

An Overview and Concerns Related to Quantum Cryptanalysis: Past, Present, and Future

Subhamoy Maitra , Indian Statistical Institute

Pantelimon Stănică , Naval Postgraduate School

We outline the important quantum algorithms that are instrumental toward cryptanalysis of classical ciphers. Here we attempt to touch on the relevant security issues and explain certain (some low-level) technical points on the cryptographic primitives.

The last few decades have experienced very serious development in the domain of quantum computing and communications. In the 1960s, certain ideas related to the quantum paradigm started revolving in academic and research circles (for example, the development of theories in the early 20th century when the formal models of classical computation were visualized). It took almost half a century to bring together mathematics and physics and achieve technological competence to have commercially working classical computers in the 1960s. Given that several researchers provided formal models of quantum simulators barely four decades back (for example, one may look at Feynman's work¹⁴), we are still in the early days of this tech-

nology. Thus, to understand the timeline, we should note the following points:



- › The physicists understood the basics of quantum mechanics in the early 20th century. This is almost the same time frame when the formal models of the classical computers could be understood.
- › The classical computers were reasonably developed from the technological viewpoint around 1960, and we saw commercially performing ones being deployed. This is the time when researchers started discussing problems related to quantum information and computing, but the formal materials could be produced only in the early 1980s.
- › The 1980s and 1990s provided tremendous research output in the domain of quantum computing and communications but mostly in theory. The outcome of that research effort includes Shor's algorithm,³⁰ which explained a solution to the factorization problem in polynomial time on a quantum infrastructure. On the other hand, solutions could be provided in terms of quantum key distribution (QKD) protocols by Bennett and Brassard.⁵ We must point out that the intellectual development that we have experienced during those two decades is unmatched in terms of fundamental development in quantum paradigm.
- › The current century concentrates toward the actual development of equipment in terms of quantum computing and communication. Unfortunately, marketing gimmicks sometimes misdirect the community to what is exactly achievable in technological terms. The main challenge presently is to understand and interpret the actual development

of commercial products so that the business potential in the near future can be predicted.

INTRODUCTION

We refer to Nielsen and Chuang¹⁹ as a textbook for the basics of quantum information, computing, and communication. The understanding of the present quantum computational scenario may be well understood from the blogs of Scott Aaronson.¹ As we will mostly explain the issues using the basics of Boolean functions, one may have a look at Carlet⁷ and Cusick and Stănică¹¹ as reference materials. A detailed background on cryptologic techniques is available in Stinson,³² for example.

We must point out that the intellectual development that we have experienced during those two decades is unmatched in terms of fundamental development in quantum paradigm.

The organization of this column is as follows. In the section "A Partial List of Relevant Quantum Algorithms," we discuss the most relevant quantum algorithms that are crucial for cryptanalytic purposes. Then, in the section "Limitations in Implementing Quantum Algorithms," we consider the actual limitations in applying such techniques for actual cryptanalysis. We conclude that while the commercial world should be prepared for quantum adversarial situations, we do not see immediate danger in the existing security products given the current hardware development in this domain.

A PARTIAL LIST OF RELEVANT QUANTUM ALGORITHMS

In this section, let us first explain a few basic quantum algorithms. The Deutsch-Jozsa problem¹² is one of the

most celebrated algorithm as it is easy to understand and provides the initial result to explain the power of quantum computation. Given a black box that takes n bits as inputs and outputs only one bit, the quantum algorithm proposed by Deutsch and Jozsa can distinguish whether the black box produces a balanced (no bias: the same number of 0 and 1) Boolean function or a constant one using a linear amount of quantum resources over n and in constant time. Note that to understand whether a function is constant or balanced, one needs to query the function $2^{n-1} + 1$ times in the worst case for the classical domain. In fact, this is quite an easy problem, and we can obtain solutions

with a randomized algorithm up to a very good accuracy using a polynomial with many queries in n . However, when we talk about the deterministic classical algorithm, the worst case requirement is exponential. Thus, this algorithm demonstrates the power of the quantum paradigm over the classical one. In fact, one may note that the Deutsch-Jozsa algorithm actually produces the superposition of states with the Walsh spectrum coefficients as the amplitudes. This is explained clearly in Maitra and Mukhopadhyay.¹⁸ In this direction, such types of techniques may be exploited in linear cryptanalysis as the Walsh spectra are related to the approximation of linear functions.

The next important technique to discuss is Grover's algorithm.¹⁶ Consider as above that a black box contains a Boolean function on n variables

having a single output. Say the function outputs 1 only for a single input, and the rest of the outputs are zero. Naturally, for a classical algorithm, it will require 2^n queries in the worst case. Grover's algorithm solves this in $O(2^{n/2})$, which is a square-root improvement, which is achieved in the quantum framework. This algorithm has several implications. First of all, this can be used to reduce the search effort in an unsorted list of N elements to a time of $O(\sqrt{N})$ through quantum algorithms. The other consequence of this is that the security of all of the symmetric ciphers is reduced to half the key size in a generic manner. Assume that the secret key size of a cipher is k in bits. Then a generic attack in the classical domain will require an exhaustive search over all of the keys, that is, a $O(2^k)$ effort. On the other hand, using Grover's algorithm, this can be achieved in $O(2^{k/2})$ queries. For all practical purposes, handling this situation is not a problem as the key size needs to be doubled. The proper designs of stream and block ciphers are possible keeping this in mind, and the overall hardware requirement or the software clocks required for execution will increase only by a constant proportion.

Let us now explain Simon's algorithm.³¹ The setting of this algorithm is almost the same as the above algorithms, with the difference that here we consider multiple output Boolean functions. That is, for the function f , the number of input bits is n , and that of output is $k \geq n/2$. The promise is that for any two arbitrary n -bit inputs, $f(x) = f(y)$ if and only if $x = y \oplus s$ for some fixed $s \in \{0, 1\}^n$. Naturally, the all-zero s is the obvious solution, but the non-trivial question is to obtain the non-zero s . While in classical domain, such solutions can be achieved in $O(2^{n/2})$ queries to the black box, Simon's algorithm solves this in $O(n)$ quantum queries only. This problem is relevant in differential cryptanalysis against a symmetric cipher, as well as obtaining collisions of a Hash function. A

detailed discussion of the above three algorithms and their implementations in Qiskit^{17,23} are available in Tharmashastha et al.³³

We next refer to the concept of Forrelation.² This was used in the seminal paper by Aaronson and Ambainis² to show that the Forrelation problem demonstrates constant versus exponential separation of query complexity in the bounded error quantum and the probabilistic classical model. It has also been noted recently¹³ that these types of techniques may be exploited to obtain different properties related to the Walsh transform as well as auto and cross-correlation of Boolean functions. In fact, the Forrelation problem estimates the correlation between a Boolean function and the Walsh spectrum of the other. Choosing the functions properly, an efficient quantum algorithm can be devised to obtain the weaknesses of Boolean functions that can be exploited in linear as well as differential cryptanalysis.

Certainly, the most impactful result in this domain of research is Shor's quantum factorization algorithm.³⁰ While subexponential algorithms are known for factorization on classical machines, they are intractable for large instances. That is why they form the basis of several public key cryptosystems. On the other hand, Shor's technique solves these efficiently with a polynomial number of gates on a quantum computer. In fact, an n -bit integer, which is a product of two large primes, can be factorized using Shor's technique in an effort of $O(n^2 \log n)$. A similar situation happens for different variants of the discrete log problem, where the classical algorithms are subexponential, making them secure in the classical paradigm. However, following Shor's technique, all such classical algorithms are insecure against quantum adversaries. The core of this algorithm is related to an efficient computation of the quantum Fourier transform.

Before proceeding further, we want to point out two issues:

- ▶ Following on the algorithms discussed above, a tremendous effort has been put forward in this domain, and several other cryptanalytic algorithms have been developed. In fact, combining these techniques and with some related advancements, several attacks on symmetric ciphers have been proposed in the last decade. A summary of such attacks is available in Tharmashastha et al., chapter 5.³³ To resist such attacks, new cryptosystems are being designed keeping quantum adversaries in mind. There are two main directions. One is producing classical algorithms that can resist quantum attacks. For example, classical algorithms related to public key cryptosystems have passed through a stringent public evaluation to provide a portfolio as available in the National Institute of Standards and Technology (NIST) suite.²¹ In the other direction, there are quantum strategies, such as QKD,⁵ that can resist such attacks. The development of QKD equipment has reached a good commercial standard, as evident from the products of ID Quantique.^{26,27}
- ▶ The other issue is an application of the quantum algorithms in different areas such as machine learning. These algorithms are not in the scope of this discussion, but one may refer to the Quantum Algorithm Zoo²⁵ for an updated list of various quantum algorithms.

LIMITATIONS IN IMPLEMENTING QUANTUM ALGORITHMS

Since the beginning of this millennium, researchers have initiated a long-term plan toward the implementation of a quantum computer. It must be noted that certain theoretical concepts such as a Turing machine can be used as a mathematical model. However, transforming the necessary physics to

actual technology requires decades to perhaps centuries to actually design and implement the machines. The development of classical computers succeeded at an outstanding pace in less than a century. We are not sure whether a similar development could be achieved for commercial quantum computers or even if it might be faster. Experimentalists are mostly concentrating on technologies exploiting trapped ions³ or superconductors.⁴ While in this column, we will not get into those experimental details, it is important to highlight that the main technological bottleneck is to obtain a noise-free environment in quantum computers. A detailed idea in this regard may be available from Preskill,²² containing a survey on noisy intermediate-scale quantum (NISQ) technology. The most important comment from the abstract of that survey is quoted below:

“Quantum computers with 50–100 qubits may be able to perform tasks which surpass the capabilities of today’s classical digital computers, but noise in quantum gates will limit the size of quantum circuits that can be executed reliably.”

Thus, the most important question is related to reliable and noise-free computation. The technology will only be able to compete with high-speed classical computers having multiple cores when the errors during the preparation, processing, and measurements of the qubits can be minimized. Each of these parts might have noisy behavior, but the idea of fault-tolerant quantum computation may guarantee scalability under certain conditions. Several concepts related to fidelity need to be studied in this regard.²⁹ That is the reason the concept of quantum supremacy is being demonstrated only on a few benchmark problems. Indeed, that has an impact on the future planning for the quantum industry (see, for example, technologies based

upon quantum annealing), but so far, we are yet to experience any public domain commercial demonstration that can transparently convince the common people of a better result than a classical setup.

Quantum attacks on symmetric ciphers

With this context, let us now concentrate on the present cryptanalytic efforts on symmetric ciphers. The symmetric ciphers have a key of n bits, where generally, n is taken as 128, 256, 384, or 512 bits. For some lightweight stream ciphers, it may be as low as 80. A design is generally accepted through some process of evaluation (such as public competitions⁹ or peer reviews). The designs of symmetric key cryptosystems are generally not provable, and they are adopted, based on assessments of cryptanalytic techniques by the community. If one can produce an attack in less time than the exhaustive key search effort of $O(2^n)$, then generally, that cipher is deprecated. One may refer to the history of the RC4 in this regard.²⁰ Thus, if there exist substantial cryptanalytic results against a cipher, either in the classical or in the quantum domain, then the cipher should not be used further (although there are exceptions to the rule: for example, still using 3DES, after its retirement about 20 years ago, since some countries do not have the resources to upgrade their security infrastructure).

On the other hand, the parameter of $O(2^n)$ that appears from the exhaustive search in the classical paradigm is not the benchmark given a quantum adversary. As we have discussed in the section “A Partial List of Relevant Quantum Algorithms,” exploiting Grover’s algorithm,¹⁶ we can have a generic attack on a symmetric cipher in $O(2^{n/2})$ time complexity. Thus, to have m -bit security against the quantum adversary, we need to employ $2m$ -bit-long keys to attain a security of $O(2^m)$. This is achievable with new designs based on the current works. That is, to have 512-bit security using some models of

Advanced Encryption Standard (AES), one requires a design with a 1,024-bit secret key. Naturally, the hardware circuit size will increase, or the software will take a little more time, but the design is achievable without much hassle. The main problem is the vast deployment of such a new algorithm, which we will discuss in the conclusion.

Now it is important to understand the resource required to mount a Grover’s algorithm-based¹⁶ generic attack as explained in Bonnetain et al., lemma 3.⁶ The authors pointed out that using Grover’s search and three classical queries to an eight-round AES-256 oracle, the key can be recovered in approximately $2^{138.04}$ reversible S boxes with approximately 1,500 qubits. Surely, given the present NISQ technology, such an attack is not practically possible. On the other hand, such a clear description of the attack shows that we need to be careful regarding the future, and thus, it is better to be prepared with symmetric key algorithms with larger key sizes.

Quantum attacks on public key cryptosystems

The most significant results related to the quantum algorithm are those of Shor.³⁰ Naturally, the famous RSA and other key agreement algorithms using elliptic curves will be completely attacked with this theory. The next question is related to actual implementation that can identify the effect in the commercial space. A very detailed analysis in this regard is available in Gidney and Ekeru,¹⁵ where it is argued “how to factor 2048 bit RSA integers in 8 h using 20 million noisy qubits.” Thus, it is quite clear that we need to wait for quite some time before such hardware is available. However, the threat has persisted since 1994, when Shor’s factorization was published. Thus, during 2010–2015, the U.S. National Security Agency kept releasing major policy statements on the need for postquantum cryptography.¹⁰ One of the excerpts is as follows:

“For those partners and vendors that have not yet made the transition to Suite B algorithms (Elliptic curve cryptography), we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition ...”

In this regard, NIST recently selected some (quantum-resistant) algorithms²¹ as follows:

- public key encryption and key establishment algorithms, including CRYSTALS-KYBER, submitted by Peter Schwabe, Roberto Avanzi, Joppe Bos, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, Damien Stehle, and Jintai Ding
- digital signature algorithms, including CRYSTALS-DILITHIUM, submitted by Vadim Lyubashevsky, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehle, and Shi Bai; FALCON, submitted by Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang; and SPHINCS+, submitted by Andreas Hulsing, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kolbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, Jean-Philippe Aumasson, Bas Westerbaan, and Ward Beullens.

Note that these are all classical algorithms and so far considered to be secure against quantum adversaries. It is important to clarify one more issue here. In the same move, NIST listed

four additional algorithms as potential replacements pending further testing with the idea that some of them may also be suitable encryption alternatives in a postquantum world. Unfortunately, one of the additional algorithms, Supersingular Isogeny Key Encapsulation, was broken quite early,⁸ which underlines that experts should be more careful in analyzing the new cryptographic algorithms designed for the postquantum world.


However, after the effort taken by NIST,²¹ the world is now equipped with a portfolio of quantum algorithms, and the main issue relates to efficient implementations. Noting that these are only classical algorithms that can resist quantum adversaries, efficient implementations are already geared up, and presently, there is a lot of effort in this direction. One may refer to another survey²⁸ in this regard. We close this part of the discussion with a general question in laymen’s language: “Should we believe that quantum computers will crack the Bitcoin blockchain? If yes, when?” This question actually takes care of the postquantum effect of a very popular application, and hence, this is important for market-related issues. Based on the discussion so far, the answer should be as follows. The present blockchain technology mainly uses two cryptologic primitives: 1) Hash function SHA-256 and 2) ECDSA Public Key Cryptosystem based on elliptic curves. Theoretically, SHA-256 is relatively secure, but ECDSA is completely broken against quantum adversaries. However, for all practical purposes, the actual implementation of the attacks on a commercially available quantum platform is still elusive. On the other hand, given the availability of postquantum algorithms, there might be certain replacements of the above two cryptographic primitives, and then the modified blockchain framework will be completely secure against the quantum adversaries.

Quantum equipment

We have so far discussed recent developments of classical cryptographic

primitives that can resist quantum attacks. However, since the 1980s, the world has experienced a huge amount of development of systems that came out of quantum phenomena. The simplest circuit in this regard is the quantum true random number generator (QTRNG) with applications in different domains such as the generation of one-time pads, in different kinds of lotteries, etc. Low-cost QTRNGs (we refer to ID Quantique,²⁴ for example) are available at a cost of around US\$2,000 or less that can be connected to classical computers in obtaining data. However, there are several research questions related to quantumness as well the true randomness of such devices.

The most important among those is the domain of QKD, which was initiated in Bennett and Brassard.⁵ It provides a method so that two parties can agree to a shared random secret key available only to them, which can be used to encrypt and decrypt messages later with a symmetric key cryptosystem. This outlines a public key kind of infrastructure based on quantum phenomena such as superposition, no-cloning, and entanglement. The main idea here is achieved through the inherent property of a qubit, that any attempt to gain information by an adversary will be understood by the two communicating parties. The initial demonstration of QKD could be presented in the last century itself, and for more than a decade, such equipment has been available in the commercial domain.^{26,27} Different directions are being considered, and the recent trend is to study device-independent schemes, which are popularly known as DI-QKD.³⁴ Various experimental demonstrations of QKDs have been studied for very long distances and even for space applications. In a related topic, there are concepts of quantum repeaters that are integral parts of long-distance quantum networks. Quantum secure communication is showing a lot of promise based on different quantum equipment, but we limit our discussion as this is not the main focus of this column.

To conclude, we want to highlight that the research and development related to quantum information has reached a juncture with huge investments, and it seems that it will continue for at least one more decade. Less excitement might be generated if the development of computing infrastructure becomes slow. However, as we already have a lot of classical cryptographic algorithms that can resist quantum attack, those will be deployed in the near future. That is, irrespective of whether a quantum computer arrives soon, these cryptanalytic results will drive the community to accept new algorithms. That deployment, in any case, will keep the domain of postquantum cryptography running. In the case where we have a commercial quantum computer that is substantially noise-free, the world may see revolutionary changes in technology. It would have a much larger impact than even what we have seen in classical computing and communication in the last half century. Due to huge computational efficiency, new quantum algorithms will appear in the market for all kinds of applications. Correspondingly, new security questions will arise. The field of quantum communication has already matured to some extent, and thus, it seems that the quantum technology, if it advances in the domain of computation quite quickly, will not be limited by the communication counterpart. 

REFERENCES

1. S. Aaronson. "Shtetl-optimized." Accessed: Jul. 20, 2023. [Online]. Available: <https://scottaaronson.blog/>
2. S. Aaronson and A. Ambainis, "Forrelation: A problem that optimally separates quantum from classical computing," *SIAM J. Comput.*, vol. 47, no. 3, pp. 982–1038, Jun. 2018, doi: 10.1137/15M1050902.
3. C. J. Ballance, T. P. Harty, N. M. Linke, M. A. Sepiol, and D. M. Lucas, "High-fidelity quantum logic gates using trapped-ion hyperfine qubits," *Phys. Rev. Lett.*, vol. 117, no. 6, Aug. 2016, Art. no. 060504, doi: 10.1103/PhysRevLett.117.060504.
4. R. Barends et al., "Superconducting quantum circuits at the surface code threshold for fault tolerance," *Nature*, vol. 508, no. 7497, pp. 500–503, Apr. 2014, doi: 10.1038/nature13171.
5. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst., Signal Process.*, Bangalore, India: IEEE, 1984, pp. 175–179.
6. X. Bonnetain, M. Naya-Plasencia, and A. Schrottenloher, "Quantum security analysis of AES," *IACR Trans. Symmetric Cryptology*, vol. 2, pp. 55–93, Jun. 2019, doi: 10.46586/tosc.v2019.i2.55-93.
7. C. Carlet, *Boolean Functions for Cryptography and Coding Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2021.
8. W. Castryck and T. Decru, "An efficient key recovery attack on SIDH (Preliminary Version)," Jul. 2022. [Online]. Available: <https://eprint.iacr.org/2022/975.pdf>
9. "Cryptographic competitions." Accessed: Jul. 20, 2023. [Online]. Available: <https://competitions.cr.yt.to/>
10. "Cryptography today," National Security Agency, Fort Meade, MD, USA, Nov. 2015. [Online]. Available: <https://tinyurl.com/SuiteB>
11. T. W. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications*, 2nd ed. New York, NY, USA: Academic, 2017.
12. D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proc. Roy. Soc. A Math. Physical Eng. Sci.*, vol. A439, pp. 553–558, Dec. 1992, doi: 10.1098/rspa.1992.0167.
13. S. Dutta, S. Maitra, and C. S. Mukherjee, "Following Forrelation – Quantum algorithms in exploring Boolean functions' spectra," *Adv. Math. Commun.*, early access, Jan. 2022, doi: 10.3934/amc.2021067. [Online]. Available: <https://www.aimsociences.org/article/doi/10.3934/amc.2021067>
14. R. P. Feynman, "Simulating physics with computers," *Int. J. Theor. Phys.*, vol. 21, nos. 6–7, pp. 467–488, Jun. 1982, doi: 10.1007/BF02650179.
15. C. Gidney and M. Eker, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, Apr. 2021, Art. no. 433, doi: 10.22331/q-2021-04-15-433.
16. L. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. Symp. Theory Comput. (STOC)*, May 1996, pp. 212–219, doi: 10.1145/237814.237866.
17. "IBM quantum experience." IBM Quantum. Accessed: Jul. 20, 2023. [Online]. Available: <https://quantum-computing.ibm.com/>
18. S. Maitra and P. Mukhopadhyay, "Deutsch-Jozsa algorithm revisited in the domain of cryptographically significant Boolean functions," *Int. J. Quantum Inf.*, vol. 3, no. 2, pp. 359–370, 2005, doi: 10.1142/S0219749905000980.
19. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. New York, NY, USA: Cambridge Univ. Press, 2010.
20. A. Popov, "Prohibiting RC4 cipher suites," Internet Engineering Task Force, Wilmington, DE, USA, RFC 7465, Feb. 2015. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc7465>
21. "Post-quantum cryptography – Selected algorithms," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, 2022. [Online]. Available: <https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022>
22. J. Preskill, "Quantum computing in the NISQ era and beyond," 2018. [Online]. Available: <https://arxiv.org/abs/1801.00862>
23. *The Programming SDK*. (2023). Qiskit. [Online]. Available: <https://qiskit.org/>
24. "Quantis QRNG chips." IDQ. Accessed: Jul. 20, 2023. [Online]. Available: <https://www.idquantique.com/random-number-generation/products/quantis-qrng-chips/>

25. "Quantum algorithm zoo," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, 2022. [Online]. Available: <https://quantumalgorithmzoo.org/>
26. "Quantum key distribution equipment." ID Quantique. Accessed: Jul. 20, 2023. [Online]. Available: <http://www.idquantique.com/>
27. "Quantum key distribution system (Q-Box)," MagiQ Technol. Inc., Somerville, MA, USA, 2023. [Online]. Available: <https://www.maqiqtech.com/solutions/network-security/>
28. P. Ravi, A. Chattopadhyay, and S. Bhasin, "Security and quantum computing: An overview," in *Proc. 23rd IEEE Latin Amer. Test Symp. (LATS)*, Montevideo, Uruguay, Sep. 2022, pp. 1–6, doi: 10.1109/LATS57337.2022.9936966.
29. Y. R. Sanders, J. J. Wallman, and B. C. Sanders, "Bounding quantum gate error rate based on reported average fidelity," *New J. Phys.*, vol. 18, no. 1, Jan. 2016, Art. no. 012002, doi: 10.1088/1367-2630/18/1/012002.
30. P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.
31. D. R. Simon, "On the power of quantum computation," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1474–1483, May 1997, doi: 10.1137/S0097539796298637.
32. D. Stinson, *Cryptography Theory and Practice*, 3rd ed. London, U.K.: Chapman & Hall, 2005.
33. S. A. P. V. Tharrmashastha, D. Bera, A. Maitra, and S. Maitra, *Quantum Algorithms for Cryptographically Significant Boolean Functions: An IBMQ Experience*. Singapore: Springer Singapore, 2021.
34. U. Vazirani and T. Vidick, "Fully device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 113, no. 14, Oct. 2014, Art. no. 140501, doi: 10.1103/PhysRevLett.113.140501.

SUBHAMOY MAITRA is a senior professor at the Applied Statistics Unit, Indian Statistical Institute, Kolkata 700108, India. Contact him at subho@isical.ac.in.

PANTELIMON STĂNICĂ is a professor in the Applied Mathematics Department, Naval Postgraduate School, Monterey, CA 93943 USA. Contact him at pstanica@nps.edu.



IEEE Security & Privacy magazine provides articles with both a practical and research bent by the top thinkers in the field.

- stay current on the latest security tools and theories and gain invaluable practical and research knowledge,
- learn more about the latest techniques and cutting-edge technology, and
- discover case studies, tutorials, columns, and in-depth interviews and podcasts for the information security industry.



computer.org/security

