.
Чтобы получить текст лицензии, посетите веб-сайт http://creativecommons.org/licenses/by-nd/3.0/
или отправьте письмо в Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Introduction

As computational resources become increasingly strained and existing technologies approach physical limits, including the limits of classical integrated-circuit scaling [Moore, 1965; Dennard et al., 1974], quantum computing is being considered as a potential driver of technological progress. Quantum devices are neither a panacea nor a universal solution; nevertheless, the quantum effects of superposition, interference, and entanglement can accelerate computation and improve performance for certain classes of problems. This computational capability and high degree of parallelism give quantum computing considerable potential while simultaneously creating distinct security risks.

In a world where processes ranging from everyday purchases and communication to public services, financial transactions, and asset management are moving into the digital environment, cybersecurity has become a central concern. Quantum computing is particularly significant for cryptography because many cryptographic algorithms rely on assumptions about computational hardness. Shor's algorithm [Shor, 1994] demonstrates the effectiveness of quantum architectures for integer factorization and discrete logarithms, which underpin RSA, classical Diffie – Hellman schemes, and elliptic-curve cryptosystems. On a sufficiently powerful and fault-tolerant quantum computer, quantum algorithms can solve the corresponding decryption problems in polynomial time. Here, a powerful computer means one whose number of qubits can scale in proportion to the cryptographic key length. Even where Shor's algorithm is inapplicable to an attack, Grover's algorithm [Grover, 1997] provides a quadratic speedup for unstructured search, affecting exhaustive key search and the parameter choices of symmetric cryptography. Research and experimental results in this area have prompted major initiatives to migrate to post-quantum cryptography, including the multi-round NIST standardization process and the development of migration guidance.

The role of quantum computing in cryptography is not, however, limited to "breaking" ciphers. The design, analysis, and implementation of cryptographic systems are closely tied to optimization problems, including key recovery as constraint satisfaction, the search for differential and linear characteristics, parameter selection under security – performance trade-offs, the configuration of countermeasures against side-channel attacks, and resource allocation in cryptographic networks. For such problems, quantum optimization is important less as a universal accelerator than as an alternative computational paradigm for families of binary optimization problems that can be expressed as minimization of a system's energy.

The Ising model [Ising, 1925] provides a key link between discrete optimization and quantum-computing architectures. It was originally introduced in statistical physics to describe interactions among spins. The fundamental optimization problem in this model is to find the system's ground state — the Hamiltonian configuration at which its energy is minimized. The model is defined by a set of spins with discrete states, local fields, and pairwise interactions. This formalism fits naturally within the paradigms of Adiabatic Quantum Computing (AQC) and Quantum Annealing (QA) [Farhi et al., 2000; Farhi et al., 2001; Albash, Lidar, 2018]. The preprint [Farhi et al., 2000] is cited as the

historically important source of the original AQC formulation, while the published study [Farhi et al., 2001] complements it with an experimental investigation of the adiabatic algorithm on random instances of an NP-complete problem. These approaches rely on an adiabatic quantum process in which the system remains in its ground state when the Hamiltonian changes sufficiently slowly. The system is initialized in a known configuration and then evolves toward the problem Hamiltonian; the resulting ground state represents a solution to the optimization problem. Quantum annealing is the corresponding quantum analog of classical simulated annealing, with transitions between states driven by quantum fluctuations rather than thermal fluctuations. The foundations of this approach were established in studies of the transverse-field Ising model [Kadowaki, Nishimori, 1998]. The experimental implementation of programmable artificial-spin systems [Johnson et al., 2011] laid the groundwork for the practical use of quantum annealing to find the global minimum of an Ising-model energy landscape.

In practice, the standard formulation for such optimization problems is Quadratic Unconstrained Binary Optimization (QUBO):

$$\min_{\mathbf{x}\in\{0,1\}^n} \mathbf{x}^T\mathbf{Q}\mathbf{x}, \tag{1}$$

which is algebraically equivalent to a broad class of problems formulated in the Ising model.

The QUBO formulation is attractive because it provides a universal objective function: constraints are incorporated as penalty terms, while higher-order Zhegalkin polynomials can be reduced to quadratic form by introducing auxiliary variables. These properties make QUBO applicable to a broad class of NP-hard and pseudo-Boolean optimization problems [Boros, Gruber, 2012]. Moreover, many NP-hard problems can be mapped explicitly to an Ising model or QUBO [Lucas, 2014], enabling both qualitative and quantitative assessment of the effects of moving to quantum-computing architectures.

Fundamental physical limitations nevertheless remain: finding the ground state of a general Ising Hamiltonian is NP-hard [Barahona, 1982]. Quantum annealing therefore does not eliminate NP-hardness; instead, it offers new heuristic — and, in some cases, algorithmic — approaches to exploring a system's energy landscape. The gap between the theoretical effectiveness and practical power of QUBO and Ising formalisms, on the one hand, and the physical limitations of real quantum devices — including noise, quantum-system stability, control precision, and embedding complexity — on the other, defines the current research agenda in quantum optimization.

The current cryptographic research agenda is highly application-oriented: many studies focus on cryptanalytic problems such as factorization, solving systems of Boolean equations, and expressing the constraints of block and stream ciphers as QUBO formulations suitable for quantum-annealing solvers [Zhang, Feng, 2022]. Study [Zhang, Feng, 2022] is included in this review because it provides a specialized account of concrete transformations from cryptographic problems to QUBO and quantum-annealing formulations rather than limiting itself to general observations about quantum optimization. Such research may contribute to alternative approaches to cryptanalysis. Unlike gate-based quantum

algorithms, which require long coherent sequences of operations as in Shor's algorithm, a cryptographic structure can be represented in QUBO form as an energy function. Quantum, classical, or hybrid annealing then drives it toward a minimum-energy configuration corresponding to an encryption key or another feasible solution.

Alongside the rapid development of quantum technologies, QUBO has become a practical tool and a universal optimization interface supporting several computational paradigms for algorithmic solvers. Solvers based on physical analogies are often classified as "quantum-inspired" algorithms. Implementations of these approaches exist on classical, hybrid, and quantum-computing architectures. On classical hardware, the simulated-annealing metaheuristic provides a robust method for finding low-energy states by gradually lowering the system temperature and imitating adiabatic evolution. It is one of the standard tools for solving QUBO problems. Other quantum-inspired algorithms likewise simulate physical processes without genuine quantum coherence. A prominent example is simulated bifurcation, which uses nonlinear system dynamics and the bifurcation phenomenon to explore an Ising-model energy landscape efficiently. Related principles are implemented on quantum architectures: in AQC and quantum annealing, problem parameters are encoded in a time-dependent Hamiltonian that evolves so that the system ends in the ground state corresponding to the global energy minimum.

This paper reviews QUBO solvers and the principal variants of quantum-annealing algorithms. It first examines the physical foundations of quantum annealing, then considers QUBO applications across cybersecurity, and finally compares the effectiveness, strengths, and limitations of the reviewed formulations and solver classes. The conclusion identifies directions for improving QUBO construction and solving, and for extending adiabatic and hybrid optimization to cybersecurity problems.

Literature selection methodology

Sources were selected in several stages. First, a broad search was conducted across major scholarly databases; the resulting publications were then screened for relevance to the review and for the presence of a reproducible optimization formulation. The initial search covered IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, Google Scholar, and arXiv. Search strings combined the terms "QUBO cybersecurity", "quantum annealing cryptanalysis", "Ising formulation cryptography", "QUBO anomaly detection", "quantum annealing network security", "quantum-inspired optimization cybersecurity", and "D-Wave QUBO security". These queries served only as an initial discovery mechanism; inclusion was determined not by the occurrence of a particular term in a title or abstract but by substantive eligibility criteria.

After the initial search, publications were screened on the basis of their abstracts, problem formulations, and experimental sections. Studies were included when they met the following conditions: the problem belonged to one of the article's application areas (cryptanalysis, anomaly detection, network security, defensive-resource placement, or cyber-risk assessment); the study explicitly specified a QUBO formulation, an Ising-model formulation, or a closely related pseudo-Boolean formalization; it described the correspondence between domain variables and binary optimization variables; and it

reported the model size, solver, experimental results, computational limitations, or the procedure used to transform the original problem into QUBO or Ising form. Following substantive screening, the studies were organized into focused thematic clusters: cryptanalytic QUBO formulations, anomaly detection, network graph problems, defensive-resource placement, security-policy optimization, and cyber-risk assessment. Formulations with similar mathematical structures were then combined into broader groups, allowing cybersecurity publications to be compared with relevant problems from neighboring fields. For example, honeypot, sensor, and defensive-node placement were considered alongside covering, facility-location, and logistics optimization, while network segmentation or sparsification was compared with graph partitioning, minimum cut, resource placement, and other QUBO-compatible graph formulations. For applied studies, priority was given to publications from the past five to seven years, when a substantial body of research on QUBO in cybersecurity emerged. Foundational work on the Ising model, AQC, and quantum and simulated annealing was included regardless of publication date as the methodological basis of the review.

Publications were excluded if they discussed quantum computing without connecting it to QUBO, the Ising model, or another reproducible optimization formalism. Cybersecurity studies lacking either a mathematical formulation or sufficient data to assess the scale and computational feasibility of the proposed approach were also excluded. Popular and technically unreviewed materials, brief review mentions without an original model, and duplicate preprints for which a later journal or conference version existed were not included. arXiv preprints were considered only when they contained a concrete QUBO or Ising formulation, experimental parameters, or results unavailable in peer-reviewed sources; for older preprints, the existence of a published version was additionally checked.

Physical foundations of quantum optimization algorithms

The Ising model

Combinatorial problems in quantum optimization are often formulated using the Ising model. The primary objective is to find the spin configuration that minimizes the system energy:

$$E_{\text{Ising}} = -\frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N} J_{i,j}s_i s_j - \sum_{i=1}^{N} h_i s_i. \tag{2}$$

In expression (2), the spin variables $s_i \in \{-1, 1\}$ take binary values, N denotes the number of spins in the system, and the pairwise interaction coefficients satisfy:

$$J_{i,i} = 0, \quad J_{i,j} = J_{j,i} \quad \forall i \neq j. \tag{3}$$

In general, the parameters h_i in the Ising energy expression (2) represent local fields acting on the ith spin. Because additional spin variables can reduce the problem to the zero-local-field case, we consider the Ising model with $h_i = 0$ below.

It is important to note that the configurations $\{s_i\}$ and $\{-s_i\}$ yield the same system energy, so the problem always has at least two symmetric solutions. Minimizing the energy of a general Ising model is NP-hard. The following sections examine several algorithmic approaches based on physical processes that can explore the state space efficiently and solve combinatorial optimization problems within this model.

The quantum adiabatic theorem

According to the quantum adiabatic theorem, a quantum system initialized in a nondegenerate ground state of a time-dependent Hamiltonian remains in the ground state over an arbitrarily long evolution provided that the Hamiltonian changes sufficiently slowly.

If the Hamiltonian of a quantum system is time independent, the system dynamics are described by the Schrödinger equation. For a time-independent Hamiltonian H, the Schrödinger equation takes the form:

$$i\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle \tag{4}$$

whose solution for an initial state $|\psi(0)\rangle$ is

$$|\psi(t)\rangle = \exp(-iHt)|\psi(0)\rangle. \tag{5}$$

Thus, any eigenstate $|E\rangle$ of the Hamiltonian H satisfying $H|E\rangle = E|E\rangle$ evolves in time only through the phase factor $\exp(-iEt)$. No transitions between eigenstates occur in this case.

If the system Hamiltonian depends on time, the resulting evolution of the quantum state can be substantially more complex, making the dynamics difficult to describe analytically. When the Hamiltonian changes sufficiently slowly, however, the system remains close to its instantaneous eigenstate. The quantum adiabatic theorem formalizes this behavior.

For illustration, consider a spin in a magnetic field that rotates smoothly from one direction to another over a finite time T:

$$H(t) = -\cos\left(\frac{\pi t}{2T}\right)\sigma_x - \sin\left(\frac{\pi t}{2T}\right)\sigma_z. \tag{6}$$

Suppose that the spin is initially aligned with the x axis, so the system is in the Hamiltonian ground state at $t = 0$. As the magnetic field slowly rotates toward the z axis, the spin state begins to precess around the field's instantaneous direction. As the evolution time T increases, the angular rate of change of the Hamiltonian decreases relative to the precession rate, reducing the amplitude of deviations from the instantaneous ground state. In the limit of infinitely slow field rotation, the quantum state remains in the Hamiltonian's ground eigenstate at every instant.

More generally, consider a Hermitian operator $H(s)$ that is continuous in the parameter $s \in [0, 1]$. Introduce the change of variable $s = \frac{t}{T}$, where T is the total system-evolution time. For sufficiently

large T, the Hamiltonian $H(t)$ changes arbitrarily slowly as a function of time t. The initial quantum state $|\psi(0)\rangle$ evolves according to the Schrödinger equation:

$$i\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle, \tag{7}$$

or, after substituting $s = \frac{t}{T}$:

$$i\frac{d}{ds}|\psi(s)\rangle = TH(s)|\psi(s)\rangle. \tag{8}$$

Suppose that the initial state $|\psi(0)\rangle$ is an eigenstate of $H(0)$ and, for simplicity, its nondegenerate ground state. Assume additionally that the ground state of $H(s)$ remains nondegenerate for every $s \in [0, 1]$. The quantum adiabatic theorem then states that, in the limit $T \to \infty$, the final system state $|\psi(T)\rangle$ coincides with the ground state of $H(1)$.

In practice, concrete bounds are required for the evolution time T needed to satisfy the adiabatic approximation. A detailed proof of the adiabatic theorem is beyond the scope of this paper. Informally, if a system is constructed whose dynamics satisfy the theorem's conditions, it will remain in its ground state at every time $\tau \in [0, T]$.

Bifurcation-based quantum computing

The dynamics of a nonlinear system depend qualitatively on its parameter values. Points at which the system's behavior changes abruptly are called bifurcation points. A quantum-mechanical oscillator can enter a superposition state through adiabatic evolution across a bifurcation point. The quantum bifurcation algorithm proposed by Hayato Goto [Goto, 2016; Goto, 2019] introduces a computational paradigm in which an ensemble of nonlinear quantum oscillators replaces a system of qubits and the optimization problem is solved through quantum adiabatic evolution.

Existing quantum-computing architectures already use nonlinear oscillators as physical implementations of qubits, including through superposition effects [Mirrahimi et al., 2014], while computation is performed by quantum-gate operations. This approach does not, however, fully exploit the continuous degrees of freedom of nonlinear oscillator systems. Through superposition, an ensemble of N nonlinear quantum oscillators can span a space of 2^N effective states. When searching for an optimum through adiabatic evolution across bifurcation points, the system's control parameters are increased gradually.

The algorithm in [Goto, 2016] uses a Kerr parametric oscillator (KPO). In a reference frame rotating at half the parametric-pump angular frequency, $\frac{\omega_p}{2}$, and under the rotating-wave approximation, the system Hamiltonian is:

$$H = \hbar\Delta a^\dagger a + \hbar\frac{K}{2}a^{\dagger 2}a^2 - \hbar\frac{p}{2}\left(a^2 + a^{\dagger 2}\right), \tag{9}$$

where a and $a^\dagger$ are the annihilation and creation operators, Δ is the detuning defined as the difference between the oscillator's natural frequency and half the pump frequency, K is the Kerr coefficient,

and p is a nonnegative control parameter corresponding to the pump amplitude. The parameters K and Δ are assumed positive, with $\Delta = \omega_{\mathrm{KPO}} - \frac{\omega_p}{2}$, where ω_{KPO} is the oscillator's resonant frequency.

The transition to superposition proceeds as follows. The system is initialized in the vacuum state, that is, the ground state $|0\rangle$ with zero field amplitude. The state $|0\rangle$ is the ground state of Hamiltonian (9) at $p = 0$. During adiabatic evolution, the control parameter p is increased slowly, causing the system Hamiltonian to change smoothly.

In the limit $p \gg \Delta$, the final state approximately equals the ground state of the Hamiltonian at $\Delta = 0$, which is a superposition of the two coherent states $\left|\pm\sqrt{\frac{p}{K}}\right\rangle$. Because the Hamiltonian is invariant under the parity transformation $a \to -a$, the final state retains the parity of the initial vacuum state $|0\rangle$. The system consequently enters the superposition:

$$\frac{\left|\sqrt{\frac{p}{K}}\right\rangle + \left|-\sqrt{\frac{p}{K}}\right\rangle}{\sqrt{2}}, \quad \left\langle\sqrt{\frac{p}{K}}\right| -\sqrt{\frac{p}{K}}\Big\rangle = e^{-2p/K} \xrightarrow{p\gg 1} 0. \tag{10}$$

Because the binary optimization problem is formulated using the Ising model (2), the Hamiltonian of the nonlinear-oscillator system must be expressed in a corresponding form. The pairwise linear nondissipative coupling between oscillators is described by:

$$H_{\mathrm{coupling}} = -\frac{\hbar\xi_0}{2}\sum_{i<j}^{N} J_{i,j}\left(a_i^\dagger a_j + a_j^\dagger a_i\right). \tag{11}$$

Combining the single parametric-oscillator Hamiltonian (9) with this coupling yields the following Hamiltonian for a system of N oscillators:

$$H(t) = \hbar\sum_{i=1}^{N}\left[\Delta_i a_i^\dagger a_i + \frac{K_i}{2}a_i^{\dagger 2}a_i^2 - \frac{p_i(t)}{2}\left(a_i^{\dagger 2} + a_i^2\right) - \left(\epsilon_i a_i^\dagger + \epsilon_i^* a_i\right)\right] - \hbar\frac{\xi_0}{2}\sum_{i<j} J_{i,j}\left(a_i^\dagger a_j + a_j^\dagger a_i\right), \tag{12}$$

where ξ_0 is a positive constant with units of frequency that characterizes the oscillator-coupling strength. Correct implementation of the adiabatic evolution requires:

$$\Delta_i = \xi_0\sum_{j=1}^{N}|J_{i,j}|. \tag{13}$$

Annealing-based quantum computing

Quantum annealing is a computational paradigm based on quantum adiabatic evolution. Historically, annealing was first introduced for classical optimization by Kirkpatrick et al. [Kirkpatrick et al., 1983] as the Simulated Annealing (SA) algorithm, which became a general method for solving a broad class of optimization problems. Its central idea is to use thermal fluctuations to escape local minima of the objective function while lowering the temperature in a controlled manner.

The cooling rate is crucial to the algorithm's performance: if the temperature decreases too quickly, the system may become trapped in local minima, whereas excessively slow cooling makes the algorithm impractical despite its theoretical convergence to the global minimum. Geman and Geman [Geman, Geman, 1984] derived a bound on the temperature schedule that guarantees convergence to the global minimum in the general case:

$$T \leqslant \frac{c}{\log t},$$

where c is a constant determined by the problem dimension and objective-function parameters, and t is the system-evolution time.

Global-minimum search algorithms generally proceed by exploring a sequence of system states and transitions among them. This naturally motivates the use of quantum effects to improve the convergence of optimization procedures. Quantum annealing builds on the concept proposed by Kadowaki and Nishimori [Kadowaki, Nishimori, 1998]: quantum tunneling allows a system to traverse potential barriers efficiently, including saddle points and local minima in the energy landscape.

To account for tunneling between states, a transverse quantum field $\Gamma(t)$ is introduced, giving the following Ising-model Hamiltonian based on expression (2):

$$H(t) = -\sum_{i=1}^{N}\sum_{j=1}^{N} J_{i,j}\sigma_i^z\sigma_j^z - \sum_{i=1}^{N} h_i\sigma_i^z - \Gamma(t)\sum_{i=1}^{N}\Delta_i\sigma_i^x, \tag{14}$$

where σ_i^x and σ_i^z are Pauli matrices acting on the ith spin, with eigenvalues ± 1, and Δ_i characterizes the quantum-tunneling strength between the basis states $|\pm 1\rangle$.

Let the Ising-model Hamiltonian without the transverse field be:

$$H_p = -\sum_{i=1}^{N}\sum_{j=1}^{N} J_{i,j}\sigma_i^z\sigma_j^z - \sum_{i=1}^{N} h_i\sigma_i^z. \tag{15}$$

The time-dependent Hamiltonian (14) can then be rewritten as:

$$H(t) = -\Gamma(t)\sum_{i=1}^{N}\Delta_i\sigma_i^x + H_p. \tag{16}$$

By varying the transverse-field amplitude $\Gamma(t)$ smoothly from a large initial value $\Gamma(0) \gg 1$ to zero, one can implement an adiabatic evolution in which the system reaches the minimum-energy ground state of H_p. For example, study [Johnson et al., 2011] implements quantum annealing using a system of artificial spins with the Hamiltonian:

$$H(t) = -\Gamma(t)\sum_{i=1}^{N}\Delta_i\sigma_i^x + \Lambda(t)H_p. \tag{17}$$

Initially, the system is set to $\Gamma(0) = 1$ and $\Lambda(0) = 0$, so its dynamics are governed entirely by the transverse terms $\Delta_i \sigma_i^x$. The ground state of this system is a superposition in the eigenbasis of σ^z. During adiabatic evolution, the contribution of the transverse field decreases gradually while that of the Ising Hamiltonian increases: $\Gamma(t)$ decreases monotonically from 1 to 0, and $\Lambda(t)$ increases monotonically from 0 to 1. If the parameters change sufficiently slowly, the quantum adiabatic theorem ensures that the system remains in its ground state throughout the evolution and ends in the ground state of H_p.

Applications of quadratic binary optimization in cybersecurity

Having reviewed the physical models and algorithmic foundations of QUBO solving, we now analyze their application to practical cybersecurity problems. The discussion distinguishes four implementation levels for QUBO approaches. Physical quantum implementations are experiments in which a problem is mapped to actual quantum hardware, such as a D-Wave quantum annealer or a neutral-atom QPU. Hybrid implementations perform decomposition, preprocessing, postprocessing, and part of the search classically while using a quantum device as a coprocessor for subproblems. Simulations and quantum-inspired algorithms run on conventional classical architectures; examples include simulated annealing, qbsolv without QPU access, simulated quantum annealing, and simulated bifurcation. Such methods may exploit mathematical analogies with physical processes, but the computation itself is classical and uses no quantum coherence. Finally, some studies provide only a QUBO formulation or scale estimate without an experimental solver run. This distinction is essential when interpreting speedup claims: physical-device results reflect a particular hardware generation, whereas simulation results primarily characterize the formulation and the selected classical solver. For each applied study discussed below, we therefore identify the implementation level to which its results belong.

Cryptanalysis in QUBO form

Cryptanalysis often reduces to difficult combinatorial problems such as recovering secret keys or identifying vulnerable structures in cryptographic algorithms. These problems are frequently expressed as NP-hard constrained systems of algebraic equations and can be converted into QUBO formulations. Several recent studies represent cryptanalytic problems as QUBOs suitable for quantum-annealing hardware. In particular, multiple works have shown that attacks on symmetric ciphers can be formalized as QUBO problems.

Studies [Burek et al., 2022; Burek, 2025] propose representing the AES-128 block cipher as a system of polynomial equations and then formulating the resulting optimization problem as a QUBO. These studies primarily concern theoretical formulations and dimension estimates rather than a full-scale attack on a real QPU. The authors note that, in terms of problem dimension, quantum-annealing cryptanalysis of AES-128 is less computationally demanding than factoring a public key with a comparable security level. Representing the factorization of 3072-bit RSA, which corresponds to the AES-128 security level, requires approximately 2 360 000 binary variables in QUBO form, whereas an

AES-128 attack requires about 30 000. This result highlights a substantial difference in computational complexity between symmetric-cipher cryptanalysis and RSA factorization under the QUBO paradigm.

A subsequent study [Burek, Wroński, 2022] applies the QUBO approach to the Speck block cipher and obtains representations even more compact than those for AES. It likewise remains primarily a theoretical formulation and heuristic assessment of quantum annealing's applicability. The proposed formulation requires 19 311 binary variables for Speck-128/128 and 33 721 for Speck-128/256, compared with 29 770 and 72 597 for AES-128 and AES-256, respectively. These results demonstrate that cryptanalytic complexity differs among ciphers even under the same algebraic attack model. The dimension is reduced substantially by optimizing the partitioning of equation systems and introducing auxiliary variables so as to minimize the total number of binary variables, indicating progress toward efficient QUBO representations of symmetric cryptographic primitives.

Another important contribution, study [Pakhomchik et al., 2022], proposes two general methods for converting Boolean expressions arising in cryptanalysis into solver-compatible forms: systems of linear equations and inequalities for Mixed Integer Linear Programming (MILP), or direct QUBO formulations with penalty terms. This is a theoretical and methodological study: it defines a Boolean-constraint conversion procedure but does not demonstrate an advantage for any particular physical quantum device. The authors illustrate the approach with symmetric cryptographic primitives, including the formulation of AES round operations as MILP followed by conversion to QUBO. The key idea is that any Boolean function, such as an S-box or round function, can be represented by linear constraints with additional binary variables and then converted into a quadratic objective. Despite the method's generality, the authors note that it can substantially increase the number of auxiliary variables.

Study [Wroński et al., 2025] examines in detail the conversion of cryptanalysis for Grain-128/128a into a QUBO requiring approximately 5 751 binary variables and 77 496 pairwise couplings to encode the cipher constraints. In implementation terms, it is primarily a formulation and hardware-feasibility estimate because the full problem remains too dense for direct embedding on current quantum annealers. Based on heuristic estimates, the authors claim that for problems of dimension N, quantum annealing provides an average speedup of approximately $\sqrt{N}$ over classical simulated annealing. Quantum-annealing optimization attacks could therefore outperform both greedy search and Grover's algorithm for sufficiently large key spaces.

Collectively, these approaches share a common idea: the logical dependencies of a cryptographic algorithm are encoded as a QUBO, after which a specialized solver such as a D-Wave quantum annealer searches for the minimum-energy Ising configuration corresponding to the secret key. The studies demonstrate that key recovery can be reduced to QUBO and addressed with quantum optimization devices. The resulting problems nevertheless remain extremely large and substantially exceed the number of qubits available in current quantum-computing systems. Even so, this work is an important step toward specialized quantum architectures — particularly quantum annealers — that might eventually support effective cryptanalysis of symmetric ciphers.

In public-key cryptography, and RSA in particular, the QUBO formalism is applied to integer factorization. Study [Dridi, Alghassi, 2017] proposes a QUBO formulation that was used to factor integers as large as 200 099 on a physical *D-Wave 2X* quantum annealer. Higher-order polynomial terms were reduced to quadratic form through Gröbner-basis decomposition. Similarly, study [Jiang et al., 2018] develops a QUBO formulation that factored integers up to 376 289 using 94 logical qubits on a physical D-Wave 2000Q. These small-integer experiments demonstrate how RSA cryptanalysis can be mapped to QUBO optimization. A related line of work considers HUBO and QUBO factorization models [Jun, Lee, 2023]; these are primarily theoretical formulations and comparisons of formalisms rather than attacks on cryptographically significant keys. Later studies show that performance depends not only on the QUBO formulation but also on how it is embedded in the annealer's physical topology. Study [Ding et al., 2024] proposes a modular, locally structured embedding of a binary multiplication circuit directly into the D-Wave Advantage Pegasus topology. A controlled full adder is encoded as an eight-qubit module, and multiplier circuits are assembled from these modules. The authors embedded multipliers of up to 21×12 bits in a 5760-qubit topology and experimentally factored $8\,219\,999 = 32\,749 \times 251$ on a real D-Wave Advantage 4.1. A subsequent report [Ding et al., 2024] details the initialization, pausing, reverse-annealing, and offset-tuning strategies. Another recent approach explicitly models carry propagation in binary multiplication [Ryou et al., 2025]. Its HUBO model remains practical only for small semiprimes, whereas a CQM formulation with a global product constraint handles semiprimes up to 60 bits in a hybrid D-Wave workflow, including $N = 1\,152\,921\,423\,002\,469\,787$. Current factorization results must therefore be divided into direct experiments on physical quantum annealers and hybrid or constrained models that improve scalability without directly embedding a large QUBO on a QPU. For cryptosystems of practical size, such as 3072-bit RSA, the QUBO representation still requires on the order of one million binary variables [Burek et al., 2022]; this is a theoretical dimension estimate, not a QPU experiment.

A comparison of the reviewed studies on symmetric-cipher cryptanalysis and factorization is presented in Table 1. The table separately indicates whether each problem was actually run on physical quantum hardware, because some studies use QUBO only for dimension estimates or for simulations and hybrid solvers.

Table 1 shows that the physical experiments among the reviewed cryptographic problems rely almost exclusively on D-Wave quantum annealers. Gate-based quantum computers appear only in the toy-cipher QAOA experiment, which did not implement a QUBO formulation. Bifurcation solvers are not a primary experimental platform in this group. They remain a relevant class of quantum-inspired QUBO methods, but the cited cryptanalysis and factorization examples provide no separate, confirmed hardware demonstration.

Quantum-annealing cryptanalysis does not guarantee an asymptotic speedup over Grover's algorithm or classical exhaustive search, although it may outperform traditional attacks in particular scenarios. On an ideal gate-based quantum computer, Grover's algorithm [Grover, 1997] provides

Table 1. Comparison of QUBO approaches to cipher cryptanalysis and factorization

Study	Задача	QUBO dimension / complexity	QPU/solver type: annealer, computer, bifurcation	Physical device
[Burek et al., 2022]	AES and SmallCipher	SmallCipher: 64 variables for one round and 200 for two rounds; AES-128: up to 237 915 binary variables; RSA-3072 estimate: approximately 2 360 000 variables	D-Wave-compatible quantum annealing; a simulator was used for small examples	No for the full attack; simulation/estimate only
[Burek, 2025]	Simon	Simon-16/16: Q matrix with 1684 nonzero entries; Simon-128/128: 27 270 variables; Simon-128/256: 49 408 variables	D-Wave quantum annealer	Yes for Simon-16/16; no for full versions
[Burek, Wroński, 2022]	Speck	Speck-128/128: 19 311 variables; Speck-128/256: 33 721 variables; heuristic annealing complexity $O\left(e^{\sqrt{N}}\right)$	Quantum annealer as the target architecture	No for full Speck; theoretical estimate
[Pakhomchik et al., 2022]	Boolean constraints for AES, MD5, and SHA-256	MD5: about 17 280 variables; SHA-256: 47 808; AES-128: about 90 000; AES-256: about 250 000	QUBO/MILP conversion; embedding tested on D-Wave topologies	No; embedding experiment only
[Phab et al., 2023]	Heys toy cipher	No QUBO constructed; CNF/MAX-SAT/QAOA ranges from 5 variables and 19 clauses to 29 variables and 164 clauses	Gate-based IBM quantum computers and QAOA simulators	Yes for a small five-qubit formula; not QUBO
[Dridi, Alghassi, 2017]	Factorization	Up to 200 099 = 499 × 401; approximately 72–75 logical variables for the column algorithm after Gröbner-basis preprocessing	D-Wave 2X quantum annealer	Yes
[Jiang et al., 2018]	Factorization	N = 143 uses 12 logical qubits; 376 289 is represented with 94 logical qubits; 249 919 is embedded in 1803 physical qubits	D-Wave 2000Q quantum annealer	Yes for small instances and embedding experiments
[Jun, Lee, 2023]	Factorization	QUBO for N = 15: 15 logical qubits; larger examples use HUBO/range models; quadratization requires up to $\frac{7}{4}n^2(n - -1)^2$ auxiliary variables for quartic terms	D-Wave Advantage for the small QUBO; Ocean/Leap and ExactPolySolver for HUBO	Yes only for the small QUBO; larger results are not direct QPU QUBOs
[Ding et al., 2024; Ding et al., 2024]	Factorization	Locally structured embedding: 8 qubits per full-adder module; up to 21 × 12 bits in an ideal Pegasus topology; solved 8 219 999	D-Wave Advantage 4.1 quantum annealer	Yes
[Ryou et al., 2025]	Factorization	HUBO becomes impractical near 10 bits; CQM tests reach 60-bit semiprimes; no single QUBO dimension comparable to direct embedding	Hybrid D-Wave CQM/Ocean; ExactPolySolver for small HUBOs	No direct large-QUBO QPU run

a quadratic speedup for unstructured search, requiring approximately $\sqrt{N}$ iterations in a space of size N. Searching a key space of 2^n possibilities therefore requires approximately $2^{n/2}$ steps. The complexity nevertheless remains exponential in the key length.

Quantum annealing instead uses tunneling to move between states, which could theoretically provide faster convergence for optimization problems [Mukherjee, Chakrabarti, 2015]. Whether quantum annealing can generally outperform Grover-accelerated search remains open. Using heuristic rules, the authors of [Burek, Wroński, 2022] estimate quantum-annealing complexity as $O\left(e^{\sqrt{N}}\right)$. Under this estimate, quantum-annealing QUBO optimization might require fewer iterations than exponential exhaustive search, but the claim currently lacks practical confirmation.

In practice, current quantum annealers are noisy and severely limited in scale. Experiments on simplified primitives, including a six-round miniature AES and the 64-bit Heys cipher, show that neither quantum annealers nor approximate quantum algorithms yet outperform classical cryptanalysis even on small problems [Phab et al., 2023]. Unlike purely theoretical QUBO formulations, this study is valuable as a comparative experiment on small model instances using both physical and simulated optimization procedures. For exhaustive key search, Grover's algorithm thus provides a guaranteed quadratic speedup, whereas quantum annealing may theoretically offer further gains for particular QUBO classes; realizing that advantage will require advances in both algorithms and hardware.

Anomaly detection as a QUBO problem

Anomaly detection identifies data points or behavioral patterns that deviate substantially from the general structure of a dataset. It is critical in finance, healthcare, and especially cybersecurity. In cybersecurity, network-intrusion and fraud detection often reduce to finding rare malicious events hidden in large data volumes. Traditional statistical and heuristic methods are widely used, but increasing data dimension and volume impose significant limitations on accuracy, processing speed, and scalability. Behavioral patterns also evolve over time, requiring detection systems to adapt.

Recent advances in artificial intelligence have popularized deep-learning and reinforcement-learning approaches that use computational accelerators to build highly accurate black-box models. These methods perform well, but further scaling and acceleration are often constrained by available computing resources. Quantum computing is consequently being explored as an alternative paradigm for difficult optimization problems [Stein et al., 2024]; the cited study uses both simulation for parameter selection and runs on D-Wave quantum annealers. Several studies formulate anomaly detection as QUBO [Mellaerts, 2023]. Study [Mellaerts, 2023] is a software-based, quantum-inspired implementation because its QUBO is solved heuristically on a classical computer without a physical QPU.

QUBO provides a convenient representation of anomaly detection as binary optimization. Each data point or feature is generally assigned a binary variable equal to 1 if the element is anomalous and 0 otherwise. A quadratic objective is then defined so that its minimum represents the most likely configuration containing anomalous elements.

Study [Mellaerts, 2023] proposes a QUBO combining statistical and density-based anomaly criteria. It is included because it provides an explicit anomaly-detection QUBO and an experimental comparison using quality metrics relevant to cybersecurity applicability. Its results should nevertheless be interpreted as classical software solutions of a QUBO rather than experiments on a quantum processor. The linear objective terms measure each point's deviation from the distribution centroid, while the quadratic terms capture pairwise distances between samples. For a dataset $X = (x_0, \ldots, x_{N-1})$

containing N elements, the QUBO is:

$$Q(x, \alpha) = \alpha \sum_{i=1}^{N} d_i x_i + (1 - \alpha) \sum_{i \neq j}^{N} d_{i,j} x_i x_j, \quad \sum_{i=1}^{N} x_i = k,$$

where d_i is the distance from point x_i to the distribution centroid, $d_{i,j}$ is the distance between sample points, $0 < k \leq N$ is the assumed number of anomalies, and $\alpha \in [0, 1]$ controls the relative contributions of the linear and quadratic terms. This formulation captures local deviations and global data structure simultaneously.

Such QUBO models often use Mahalanobis distance, which accounts for feature correlations and provides a robust multivariate measure of deviation. Experiments in [Mellaerts, 2023] report better *ROC AUC* than classical methods on several datasets. Unlike many deep-learning models, the QUBO approach is unsupervised [Stein et al., 2024] and requires no prior labels, an important advantage for practical cybersecurity systems. Study [Stein et al., 2024] evaluates this property in a QBM using simulated annealing and physical D-Wave annealers.

Several studies use quantum hardware to solve anomaly-detection QUBOs. Study [Stein et al., 2024], for example, implements a Quantum Boltzmann Machine (QBM) on a D-Wave annealer for anomaly detection in Endpoint Detection and Response (EDR). This is a mixed implementation: classical simulated annealing selects hyperparameters, and the final model variants are tested on physical D-Wave 2000Q and Advantage systems. The quantum model outperformed a classical Boltzmann machine on the same dataset, suggesting potential advantages for quantum annealing.

Despite current hardware limitations, some studies demonstrate practical quantum anomaly detection on real devices. In [Canonici, Caruso, 2024], the authors reformulate a Support Vector Machine (SVM) as a QUBO and implement it on a neutral-atom Quantum Processing Unit (QPU). The study is included because it provides both a theoretical formulation and an experimental QUBO-SVM implementation on real quantum hardware. It also uses ideal and noisy simulations, so the hardware and simulation results must be distinguished. Several quantum SVM variants are proposed, some of which achieve lower test error in fraud detection than several popular classical machine-learning models. The results suggest that directly expressing anomaly detection as optimization can improve solution quality and potentially facilitate scaling to high-dimensional data.

This approach generally produces a dense QUBO matrix Q, requiring long chains of coupled qubits when embedded on real hardware. The authors therefore note that full-scale problems remain beyond current processors. Experiments on a 24-qubit QPU nevertheless show that the quantum SVM is highly noise tolerant and that quantum noise can sometimes reduce overfitting. Devices with several dozen qubits can thus solve small anomaly-detection problems effectively and achieve competitive accuracy, supporting the promise of QUBO for quantum machine learning in cybersecurity.

A distinct anomaly-detection class concerns intrusion detection and Intrusion Detection Systems (IDS). These systems identify malicious activity in networks or on individual hosts and typically

classify traffic as “normal” or “malicious”. IDS models process high-dimensional data to uncover latent behavioral patterns. QUBO can serve either as a preprocessing layer for machine learning or as a standalone classifier.

The preprocessing approach is common in stochastic neural networks, particularly Restricted Boltzmann Machines (RBMs). An RBM has a quadratic energy function compatible with Ising solvers, including quantum annealers [Moro, Prati, 2023]; this reference provides the methodological link between RBM/QBM and Ising models rather than a standalone cybersecurity QUBO benchmark. Study [Dixit et al., 2021] was among the first to train an RBM for intrusion detection on a physical D-Wave 2000Q annealer. The RBM served as both a classifier and a generator of synthetic events. Hardware constraints severely limited the problem dimension, leading to the use of 64-bit binary vectors. The Quantum Annealing RBM (QARBM) achieved accuracy comparable to a classically trained RBM.

Another direction develops hybrid architectures [Li et al., 2015; Salama et al., 2011] in which classical models reduce input dimension before quantum processing, or quantum methods generate additional features for subsequent classical learning. Here, these studies serve as classical and hybrid IDS baselines, not as examples of QUBO runs on physical quantum hardware.

Table 2 compares the reviewed anomaly-detection studies. It separately reports QUBO or Ising-model scale, platform type, and whether a physical quantum run was performed, because the literature includes full QPU experiments, classical quantum-inspired solutions, and methodologically related RBM/DBN baselines.

Table 2 shows that the most mature hardware experiments in anomaly detection use D-Wave annealers and small analog neutral-atom QPUs. Explicit sample-wide QUBO anomaly selection quickly produces dense matrices and quadratic growth in couplings, whereas RBM/QBM approaches shift the computational burden to sampling from an energy model. Bifurcation solvers are not used experimentally in the reviewed anomaly-detection studies, although they remain a potentially applicable class of quantum-inspired QUBO methods.

Anomaly-detection QUBOs are highly flexible: adjusting objective weights and structure can incorporate domain knowledge, including specialized distance metrics. QUBO naturally supports a binary decision for every sample point, which is useful when an explicit subset of anomalous events must be selected for further analysis. It can also constrain the number of anomalies directly in the objective without additional heuristics, for example through linear limiting terms — a capability not always available directly in machine- and deep-learning models.

The primary limitation is the difficulty of implementing optimization algorithms on quantum architectures in practice. Additional heuristics can reduce the computational burden but do not guarantee convergence to the global minimum. Selecting an appropriate distance metric in a high-dimensional feature space is another nontrivial problem. An overly simple metric may produce many false positives, placing additional load on downstream analytical modules.

Table 2. Comparison of QUBO approaches to anomaly detection

Study	Problem and model	QUBO dimension / complexity	QPU/solver type: annealer, computer, bifurcation	Physical quantum device
[Stein et al., 2024]	Unsupervised anomaly detection / fraud-like EDR; QBM	Best SA model: 21 visible and 82 hidden variables, totaling 103 logical binary variables and about $21 \cdot 82 + \binom{21}{2} = 1932$ quadratic couplings before embedding; hardware limits: up to 94 hidden variables on D-Wave 2000Q and 632 on Advantage 4.1	Simulated annealing for hyperparameter selection; physical D-Wave 2000Q and Advantage 4.1 annealers; no bifurcation solver	Yes; final validation on D-Wave
[Mellaerts, 2023]	Unsupervised outlier detection; explicit QUBO anomaly selection	N binary variables, one per data point; pairwise terms scale as $O\left(N^2\right)$ without sparsification and $O(Nk)$ with k-furthest-neighbor, but the penalty $\left(\sum_i x_i - k\right)^2$ again creates dense couplings; MNIST tests use 50 variables and $k = 5$	Classical computer / quantum-inspired QUBO through `qbsolv`; SA/SQA/QUBO heuristics proposed; no physical annealer or bifurcation computer	No; classical QUBO solution only
[Canonici, Caruso, 2024]	Credit-card fraud detection; QUBO-SVM	$KN \times KN$ QUBO matrix; construction time $O\left(N^2K^2N_{\text{features}}\right)$, quantum component $O\left(N^2K^2\right)$, atom count $O(NK)$; for $K = 2$, simulations use 8–16 atoms and physical runs 18–24	Analog neutral-atom Pasqal Fresnel quantum computer; ideal and noisy Pulser simulations; atom placement optimized classically; no bifurcation solver	Yes; real neutral-atom QPU runs
[Moro, Prati, 2023]	IDS anomaly detection; QRBM/RBM	NSL-KDD: 85 visible and 30 hidden bits, totaling 115 logical units; CSE-CIC-IDS2018: 156 visible and 90 hidden bits, totaling 246; classical CD scales as $O(kN)$, while QPU access time is empirically near $O(Ns)$	Physical D-Wave Advantage 4.1 annealer; classical CPU baselines; no bifurcation solver	Yes; D-Wave Advantage 4.1 experiments
[Dixit et al., 2021]	IDS on ISCX IDS 2012; QARBM	64 visible and 64 hidden logical units, totaling 128 binary variables and up to $64 \cdot 64 = 4096$ visible–hidden couplings before embedding; each logical node is a chain of 16 physical qubits	Physical D-Wave 2000Q annealer; classical RBM CD-1 baseline; no bifurcation solver	Yes; D-Wave 2000Q
[Li et al., 2015]	Malicious-code / IDS classification; AutoEncoder+DBN	No explicit QUBO; a classical compressed neural model is used, for example AutoEncoder 41 → 300 → → 150 → 75 and a DBN on 2000 KDDCUP'99 records	Classical MATLAB computer; no QPU, annealer, or bifurcation solver	No; classical baseline
[Salama et al., 2011]	IDS on NSL-KDD; DBN-SVM	No explicit QUBO; DBN reduces dimension, for example from 41 → → 13 → 5 features, followed by SVM classification	Classical computer / Weka; no QPU, annealer, or bifurcation solver	No; classical baseline

Hybrid strategies can partially mitigate these limitations, for example by using classical machine learning to preselect potential anomalies or relevant features before final QUBO-based optimization.

Formulating anomaly detection as QUBO enables specialized solvers that may outperform classical algorithms in both accuracy and speed. The formalism combines several anomaly criteria in a single objective, which has improved outlier-detection quality in several scenarios.

At the solver level, quantum annealers introduce a fundamentally different search mechanism based on quantum effects. Some studies report better model quality, but practical use is limited by noise, connectivity, and hardware scalability. Quantum-inspired algorithms help bridge theory and practice by solving QUBOs efficiently on classical architectures.

Current trends suggest that QUBO anomaly detection, supported by both quantum and high-performance classical solvers, could become an important standalone or integrated component of future cybersecurity systems as data volumes continue to grow.

Network security

Securing communication networks involves optimization problems such as finding secure data routes, placing defensive resources (including honeypots and sensors), and segmenting networks to contain threats. These problems have traditionally been addressed with heuristics or manual design. As network infrastructures grow and become more complex, however, such approaches scale poorly and optimal solutions become harder to find.

QUBO and specialized solvers, including quantum annealers, offer a promising means of automating network defense and solving difficult optimization problems efficiently. Current research covers secure routing, attack-chain reconstruction, honeypot deployment, firewall configuration, and optimal sensor placement. Because QUBOs can be processed by both classical and quantum solvers, classical, quantum, and hybrid implementations are possible.

Routing in secure communication networks requires minimum-risk paths that avoid compromised nodes and congested links while satisfying Quality of Service (QoS) constraints. The problem is particularly difficult in wireless sensor and ad-hoc networks, where energy efficiency, reliability, and security must be considered simultaneously.

Study [Chen et al., 2022] proposes a QUBO for energy-efficient routing in Wireless Sensor Networks (WSNs) and implements it on physical D-Wave 2000Q and Advantage annealers. Each candidate route is represented by a binary variable, and the objective incorporates total network energy consumption and routing constraints. On small networks, the D-Wave processors found optimal or near-optimal routes faster than classical optimization solvers.

Although hardware capabilities limited the network sizes, the results demonstrate the potential of quantum annealing to accelerate route optimization. QUBO can naturally incorporate both energy and security criteria, for example by assigning higher costs to routes through vulnerable or unreliable nodes.

Reconstructing attack paths is another important and computationally demanding network-security problem. When an intrusion is detected, the propagation route of malicious traffic from its source to the target must be determined. Classical traffic analysis often incurs high computational load and processing delays, especially in distributed networks.

In [Antwi et al., 2025], QUBO is applied to attack traceback in WSNs. The implementation combines ns-3 network simulation with physical quantum annealing on D-Wave. The optimization

problem is formulated as:

$$\min_x \sum_{i,j} c_{i,j} x_{i,j} + \lambda \sum_{i,j,k} (x_{i,j} + x_{j,k} - x_{i,k})^2,$$

where $c_{i,j}$ is a link weight or transmission delay between nodes i and j, and λ penalizes violations of path transitivity. Experiments used a D-Wave quantum annealer together with the ns-3 simulation environment. Binary variables $x_{i,j}$ encode hypotheses about packet transfers, and the minimum-energy configuration represents the most likely attack path.

The experiments report substantially better route reconstruction, with accuracy near 90 %, exceeding classical methods. The false-positive rate decreased by 5–10 % while latency and energy consumption remained comparable. These results highlight the practical potential of quantum optimization for network-security analysis.

Optimal honeypot placement is another important network-security problem. Honeypots attract and analyze attacks without exposing real services. Choosing their number and locations requires maximizing the probability that attacks encounter a trap while minimizing deployment cost and avoiding network overload from excessive decoys. In general, a subset of network nodes must be selected as traps while accounting for intersecting attack paths.

The authors of [Ngo et al., 2023] show that optimal network honeypot placement is NP-hard even for static graphs. The study is used here as an applied formulation and theoretical justification of complexity; it does not run a QUBO on a QPU. It nevertheless notes that small instances can be addressed efficiently as QUBOs using quantum optimization solvers.

To our knowledge, no comprehensive study has yet applied QUBO directly to honeypot-placement optimization. Nevertheless, a suitable QUBO can be constructed as follows. Represent the network as a graph and assign each node a binary variable equal to 1 when a honeypot is placed there and 0 otherwise. The objective can be designed so that its minimum maximizes intersections between possible attack paths and honeypot nodes. Each potential attack contributes to the energy according to whether its path crosses at least one trap. This reduces to maximum subgraph coverage or dominating-set problems with known QUBO formulations.

Network infrastructures are also dynamic. As topology changes over time, honeypot-placement strategies must adapt. Manual management requires continuous monitoring and redesign after every topology change, which is labor intensive and poorly scalable.

Quantum or hybrid solvers could automate placement and reoptimize almost in real time as the network graph changes. This would enable an active defense layer that adapts dynamically to infrastructure state and evolving threats.

Another important class of network-security problems concerns network segmentation and firewall optimization. Effective segmentation — dividing infrastructure into isolated zones or communities with restricted interaction — is a key defense against lateral movement. Lateral movement refers to the spread of malicious actors through an internal network after the initial compromise.

Similarly, firewall-rule optimization involves selecting, configuring, and ordering access-control policies so that malicious traffic is blocked while legitimate traffic continues to flow. Both problems can be expressed as combinatorial optimization over graphs or sets, making them natural candidates for QUBO modeling.

Segmentation can be formalized as graph partitioning or clustering. The goal is to divide a network graph into segment subgraphs while minimizing security-critical intersegment connections and satisfying constraints such as segment size or permitted interactions. Graph partitioning is a classical NP-hard problem with a natural QUBO formulation. Quantum annealers have already been applied to related problems, including community detection in complex networks.

Study [Negre et al., 2020] demonstrates an Ising-model approach to graph community detection using a D-Wave quantum annealer. Small problems are run physically on D-Wave 2X/2000Q systems, whereas larger graphs use hybrid decomposition through qbsolv and D-Wave Ocean tools. Communities are clusters of nodes with dense internal connections and comparatively sparse external links. The authors show that detecting at most two communities maps naturally to the D-Wave architecture and requires little additional reformulation.

For small graphs, the quantum-annealing solutions matched those of classical clustering algorithms. The study illustrates quantum annealing's ability to solve basic graph-partitioning problems and therefore supports its potential for security-oriented network segmentation.

Consider a QUBO for partitioning a network into clusters A and B. Each node is assigned a binary variable indicating its segment. Quadratic objective terms penalize graph edges cut between the segments. The objective is to find a bipartition with the fewest intersegment links. Minimizing the QUBO energy therefore implements a minimum graph cut.

Additional terms can balance the segments or enforce size and capacity constraints by penalizing excessively uneven partitions. This formulation is structurally equivalent to image-segmentation models already implemented on quantum annealers [Venkatesh et al., 2024]. Although that study is not about network security, it provides a relevant example of quantum-annealed QUBO graph partitioning. The methodological foundation for quantum-assisted network segmentation therefore already exists.

Quantum or hybrid solvers can search an exponentially large space of network segmentations for partitions that best contain threats while satisfying business constraints. For example, high-risk nodes could be isolated in a dedicated quarantine segment.

For clarity, consider the analogy with image segmentation [Venkatesh et al., 2024]; this is a transferable methodological analog, not a direct computer-network experiment. Each pixel is treated as a graph node, and edges measure pixel similarity. Similarity is commonly evaluated with a Gaussian metric:

$$w'(p_i, p_j) = 1 - \exp\left(-\frac{(I(p_i) - I(p_j))^2}{2\sigma^2}\right), \tag{18}$$

where p_i and p_j are image pixels, $I(p_i)$ and $I(p_j)$ are their respective intensities, and σ is a hyperparameter controlling the metric's sensitivity scale. The values of w' lie in [0, 1]. They are

then normalized to $[-1, 1]$ as follows:

$$w(p_i, p_j) = -1 \cdot \left(\frac{(b-a)(w'(p_i, p_j) - \min(w'))}{\max(w') - \min(w')} + a \right), \tag{19}$$

where $a = -1$ and $b = 1$ define the normalization bounds, and $\max(w')$ and $\min(w')$ are the maximum and minimum over all pixel pairs.

Using expressions (18) and (19), the QUBO becomes:

$$\mathbf{x}^* = \arg\min_{\mathbf{x}} \sum_{1 \leqslant i < j \leqslant n} x_{p_i} \left(1 - x_{p_j}\right) w(p_i, p_j), \tag{20}$$

where $\mathbf{x} = \left(x_{p_1}, x_{p_2}, \ldots, x_{p_n}\right)$, and $x_{p_i} \in \{0, 1\}$ indicates the segment assigned to pixel p_i.

The reported experiments show an advantage for quantum optimization over leading classical algorithms on large-scale image segmentation. The authors [Venkatesh et al., 2024] also report particularly strong performance on noisy images, although transferring that result to network data requires separate validation.

Firewall-rule configuration is another important network-security problem with several possible formulations. Key subproblems include finding the smallest rule set that provides the required protection and ordering rules to minimize traffic-processing time. Rule-set minimization can be reduced to minimum set cover, while rule ordering can be treated as a scheduling or sequencing problem.

Because these optimization problems are generally NP-hard, they admit natural QUBO formulations and may benefit from quantum optimization. To our knowledge, no dedicated study had applied quantum optimization to firewall configuration at the time of this review. Given successful QUBO applications in adjacent areas, future work can reasonably be expected to automate network-security policy configuration, particularly as enterprise networks become more complex and defense systems more autonomous.

Both network segmentation and firewall configuration can therefore be formulated naturally as QUBOs. Early results in adjacent fields demonstrate that quantum hardware can solve small optimization instances effectively. The potential security benefit is substantial: optimized segmentation could isolate compromised regions dynamically with minimal operational impact, while optimized firewall rules could shorten exposure windows and reduce traffic-processing latency.

In secure environments such as enterprise IT and critical information infrastructure, sensors — including Intrusion Detection Systems (IDS) and monitoring probes — are essential for early threat detection. The objective is to place a limited number of sensors so as to maximize coverage of critical assets and key data routes. This is another combinatorial problem: an optimal subset of k locations must be selected from candidate network nodes or links.

Formally, these problems often reduce to variants of set cover or facility location. Although NP-hard, they admit QUBO formulations solvable by classical or quantum optimizers, including quantum annealers.

Quantum annealing and hybrid quantum – classical methods have been applied successfully to sensor placement. Study [Speziali et al., 2021], conducted by *Idea-re S.r.l.*, considers optimal pressure-sensor placement in a water-distribution network. It is a hybrid implementation comparing classical simulated annealing with the D-Wave hybrid quantum – classical solver on a QUBO formulation. This comparison separates the effect of the formulation from that of the solver architecture.

The objective was timely detection and localization of leaks and infrastructure failures. The authors construct a QUBO from the network graph and specified adverse scenarios, with the objective minimum corresponding to the optimal monitoring-sensor locations. They solve it using both classical simulated annealing and the D-Wave hybrid solver. The hybrid approach performed best on this practical water-network optimization problem.

The QUBO Hamiltonian minimum identified sensor configurations that optimized event detection and localization. The methodology transfers naturally to cybersecurity by replacing pressure sensors and pipeline leaks with IDS sensors and cyberattacks. Network topology and possible attack-propagation paths then determine the QUBO structure, while node-criticality weights can prioritize the protection of high-value assets.

Having considered specific defensive mechanisms, we now turn to the broader problem of resource allocation and cyber-defense optimization. Modern enterprise security requires efficient allocation of limited resources, including honeypots, monitoring sensors, access controls, and optimized network-security rule sets.

Choosing which vulnerabilities to remediate, where and in what order to deploy defenses, and which infrastructure elements to monitor with what priority is a difficult combinatorial problem. Modern adversaries often use multistage strategies that exploit several vulnerabilities in sequence. This sequence is commonly described by the **cyber kill chain** concept.

Defenders must therefore select measures that break every critical attack path at minimum resource cost. Formally, finding the optimal defense is NP-hard and resembles set cover or vertex cover on an attack graph.

Classical approaches such as integer linear programming and game-theoretic models perform well on small and medium-sized networks; heuristics provide an alternative. Study [Durkota et al., 2019], for example, uses Stackelberg games and dynamic programming to place defensive traps optimally on an attack graph. It is a classical baseline without QUBO or quantum hardware, included for comparison with potential QUBO approaches to defensive-resource placement. Such solutions scale poorly because computational complexity grows exponentially with network size.

Study [Carney, 2022] formulates disruption of attack chains in a vulnerability graph as a QUBO and implements it using quantum annealing. The applied formulation is run on a physical D-Wave

Advantage Solver 4.1 and compared with a classical ExactSolver on model graphs. Although no journal version was identified, the study is retained because it unusually connects the kill-chain model, vulnerability graphs, and a QUBO formalization of defensive actions. The objective minimum maximizes the number of disrupted attack chains subject to limited vulnerability-remediation resources.

Study [Marini, Arpe, 2025] develops a rigorous cyber-risk QUBO combining local node-risk factors with penalties for risk coupling and threat propagation through the infrastructure. It compares classical, quantum, and hybrid solvers, so its conclusions concern the complete workflow rather than only physical quantum annealing. The study is included because the problem is novel and the reproducible model represents cyber risk through local node properties, network links, and threat-propagation constraints. The system Hamiltonian is a linear combination of subproblem Hamiltonians:

$$H = \lambda_1 H_1 + \lambda_2 H_2 + \lambda_3 H_3 + \lambda_4 H_4 + \lambda_5 H_5, \tag{21}$$

where each H_k represents a particular risk type, and the coefficients λ_k specify the relative importance of the corresponding factors and serve as tunable model hyperparameters. The authors then analyze how each Hamiltonian component contributes to the final risk score.

The first Hamiltonian, H_1, keeps final node-risk levels close to their initial values. It prevents collective drift toward average risk and makes large reductions less likely for nodes with high initial risk:

$$H_1 = \sum_i IS_i \cdot (IS_i - FS_i)^2,$$

where IS_i and FS_i are the initial and final risk levels of node i, respectively.

The second Hamiltonian, H_2, penalizes configurations in which highly connected nodes retain high risk because such nodes can accelerate threat propagation:

$$H_2 = \sum_{i<j} S_{i,j} \cdot FS_i \cdot FS_j,$$

where $S_{i,j}$ is the connection strength between nodes i and j, and FS_i and FS_j are their final risk levels.

The third Hamiltonian, H_3, models the influence of neighboring nodes on each network element's risk:

$$H_3 = \sum_i \left(FS_i - \frac{1}{|N(i)|} \sum_{j \in N(i)} FS_j \right)^2,$$

where $N(i)$ is the set of nodes adjacent to node i, and $|N(i)|$ is its cardinality.

The fourth Hamiltonian, H_4, penalizes connections between nodes exhibiting critical-vulnerability indicators because such configurations can accelerate system-wide compromise:

$$H_4 = -\sum_{i<j} \left(f_i^{\text{patched}} + f_i^{\text{internet}} + f_j^{\text{patched}} + f_j^{\text{internet}} \right) (FS_i + FS_j),$$

where $f_i^{\text{patched}} = 0$ means that node i has been patched and is therefore less vulnerable, while $f_i^{\text{internet}} = = 1$ indicates Internet access.

The fifth and final Hamiltonian, H_5, isolates and strongly penalizes risk reductions for critical nodes ($IS_i \geqslant 7$), since such infrastructure elements generally remain highly vulnerable even when surrounded by low-risk nodes:

$$H_5 = - \sum_{i:\, IS_i \geqslant 7} FS_i.$$

The authors solve the problem using classical optimization, particularly tabu search, as well as quantum annealing and hybrid quantum – classical approaches. They identify the model's flexibility as a key advantage because every objective component is readily modifiable. The algorithm can therefore be adapted to different network configurations and cyber-risk scenarios.

The authors [Marini, Arpe, 2025] also note that classical algorithms perform well on small problems, but solution time grows exponentially with network size and sharply limits practical use. Quantum algorithms theoretically offer a more scalable approach. Current quantum hardware remains constrained, however, and substantial computation is spent preprocessing QUBOs for embedding, especially when interaction matrices are dense.

Hybrid quantum – classical algorithms mitigate the difficulty of placing a complete QUBO matrix on a quantum device by distributing the workload between classical and quantum components. This approach provides more stable scaling and high-quality solutions in practical scenarios.

Table 3 compares the reviewed network-security studies and methodologically related graph problems. It reports QUBO dimension and structural complexity, solver type, and whether a physical quantum run was performed. This distinction is important because some studies report direct annealer experiments, others use hybrid or classical computation, and honeypot-placement and attack-graph game studies are included only as classical comparison models.

Table 3 shows that confirmed physical experiments in this group rely mainly on D-Wave quantum annealers; the reviewed studies use neither gate-based quantum computers nor bifurcation solvers. Direct runs are limited to small or sparse QUBOs, while increasing variable counts and coupling density leads to decomposition, classical solution, or managed hybrid services. Results for community detection, image segmentation, and sensor placement should be interpreted as transferable graph analogues rather than direct computer-network defense experiments.

Conclusion

This review shows that quantum optimization, and Quadratic Unconstrained Binary Optimization (QUBO) in particular, provides a general computational foundation for a broad class of cybersecurity problems. By expressing cryptanalysis, anomaly detection, network segmentation, defensive-resource placement, and cyber-risk management as unified optimization models, QUBO enables quantum devices and high-performance classical and hybrid solvers to operate within a common methodology.

Table 3. Comparison of QUBO approaches and related models in network security

Study	Problem and model	QUBO dimension / complexity	QPU/solver type: annealer, computer, bifurcation	Physical quantum device
[Chen et al., 2022]	Energy-efficient WSN routing; one path selected per flow	Variable count depends on candidate paths and slack variables; graphs contain 4–12 nodes and up to 11 sources. Most successful direct runs had fewer than 20 variables; reduced dense instances reached the low hundreds	Physical D-Wave 2000Q and Advantage System 1.1 annealers; classical CPLEX and Gurobi; no bifurcation solver	Yes; D-Wave 2000Q and Advantage
[Antwi et al., 2025]	IP traceback in a WSN; one binary variable per candidate directed edge	$\|E\|$ logical variables, up to $O\left(\|V\|^2\right)$ in a dense directed graph; a 100-node network was modeled. Exact logical- and physical-qubit counts are not reported	D-Wave Advantage annealer for small instances; D-Wave hybrid and classical `qbsolv` for large instances; no bifurcation solver	Yes for small instances; larger ones solved hybrid / classically
[Ngo et al., 2023]	Honeypot placement in dynamic Active Directory graphs; MIP, not QUBO	No QUBO; the static problem is NP-hard. For m graph snapshots with n nodes, the MIP has $O(mn)$ variables; instances include thousands of nodes, hundreds of thousands of edges, and millions of paths	Classical MIP, dynamic programming, and greedy methods; no QPU, annealer, or bifurcation solver	No; classical baseline
[Negre et al., 2020]	Community detection by modularity maximization; network-segmentation analog	Two communities require n variables; k communities require nk one-hot variables with dense couplings inside k blocks. Tests use 34–453 nodes and up to 2265 variables; complete direct embedding is limited to 46/64 variables	Physical D-Wave 2X and 2000Q annealers; hybrid `qbsolv` and classical simulated annealing; no bifurcation solver	Yes for subproblems and small instances; large instances decomposed
[Venkatesh et al., 2024]	Minimum graph cut for image segmentation; transferable network-segmentation analog	n variables and $O(n)$ couplings for a grid of maximum degree four; solution space 2^n, and general signed-weight minimum cut is NP-hard. Experiments use 4–1936 variables; real images use 1024-variable patches	Physical D-Wave Advantage annealer (5670 qubits); classical Gurobi; no bifurcation solver	Yes; real D-Wave, but not a direct cybersecurity problem
[Speziali et al., 2021]	Sensor placement as capacity-constrained weighted vertex cover	1368 variables for $s = 48$, or up to 1416 with one-hot variables; penalty $\left(\sum_i x_i - s\right)^2$ makes the QUBO dense. Direct Chimera/Pegasus embedding was impossible	D-Wave Leap Hybrid Solver and classical simulated annealing; no direct QPU or bifurcation solver	No; managed hybrid solver only
[Durkota et al., 2019]	Network defense as a game on an attack graph; classical comparison model, not QUBO	No QUBO dimension; attack-graph optimization uses Stackelberg games and dynamic programming	Classical computer; no QPU, annealer, or bifurcation solver	No; classical baseline
[Carney, 2022]	Kill-chain disruption on a vulnerability graph; defensive-action QUBO	QUBO dimension is not reported in the available comparison; solutions were tested on model graphs	Physical D-Wave Advantage Solver 4.1; classical ExactSolver; no bifurcation solver	Yes; D-Wave Advantage 4.1
[Marini, Arpe, 2025]	Cyber-risk scoring from local factors and inter-node links	Exact QUBO dimension is undetermined: the supplied source PDF does not match the bibliographic record and instead contains the Speziali et al. sensor-placement paper	The text claims comparison of classical tabu search, quantum annealing, and a hybrid solver; no bifurcation solver	Not confirmed from the supplied source

The literature indicates that quantum algorithms, especially quantum annealing and adiabatic-evolution methods, can improve solution quality and accelerate the search for optimal configurations in small and medium-sized problems. Current quantum hardware nevertheless severely restricts practical application to full-scale cybersecurity. The principal barriers are limited qubit counts, noise, difficult embedding of dense QUBO matrices, and substantial preprocessing overhead.

Hybrid quantum – classical approaches therefore offer the greatest practical potential by combining classical computing power with the heuristic advantages of quantum optimizers. They already provide greater scalability and solution robustness, forming a realistic path toward quantum optimization in applied cybersecurity systems. Quantum-inspired algorithms further bridge theory and practice by solving QUBOs effectively without physical quantum hardware.

QUBO's flexibility is especially important because domain knowledge, constraints, and priorities can be incorporated directly into the objective. Security models can consequently adapt dynamically to changing infrastructure, threats, and business requirements, potentially operating near real time. QUBO is therefore not merely a quantum-optimization technique but also a general language for formalizing complex cyber-defense systems.

Although quantum cryptanalysis attracts substantial interest, network-configuration optimization, defensive-resource allocation, cyber-risk management, and anomaly detection are equally promising. These areas remain less studied but have considerable practical potential. Many also have direct analogues in logistics, infrastructure management, and complex-network analysis, enabling existing QUBO models and optimization strategies to be transferred.

Key future directions include general QUBO frameworks for classes of security problems, improved decomposition and sparsification, and algorithms for efficient embedding on quantum architectures. Progress in these areas will reduce computational overhead and broaden the applicability of quantum optimization to real systems.

Overall, QUBO-based quantum optimization is already laying the foundation for a new generation of intelligent cybersecurity systems. Despite hardware limitations, quantum, quantum-inspired, and hybrid methods show steady progress and practical value. As quantum technology develops, QUBO can be expected to become an important tool for automated, scalable, and adaptive security management in increasingly complex digital ecosystems.

References

Albash T., Lidar D. A. Adiabatic Quantum Computation // Reviews of Modern Physics. — 2018. — Vol. 90, No. 1. — P. 015002. — DOI: 10.1103/RevModPhys.90.015002

Antwi M., Osei-Wusu F., Asiedu W., Barfi M., Atuahene W. A., Muntaka S. A. A quantum annealing-based approach for IP traceback in WSNs // Journal of Electrical Systems and Information Technology. — 2025. — Vol. 12. — Art. 85. — DOI: 10.1186/s43067-025-00279-w

Barahona F. On the computational complexity of Ising spin glass models // Journal of Physics A: Mathematical and General. — 1982. — Vol. 15, No. 10. — P. 3241–3253.

Boros E., Gruber A. On quadratization of pseudo-Boolean functions // International Symposium on Artificial Intelligence and Mathematics (ISAIM). — 2012.

Burek E. Converting of Simon cipher multivariate polynomial equations to QUBO problem // Tatra Mountains Mathematical Publications. — 2025. — Vol. 91, No. 3. — P. 23–50. — DOI: 10.2478/tmmp-2025-0006

Burek E., Wroński M. Quantum annealing and algebraic attack on speck cipher // Proceedings of ICCS 2022. — Lecture Notes in Computer Science (LNCS). — Springer, 2022. — Vol. 13353. — P. 130–143. — DOI: 10.1007/978-3-031-08760-8_12

Burek E., Wroński M. J., Mańk K., Misztal M. Algebraic attacks on block ciphers using quantum annealing // IEEE Transactions on Emerging Topics in Computing. — 2022. — Vol. 10, No. 2. — P. 678–689. — DOI: 10.1109/TETC.2022.3143152

Canonici E., Caruso F. QUBO-based SVM for credit card fraud detection on a real QPU // arXiv preprint. — 2024. — arXiv:2409.11876 [quant-ph]

Carney M. Cutting medusa's path — tackling kill-chains with quantum computing // arXiv preprint. — 2022. — arXiv:2211.13740 [quant-ph]

Chen J., Date P., Chancellor N., Atiquzzaman M., Sreenan C. Controller-based energy-aware wireless sensor network routing using quantum algorithms // IEEE Transactions on Quantum Engineering. — 2022. — Vol. 3. — Art. 3102912. — P. 1–12. — DOI: 10.1109/TQE.2022.3217297.

Dennard R. H., Gaensslen F. H., Yu H.-N., Rideout V. L., Bassous E., LeBlanc A. R. Design of ion-implanted MOSFET's with very small physical dimensions // IEEE Journal of Solid-State Circuits. — 1974. — Vol. 9, No. 5. — P. 256–268. — DOI: 10.1109/JSSC.1974.1050511

Ding J., Spallitta G., Sebastiani R. Effective prime factorization via quantum annealing by modular locally-structured embedding // Scientific Reports. — 2024. — Vol. 14. — P. 3518. — DOI: 10.1038/s41598-024-53708-7

Ding J., Spallitta G., Sebastiani R. Experimenting with D-Wave quantum annealers on prime factorization problems // Frontiers in Computer Science. — 2024. — Vol. 6. — P. 1335369. — DOI: 10.3389/fcomp.2024.1335369

Dixit V., Selvarajan R., Aldwairi T., Koshka Y., Novotny M. A., Humble T. S., Alam M. A., Kais S. Training a quantum annealing based restricted Boltzmann machine on cybersecurity data // IEEE Transactions on Emerging Topics in Computational Intelligence. — 2021. — Vol. 6. — P. 417–428.

Dridi R., Alghassi H. Prime factorization using quantum annealing and computational algebraic geometry // Scientific Reports. — 2017. — Vol. 7. — P. 43048. — DOI: 10.1038/srep43048

Durkota K., Lisý V., Bosanský B., Kiekintveld C., Pechouček M. Hardening networks against strategic attackers using attack graph games // Computers & Security. — 2019. — Vol. 87. — P. 101578. — DOI: 10.1016/j.cose.2019.101578

Farhi E., Goldstone J., Gutmann S., Lapan J., Lundgren A., Preda D. A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem // Science. — 2001. — Vol. 292, No. 5516. — P. 472–475. — DOI: 10.1126/science.1057726

Farhi E., Goldstone J., Gutmann S., Sipser M. Quantum computation by adiabatic evolution // arXiv preprint. — 2000. — arXiv:quant-ph/0001106

Geman S., Geman D. Stochastic relaxation, Gibbs distributions, and the Bayesian restoration of images // IEEE Transactions on Pattern Analysis and Machine Intelligence. — 1984. — Vol. 6, No. 6. — P. 721–741. — DOI: 10.1109/TPAMI.1984.4767596

Goto H. Bifurcation-based adiabatic quantum computation with a nonlinear oscillator network // Scientific Reports. — 2016. — Vol. 6. — P. 21686. — DOI: 10.1038/srep21686

Goto H. Quantum computation based on quantum adiabatic bifurcations of Kerr-nonlinear parametric oscillators // Journal of the Physical Society of Japan. — 2019. — Vol. 88. — P. 061015. — DOI: 10.7566/JPSJ.88.061015

Grover L. K. Quantum mechanics helps in searching for a needle in a haystack // Physical Review Letters. — 1997. — Vol. 79, No. 2. — P. 325–328. — DOI: 10.1103/PhysRevLett.79.325

Ising E. Beitrag zur theorie des ferromagnetismus // Zeitschrift für Physik. — 1925. — Vol. 31. — P. 253–258.

Jiang S., Britt K. A., McCaskey A. J., Humble T. S., Kais S. Quantum annealing for prime factorization // Scientific Reports. — 2018. — Vol. 8. — P. 17667. — DOI: 10.1038/s41598-018-36058-z

Johnson M. W., Amin M. H. S., Gildert S., Lanting T., Hamze F., Dickson N., Harris R., Berkley A. J., Bunyk P., Chapple E. M., Enderud C., Hilton J. P., Karimi K., Ladizinsky E., Ladizinsky N., Oh T., Perminov I., Rich C., Thom M. C., Tolkacheva E., Uchaikin S., Wang J., Wilson B., Rose G. Quantum annealing with manufactured spins // Nature. — 2011. — Vol. 473. — P. 194–198. — DOI: 10.1038/nature10012

Jun K., Lee H. HUBO and QUBO models for prime factorization // Scientific Reports. — 2023. — Vol. 13. — P. 10080. — DOI: 10.1038/s41598-023-36813-x

Kadowaki T., Nishimori H. Quantum annealing in the transverse Ising model // Physical Review E. — 1998. — Vol. 58, No. 5. — P. 5355–5363. — DOI: 10.1103/PhysRevE.58.5355

Kirkpatrick S., Gelatt C. D., Vecchi M. P. Optimization by simulated annealing // Science. — 1983. — Vol. 220, No. 4598. — P. 671–680.

Li Y., Ma R., Jiao R. A hybrid malicious code detection method based on deep learning // International Journal of Security and Its Applications. — 2015. — Vol. 9, No. 5. — P. 205–216. — DOI: 10.14257/ijsia.2015.9.5.21

Lucas A. Ising formulations of many NP problems // Frontiers in Physics. — 2014. — Vol. 2. — P. 5. — DOI: 10.3389/fphy.2014.00005

Marini R., Arpe R. Cyber risk scoring with QUBO: A quantum and hybrid benchmark study // arXiv preprint. — 2025. — arXiv:2512.18305 [quant-ph]

Mellaerts J. Quantum-inspired anomaly detection, a QUBO formulation // arXiv preprint. — 2023. — arXiv:2311.03227 [quant-ph]

Mirrahimi M., Leghtas Z., Albert V. V., Touzard S., Schoelkopf R. J., Jiang L., Devoret M. H. Dynamically protected cat-qubits: A new paradigm for universal quantum computation // New Journal of Physics. — 2014. — Vol. 16. — P. 045014. — DOI: 10.1088/1367-2630/16/4/045014

Moore G. E. Cramming more components onto integrated circuits // Electronics. — 1965. — Vol. 38, No. 8. — P. 114–117.

Moro L., Prati E. Anomaly detection speed-up by quantum restricted Boltzmann machines // Communications Physics. — 2023. — Vol. 6, No. 1. — P. 269. — DOI: 10.1038/s42005-023-01390-y

Mukherjee S., Chakrabarti B. K. Multivariable optimization: quantum annealing and computation // The European Physical Journal Special Topics. — 2015. — Vol. 224, No. 1. — P. 17–24. — DOI: 10.1140/epjst/e2015-02346-8

Negre C. F. A., Ushijima-Mwesigwa H., Mniszewski S. M. Detecting multiple communities using quantum annealing on the D-Wave system // PLOS ONE. — 2020. — Vol. 15, No. 2. — P. e0227538. — DOI: 10.1371/journal.pone.0227538

Ngo Q. H., Guo M., Nguyen H. Near optimal strategies for honeypots placement in dynamic and large active directory networks // Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2023), Poster Session / Innovative Applications Track. — 2023. — P. 2517–2519.

Pakhomchik A. I., Voloshinov V. V., Vinokur V. M., Lesovik G. B. Converting of Boolean expression to linear equations, inequalities and QUBO penalties for cryptanalysis // Algorithms. — 2022. — Vol. 15, No. 2. — P. 33. — DOI: 10.3390/a15020033

Phab L., Louise S., Sirdey R. First attempts at cryptanalyzing a (toy) block cipher by means of quantum optimization approaches // Journal of Computational Science. — 2023. — Vol. 69. — P. 102004. — DOI: 10.1016/j.jocs.2023.102004

Ryou A., Kim K., Jun K. Quantum prime factorization algorithms using binary carry propagation // arXiv preprint. — 2025. — arXiv:2506.16799 [quant-ph]

Salama M. A., Eid H. F., Ramadan R. A., Darwish A., Hassanien A. E. Hybrid intelligent intrusion detection scheme // Soft Computing in Industrial Applications / eds. A. Gaspar-Cunha, R. Takahashi, G. Schaefer, L. Costa. — Advances in Intelligent and Soft Computing. — Berlin, Heidelberg: Springer, 2011. — Vol. 96. — P. 293–303. — DOI: 10.1007/978-3-642-20505-7_26

Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring // Proceedings of the 35th Annual Symposium on Foundations of Computer Science (SFCS'94). — 1994. — P. 124–134. — DOI: 10.1109/SFCS.1994.365700

Speziali S., Bianchi F., Marini A., Menculini L., Proietti M., Termite L. F., Garinei A., Marconi M., Delogu A. Solving sensor placement problems in real water distribution networks using adiabatic quantum computation // Proceedings of the IEEE International Conference on

Quantum Computing and Engineering (QCE 2021). — IEEE, 2021. — P. 463–464. — DOI: 10.1109/QCE52317.2021.00079

Stein J., Schuman D., Benkard M., Holger T., Sajko W., Kölle M., Nüßlein J., Sünkel L., Salomon O., Linnhoff-Popien C. Exploring unsupervised anomaly detection with quantum Boltzmann machines in fraud detection // Proceedings of the 16th International Conference on Agents and Artificial Intelligence (ICAART 2024). — SCITEPRESS, 2024. — Vol. 2. — P. 177–185. — DOI: 10.5220/0012326100003636

Venkatesh S. M., Macaluso A., Nuske M., Klusch M., Dengel A. Q-Seg: quantum annealing-based unsupervised image segmentation // IEEE Computer Graphics and Applications. — 2024. — Vol. 44. — P. 27–39. — DOI: 10.1109/MCG.2024.3455012

Wroński M., Burek E., Leśniak M. (In)security of stream ciphers against quantum annealing attacks on the example of the Grain 128 and Grain 128a ciphers // IEEE Transactions on Emerging Topics in Computing. — 2025. — Vol. 13, No. 3. — P. 614–627. — DOI: 10.1109/TETC.2024.3474856

Zhang A., Feng X. Applications of quantum annealing in cryptography // arXiv preprint. — 2022. — arXiv:2211.10076