Version of Record: https://www.sciencedirect.com/science/article/pii/S0375960119311569
Manuscript_1df28285e1745800eb4b7ba890678a54

Quantum computing cryptography: Finding cryptographic Boolean functions with quantum annealing by a 2000 qubit D-wave Quantum Computer

Feng Hu,[1,2,*] Lucas Lamata,[3,4] Mikel Sanz,[4] Xi Chen,[4,5] Xingyuan Chen,[6] Chao Wang,[1,2,7,†] and Enrique Solano[4,8,9,‡]

[1]*China Key laboratory of Specialty Fiber Optics and Optical Access Networks, Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai Institute for Advanced Communication and Data Science, Shanghai University, Shanghai 200444, China*
[2]*State Key Laboratory of Cryptology, P. O. Box 5159, Beijing, 100878, China*
[3]*Departamento de Física Atómica, Molecular y Nuclear, Universidad de Sevilla, 41080, Sevilla, Spain*
[4]*Quantum Technologies for Information Science (QUTIS), Department of Physical Chemistry, University of the Basque Country UPV/EHU, Apartado 644, 48080 Bilbao, Spain*
[5]*Department of Physics, Shanghai University, 200444 Shanghai, China*
[6]*State Key Laboratory of Cryptology, 100094 Beijing, China*
[7]*Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen 518000, China*
[8]*IKERBASQUE, Basque Foundation for Science, María Díaz de Haro 3, 48013 Bilbao, Spain*
[9]*International Center of Quantum Artificial Intelligence for Science and Technology (QuArtist) and Department of Physics, Shanghai University, 200444 Shanghai, China*

As the building block in symmetric cryptography, designing Boolean functions satisfying multiple properties is an important problem in sequence ciphers, block ciphers, and hash functions. However, the search of n-variable Boolean functions fulfilling global cryptographic constraints is computationally hard due to the super-exponential size $\mathcal{O}(2^{2^n})$ of the space. Here, we introduce a codification of the cryptographically relevant constraints in the ground state of an Ising Hamiltonian, allowing us to naturally encode it in a quantum annealer, which seems to provide a quantum speedup. Additionally, we benchmark small n cases in a D-Wave machine, showing its capacity of devising cryptographic Boolean functions with certain relevant properties. We have complemented it with local search and chain repair to improve the D-Wave quantum annealer performance related to the low connectivity. This work shows how to codify super-exponential cryptographic problems into quantum annealers and paves the way for reaching quantum supremacy.

I. INTRODUCTION

Information security is of increasing concern involving in politics, military affairs, diplomacy, as well as in our daily life, where the security of communication systems plays a central role. Cryptography is important for the information security aiming at hiding the key information based on secure channels to defend from malicious parties.

The symmetric cryptosystem, including stream ciphers and block ciphers, is a typical way of implementing the encryption and decryption with the same key so that the high communication efficiency and security lead to wide applications in military defense, finance, and society. The performance of core cryptographic components that offer high security as the filter model, the combiner model, and S-box relies on the availability of Boolean functions [1]. In fact, different cryptographic attacks [2, 3] require different properties such as, e.g., nonlinearity, balancedness, and correlation immunity.

However, there is a tradeoff among different criteria and it remains a challenge to achieve the best tradeoff to date [4–6]. Resiliency and high nonlinearity are two important criteria proposed versus (fast) correlation attacks and best affine approximation (BAA) attacks [7]. The properties of low-order resilient Boolean functions with high nonlinearity are important in stream ciphers. Although there exist several ways to find low-resilient and highly nonlinear Boolean functions, they may be limited by the search procedure of classical computers and the given functions with certain desired properties [8–10].

Although the size of the 1-resilient Boolean function with high nonlinearity is exponentially smaller than 2^{2^n}, it is still difficult for classical computers in the sub-exponential space. It is necessary to find a new computing paradigm to explore the global properties of Boolean functions characterized in their exponential space.

Quantum annealing [11] is an interesting alternative, and if the annealing progresses is sufficiently slow, natural quantum properties as quantum fluctuations and quantum tunneling effects can provide a quantum speedup in theory, at least for specific cases. More precisely, from the perspective of statistical theory, quantum-inspired systems can show a higher probability potentially to find the global optimum of multi-dimensional functions and can be seen as a global searching algorithm as compared with classical ones.

Google, Microsoft, IBM and a host of labs and start-ups are on the verge of a quantum technology breakthrough [12–14]. Among them, D-Wave Systems, Inc. [15] is devoted to commercial quantum computing with prototypes based on the quantum annealing paradigm [16], and mainly aimed at three categories of software applications and algorithms: Monte Carlo simulations, optimization, and machine learning. These include, among others, pattern recognition and anomaly de-

* f.hu.121214@gmail.com
† wangchao@staff.shu.edu.cn
‡ enr.solano@gmail.com

© 2019 published by Elsevier. This manuscript is made available under the Elsevier user license
https://www.elsevier.com/open-access/userlicense/1.0/

tection, cyber security, image analysis, financial analysis, verification and validation [17–21]. Additionally, we should also pay attention to the potential applications on encryption and decryption [22–24].

Nevertheless, up to now applications of the cryptography design by means of quantum computing have not been found. It is of great interest to consider the quantum annealing paradigm for Boolean function design as a way forward to implement the key cryptographic components design. The core quantum model underlying state-of-the-art D-Wave quantum annealing devices is the transverse-field Ising model, a basic model for mapping optimization problems onto a physical quantum annealer.

In this article, we propose, analyze, and experimentally implement a quantum annealing algorithm to design even-variable Boolean functions for use in cryptography. To this aim, we utilize the quantum theory to map the problem of designing Boolean functions with several criteria into the ground states of an Ising Hamiltonian. We consider n to be even throughout the paper. Then, we obtain the Ising model ground states by quantum annealing experiments in the D-Wave cloud quantum computer, to illustrate a first demonstration of Boolean function design in a quantum computing way.

Up to now, no report has been produced on the cryptography designing and relevant issues by a quantum computer. First of all, the two typical applications of quantum computer reported earlier are the code-breaking technique and database searching method, both of which have nothing to do with the cryptography design. D-Wave Systems, Inc. realized a quantum annealing (QA) algorithm by using quantum tunneling effects, and this can be used to solve combinatorial optimization as well as some problems in the field of artificial intelligence. Moreover, even 2000-qubit problems were declared to be solved by D-wave 2X quantum computer. Up to now, however, none of the reports has announced to be able to handle the issues of cryptography designing. Thus, this article tries to apply the quantum annealing theory, based on quantum tunneling effects, to the cryptographic design and constructs the Boolean functions with multiple security criteria. This paper indicates the feasibility of applying D-Wave quantum computer to cryptography design. Finally, we have proposed that Quantum Computing Cryptography: A new age of critical applications of quantum computers, is coming.

This article considers the construction of Boolean functions with two important criteria, namely, nonlinearity and resiliency. We will consider the design problem as a search problem in an exponentially large solution space. All of our design procedures are based on the Walsh spectra to characterize the two criteria. Our research focuses on bent functions design and m-resilient functions design ($m \geq 1$) with high nonlinearity in small n cases.

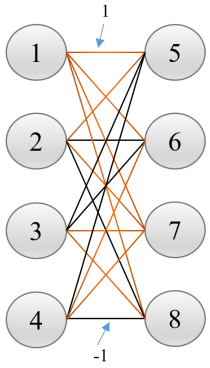

FIG. 1. Hardware architecture for designing 2-variable bent functions. Each circle i denotes the qubit σ_i and the lines between them give the strengths of the couplers between σ_i and σ_j. The red line implies the coupler strength to be 1 while the black to be -1.

II. BOOLEAN DESIGN SCHEME WITH A D-WAVE QUANTUM ANNEALER

A. Boolean functions

An n-variable Boolean function $f(x) \in \mathfrak{B}_n$ is defined as the function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ and is generally represented by its algebraic normal form,

$$f(x) = f(x_1, ..., x_n) = \bigoplus_{u \in \mathbb{F}_2^n} \lambda_u (\prod_{i=1}^{n} x_i^{u_i}), \tag{1}$$

where $\lambda_u \in \mathbb{F}_2$, $u = (u_1, ..., u_n) \in \mathbb{F}_2^n$, and the addition is denoted over $\mathbb{F}_2$.

Any $f(x)$ could also be given in another form of a truth table as $[f(0, .., 0), f(0, ..., 1), ..., f(1, ..., 1)]$. The truth table consists of 2^n outputs of $f(x) \in \{0, 1\}$, which is actually an exponential space with the size of 2^{2^n}.

The algebraic degree $\deg(f) < 2$ of $f(x)$ is denoted by $\max\{wt(u), \lambda_u \neq 0\}$, where $wt(u)$ is the Hamming weight of u. If $wt(f) = 2^{n-1}$, the function is balanced. The Boolean function with $\deg(f) < 2$, where $\deg(f)$ denotes the degree of f, is named "affine function". If the constant term equals to zero, it is called linear function, as below,

$$a \cdot x = a_1 x_1 \oplus a_2 x_2 \oplus ... \oplus a_n x_n \tag{2}$$

where $a = (a_1, a_2, ..., a_n)$, $x = (x_1, x_2..., x_n) \in \mathbb{F}_2^n$, and "$\cdot$" is the inner product of vectors a and x.

The Walsh spectrum is an important concept to characterize different criteria. For any $a \cdot x \in \mathbb{F}_2$, the Walsh transform is the real-valued function over $\mathbb{F}_2^n$ defined as,

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + a \cdot x} \tag{3}$$

In order to resist the best affine approximation [25] and fast correlation attacks [26], the Hamming distance, which is

characterized as the nonlinearity, to affine functions should be large enough. The nonlinearity of $f(x)$ is given by,

$$nl(f) = 2^{n-1} - \frac{1}{2} \cdot \max_{a \in \mathbb{F}_2^n} |W_f(a)| \tag{4}$$

Based on the Parseval's theorem [27], if n is even, $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$, and even-variable Boolean functions with the nonlinearity achieving the upper bound are called bent functions.

Another criterion called correlation immunity is employed to characterize the ability of Boolean functions to resist the correlation attacks. For any $1 \leq wt(a) \leq m$, if $W_f(a) = 0$, f is an m-order correlation-immunity function. And if f with m-th order of correlation immunity is balanced, then we call it m-resilient function.

Generally, there are three ways to build Boolean functions: algebraic constructions, random search, and heuristics (and their combinations) [28–31].

1) Algebraic constructions are provable in mathematics and can construct a class of Boolean functions with multiple criteria. Actually they are theoretically deterministic constructions to characterize a class of Boolean functions under specific conditions. Thus, they may result in certain classes of functions with similar properties, which are only a (small in most cases) subclass of functions relative to the size of 2^{2^n}. Furthermore, it is not easy to find a good construction that could achieve the tradeoff among many criteria.

2) Random search is a relatively fast method to obtain many Boolean functions. Due to the vast size of the search space, it is not a sufficient way to find functions with excellent properties.

3) The last method lies in the intermediate position between the algebraic construction and random search. It usually divides the two-stage optimization as primary construction and secondary construction, where the outputs of the former are sent to be the inputs of the latter. Algebraic construction and heuristic technologies can be either the first or the second optimization (even both). However, from the perspective of heuristics as the size scales up, it is likely to get trapped in a local optimum and fail in scanning the whole exponential space.

Briefly speaking, known methods are unavailable to evaluate the global properties of Boolean functions, while designing the Boolean functions satisfying multiple criteria in the exponential-solution space is challenging. From the point of view of classical computers, it is hard to complete the optimization in an exponential search space. Therefore, here we employ the Ising model, a widely used model in quantum annealing algorithms, to globally characterize the class of Boolean functions with certain properties and solve it by means of the cloud quantum computer provided by D-Wave.

B. Design procedure

An introduction to the design procedure is given below. However, there exist topological restrictions as shown in Fig. 2, given that, in the D-Wave device, any qubits in two neighboring unit cells could only directly connect to the nearest neighbour qubits vertically or horizontally. This limits the scalability for large-scale systems such that we also introduce chains constructed with multiple physical qubits for representing one logical qubit for further scalability.

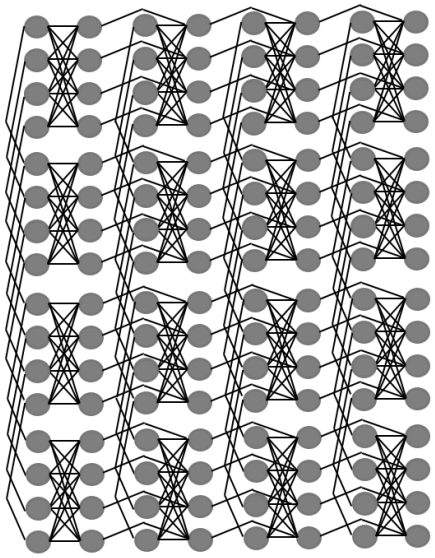

FIG. 2. Hardware architecture

D-Wave provides a cloud quantum computer platform for connecting to via a local classical computer. In this work, the first step to design cryptographic Boolean functions in a quantum computing fashion consists of three steps, namely, 1) Recast the objective function into a set of polynomial terms and map it to an Ising model. 2) Design the hardware graph to solve the Ising model in a D-Wave quantum device. 3) Perform the quantum annealing computation via D-Wave cloud quantum computer and retrieve the corresponding Boolean functions with applications in cryptography.

Actually, we should first analyze the basic criterion, nonlinearity, in a logical way. For illustrative purposes, the case of 2-variable Boolean functions is given. Based on the Walsh spectra transformation introduced in Ref. [1], the Walsh spectra may be given in terms of a generalized matrix operation on the variants of the truth table.

Assuming that the truth table is $[\lambda_1, \lambda_2, \lambda_3, \lambda_4]$, where $\lambda_u \in \{0, 1\}$, $u = 1, 2, 3, 4$, then a shift transformation $b_u = 1 - 2\lambda_u \in \{-1, 1\}$ maps the truth table onto $[b_1, b_2, b_3, b_4]$. Then, the Walsh spectrum can be given as,

$$W_f(b) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{bmatrix} = \begin{bmatrix} W_{f_1}(b) \\ W_{f_2}(b) \\ W_{f_3}(b) \\ W_{f_4}(b) \end{bmatrix} \tag{5}$$

Accordingly, the function is bent with the maximal nonlinearity if and only if $|W_{f_1}(b)| = |W_{f_2}(b)| = ... = |W_{f_{2^n}}(b)|$. This is, the nonlinearity can become maximal if and only if all the absolute values of the Walsh spectrum are the same.

In other words, the more uniform the absolute value of the Walsh spectrum, the higher the nonlinearity of the functions. Then, one can construct the Ising model for 2-variable bent functions in one unit cell as shown in Figure 1 based on the Hamiltonian as below,

$$H_{\text{non}} = \sigma_5(\sigma_1 + \sigma_2 + \sigma_3 + \sigma_4) + \sigma_6(\sigma_1 - \sigma_2 + \sigma_3 - \sigma_4) + \sigma_7(\sigma_1 + \sigma_2 - \sigma_3 - \sigma_4) + \sigma_8(\sigma_1 - \sigma_2 - \sigma_3 + \sigma_4). \tag{6}$$

Based on the scalable structure given in Step 2, we employed the API provided by D-Wave to deliver the coefficients defined in the Ising model to the cloud quantum platform and can retrieve 1000 readouts at most in seconds.

III. PRELIMINARY EXPERIMENTS AND ANALYSIS

Bent function (single criterion) design is a good benchmark choice as a step towards the goal of satisfying several appropriate criteria. In principle, the number of n-variable bent functions is exponential as shown in Table I [32].

TABLE I. n-variable Boolean functions

n	2	4	6	8
Boolean functions	2^4	2^{16}	2^{64}	2^{256}
bent functions	2^3	$\approx 2^{9.8}$	$\approx 2^{32.3}$	$\approx 2^{106.3}$
relative frequency	2^{-1}	$\approx 2^{-6.2}$	$\approx 2^{-31.7}$	$\approx 2^{-149.7}$

Based on the model constructed in Section II, it can be generalized to n-variable bent functions that need 2^{n+1} logical qubits represented by 2^{2n-1} physical qubits, where the topological limitation requires 2^{n-2} physical qubits to define a chain.

As an illustrative example with one unit cell consisting of eight working qubits, we obtain exactly eight bent functions out of 1, 000 readouts. We depict one of the cases in Fig. 3, for which the left part ($[1, -1, 1, 1]$) and right part ($[-1, -1, 1, -1]$) can be turned into two 2-variable bent functions as $[0, 1, 0, 0]$ and $[1, 1, 0, 1]$.

The cases of 4-variable and 6-variable bent functions are given in Section V. What should be pointed out is that there exist two types of couplers in these cases: 1) the couplers between different chains (denoted as coupler strength), and 2) the couplers within the chains (denoted as chain strength). With the comparison between the 4-variable case and 6-variable case, we find there exists a tradeoff between the coupler strength and the chain strength. Namely, the chains should be highly stable while the interactions between different chains should produce the optimal solutions.

As a consequence, we can find all the 4-variable bent functions, but can only find a reduced number of 6-variable bent functions due to several broken chains according to the considered regimes. Therefore, the quantum annealing protocol may end up with some suboptimal result.

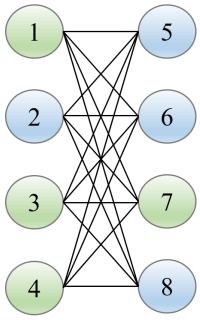

FIG. 3. One of the outcomes by the annealer on 2-variable bent case. If the green part represents state '1' and the blue part represents state '-1', it gives the corresponding truth table of the 2-variable Bent function in both sides. With more readouts from the machine, all the possible 2-variable bent functions can be obtained.

Increasing the annealing time would not always work for different scenarios and some optimizations should be introduced based on the properties of D-Wave machine(the annealing time is fixed to 20 μs). We find that an additional local search algorithm may be useful for enhancement of our protocol. Here, we employ a basic greedy search algorithm, hill-climbing, to improve the results of the quantum annealer.

- *Experiment 1: 6-variable bent functions*. In order to greatly utilize sub-optimal solutions, to select the ones with the nonlinearity more close to the maximum is important to achieve the tradeoff between the speed of postprocessing and the efficiency of the generation on bent functions. On the other hand, the readouts are given in order of increasing energies and in principle, the bent function is likely to occur with lower energy, such that applying the local search to the part of the results with lower energy can accelerate the design procedure.

Taking these two issues into account, Table II gives the number of distinct 6-variable bent functions out of 10 experiments. The coupler strength is fixed to 0.4 in order to maximize the performance to achieve the tradeoff between chain strength and coupler strength. The "readouts" column denotes the number of outputs once optimized by local search. The "optimized range" column denotes the nonlinearity of the suboptimal Boolean functions produced by the D-Wave machine before the second optimization by local search. The "numbers" column denotes the number of 6-variable bent functions obtained with the D-Wave quantum processor and local search out of ten experiments. It is intuitive that the local search can greatly improve the performance of the quantum device.

Furthermore, more readouts with the nonlinearity to be considered in the optimized range give more samples for the search and, accordingly, the system could obtain more bent functions. In other words, this indicates that the system can find many local points near to the optimal ones, while the classical one may get trapped in the local optimum, which is not a real bent function and can not be optimized directly by a local search.

- *Experiment 2: 4-variable m-resilient Boolean functions with high nonlinearity*. Due to the connectivity limit of the

TABLE II. 6-variable bent functions design

coupler strength	readouts	optimized range	numbers
0.4	50	27	134
0.4	50	26-27	296
0.4	50	25-27	664
0.4	100	27-28	208
0.4	100	26-27	354
0.4	100	25-27	864
0.4	200	27-28	218
0.4	200	26-27	558
0.4	200	25-27	1202

machine, we only consider the construction on 4-variable m-resilient Boolean functions with high nonlinearity. In theory, there is a tradeoff between the nonlinearity and resiliency order of a function [1].

Actually, the mapping of resiliency is a complete graph problem that cannot be directly merged into the nonlinearity. Although the number of logical qubits remains the same, the connectivity problem is more complicated such that the strength should be considered more carefully to ensure the stability of the chains. Relatively high coupler strength may lead to more broken chains and how to find the tradeoff between two different criteria should also be considered. Unfortunately, due to the complicated relationship between nonlinearity and resiliency, local search is unavailable in the case with several criteria.

To analyze it further, it is similar to add a new penalty term deduced by the truth table of the functions to the Ising model, which is a way to combine the nonlinearity and balancedness to characterize the final objective. We consider this according to the following four aspects: 1) The aim is to guarantee the function to be 1-resilient while maximizing the nonlinearity. 2) The working qubits for resiliency should relatively dominate the whole annealing procedure while the nonlinearity condition may also be fulfilled under the previous constraint. 3) Logically, normalization is necessary to balance the contributions of nonlinearity and resiliency to the objective functions. 4) Physically, the coupler strengths to stabilize the chains for different criteria should be considered separately. Thus, here we need another skill called chain repair to complete a majority vote to obtain the desired function.

As a result, all the 4-variable 1-resilient Boolean functions with nonlinearity 4 have been found. Additionally, we observe that the chain repair can improve a relatively frustrating condition in the sense that the criteria require the regulation as accurate as possible on the chain strength and coupler strength. Therefore, with the chain repair, the parameter range may enable that some errors are eliminated or ignored as an error correction technique. In other words, to guarantee certain objectives with high loss at the cost of others with low loss is necessary to design the Boolean function satisfying multiple criteria.

IV. TOPOLOGICAL RESTRICTION OF THE QUANTUM DEVICE

Figure 2 shows the partial $4 \times 4 \times 4$ chimera graph of the D-Wave 2000Q system ($16 \times 16 \times 4$) consisting of 4×4 unit cells including a 4×2 array. It intuitively illustrates the topological restrictions of the architecture, for which each qubit could only directly connect to the nearest neighbour qubits.

1) Given a single unit cell, it is divided into two parts: left and right. Each part contains 4 individual physical qubits without any connections while any two qubits in different parts can be connected with each other through the so-called couplers.

2) Different unit cells connect only in two ways: the left part within each block connects vertically with other blocks, while the right part does it horizontally.

Obviously, each physical qubit could connect up to other neighboring six physical qubits (four qubits within the unit cell and up to two qubits connecting to the neighbouring unit cell). Users could set the weight of single qubit and coupler strength between two connected qubits. However, in most cases it is not sufficient to solve a practical problem with such a limited connectivity, thus a chain consisting of multiple physical qubits is introduced to represent one logical qubit to expand the connectivity.

In this way, the limited hardware architecture can be generalized to the condition of n-variable Boolean function as n increases. Briefly, n-variable Boolean functions yield a $2^n \times 2^n$ coefficient matrix characterizing the Walsh spectra. For instance, the bent function requires in total $2^{n-2} \times 2^{n-2}$ unit cells and 2^{2n-1} physical qubits, which has been analyzed in the article.

V. ADDITIONAL EXPERIMENTS

As an extension of the previous constructions on the nonlinearity above, here we show how to implement the correlation immunity criterion, which is a similar model to the balancedness. With respect to the 2-variable Boolean function, the key is to find the corresponding coefficients if $m > 0$ where m is the total number of $'1'$ in the sequence ranging from $\{0, 0\}$ to $\{1, 1\}$, which is a one-to-one correspondence to the raw number. Thus, the cost function of 2-variable Boolean functions with the order of correlation immunity 1 is given by Eq. 7,

$$f_{\text{corr}} = (b_1 - b_2 + b_3 - b_4)^2 + (b_1 + b_2 - b_3 - b_4)^2 \quad (7)$$

If we add the term $(b_1+b_2+b_3+b_4)^2$ defining the balancedness, the resiliency criterion can be mapped into the Ising model as,

$$H_{\text{resi}} = \sigma_1\sigma_2 + \sigma_1\sigma_3 - \sigma_1\sigma_4 - \sigma_2\sigma_3 + \sigma_2\sigma_4 + \sigma_3\sigma_4 \quad (8)$$

Experiment 1: 2-variable bent functions A 2-variable bent function design can be regarded as a proof of principle to

check whether the protocol and device work as expected. The corresponding Hamiltonian reads,

$$H_{\text{non}} = \left(\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \\ \sigma_4 \end{bmatrix} \right)^T \cdot \begin{bmatrix} \sigma_5 \\ \sigma_6 \\ \sigma_7 \\ \sigma_8 \end{bmatrix} \quad (9)$$

Based on the Ising model as the input of D-Wave, we attain 1, 000 readouts, among which eight exactly distinct bent solutions are found.

Experiment 2: 4-variable bent functions

A more important issue is how to generalize the previous example to a high-variable case. Here, we denote the coefficient as A, and a new matrix, a 16×16 constant matrix, is easy to construct as,

$$H_{4-non} = \left(\begin{bmatrix} A & A & A & A \\ A & -A & A & -A \\ A & A & -A & -A \\ A & -A & -A & A \end{bmatrix} \begin{bmatrix} \sigma_1 \\ ... \\ ... \\ \sigma_{16} \end{bmatrix} \right)^T \cdot \begin{bmatrix} \sigma_{17} \\ ... \\ ... \\ \sigma_{32} \end{bmatrix} \quad (10)$$

It indicates that each logical qubit should interact with another 16 qubits. Thus, each chain indexing with the same color should be made up of 4 physical qubits to map the coefficients to the 4×4 arrays as in Fig 4.

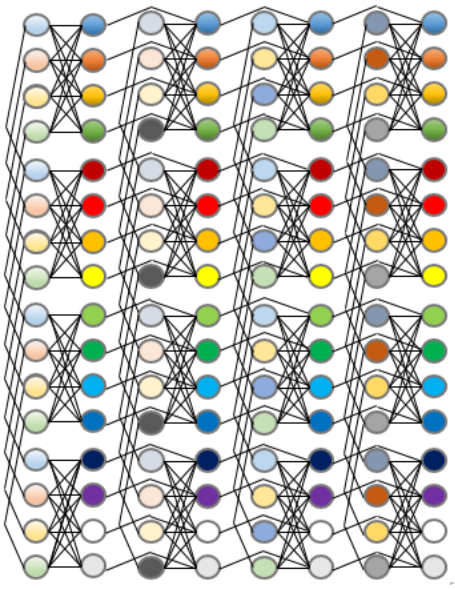

FIG. 4. The chain distributions for the 4-variable bent function design problem.

The most important point is that there are two types of couplers in this case: 1) the couplers between different chains (denoted as coupler strength), and 2) the couplers within the chains (denoted as chain strength).

In order to clarify how they work, we fix the chain strength to -1 while varying the coupler strength from 2 to 0.1. The results are given in the Table III. We read 1, 000 solutions, each of which contains eight functions, to explore how many bent functions the system could generate and give the average frequency out of 10 experiments.

TABLE III. The frequency of 4-variable bent functions

coupler strength	bent frequency (%)
2	25.76
1	45.80
0.5	50.21
0.25	95.86
0.1	25.32

Here bent frequency denotes the frequency of bent functions obtained in the whole solution space derived from the D-Wave quantum annealer. That is, if the frequency is 95.86%, it means the D-Wave machine can output about 96 bent functions out of 100 solutions. It also equals the success rate.

The exact number of 4-variable bent functions is 894, and there are many redundant ones. Thus, regardless of the randomness of the quantum platform, to improve the frequency can help us find more distinct bent functions. The table tells us that a suitable configuration could achieve a good performance. If the coupler strength is set to 0.25, all the results of the system are almost optimal with the same annealing time $20\mu s$, which is enough for the machine to find the majority of optimal solutions. To analyze it further, we point out:

1) Large coupler strength will break the default chains such that the results are not the theoretical optimum all the time.

2) Similarly, small coupler strength cannot guarantee the interactions between different chains dominating the quantum annealing procedure such that the results may be affected by the chain strength to give suboptimal outputs.

3) There exists a tradeoff between the coupler strength and the chain strength in the sense that the chains should be highly stable while the interactions between different chains do still work to achieve the optimal solutions.

4) When it comes to large-scale systems, it can be predicted that small biases in the logical term will lead to nontrivial errors in the hardware graph and it may not be well corrected only by selecting the suitable chain strengths in long chain cases. The device may not always work consistently with the theoretical design due to the connectivity limitation of the hardware architecture.

Experiment 3: 6-variable bent functions

As it comes to 6-variable case, it requires 2048 physical qubits representing 128 logical qubits, each of which is made up of 16 physical qubits as a chain, which is a more complicated condition compared with Exp. 2. By similar adjustments than with Exp. 2 on the device, we found it can hardly obtain 6-variable bent functions. In other words, too long and many chains will yield a significant amount of errors as compared with the 4-variable bent function design experiments. Although increasing the annealing time could find more optimal and suboptimal solutions, longer annealing times may be a trivial choice for optimization, and they also increase the risk of being affected by thermalization.

TABLE IV. Average number of 4-variable bent functions before and after local search out of 10 experiments

Coupler strength	Initialized	Optimized
1	85	164.8
0.5	283.6	663.8
0.25	812	814.6

On the other hand, the advantage is that the running time of the quantum annealing processor does not grow as we extend the 2-variable case to the 6-variable case, although the qubit resources grow exponentially. Therefore, if some basic post-processing technique could be introduced based on the properties of the quantum device, the performance will be better with the combination of the quantum annealing algorithm and classical algorithms.

VI. OPTIMIZATION

Section V provided the experimental results of designing n-variable bent functions ($n = 2, 4, 6$) by a quantum computer. Limited by the connectivity of the chimera graph, our protocol only works well on small cases (2 and 4-variable bent functions) and large case will cause many errors that could prevent obtaining suitable solutions. As a consequence, the chains are actually broken such that the qubits within the chain are not always aligned during the annealing. Here, we consider two improved strategies to optimize the results, based on the properties of the D-Wave quantum platform: 1) local search; 2) repairing the chain via majority vote [33].

As the evolutionary procedure of the quantum annealing is natural, each annealing procedure will give a number of optimal or suboptimal results including some identical ones. Accordingly, the most simple way is to execute a number of experiments initialized with the same configuration to generate many different bent functions. But this approach is highly time-consuming, while optimization on the suboptimal outcomes offers a new feasible path to achieve the optimal solutions.

The local search algorithm is a simple but effective way to use the approximately optimal outcomes to obtain more desired functions. This article only employs a basic hill-climbing algorithm, to verify the advantage of introducing local search methods. Hill-climbing is a greedy search algorithm and always aims at the better solutions with multiple iterations in its local search field. Therefore, it can work well in the case of optimizing one criterion.

Experiment 4: Employing local search to optimize 4-variable generation

Considering postprocessing, our objective becomes to obtain the suboptimal solutions via our original protocol and subsequently apply the hill-climbing algorithm to achieve the ones with the nonlinearity closer to the maximal nonlinearity. Additionally, this strategy can help to find more bent functions at once, to contribute to find all the 4-variable bent functions within several experiments.

As shown in Table IV, with a simple test based on the relatively suitable coupler strength for the 4-variable bent functions, local search gives a significant improvement on the relatively worse case and also slightly improves the better case. As a consequence, we could find all the 4-variable bent functions faster and it would also work in the more complicated case.

This means that the the device could provide suboptimal solutions near to the optimum within a few bit-flips, which may be more important in a large-scale system. Moreover, we also discuss in the article that the optimization procedure on the 6-variable bent functions can be significantly improved via a basic search algorithm.

Experiment 5: Balanced 4-variable Boolean functions

We consider now balancedness as a typical case of resiliency. Due to the connectivity limit of the chimera architecture, here we only analyze the design scheme of balanced 4-variable Boolean functions as the basis for further optimization on resiliency.

The mapping of balancedness is actually a complete graph problem that cannot be directly transformed from the nonlinearity. Thus, we need to introduce another 4×4 array to design the balancedness criterion.

In this case, the interactions between different qubits are more complicated than the case of optimizing the nonlinearity, for which each qubit should interact with another fifteen qubits. Here, we construct a symmetric structure consisting of sixteen chains, each of them containing eight physical qubits.

If the coupler strength is set to 0.25, i.e., a more suitable value for optimizing the nonlinearity, it seems unfeasible to achieve balanced ones. This is because the chains constructed for the balancedness criterion are longer than for the nonlinearity, such that the chains are more unstable and the coupler strength should be accordingly smaller. As the coupler strength decreases further, we could find many balanced functions.

The previous is an intermediate approach towards resiliency optimization due to the similar formalization of nonlinearity and resiliency. From the perspective of the Ising Hamiltonian, designing Boolean functions with several criteria seems that adding a penalty term to the initial Hamiltonian for improving one criterion requires more physical qubits although the number of logical ones remains the same.

Experiment 6: 4-variable m-resilient Boolean functions with high nonlinearity

We know that low-resilient functions must be balanced and Experiment 6 aims at combining all the penalty terms together to design the 4-variable m-resilient Boolean functions with the best known nonlinearity and in principle there are only 222 m-resilient functions in the solution space with the size of 2^{16}. However, Exp. 5 shows that different criteria require different coupler strengths. Moreover, the chains optimal for the resiliency criterion may be more easily broken than the ones optimized for nonlinearity.

Therefore, the best tradeoff may be achieved at the cost of more stable chains. We analyze the effects between the two criteria as shown in Table V based on the connectivity of nonlinearity and resiliency.

TABLE V. Average number of Boolean functions with m-th order of resiliency out of 10 experiments

strength (N)	strength (R)	Initialized	Optimized
0.25	0.125	104	113.2
0.5	0.125	28.4	32
0.125	0.125	150.8	157.6
0.05	0.125	191.6	196

Here, the first and second columns give the coupler strengths for the nonlinearity (N) and resiliency (R), respectively. The "Initialized" column gives the number of m-resilient Boolean functions given by the D-Wave device, and the "Optimized" column gives the number of m-resilient functions after repairing the chain via majority vote.

It seems the improvement is not significant, but what should be pointed out is that the initialized solutions are based on all the solutions included in the architecture, where each one could give at least nine outcomes considering there exist broken chains while the majority vote only gives one solution. Therefore, not only we can get more optimums, but also the sufficiency of postprocessing has been improved.

Because the length of chains for resiliency is double than for nonlinearity, the former two cases in Table V imply that the resiliency does not dominate the annealing procedure. Thus, when we fix the coupler strength of resiliency to a suitable value, as the coupler strength of nonlinearity increases, the number of m-resilient functions decreases. In the latter two cases, the couplers of resiliency dominate the annealing procedure while the other parts do still work such that the machine can output more desired solutions.

Moreover, the nonlinearity of 4-variable m-resilient functions (for $m > 1$) is 0, because the high resiliency order will limit the nonlinearity. The coupler strength in the last case is smaller than the third case, such that one may find more m-resilient functions and the condition for the nonlinearity will not work well. Thus, we point out that:

1) If the strength for the resiliency condition is too large relative to the nonlinearity condition, the mapping of the nonlinearity may not work well.

2) The resiliency and nonlinearity conditions limit each other and optimizing the relative strength may help to obtain desired functions with specific properties, e.g., 4-variable 1-resilient functions with high nonlinearity.

3) Although the small coupler strength may produce more errors, it can also be a good choice to find the functions with similar properties (like high resiliency order) as a consequence of the sub-optimal results. For example, in this case we have found all the 2-resilient and 3-resilient Boolean functions simultaneously.

In small cases, the errors may lead to a small part of nonaligned qubits in a chain, for which the majority vote can simply obtain the corrected state of the qubits. Certainly, this will not always work, especially for more complicated cases. Thus, the majority vote could improve the performance near the critical point corresponding to the case relatively worse to the best case. Moreover, how to select the suitable strength for majority vote is also important, as near the almost optimal boundary of the different criteria.

VII. SCALABILITY

The Walsh spectra of Boolean functions with n variables require 2^n logical qubits to characterize, which allows for a simplified model for nonlinearity, balancedness, and resiliency. In fact, to characterize the balancedness or resiliency one needs 2^n logical qubits and one requires extra 2^n qubits to represent the nonlinearity. Intuitively, the m-resilient Boolean function is balanced to reduce the search space with size of 2^{2^n} into the size of $\binom{2^n}{2^{n-1}}$, in which the classical computer may find a subclass of optimal functions but wŒÆould fail in getting all the globally optimal ones.

As further mapped into the hardware architecture of the D-Wave, the quantum annealing is a potential way to search in the globally exponential space to explore the global properties of the Boolean function. However, the connectivity limits the direct interactions between different logical qubits and the chain is constructed to implement the logical connectivity at the physical level. For example, for n-variable Boolean functions, the nonlinearity requires 2^n physical qubits as a chain to represent a logical qubit, such that in total 2^{2n-1} physical qubits are needed. Moreover, additional 2^{2n-1} physical qubits are arranged as a second part connected to the part for nonlinearity to design the Boolean functions satisfying more criteria such as balancedness and resiliency.

However, as n grows up within the limited hardware architecture, more qubits would be turned into one chain as shown in Table VI. This will cause more errors in the annealing procedure and the majority of chains will be broken, resulting in suboptimal results. The adjustment of the strength of the qubits and couplers can correct some errors but will be in principle unavailable when it comes to a large-scale system.

TABLE VI. Number of qubits required at the logical and physical level

	2	4	6	8
Logical(2^{n+1})	8	32	128	512
Physical(2^{2n-1})	8	128	2048	2^{15}

Actually, the connectivity problem is related to the accuracy problem. The chain is unstable because the strength of the coupler in the chain is finite (-1). The experiments show that if the chain strength can be made stronger, the robustness could be better but correspondingly the logical interactions characterized by the physical chains may be weaker with respect to the chain.

Actually, the scheme gives a generalized model for n-variable Boolean functions (for even n) in theory, and, if a full-connectivity quantum computer with high fidelity is provided, the results can be better. With a full-connectivity and low-error-rate device, it is possible to explore the global properties of Boolean functions in the exponential space, which is

hard for classical computers. Therefore, the connectivity of the quantum annealer physical hardware is the key problem for the scalability.

VIII. DISCUSSION

In summary, we have introduced a quantum annealing protocol to design even-variable Boolean functions with suitably designed criteria based on the D-Wave quantum computing platform. Quantum annealing can be seen as a new computing paradigm for cryptography design with the potential to explore the global properties of Boolean functions.

Based on the experiments on the 2048-qubit chimera hardware architecture, we implement 2, 4, and 6-variable bent function design, balanced 4-variable Boolean function design, and 4-variable m-resilient Boolean function design with high nonlinearity, respectively. One of the main problems is to achieve the tradeoff between the stability of the chains and the coupler strengths. Moreover, the suboptimal results provided by the machine allow the classical algorithm to improve outcomes and find the optimal ones. The local search was able to effectively optimize the approximately optimal solutions to generate different bent functions, where classical computers may easily be trapped in suboptimal results. The majority vote is a suitable way for the experiments involving multiple criteria to estimate that the best tradeoff between the coupler strength and the chain strength has been achieved, while it could improve the efficiency of function generating procedure as well. Additionally, as the system scales up, the total execution time almost remains the same, which is a main advantage of the D-Wave device compared to classical computers, although a large system may lead to more errors in our cases.

Furthermore, this is a novel quantum computing application and it is also a new way to design cryptographic keys. Additionally, the D-Wave device actually completes the search problem in an exponential space with dimension of up to 2^{2048} and outputs the optimal solutions, which shows the ability of global search compared to classical computing methods.

As a step forward towards a quantum advantage under these cases, one will need 512 logical qubits to design the 8-variable Boolean function with multiple criteria, for which classical computers may only find a small subclass of good solutions. Both new models to decrease the demands on qubit numbers and better-connectivity quantum devices are necessary in the future to breakthrough the bottleneck in cryptography by quantum computing.

ACKNOWLEDGEMENTS

This work is supported by the grant of "the Special Zone Project of National Defense Innovation", the National Natural Science Foundation of China (61572304 and 61272096), and the Key Program of the National Natural Science Foundation of China (61332019), Open Research Fund of State Key Laboratory of Cryptology. We also acknowledge support from the program of Shanghai Municipal Science and Technology Commission (18010500400 and 18ZR1415500), the Shanghai Program for Eastern Scholar, Ramón y Cajal Grant RYC-2017-22482, Grant PGC2018-095113-B-I00 (MCIU/AEI/FEDER, UE), Basque Government IT986-16, the projects QMiCS (820505) and OpenSuperQ (820363) of the EU Flagship on Quantum Technologies, and the EU FET Open project Quromorphic. We acknowledge the use of D-Wave quantum computing facilities through Oak Ridge National Laboratory (ORNL).

[1] C. Carlet, Boolean functions for cryptography and error correcting codes, Boolean models and methods in mathematics, computer science, and engineering **2**, 257 (2010).

[2] M. Willi and S. Othmar, Fast correlation attacks on stream ciphers, Advances in cryptology EUROCRYPT **88**, 301 (1988).

[3] N. T. Courtois, Fast algebraic attacks on stream ciphers with linear feedback, Annual International Cryptology Conference, 176 (2003).

[4] C. Carlet, A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland construction, Annual International Cryptology Conference, 549 (2002).

[5] D. Tang, C. Carlet, and X. H. Tang, Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks, IEEE Trans. Inf. Theory **59**, 653 (2013).

[6] S. Picek, D. Jakobovic, J. F. Miller, L. Batina, and M. Cupic, Cryptographic Boolean functions: One output, many design criteria, Appl. Soft. Comput. **40**, 635 (2016).

[7] C. S. Ding, G. Z. Xiao, and W. J. Shan, *The stability theory of stream ciphers* (Springer Science & Business Media, 1991).

[8] W. G. Zhang and P. Enes, Improving the lower bound on the maximum nonlinearity of 1-resilient Boolean functions and designing functions satisfying all cryptographic criteria, Inf. Sci. **376**, 21 (2017)

[9] C. Carlet and A. Klapper, Upper bounds on the numbers of resilient functions and of bent functions, Proc. of 23rd Symposium on Information Theory in the Benelux (2002)

[10] S. Q. Pang, X. Wang, D. Jing, J. Du, and M. Feng, Construction and count of 1-resilient rotation symmetric Boolean functions, Inf. Sci. **450**, 336 (2018).

[11] A. B. Finnila, M. A. Gomez, C. Sebenik, C. Stenson, and J. D. Doll, Quantum annealing: a new method for minimizing multidimensional functions, Chem. Phys. Lett. **219**, 343 (1994).

[12] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, Zhang, J. M. Martinis, and H. Neven, Characterizing quantum supremacy in near-term devices, Nature Phys. **14**, 595 (2018).

[13] D. Castelvecchi, Quantum computers ready to leap out of the lab in 2017, Nature News **541**, 7635 (2017).

[14] E. Pednault, J. A. Gunnels, G. Nannicini, L. Horesh, T. Magerlein, E. Solomonik, and R. Wisnieff, Breaking the 49-qubit barrier in the simulation of quantum circuits, arXiv:1710.05867 (2017).

[15] https://www.dwavesys.com/home

[16] M. W. Johnson *et al.*, Quantum annealing with manufactured spins, Nature **473**, 194-198 (2011).

[17] D. O'Malley, An approach to quantum-computational hydrologic inverse analysis, Sci. Rep. **8**, 6919 (2018).

[18] A. Mott *et al.*, Solving a Higgs optimization problem with quantum annealing for machine learning, Nature **550**, 375-379 (2017).

[19] R. Dridi and H. Alghassi. Prime factorization using quantum annealing and computational algebraic geometry, Sci. Rep. **7**, 43048(2017).

[20] A. Perdomo-Ortiz, N. Dickson, M. Drew-Brook, G. Rose, and A. Aspuru-Guzik, Finding low-energy conformations of lattice protein models by quantum annealing, Sci. Rep. **2**, 571 (2012).

[21] R. Courtland, D-Wave Aims to Bring Quantum Computing to the Cloud, IEEE Spectrum (2014).

[22] C. Wang and H. G. Zhang, Impact of Commercial Quantum Computer on Cryptography, Information Security and Communications Privacy **2**, 31 (2012)

[23] C. Wang, Y. J. Wang, and F. Hu, Shaping the future of commercial quantum computer and the challenge for information security, Chinese Journal of Network and Information Security **2**, 3 (2016).

[24] S. Jiang, K. A. Britt, T. S. Humble, and S. Kais, Quantum Annealing for Prime Factorization. Sci. Rep. **8**, 17667 (2018).

[25] C. S. Ding, G. Z. Xiao, and W. J. Shan, *The stability theory of stream ciphers* (Springer Science & Business Media, 1991).

[26] M. Willi and S. Othmar, Fast correlation attacks on stream ciphers, Advances in cryptology-EUROCRYPT 88, 301 (1988).

[27] F. J. MacWilliams, and N. J. A. Sloane, *The theory of error-correcting codes* (Elsevier, 1977).

[28] W. Millan, A. Clark, and E. Dawson, Heuristic design of cryptographically strong balanced Boolean functions, International Conference on the Theory and Applications of Cryptographic Techniques, 489 (1998).

[29] C. Carlet, A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland construction, Annual International Cryptology Conference, 549 (2002).

[30] Z. R. Tu, and Y. P. Deng, A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity, Designs, Codes and Cryptography **60**, 1 (2011).

[31] S. Picek, D. Jakobovic, J. F. Miller, L. Batina, and M. Cupic, Cryptographic Boolean functions: One output, many design criteria, Appl. Soft. Comput. **40**, 635 (2016).

[32] R. Hrbacek and V. Dvorak, Bent function synthesis by means of Cartesian genetic programming, International Conference on Parallel Problem Solving from Nature, 414 (2014).

[33] K. L. Pudenz, T. Albash, and D. A. Lidar, Error-corrected quantum annealing with hundreds of qubits, Nat. Comm. **5**, 3243 (2014).