TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 09/10 pp751–759
DOI: 10.26599/TST.2021.9010022
Volume 27, Number 4, August 2022

New Advanced Computing Architecture for Cryptography Design and Analysis by D-Wave Quantum Annealer

Xiangmin Ji, Baonan Wang*, Feng Hu, Chao Wang, and Huanguo Zhang

Abstract: Universal quantum computers are far from achieving practical applications. The D-Wave quantum computer is initially designed for combinatorial optimizations. Therefore, exploring the potential applications of the D-Wave device in the field of cryptography is of great importance. First, although we optimize the general quantum Hamiltonian on the basis of the structure of the multiplication table (factor up to 1 005 973), this study attempts to explore the simplification of Hamiltonian derived from the binary structure of the integers to be factored. A simple factorization on 143 with four qubits is provided to verify the potential of further advancing the integer-factoring ability of the D-Wave device. Second, by using the quantum computing cryptography based on the D-Wave 2000Q system, this research further constructs a simple version of quantum-classical computing architecture and a Quantum-Inspired Simulated Annealing (QISA) framework. Good functions and a high-performance platform are introduced, and additional balanced Boolean functions with high nonlinearity and optimal algebraic immunity can be found. Further comparison between QISA and Quantum Annealing (QA) on six-variable bent functions not only shows the potential speedup of QA, but also suggests the potential of architecture to be a scalable way of D-Wave annealer toward a practical cryptography design.

Key words: Quantum Annealing (QA); factorization; Boolean functions; brain-inspired cognition

1 Introduction

In the quantum computing era, the fierce competition on the construction of universal quantum computers is advancing the development of quantum computing technology for our daily lives[1, 2]. Although many potential applications exist, such as factoring and code breaking, quantum chemistry and material simulation, solving linear systems, and machine learning problems[3–5], universal quantum computers still have a long way to go before achieving killer applications[6–8].

In the field of cryptography, Shor's algorithm is

• Xiangmin Ji is with College of Computer Information Science, Fujian Agriculture and Forestry University, Fuzhou 350002, China, and also with School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China. E-mail: jixm168@126.com.
• Baonan Wang is with College of Computer Science and Technology, Shanghai University of Electric Power, Shanghai 200090, China. E-mail: wbn_shu0099@163.com.
• Feng Hu is with Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai University, Shanghai 200444, and also with State Key Laboratory of Cryptology, Beijing 100878, China. E-mail: sdhf911103@163.com.
• Chao Wang is with Key laboratory of Specialty Fiber Optics and Optical Access Networks, Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai University, Shanghai 200444, and with State Key Laboratory of Cryptology, Beijing 100878, and also with Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen 518000, China. E-mail: wangchao@shu.edu.cn.
• Huanguo Zhang is with School of Cyber Science and Engineering, Wuhan University, Wuhan 430072. E-mail: liss@whu.edu.cn.
$*$To whom correspondence should be addressed.

Manuscript received: 2021-02-20; accepted: 2021-03-12

considered a unique and powerful quantum algorithm for the cryptanalysis of RSA. Thus, the threats of Shor's algorithm attract increasing attention as universal quantum computers develop. However, universal quantum computers are not good enough for code cracking[8]. Thus, further attention should be paid to the cryptographic applications of the special-purpose quantum computer, D-Wave quantum annealer[9].

The D-Wave device, collaborated with Lockheed Martin Corporation and Google, has been initially used for image processing, combinatorial optimization, and software verification[4, 10]. The machine is built on the basis of the adiabatic theorem[11–13], different from the gate-model universal ones. Quantum annealing (QA), as the core principle, can work for finding the ground state of Hamiltonian characterized by the manufactured spins[14] of the Ising models.

In principle, QA can utilize the quantum mechanics and quantum tunneling effects to find approximate answers to certain important problems with exponential levels in computer science. These problems can only be truly solved by exhaustively trying every possible solution. Meanwhile, the quantum spin models, for example, the Ising model, comprise spins that may stay in either up or down aligned with a preferred axis[15]. It can be given as follows:

$$H_{\text{Ising}} = \sum_{i=1}^{N} h_i \sigma_i^z + \sum_{i,j=1}^{N} J_{i,j} \sigma_i^z \sigma_j^z \tag{1}$$

where σ_i^z is the Pauli spin matrix with two values ± 1, Spin i and Spin j are coupled by J_{ij}, and h_i is the local field. During the QA procedure, another kinetic term exists in the x axis to utilize the quantum tunneling effects, so that, on the basis of the adiabatic theorem[11], the system can evolve from the ground state of the initial Hamiltonian to the ground state of H_{Ising} if the annealing progresses slowly.

Thus, the theoretical speedup potentials of QA, along with the feasibility of characterizing problems by Ising models, allow for the wide applications of the D-Wave machine in various areas[16–22]. Furthermore, the capacity of QA for factorizations needs further exploration for improving the deciphering ability of the D-Wave machine in the condition of limited qubit resource and hardware connectivity. However, almost no one pays attention to the capacity of D-Wave for cryptography design[3].

1.1 Cryptography analysis

Shor's algorithm is considered a unique and powerful quantum algorithm for the cryptanalysis of RSA. Therefore, the current state of post-quantum cryptography research exclusively refers to the potential threats of Shor's algorithm. However, the physical implementations of Shor's algorithm can only achieve up to factorization on 85[23]. In 2008, Adiabatic Quantum Computing (AQC) was first introduced to factor 21 in a three-qubit NMR quantum processor[24]. Special properties of certain integers help advance the developments of factorizations by AQC (quantum factorization on 56 153 with only four qubits, high-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system, application to the experimental factorization on 291 311). However, the scalability of these methods cannot be guaranteed.

In 2018, Jiang et al.[21] proposed a generalized Quadratic Unconstrained Binary Optimization (QUBO) model to embed the multiplication table for prime number factorization into the D-Wave quantum computer. Peng et al.[17] and Wang[18] advanced it by introducing the extra limitations given by the object values in the multiplication table.

The present study regards QA as a second way, different from Shor's algorithm, for attacking RSA and further analyzes the feasibility of optimizing the original quantum spin models for factorizations with a simple example of factoring 143. It suggests that the special 0–1 distributions (binary structures) of the integers to be factored in have great potentials of simplifying the final quantum spin models.

1.2 Cryptography design

The existing traditional cryptography design has made some progress[25–28]. Currently, the post-quantum cryptography against quantum attacks attracts increasing attention[29], whereas the capacity of quantum computing to design cryptography is neglected. The most advanced quantum computers, including the D-Wave machine and the universal ones, have nothing to do with cryptography design.

Hu et al.[30, 31] proposed a novel way of characterizing the Boolean functions by using Ising models. The principle-of-proof experiments verified the capacity of D-Wave annealer for designing the cryptographic components of traditional cryptography, which is called quantum computing cryptography.

However, the current hardware connectivity of the D-Wave machine limits the scalability and accuracy of generating Boolean functions, which should be constructed via the quantum spin models. Thus, this study further explores the potentials of quantum-assisted cryptography design with a simplified verification on the basis of the hybrid computing architecture, inspired by quantum computing, classical computing, and brain-inspired cognition. The new architecture explores the potentials of D-Wave annealer acting as a classical accelerator on a large-scale cryptography design with the directional searching provided by brain-like methods. It is expected to be a scalable way for the D-Wave quantum computer toward a practical cryptography design in the future.

2 Large Number Factorization by QA

Prime number factorization problem refers to finding two unique prime numbers factored by large numbers where the best-known algorithm, general number field sieve method[32], grows exponentially in the number of operations. Performing Shor's algorithm to factor an n-bit number still requires at least $2n$ logical qubits[33]. In such a condition, deciphering a 1024-bit RSA cryptosystem requires approximately 2048 logical qubits, which is far larger than the capacity of the known quantum chips.

Although Peng et al.[17] verified the superiority of the D-Wave machine to Shor's algorithm that can factor up to 1 005 973, the limitations on the topological connectivity of the Chimera graph and the accuracy of characterizing the integer problems remain challenging. Therefore, a theoretical analysis is conducted on the further simplification of constructing QUBO models for factoring large integers.

Assuming that integer N is to be factored by two prime factors p and q, they can be represented by $p = (1p_{k_1-1}p_{k_1-2}\dots 1)_2$ and $q = (1q_{k_2-1}q_{k_2-2}\dots 1)_2, p_i$ and $q_j \in \{0,1\}, i = 1,2,\dots,k_1, j = 1,2,\dots,k_2$, where $k_1 = \lfloor \log_2(p) \rfloor$ and $k_2 = \lfloor \log_2(q) \rfloor$,which denote the lengths of p and q, respectively. Here each bit represented by p_i or q_j can be seen as a qubit in the QUBO model.

Taking the factorization on 143 as an example, the multiplication table based on the work of Jiang et al.[21] is presented.

As presented in Table 1, the construction can be provided on the basis of the three columns with the carries before or next to themselves. The energy function can be given as follows:

Table 1 Multiplication table for 143=11 × 13 in binary.

Variavble	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
p					1	p_2	p_1	1
q					1	q_2	q_1	1
Binary-multiplication					1	p_2	p_1	
				q_1	p_2q_1	p_1q_1	q_1	
			q_2	p_2q_2	p_1q_2	q_2		
		1	p_2	p_1	1			
Carry		c_4	c_3	c_2	c_1			
Target value	1	0	0	0	1	1	1	1

Note: In the row of "Binary-multiplication", the three parts are denoted as Column$_1$, Column$_2$, and Column$_3$ form right to left.

$$f = (2p_2+2p_1q_1+2q_2-8c_2-4c_1+p_1+q_1-3)^2 + (2q_1+2p_2q_2+2p_1+2c_2-8c_4-4c_3+p_2q_1+ p_1q_2+c_1+1)^2+(q_2+p_2+c_3+2c_4-2)^2 \tag{2}$$

Each part in Eq. (2) corresponds to the relationships given in Column$_1$ − Column$_3$. If and only if all the conditions are satisfied (the energies in each part achieve zero), $\{p_1, p_2, q_1, q_2\}$ can be used for generating two primes p and q to be the prime factors of 143.

However, the qubit weights and coupler strengths vary too much that they can cause inaccurate QA and fail in achieving the ground state of the Hamiltonian (energy functions). As a result, the models cost more qubit resources and more time to solve large-scale factorizations than usual.

To analyze it in theory, the complexity of models and the failure of QA lie in the dividing columns with carries. Given that the main multiplying part is fixed, if the target values in the last row can help eliminate some carries first before constructing the final Hamiltonian, then the aforesaid challenges can be relieved.

Take Table 1 as an example. We first refer to Column$_1$, which is given as follows:

$$p_1 + q_1 + 2(p_2 + q_2 + p_1q_1) = 3 + 4c_1 + 8c_2 \tag{3}$$

If the object values are considered, then $p_1 + q_1 = 1$; hence, $p_1q_1 = 0$. With the above conditions to simplify Eq. (3), it becomes $2(p_2 + q_2) = 2 + 4c_1 + 8c_2$. Then, we can obtain $c_1 = c_2 = 0$ and $p_2 + q_2 = 1$. In this way, the condition given in Column$_1$ can be transformed as $p_1 + q_1 = 1$ and $p_2 + q_2 = 1$.

To employ it further in Column$_2$, we can obtain $p_2q_1 + p_1q_2 + 4 = 1 + 4c_3 + 8c_4$. Then, $c_3 = 1$ and $c_4 = 0$ can be obtained while the conditions provided in Column$_2$ can be given as $p_2q_1 + p_1q_2 = 1$.

With the above conditions, the relationships in Column_3 must be satisfied. In this way, the complex Eq. (3) can be simplified as $p_1 + q_1 = 1$, $p_2 + q_2 = 1$, and $p_2 q_1 + p_1 q_2 = 1$. Only four qubits without extra carries are enough to characterize the factorization on 143 as follows:

$$f = (p_1+q_1-1)^2+(p_2+q_2-1)^2+(p_2q_1+p_1q_2-1)^2 \tag{4}$$

Note that the term $p_1 p_2 q_1 q_2$ is eliminated due to $p_1 p_2 = 0$ and $q_1 q_2 = 0$. Thus, the final simplified energy function only contains single qubits and two-qubit couplers. That is, no further reduction for k-coupler ($k > 2$) is required and only four qubits are required to factor 143, whereas Peng et al.[17] required five qubits.

Obviously, this kind of reductions based on the binary structure of the integers can be generalized further, and some of the values represented by the qubits can be fixed, especially for the carries. In this way, the sufficiency and accuracy of QA can be improved.

Briefly speaking, this study proposes an optimized strategy of further considering the relationships between the target values and the divided columns that certain properties of the integers can be used to fix certain values in the multiplication table. Then, the complexity of the final Hamiltonian can be reduced directly. This study takes the factorization on 143 as an example, and the result indicates that if the target values in the first column are given as “1 1”, then at least four conditions can be used to simplify the multiplication table first, namely, $p_1 + q_1 = 0$, $p_2 + q_2 = 0$, $c_1 = 0$, and $c_2 = 0$.

To sum up, a new simple verification of the feasibility of the optimizations on the factorization problem is proposed. Moreover, the simplification derived from the binary structure of integers provides an important optimized way on the basis of the combination of classical optimization and quantum computing. It can be seen as a novel quantum-classical hybrid computing architecture, and the generalized structure combined with previous work[17] for large-scale factorizations should be further explored.

3 Boolean Functions Designed by Quantum Inspired Algorithm

The last part shows the potential of quantum computing on cryptography analysis. This part also explores the feasibility of devising Boolean functions based on the advanced computing architecture, combining quantum computing with the brain-inspired approach.

3.1 Quantum-Inspired Simulated Annealing (QISA)

QA is expected to solve the problems without a sufficient theoretical basis, which is also intractable for computer science[34]. We utilize the D-Wave 2000Q platform to design small-scale Boolean functions with a potential speedup advantage to the classical ones[30]. From the aspect of cognitive science, QA still suffers from a lack of cognitive capacity that various experiments are required for finding exact solutions, especially for large-scale cases. That is, if QA is further combined with brain-inspired computing architecture, where the brain-like cognition provides directional searching guidance for quantum computing[35], then the new architecture is expected to maximize the potentials of quantum computing and classical computing. For example, if an improved Boolean function can be delivered to the quantum annealer as the initialized state, then QA can work well, because the initial state may be closer to the ground state than a random initialization.

To verify the potentials of the new architecture, a simplified version of QISA is proposed for designing large-scale Boolean functions with multiple criteria. In different cryptographic scenarios, high nonlinearity is required to withstand the best affine approximation and fast correlation attack, high algebraic immunity is required to resist algebraic attack, and the state of being balanced is required to avoid statistical dependence between the plaintext and the ciphertext[36]. This study aims at these three important criteria.

Before constructing the models for QISA, several assumptions and key points should be given first as follows:

(1) As a simplified version, the criteria are given by the classical algorithm directly without the mapping to the spin models.

(2) Inspired by the QA principle[14], extra kinetic terms and a simplified annealing schedule are introduced to simulate the annealing procedure toward the “tunneling-like effect”.

(3) To approximate the real quantum evolution, the cooling strategy and metropolis criterion are required to simulate the QA.

Note that due to some different properties between even-variable Boolean functions and odd-variable ones, all the Boolean functions referred to in this paper are even-variable Boolean functions, which mean n is an even number.

We first provide a model for nonlinearity and algebraic immunity as $H_p(f)$, and then search for the balanced functions in a relatively small region,

$$H_p(f) = w_1(\mathrm{AI}_{\max} - \mathrm{AI}_{\text{current}}) + w_2(N_{\max} - N_{\text{current}}) \tag{5}$$

where AI and N are the key parameters for our construction that indicate the algebraic immunity and the nonlinearity of the derived eight-variable Boolean functions, respectively. $\mathrm{AI}_{\max} = n/2$ and $N_{\max} = 1/2^n - 2^{n/2}$ (n is even) stand for the maximam values of the algebraic immunity and the nonlinearity, respectively. $\mathrm{AI}_{\text{current}}$ and N_{current} denote the algebraic immunity and nonlinearity of the newly derived Boolean functions in the current annealing stage, respectively. To balance the effects of different criteria, w_1 and w_2 are designed on the basis of the multi-object optimization as follows:

$$\begin{cases} w_1 + w_2 = 1, \\ w_1/w_2 = \mathrm{AI}_{\max}/N_{\max} \end{cases} \tag{6}$$

Then, the kinetic energy term H_{kin} is introduced as follows:

$$H_{\text{kin}} = \sum_{i=0}^{2^n-1} a_i \tag{7}$$

where a_i denotes the i-th coefficient of the Boolean functions. Then, the Hamiltonian of the system H_{bool} is given by

$$H_{\text{bool}} = \Lambda(t)H_p + \Gamma(t)H_{\text{kin}} \tag{8}$$

where $\Lambda(t)$ and $\Gamma(t)$ adjust the annealing schedule similar to the QA schedule. Figure 1 illustrates a simplified version of the annealing scheme as in the eight-qubit experiments of the D-Wave one[14].

3.2 Experiments

Initialized with random Boolean functions in the term of truth table, the annealing schedule is designed as shown in Fig. 1. In each annealing, random perturbation is given for generating a new Boolean function H_{boolnew}, which can be accepted as follows (set $T = T - E_{\text{cop}}$, where E_{cop} indicates the annealing rate).

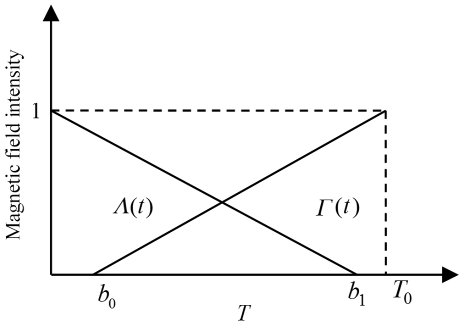

Fig. 1 Configuration of magnetic strength. T_0 denotes the initial temperature, which can decrease according to the annealing rate along with the process of annealing. b_0 and b_1 denote the ending temperature of $\Lambda(t)$ and the beginning temperature of $\Gamma(t)$, respectively.

if $\Delta E = H_{\text{boolnew}} - H_{\text{bool}} < 0$, then accept it; else if $e^{\Delta E/T} >$ random (0, 1), where T is the current temperature, then accept it.

To find the approximate thermodynamic equilibrium, the Boolean functions update up to D times, which is the length of the Markov chain during the annealing.

The initialized eight-variable Boolean functions are optimized, and a group of functions with relatively high nonlinearity and optimal algebraic immunity are obtained, as presented in Table 2.

The initial magnetic strength and temperature used in the simulations are denoted by Γ_0 and T_0, respectively.

Case 1 begins with a relatively high temperature and sets a relatively large annealing rate. As the annealing progresses, the system can finally find a group of Boolean functions with optimal algebraic immunity and high nonlinearity being 113, where the nonlinearity is improved by 10 percent compared with the initially generated Boolean functions.

To further optimize the cooling strategy as in Case 2, annealing begins with $T_0 = 50$ ℃ and then cools the system by the step of 0.2 ℃ toward 6 ℃. The second stage starts with $T_0 = 6$ ℃ with an annealing rate of 0.002 until the annealing stops at 0. Finally, the eight-variable Boolean functions with optimal algebraic immunity and high nonlinearity being 114 can be found, among which also include some balanced functions.

Inspired by Case 2, a relatively low initial temperature (e.g., $T_0 = 2$ ℃) and low step (e.g., $E_{\text{cop}} = 0.005$ ℃) are initialized. Along with a relatively long Markov chain (e.g., $D = 25$), we find that the initial configurations are sufficient to generate the balanced eight-variable Boolean functions with optimal algebraic immunity and nonlinearity.

That is, by carefully selecting the parameters to manipulate the evolution procedure, the advantages of deriving improved solutions in the exponential-

Table 2 Construction of eight-variable Boolean functions.

Case	Γ_0	T_0 (℃)	E_{cop} (℃)	D	AI	N
1	1	6	0.020	20	4	113
2	1	50	0.200	30	4	114
	0	6	0.002	30	4	114
3	1	2	0.005	25	4	114
	1	2	0.020	25	4	114

level space may be presented. In addition, evolving in low temperature likely refers to activating "tunneling-like effects" in accordance with the quantum annealer, which requires low-temperature environments to realize quantum effects.

To further simulate the QA algorithm, a high-performance computer is introduced to provide a high-precision computing capacity and advance the 8-variable cases to 10- and 12-variable cases. To further investigate the advantage of the new computing architecture, as a simplified pattern of a brain-inspired approach, we introduce the relatively better Boolean functions[37] as the initial functions.

The results are given in Table 3. On the basis of the optimizations for Ising spin glasses, 10- and 12-variable Boolean functions with high nonlinearity (478 and 1970, respectively) can be obtained. Furthermore, the balanced 10- and 12-variable Boolean functions with nonlinearity respectively being 476 and 1968 can be found, where the nonlinearity is optimized.

The definitions of the parameters can refer to the ones in Table 2.

From the aspect of high-performance computing architecture, it offers an improved scalability to high-variable cases solved by powerful calculations. Although our simulations are based on the simplified quantum-inspired model and basic optimized methods, good initializations inspired by brain-inspired cognition can help accelerate the optimizations of Boolean functions, which can enable QA to realize directional searching with cognitive ability and interpretability.

We consider that quantum computing cryptography can derive six-variable bent functions whose nonlinearity achieves the maximal. This study further utilizes the QISA framework to design Boolean functions with single criterion nonlinearity. Although six-variable bent functions can be found, it requires a certain amount of computing time and carefully designed annealing parameters. That is, to embed the QPU of the D-Wave into the classical computing architecture, many computing resources are expectedly saved further for specialized problems, such as the bent function design.

Table 3 Construction of 10- and 12-variable Boolean functions.

Experiment	n	Γ_0	T_0 (°C)	E_{cop} (°C)	D	AI	N
1	10	1	100	0.001	30	5	478
2	10	1	100	0.001	80	5	478
3	12	1	100	0.010	30	6	1968
4	12	1	100	0.001	30	6	1970

Thus, we expect that the real quantum annealer may provide a potential advantage in the small-scale case, similar to the six-variable Boolean function design. Meanwhile, quantum computing or quantum-inspired methods can be embedded as a part of the advanced computing architecture, which can be well collaborated with brain-inspired cognition to maximize the potentials of quantum-classical hybrid computing. In this way, the directional searching capacity can be further combined with the national quantum evolutionary properties toward robust global searching algorithms, whereas the brain-inspired cognition can provide explicit physical meanings characterized by the quantum spin models.

4 Discussion and Conclusion

Quantum computing provides powerful potential for solving intractable problems. However, as for the cryptography design and analysis, universal quantum computers and special-purpose ones are still in fancy. In the 6th ETSI/IQC Quantum Safe Workshop (November 2018), some experts shared great interests in the proposal of factorization by D-Wave annealer[17] and analyzed the reason for neglecting the attacks from the D-Wave machine in the post-quantum cryptography research that the D-Wave, purchased by Lockheed Martin and Google, has been initially used for image processing, machine learning, combinatorial optimization, and software verification.

The D-Wave machine provides a new (second) way, completely different from Shor's algorithm, and may be closer to cracking practical RSA codes than Shor's algorithm. We verify the optimized version[21] for factoring 20-bit integers[17] with superiority to the latest IBM Q System One$^{\mathrm{TM}}$ (January 8, 2019), which can only factor up to 10-bit integers via Shor's algorithm. The present study further explores the introduction of extra limitations for simplifying the Hamiltonian to be solved. It shows the potential to further improve the real factoring capacity of the D-Wave machine with superiority to other quantum platforms.

Furthermore, due to the fact that most scholars consider Shor's algorithm as a unique and powerful quantum algorithm for the cryptanalysis of RSA, the current state of post-quantum cryptography research exclusively refers to the potential threats of Shor's algorithm. Thus, post-quantum cryptography research should further consider the potentials of the D-Wave quantum computer for deciphering the RSA cryptosystem in the future.

From the aspect of cryptography design, this study attempts to construct a simple but effective advanced computing architecture combining quantum computing with an intelligent pattern on devising Boolean functions, which satisfy multiple criteria. Through the combination of classical simulation and specialized initial points, a high-performance computer can effectively improve certain criteria via the annealing schedule, compared with the ones given by mathematics. The model used in the simulations can be seen as a simplified advanced computing architecture, which is expected to utilize the quantum effects for constructing a high-security and one-time-pad cryptosystem.

Further analyzed through the comparison to the real quantum computing experiments, QA shows a potential speed up in the Boolean function design problems. Thus, the new advanced quantum computing architecture shows powerful potentials for cryptography design with the introduction of brain-inspired cognition. Further attention and efforts are required for the new computing architecture and its applications.

Acknowledgment

This study was supported by the Special Zone Project of National Defense Innovation, the National Natural Science Foundation of China (Nos. 61572304 and 61272096), the Key Program of the National Natural Science Foundation of China (No. 61332019), the Shanghai Sailing Plan of "Science and Technology Innovation Action Plan" (No. 21YF1415100), Fujian Provincial Natural Science Foundation Project (No. 2021J01129), and Open Research Fund of State Key Laboratory of Cryptology.

References

[1] K. R. Brown, Quantum technologies and the National Quantum Initiative, *Quantum Engineering*, vol. 1, no. 1, p. e7, 2019.

[2] J. Mlynek, The European quantum technology flagship: Paving the way for the second quantum revolution, *Quantum Engineering*, vol. 1, no. 1, p. e5, 2019.

[3] C. Wang and H. G. Zhang, Impact of commercial quantum computer on cryptography, (in Chinese), *Information Security and Communications Privacy*, no. 2, pp. 31–32&35, 2012.

[4] 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, *Scientific Reports*, vol. 2, p. 571, 2012.

[5] R. Martoňák, G. E. Santoro, and E. Tosatti, Quantum annealing of the traveling-salesman problem, *Phys. Rev. E*, vol. 70, no. 5, p. 057701, 2004.

[6] A. Cho, DOE pushes for useful quantum computing, *Science*, vol. 359, no. 6372, pp. 141–142, 2018.

[7] J. Brainard, What's coming up in 2018, *Science*, vol. 359, no. 6371, pp. 10–12, 2018.

[8] E. Gibney, Physics: Quantum computer quest, *Nature*, vol. 516, no. 7529, pp. 24–26, 2014.

[9] B. N. Wang, F. Hu, H. N. Yao, and C. Wang, Prime factorization algorithm based on parameter optimization of Ising model, *Scientific Reports*, vol. 10, p. 7106, 2020.

[10] H. Neven, V. S. Denchev, M. Drew-Brook, J. Y. Zhang, W. G. Macready, and G. Rose, NIPS 2009 demonstration: Binary classification using hardware implementation of quantum annealing, *Quantum*, https://www.mendeley.com/catalogue/1a199e97-f0c3-35c1-ae5f-db23280f06a9/, 2009.

[11] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda, A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem, *Science*, vol. 292, no. 5516, pp. 472–475, 2001.

[12] B. N. Wang, F. Hu, and C. Wang, Optimization of quantum computing models inspired by D-Wave quantum annealing, *Tsinghua Science and Technology*, vol. 25, no. 4, pp. 508–515, 2020.

[13] N. Wang, G. G. Guo, B. N. Wang, and C. Wang, Traffic clustering algorithm of urban data brain based on a hybrid-augmented architecture of quantum annealing and brain-inspired cognitive computing, *Tsinghua Science and Technology*, vol. 25, no. 6, pp. 813–825, 2020.

[14] M. W. Johnson, M. H. S. Amin, S. Gildert, T. Lanting, F. Hamze, N. Dickson, R. Harris, A. J. Berkley, J. Johansson, P. Bunyk, et al., Quantum annealing with manufactured spins, *Nature*, vol. 473, no. 7346, pp. 194–198, 2011.

[15] O. Titiloye and A. Crispin, Quantum annealing of the graph coloring problem, *Discrete Optimization*, vol. 8, no. 2, pp. 376–384, 2011.

[16] F. Neukart, G. Compostella, C. Seidel, D. von Dollen, S. Yarkoni, and B. Parney, Traffic flow optimization using a quantum annealer, *Frontiers in ICT*, vol. 4, p. 29, 2017.

[17] W. C. Peng, B. N. Wang, F. Hu, Y. J. Wang, X. J. Fang, X. Y. Chen, and C. Wang, Factoring larger integers with fewer qubits via quantum annealing with optimized parameters, *Sci. China Phys. Mech. Astron.*, vol. 62, no. 6, p. 60311, 2019.

[18] X. M. Wang, Quest towards "factoring larger integers with commercial D-Wave quantum annealing machines", *Sci. China Phys. Mech. Astron.*, vol. 62, no. 6, p. 960331, 2019.

[19] A. D. King, J. Carrasquilla, J. Raymond, I. Ozfidan, E. Andriyash, A. Berkley, M. Reis, T. Lanting, R. Harris, F. Altomare, et al., Observation of topological phenomena in a programmable lattice of 1800 qubits, *Nature*, vol. 560, no. 7719, pp. 456–460, 2018.

[20] R. Harris, Y. Sato, A. J. Berkley, M. Reis, F. Altomare, M. H. Amin, K. Boothby, P. Bunyk, C. Deng, C. Enderud, et al., Phase transitions in a programmable quantum spin glass simulator, *Science*, vol. 361, no. 6398, pp. 162–165, 2018.

[21] S. X. Jiang, K. A. Britt, A. J. McCaskey, T. S. Humble,

and S. Kais, Quantum annealing for prime factorization, *Scientific Reports*, vol. 8, p. 17667, 2018.

[22] B. N. Wang, F. Hu, H. G. Zhang, and C. Wang, From evolutionary cryptography to quantum artificial intelligent cryptography, (in Chinese), *Journal of Computer Research and Development*, vol. 56, no. 10, pp. 2112–2134, 2019.

[23] M. R. Geller and Z. Y. Zhou, Factoring 51 and 85 with 8 qubits, *Scientific Reports*, vol. 3, p. 3023, 2013.

[24] X. H. Peng, Z. Y. Liao, N. Y. Xu, G. Qin, X. Y. Zhou, D. Suter, and J. F. Du, Quantum adiabatic algorithm for factorization and its experimental implementation, *Phys. Rev. Lett.*, vol. 101, no. 22, p. 220405, 2008.

[25] J. H. Chen, C. H. Tan, and X. Y. Li, Practical cryptanalysis of a public key cryptosystem based on the Morphism of polynomials problem, *Tsinghua Science and Technology*, vol. 23, no. 6, pp. 671–679, 2018.

[26] C. Wang, F. Hu, H. G. Zhang, and J. Wu, Evolutionary cryptography theory-based generating method for secure ECs, *Tsinghua Science and Technology*, vol. 22, no. 5, pp. 499–510, 2017.

[27] H. Z. Wang, H. G. Zhang, S. W. Mao, W. Q. Wu, and L. Q. Zhang, New public-key cryptosystem based on the morphism of polynomials problem, *Tsinghua Science and Technology*, vol. 21, no. 3, pp. 302–311, 2016.

[28] D. Połap and M. Woźniak, Voice recognition by neuro-heuristic method, *Tsinghua Science and Technology*, vol. 24, no. 1, pp. 9–17, 2019.

[29] D. J. Bernstein, Introduction to post-quantum cryptography, in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, eds. Berlin, Germany: Springer, 2009, pp. 1–14.

[30] F. Hu, L. Lamata, M. Sanz, X. Chen, X. Y. Chen, C. Wang, and E. Solano, Quantum computing cryptography: Finding cryptographic Boolean functions with quantum annealing by a 2000 qubit D-Wave quantum computer, arXiv preprint arXiv: 1806.08706, 2020.

[31] F. Hu, L. Lamata, M. Sanz, X. Chen, X. Y. Chen, C. Wang, and E. Solano, Quantum computing cryptography: Finding cryptographic Boolean functions with quantum annealing by a 2000 qubit D-Wave quantum computer, *Physics Letters A*, vol. 384, p. 126214, 2020.

[32] A. K. Lenstra, H. W. Lenstra, M. S. Manasse, and J. M. Pollard, The number field sieve, in *Proc. 22nd Annu. ACM Symp. Theory of Computing*, Baltimore, MD, USA, 1990, pp. 564–572.

[33] C. Gidney, Factoring with $n+2$ clean qubits and $n-1$ dirty qubits, arXiv preprint arXiv: 1706.07884v2, 2018.

[34] C. Wang, Y. J. Wang, and F. Hu, Shaping the future of commercial quantum computer and the challenge for information security, (in Chinese), *Chinese Journal of Network and Information Security*, vol. 2, no. 3, pp. 17–27, 2016.

[35] H. P. Liu, D. Guo, F. C. Sun, W. Q. Yang, S. Furber, and T. C. Sun, Embodied tactile perception and learning, *Brain Science Advances*, vol. 6, no. 2, pp.132–158, 2020.

[36] D. Tang, Recent progress in (fast) algebraic immunity of Boolean functions, (in Chinese), *Journal of Cryptologic Research*, vol. 4, no. 3, pp. 262–272, 2017.

[37] W. G. Zhang and E. Pasalic, Constructions of resilient S-boxes with strictly almost optimal nonlinearity through disjoint linear codes, *IEEE Transactions on Information Theory*, vol. 60, no. 3, pp. 1638–1651, 2014.

Xiangmin Ji received the MEng degree from the Graduate School of Chinese Academy of Sciences, China in 2005. He is currently a PhD candidate at the School of Cyber Science and Engineering, Wuhan University, he is also an associate professor at the College of Computer Information Science, Fujian Agriculture and Forestry University. His current research interests include information security, trusted computing, and quantum computing cryptography.

Chao Wang received the MEng degree from Xidian University, China in 1995, and the PhD degree from Tongji University, China in 1999. He is currently a professor and doctoral supervisor at Shanghai University. He is also the vice chair of IEEE China Council. In recent years, he has conducted the first exploratory experiment of the D-Wave quantum computer (principle) to decipher RSA public key cryptography in China, obtained the best indicators of quantum computing attack on public key cryptography in the world. Specifically, he performed the exploratory experiment of designing a cryptographic function with a quantum computer (principle) for the first time in the world to provide an effective way to design a cryptographic function with a Canadian quantum computer and optimize the existing cryptographic results. His current research interests include artificial intelligence, network information security, and quantum computing cryptography.

Baonan Wang received the MEng degree from Anhui University of Science and Technology, China in 2016, and the PhD degree from Shanghai University, China in 2020. She is currently a lecturer at Shanghai University of Electric Power. Her current research interests include information security and quantum computing cryptography.

Feng Hu received the PhD degree from Shanghai University, China in 2019. He is currently an engineer at the Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai University, and also at State Key Laboratory of Cryptology, Beijing. His research interests include information security and quantum computing cryptography.

Huanguo Zhang received the BEng degree from Xidian University, China in 1970. He is currently a professor, a doctoral supervisor, and a chief advisor at the School of Cyber Science and Engineering, Wuhan University. He is a famous scholar in the field of cyberspace security in China and one of the founders of information security. He has undertaken national key and major projects, such as the 973 Program and key projects of the Natural Science Foundation of China. His main research interests include cryptography, cryptographic protocols, and trusted computing.