REVIEW ARTICLE

Quantum Cryptography for Securing Personal Health Information in Hospitals

Harshvardhan Mantry[1], Akhil Maheshwari[2]

Received on: 03 November 2022; *Accepted on:* 10 November 2022; *Published on:* 23 December 2022

Abstract

Healthcare systems widely use information technology (IT) for system authentication (digital signatures), web surfing, e-mails, instant messaging, protecting data at rest, Voice over Internet Protocol (VoIP) telephony, and cellular telephony. To protect patient identification and healthcare information, cryptographic systems are widely used to secure these data from malicious third parties (adversaries). In our healthcare systems, we have had reasonable success in the efficient storage of the information of our patients and their families, in its timely retrieval, and in ensuring its safety from adversaries. However, the data are increasing rapidly and our current computational systems could be inadequate in the not-so-distant future. In this context, there is a need for novel solutions. One possibility can be seen in quantum computing (QC) algorithms/devices that can provide elegant solutions based on subatomic interactions. In this review, we have summarized current information on the need, current options, and future possibilities for the use of QC algorithms/devices in large data systems such as healthcare. This article combines peer-reviewed evidence from our own clinical studies with the results of an extensive literature search in the databases PubMed, EMBASE, and Scopus.

Keywords: Cryptographic systems, Health information, Healthcare, Hospital, Newborn.

Newborn (2022): 10.5005/jp-journals-11002-0043

Highlights

- In our healthcare systems, we have had reasonable success in the efficient storage of the information of our patients and their families, in its timely retrieval, and in ensuring its safety from adversaries. However, the data are increasing rapidly and our current computational systems could be inadequate in the not-so-distant future.
- In this article, we have reviewed possible solutions based on QC algorithms/devices that can provide elegant solutions based on subatomic interactions.
- Quantum cryptography focuses on protecting patient health information (PHI). During the transfer, data are first encrypted (encoded) and the recipient then decrypts (decodes) the information.
- Details of various methods of encrypting and decrypting have been provided. Current information on various protocols for QC has been summarized, and future possibilities have been discussed.

Introduction

Healthcare systems widely use IT for system authentication (digital signatures), web surfing, e-mails, instant messaging, protecting data at rest, VoIP telephony, and cellular telephony.[1–3] To protect patient identification and healthcare information, cryptographic systems are widely used to secure these data from malicious third parties (adversaries).[4,5] Several strong encryption algorithms are well-known, such as the secure hash algorithm (SHA)-1, SHA-2, triple data encryption algorithm system (TripleDES), advanced encryption standard (AES), message digest (MD)-5, and Rivest–Shamir–Adleman (RSA, named after the last names of Ron Rivest, Adi Shamir, and Leonard Adleman).[6–9] Conventional cryptographic algorithms have been used in our healthcare system, but these systems are now beginning to show limitations with the ever-increasing amounts of private information being accrued and produced.[7] These difficulties are particularly important in mother–infant and neonatal intensive care units (NICUs) as there is a need to secure the personal health information (PHI) that has been obtained from the whole family.[10,11]

In our healthcare systems, we have had reasonable success in the efficient storage of the information of our patients and their families, in its timely retrieval, and in ensuring its safety from adversaries.[12] However, the data are increasing rapidly and our current computational systems could well become inadequate in the not-so-distant future.[13] In this context, there is a need for novel solutions. One possibility can be seen in QC algorithms/devices that can provide elegant solutions based on subatomic interactions.[14] These devices resemble classical computers in the need for a defined input, and processing of data, and show a recognizable output, but do not need conventional digital semiconductor processors with interface busses and external networks.[14] Unlike conventional devices, a fully-functional QC algorithm/device might paradoxically show an exponential increase in its capacity to process

[1]Department of Physics, University of Illinois at Urbana-Champaign, Urbana, Illinois, United States of America

[2]Global Newborn Society, Clarksville, Maryland, United States of America

Corresponding Author: Harshvardhan Mantry, Department of Physics, University of Illinois at Urbana-Champaign, Urbana, Illinois, United States of America, Phone: +1 4479021019, e-mail: harshvardhanmantry.28@gmail.com

How to cite this article: Mantry H, Maheshwari A. Quantum Cryptography for Securing Personal Health Information in Hospitals. Newborn 2022;1(4):333–339.

Source of support: Nil

Conflict of interest: None

data.[15–19] These should be able to handle the increasing workload in progressively smaller intervals of time that might eventually become nearly immeasurable.[13,14,19–22] Many of these devices currently do show high margins of errors, but encouragingly, many potential solutions can now also be seen.[23]

The QC models have brought exciting possibilities for outcomes prediction in many situations with large datasets, such as in hurricanes, global warming, forest fires, and pandemics.[24] These non-canonical prediction models have shown new possibilities for improving the efficiency and prediction of outcomes in our healthcare systems.[14,24] The QC systems can help analyze large, private patient datasets without the risks of decryption.[7,25] A staggering number of implausible events could possibly be solved if we can develop mechanisms to manage entropy related to multiple concurrent events and lower the error rates to levels that we tolerate in our current electronic semiconductor systems.[13,26–28] The only dilemma is whether we are ready in our technological quest for solutions to accept probabilities instead of certainties.[29,30] In this review, we have described the need, current options, and future possibilities for the use of QC algorithms/devices in large data systems such as healthcare.

Need

In the last two decades, technological advances in electronic medical records (EMRs), continuous monitoring of vital signs, telehealth, and affordable at-home testing devices have improved neonatal care.[31–33] With families' consent, sharing of the data obtained from these devices can improve efficiency in patient care and minimize errors.[32,34] Healthcare providers can utilize these real-time data not only to improve patient care but also for clinical research focused on recording outcomes and drug trials.[35] Families' satisfaction can also be recorded, and education can be more focused and improved. Diagnostics can also be evaluated with greater conviction by an improved recording of data and coordination between various medical subspecialties. Findings can also be analyzed better using newer modalities such as machine learning (ML). The entire health sector can become more data-driven.[35]

The concerns are that all the above-mentioned datasets contain the PHI of the patients in electronic health records (EHRs)/EMRs, medical devices, computers, the cloud, emails, servers, databases, and other associated systems.[5,36] These detailed data make the healthcare sector easy prey to cyberattacks.[5,17,36] The hospital systems and medical companies need to retain the trust of the infants' families by focusing on patient security and access to their data. The Health Insurance Portability and Accountability Act (HIPAA) is one important example of legislation that outlines the maintenance of PHI and the protection of identity from fraud/theft.[37–39] The HIPAA journal[40] reports an unsettling trend, showing a conspicuous rise in the number of healthcare records getting exposed every year.[41] According to the data breach statistics published so far, 2015 has been one of the worst years with more than 113.27 million records being exposed. Nobody wants to remember the infamous "WannaCry" malware attacks of May 2017 with data breaches in the British National Health Service and many reputable medical companies in the USA information.[42] Investigations showed loss of information such as dates of birth, credit card information, social security numbers, addresses, email IDs, and phone numbers, which were sold on the dark web; some patient records fetched up to US$1000. According to the US Department of Health and Human Services, such deliberate hacking accounts for about 75% of healthcare breaches.[43] The affected people continue to face the brunt for the rest of their lives.

Mother–infant units and NICUs are high-priority areas in hospitals where the PHI needs to be secured.[44] Infants and their families are a heterogeneous population, with varying capacities to protect their identifiers and their social, financial, and health information.[45] Mothers and other family members are at risk of developing transient psychological conditions which might affect their employability even after they have fully recovered.[46] Infants are a uniquely vulnerable population because of limitations in their legal rights and capacities for autonomous decision-making.[47] This means that special provisions are needed to ensure their protection from these risks, which include, but do need to extend beyond parental proxy consent on their behalf.[47,48] We also need special considerations in the storage of biomedical information because of the sensitive nature of such data, and the potential immediate and longer-term implications of PHI in the context of family dynamics.[48] These require immediate determinations about who has access to, and control over, the infants' PHI that can alter the life course of these children.[48,49]

Cryptography

Overview of Modern Cryptography

The term cryptography was derived from two Greek roots, *kryptos* meaning secret, and *graphein* meaning to study/write. The composite word, cryptography, refers to the art of securing private communications in presence of an eavesdropper or adversary.[50] Messages are secured by first "encrypting" the plain text into a cipher (a way of disguising in code) in a message that is then sent to the recipient.[51] The recipient "decrypts" the message from cipher to plain text using a tool for back translation, usually referred to as a "key."[52] This process reduces the risk of loss of important information. Cryptography is broadly classified into two categories: Private/symmetric key cryptography and public/asymmetric key cryptography.[53]

- **Private/symmetric key cryptography:** In private systems, a single key is used for both encryption and decryption, hence the name symmetric. In one experiment, one of two members of the team wants to send a sequence of bits, 0110100 to another with the shared key 1110101.[54] She/he encrypts the message using a bitwise "XOR" operation (a logical operation that stands for "exclusive or"). The encrypted message looks like 1000001. An eavesdropper who does not have access to the key fails to comprehend the message while the original recipient can decrypt it by applying the "reverse XOR" operation, yielding the message sequence bits 0110100. This is a classic example of a one-time pad encryption technique.
- **Public key cryptography:** Public systems are more complex than private key cryptography.[55] The team members use more than one key for sending different messages to reduce the chances of hacking. The public key may include two mathematically-related keys, one (public) used for encrypting that can be made freely available, and another (private) key that is protected and is needed for decrypting. The private key is usually derived using complex, more sophisticated mathematical systems. Besides the Diffie–Hellman key exchange protocol,[56] two other public key encryption techniques are the RSA and the Elliptic

Curve Cryptography (ECC).[57,58] Trapdoor functions that are easy to compute in one direction but not in the other, are used extensively to build public key cryptosystems.[59,60]

Advanced Encryption Standard

Advanced encryption standard is a kind of symmetric block cipher that cuts input data into chunks of fixed length and encrypts using a key.[61,62] This is currently being used in government agencies to protect the data encryption standard (DES), another symmetric key encryption algorithm that uses a key of only 56 bits.[63] Even though it is vulnerable to quantum attacks, higher AES key lengths with compounded complexity increase its safety.

Rivest–Shamir–Adleman Encryption

In the RSA encryption systems, it might be possible to create a public key such as the product of two large prime numbers, p and q.[64] The encoding value may be large, c. Since the prime numbers are kept secret, most observers will be able to encrypt a message but only an operator who knows the primes will be able to decrypt it. The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, which serves as its trapdoor function.[65]

Elliptic Curve Cryptography

Elliptic curve cryptography is the study of mathematical properties of elliptic curves, which are a set of points (x, y), where $y^2 = x^3 + ax + b$.[58] The variables a and b belong to a field K that may be made up of real, rational, or complex numbers. Fields are important algebraic structures that permit the application of certain operations on the members of the field. Elliptic curves use shorter keys to optimize memory storage.[66] For example, the security provided by a 256-bit key in ECC is comparable to a 3,072-bit key in RSA.

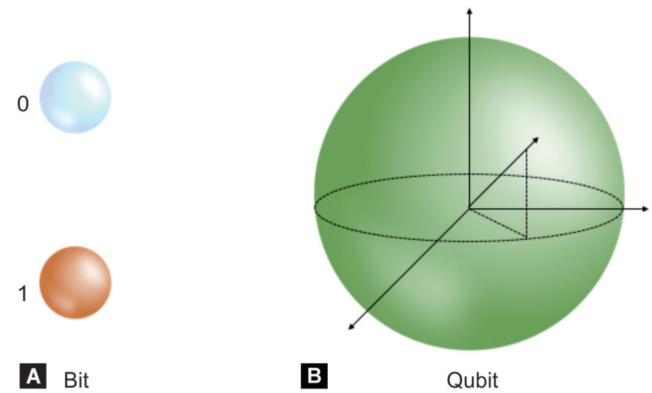
Quantum Computing

With the increasing number of transistors being used in a given chip, the speed of classical computers has increased but there are limits posed by the laws of quantum mechanics.[18,67] Classical computers are known to operate on a binary string of "bits," which are referred to as zeros and ones, and notated as "kets" (Dirac notations) $|0\rangle$ and $|1\rangle$.[68,69]

The key distinguishing feature of a quantum computer is referred to as a "qubit."[70] Figure 1 show a schematic representation of bits and a qubit. Each qubit is a superposition of two independent unit vectors in a 2-dimensional space and can be represented by the column vectors.[71] In other words, $|0\rangle$ and $|1\rangle$, which are independent unit vectors, would make our choice for the bases of the 2-dimensional vector space.[71] A $2n$ dimensional vector space would be having $2n$ basis vectors. In summary, a qubit state is a superposition of the two basis vectors such that the vector is normalized.[72]

Tensor Product

Tensor product (TP) results from an interaction between ≥2 qubit states. This concept helps us mathematically characterize the phenomenon of quantum entanglement (QE) (*vide infra*).[73] This needs to be differentiated from TensorFlow quantum (TFQ), which is a quantum ML library for rapid prototyping of hybrid quantum–classical ML models.[74]



Figs 1A and B: (A) A classical binary bit can only represent a single binary value, such as 0 or 1, meaning that it can only be seen in one of two possible states (off or on, false or true, low or high). Classical computing devices manipulate those bits with the help of logical gates (AND, OR, NOT); (B) In QC, a qubit or quantum bit is the basic unit of quantum information. It is a two-state quantum-mechanical system, represented by a superposition to achieve a linear combination of two states. Information is stored in quantum bits, or qbits. A qbit can be in states labelled |0> and |1>, but it can also be in a superposition of these states, a|0> + b|1>, where a and b are complex numbers. If we think of the state of a qbit as a vector, then superposition of states is just vector addition. Every extra added qbit can help store twice as many numbers. For example, with 3 qbits, it is possible to get coefficients for |000>, |001>, |010>, |011>, |100>, |101>, |110> and |111>

Quantum Entanglement

Quantum entanglement is a physical phenomenon seen in quantum physics, but not in classical mechanics. QE is seen when the physical properties of two particles such as position, momentum, spin, and polarization are perfectly correlated, even when these particles are separated by a large distance.[75] In this situation, the total spin of these two particles will be predictable.[76] Measurements of a particle's properties will result in an irreversible wave function collapse of that particle and will change the original quantum state, affecting the entangled system as a whole.[76]

Measurement Postulate

The MP in quantum mechanics pertains to the degree the wave function collapse occurs.[77] According to the Schrödinger equation, which describes the wave function in a quantum-mechanical system, the wave function evolves deterministically as a linear superposition on different states.[78] In other words, after one initial observation, all subsequent measurements remain consistent with these first-time observations.

No-cloning Theorem

This admits our inability to clone any arbitrary quantum state into multiple copies of itself.[79] If we could, this would have informed us about the behavior and properties of the state by applying different measurement operators to the state countless times. Despite all the measurements, we would always have information about the initial state.

Quantum Algorithms

Quantum algorithms are a set of instructions run on quantum computers similar to how classical algorithms are meant for classical computers.[80] The two most popular quantum algorithms are Shor's algorithm and Grover's algorithm.[81,82] Shor's algorithm is an algorithm for finding the prime factors of an integer using a specific unitary operator. Unfortunately, this algorithm can undermine the security of RSA and ECC due to program-related issues.

Modular arithmetic can provide insights into these algorithms. Grover's algorithm, also known as the quantum search algorithm, is a quantum algorithm that can reduce the time needed for an unordered search.[83,84] Simply put, an unordered search refers to searching for a particular element in a random list of elements such that no guess would bring us closer to the element we are looking for. The obvious way to do this would be to start from the first element and move onwards. Grover's algorithm can improve these searches as it is based on the properties of superposition, entanglement, and interference.[82] There is a special qubit gate called oracle which takes the input state and flips the phase of the chosen ket we are looking for and another gate which inverts the amplitudes of all the component kets about the mean of all the associated amplitudes.[85] However, all problems are still not resolved, and some limitations might appear when full-fledged quantum computers become a reality. Many algorithms such as Deutsch–Jozsa, Bernstein–Vazirani, Simon, quantum Fourier transform, quantum phase estimation, quantum counting, quantum walk search, and dense coding are being investigated.[86–91]

Quantum Key Distribution

The quantum key distribution (QKD) is a secure channel for encryption and decryption using the principles of quantum mechanics. The main tenets of quantum mechanics that makes QKD secure is the measurement postulate, where measurements of an unknown quantum system lead to a change in its state and any information about the initial state is lost after the measurement.[92] There are also possibilities of changes related to the no-cloning theorem and entanglement.

The BB84 Protocol

Named after its creators, Charles Bennett and Giles Brassard, BB84 is a quantum protocol used to generate a private key.[93] In this protocol, the first observer takes a series of qubits and performs any one of two orthogonal measurements on each qubit, such as the measurement of spin in the x and z directions. The first then send those to the second, who repeats the same job. The first operator, however, does not inform the second about which measurements were made and so the second operator will likely measure 50% of the qubits in the same manner as the first operator. After performing the experiments, they could publicly announce their readings and discard the measurements where they differ. The remaining set of measurements becomes their private key. An eavesdropper could then make major efforts to intercept the message qubit but due to the measurement postulate, she/he will be changing the qubit nearly 50% of the time. The no-cloning theorem suggests that she/he will not be able to copy these either. The original two operators will be able to publish a subset of their results and using the correlation they will be able to determine whether there has been any meddling with their key.

The E91 Protocol

This is a slight variation of the BB84 protocol and uses entanglement.[94] The first operator prepares several entangled qubits[95] and sends those to the second; she/he will keep one qubit and send the entangled partner to the second operator. The rest of the protocol resembles BB84. However, it is worthwhile to note that the first operator will not have to tabulate the measurements as the "correlatedness" of the entangled pairs will be certain.

Future Possibilities

Shor's algorithm suggests that many public key encryption techniques like ECC and RSA that are based on factoring and discrete logarithmic problems will remain considerably insecure in the face of QC.[96] However, there are a few quantum-safe encryption techniques today that would last at least for the next century, even if QC becomes a reality in the next 2–3 decades. The National Institute of Standards and Technology had recently listed four encryption methods that are ready for the post-quantum world: Cryptographic Suite for Algebraic Lattices (CRYSTALS)-Dilithium (a lattice-based signature scheme), a cryptographic signature algorithm FALCON, SPHINCS+ (a stateless hash-based signature scheme, which advances the SPHINCS signature), and CRYSTALS-Kyber.[97–99] Active research is going on developing lattice cryptography, multivariate cryptography, code-based cryptography, supersingular isogeny key exchange protocol, and symmetric key systems like AES and SNOW- 3G.[100–104] Campagna recently postulated that there will be three main questions about the number of years needed to fulfill our health sector needs: (a) Our encryption to be secure; (b) to make our IT infrastructure quantum-safe; and (c) before a large-scale quantum computer will be built.[105] The physical hardware required to build qubits includes transmons and superconductivity traps, and we will also need insights into cavity quantum electrodynamics.[13,106,107] Significant efforts are also being propagated toward developing topological quantum computers. On a positive note, researchers have recently built the world's largest functioning QKD network using photons and relay optics.[108]

Orcid

Akhil Maheshwari https://orcid.org/0000-0003-3613-4054

References

1. Liu X, Sutton PR, McKenna R, et al. Evaluation of Secure Messaging Applications for a Health Care System: A Case Study. Appl Clin Inform 2019;10(1):140–150. DOI: 10.1055/s-0039-1678607.
2. De Moor G, Claerhout B, De Meyer F. Implementation framework for digital signatures for electronic data interchange in healthcare. Stud Health Technol Inform 2004;110:90–111. PMID: 15853257.
3. Kane B, Sands DZ. Guidelines for the clinical use of electronic mail with patients. The AMIA Internet Working Group, Task Force on Guidelines for the Use of Clinic–Patient Electronic Mail. J Am Med Inform Assoc 1998;5(1):104–111. DOI: 10.1136/jamia.1998.0050104.
4. Donaldson A. Policy for cryptography in healthcare: A view from the NHS. Int J Med Inform 2000;60(2):105–110. DOI: 10.1016/s1386-5056(00)00109-x.
5. He Y, Aliyu A, Evans M, et al. Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. J Med Internet Res 2021;23(4):e21747. DOI: 10.2196/21747.
6. Yu YW, Weber GM. Balancing accuracy and privacy in federated queries of clinical data repositories: Algorithm development and validation. J Med Internet Res 2020;22(11):e18735. DOI: 10.2196/18735.

7. Bos JW, Lauter K, Naehrig M. Private predictive analysis on encrypted medical data. J Biomed Inform 2014;50:234–243. DOI: 10.1016/j.jbi.2014.04.003.
8. Mohammed EA, Slack JC, Naugler CT. Generating unique IDs from patient identification data using security models. J Pathol Inform 2016;7:55. DOI: 10.4103/2153-3539.197203.
9. Malmurugan N, Nelson SC, Altuwairiqi M, et al. Hybrid encryption method for health monitoring systems based on machine learning. Comput Intell Neurosci 2022;2022:7348488. DOI: 10.1155/2022/7348488.
10. Filkins BL, Kim JY, Roberts B, et al. Privacy and security in the era of digital health: What should translational researchers know and do about it? Am J Transl Res 2016;8(3):1560–1580. PMID: 27186282.
11. Asai A, Konno M, Taniguchi M, et al. Computational healthcare: Present and future perspectives (Review). Exp Ther Med 2021;22(6):1351. DOI: 10.3892/etm.2021.10786.
12. Tariq RA, Hackert PB. Patient Confidentiality. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing, 2022.
13. Yang L, Brome CR, Butterworth JS, et al. Invited article: Development of high-field superconducting Ioffe magnetic traps. Rev Sci Instrum 2008;79(3):031301. DOI: 10.1063/1.2897133.
14. Solenov D, Brieler J, Scherrer JF. The Potential of quantum computing and machine learning to advance clinical research and change the practice of medicine. Mo Med 2018;115(5):463–467. PMID: 30385997.
15. Tim Hollebeek. How long before quantum computers break encryption? Available at: https://www.helpnetsecurity.com/2019/09/30/quantum-computers-break-encryption/ 2019. Accessed date: 31 October 2022.
16. Vinod Vaikuntanathan. Quantum computing: The new moonshot in the cyber space race Available at: https://www.helpnetsecurity.com/2019/08/23/cyber-space-race/ 2019. Accessed date: 31 October 2022.
17. Brendyn Lotz. What does quantum computing mean for cybersecurity, healthcare and the internet? Available at: https://www.htxt.co.za/2019/04/02/what-does-quantum-computing-mean-for-cybersecurity-healthcare-and-the-internet/ 2019. Accessed date: 31 October 2022.
18. Gulbahar B. Theory of quantum path computing with Fourier optics and future applications for quantum supremacy, neural networks and nonlinear Schrodinger equations. Sci Rep 2020;10(1):10968. DOI: 10.1038/s41598-020-67364-0.
19. Kuhn MG. Some introductory notes on quantum computing. Available at: https://www.cl.cam.ac.uk/~mgk25/quantum.pdf 2000. Accessed date: 31 October 2022.
20. Sengupta K, Srivastava PR. Quantum algorithm for quicker clinical prognostic analysis: An application and experimental study using CT scan images of COVID-19 patients. BMC Med Inform Decis Mak 2021;21(1):227. DOI: 10.1186/s12911-021-01588-6.
21. Mallow GM, Hornung A, Barajas JN, et al. Quantum computing: The future of big data and artificial intelligence in spine. Spine Surg Relat Res 2022;6(2):93–98. DOI: 10.22603/ssrr.2021-0251.
22. Wang X, Williams C, Liu ZH, et al. Big data management challenges in health research: A literature review. Brief Bioinform 2019;20(1):156-167. DOI: 10.1093/bib/bbx086.
23. Ozada C. The path to revolutionary healthcare. Available at: https://www.pathstone.com/the-path-to-revolutionary-healthcare/2000. Accessed date: 31 October 2022.
24. Faghmous JH, Kumar V. A big data guide to understanding climate change: The case for theory-guided data science. Big Data 2014;2(3):155–163. DOI: 10.1089/big.2014.0026.
25. Jordan S, Fontaine C, Hendricks–Sturrup R. Selecting privacy-enhancing technologies for managing health data use. Front Public Health 2022;10:814163. DOI: 10.3389/fpubh.2022.814163. DOI: 10.3389/fpubh.2022.814163.
26. Silva LM, Felgueiras CS, Alexandre LA, Marques de Sa J. Error entropy in classification problems: A univariate data analysis. Neural Comput 2006;18(9):2036–2061. DOI: 10.1162/neco.2006.18.9.2036.
27. Mandava P, Krumpelman CS, Shah JN, et al. Quantification of errors in ordinal outcome scales using shannon entropy: Effect on sample size calculations. PLoS One 2013;8(7):e67754. DOI: 10.1371/journal.pone.0067754.
28. Mackay MA, Badrick TC. Steady state errors and risk of a QC strategy. Clin Biochem 2019;64:37–43. DOI: 10.1016/j.clinbiochem.2018.12.005.
29. Ruggeri M, Coretti S. Do probability and certainty equivalent techniques lead to inconsistent results? Evidence from gambles involving life-years and quality of life. Value Health 2015;18(4):413–424. DOI: 10.1016/j.jval.2014.12.019.
30. Pouget A, Drugowitsch J, Kepecs A. Confidence and certainty: Distinct probabilistic quantities for different goals. Nat Neurosci 2016;19(3):366–374. DOI: 10.1038/nn.4240.
31. Evans RS. Electronic health records: Then, now, and in the future. Yearb Med Inform 2016;Suppl. 1:S48–S61. DOI: 10.15265/IYS-2016-s006.
32. Keerthy S, Nagesh NK. Efficacious continuous monitoring of infants using wireless remote monitoring technology. Indian J Pediatr 2022;89(8):771–775. DOI: 10.1007/s12098-021-04035-6.
33. Safavi KC, Driscoll W, Wiener–Kronish JP. Remote surveillance technologies: Realizing the aim of right patient, right data, right time. Anesth Analg 2019;129(3):726–734. DOI: 10.1213/ANE.0000000000003948.
34. Riplinger L, Piera–Jimenez J, Dooling JP. Patient identification techniques: Approaches, implications, and findings. Yearb Med Inform 2020;29(1):81–86. DOI: 10.1055/s-0040-1701984.
35. Modi N, Ashby D, Battersby C, et al. Developing routinely recorded clinical data from electronic patient records as a national resource to improve neonatal health care: The medicines for neonates research programme. Southampton (UK): NIHR Journals Library; 2019. Programme Grants for Applied Research. DOI: 10.3310/pgfar07060.
36. Jalali MS, Kaiser JP. Cybersecurity in hospitals: A systematic, organizational perspective. J Med Internet Res 2018;20(5):e10059. DOI: 10.2196/10059.
37. Chung K, Chung D, Joo Y. Overview of administrative simplification provisions of HIPAA. J Med Syst 2006;30(1):51–55. DOI: 10.1007/s10916-006-7404-1.
38. Banks DL. The health Insurance portability and accountability act: Does it live up to the promise? J Med Syst 2006;30(1):45–50. DOI: 10.1007/s10916-006-7403-2.
39. Feld AD. The Health Insurance Portability and Accountability Act (HIPAA): Its broad effect on practice. Am J Gastroenterol 2005;100(7):1440–1443. DOI: 10.1111/j.1572-0241.2005.50621.x.
40. HIPAA Journal. Available at: https://www.hipaajournal.com.
41. HIPAA Journal. Healthcare data breach statistics. Available at: https://www.hipaajournal.com/healthcare-data-breach-statistics/ 2022. Accessed date: 31 October 2022.
42. Collier R. NHS ransomware attack spreads worldwide. CMAJ 2017;189(22):E786–E787. DOI: 10.1503/cmaj.1095434.
43. Seh AH, Zarour M, Alenezi M, et al. Healthcare data breaches: Insights and implications. Healthcare (Basel) 2020;8(2):133. DOI: 10.3390/healthcare8020133.
44. National Guideline Alliance (UK). NICE Guideline No. 204. Consent, privacy and confidentiality: Babies, children and young people's experience of healthcare – Evidence review. London: National Institute for Health and Care Excellence (NICE), 2021. Available at: https://www.ncbi.nlm.nih.gov/books/NBK574977/.
45. Hilton RP, Zheng Y, Serban N. Modeling heterogeneity in healthcare utilization using massive medical claims data. J Am Stat Assoc 2018;113(521):111–121. DOI: 10.1080/01621459.2017.1330203.
46. Belsky J, Crnic K, Woodworth S. Personality and parenting: exploring the mediating role of transient mood and daily hassles. J Pers 1995;63(4):905–929. DOI: 10.1111/j.1467-6494.1995.tb00320.x.
47. McHaffie HE, Laing IA, Parker M, et al. Deciding for imperilled newborns: Medical authority or parental autonomy? J Med Ethics 2001;27(2):104–109. DOI: 10.1136/jme.27.2.104.

48. Manning D. Proxy consent in neonatal care: Goal-directed or procedure-specific? Health Care Anal 2005;13(1):1–9. DOI: 10.1007/s10728-005-2566-4.
49. Obeidat HM, Bond EA, Callister LC. The parental experience of having an infant in the newborn intensive care unit. J Perinat Educ Summer 2009;18(3):23–29. DOI: 10.1624/105812409X461199.
50. West SM. Cryptography as information control. Soc Stud Sci 2022;52(3):353–375. DOI: 10.1177/03063127221078314.
51. Jiang H, Li X, Xu Q. An Improvement to a multi-client searchable encryption scheme for Boolean queries. J Med Syst 2016;40(12):255. DOI: 10.1007/s10916-016-0610-6.
52. Quantin C, Bouzelat H, Dusserre L. Irreversible encryption method by generation of polynomials. Med Inform (Lond) 1996;21(2):113–21. DOI: 10.3109/14639239608995013.
53. Thilakanathan D, Calvo RA, Chen S, et al. Facilitating secure sharing of personal health data in the cloud. JMIR Med Inform 2016;4(2):e15. DOI: 10.2196/medinform.4756.
54. Kon WY, Lim CCW. Provably secure symmetric private information retrieval with quantum cryptography. Entropy (Basel) 2020;23(1):54. DOI: 10.3390/e23010054.
55. Kambourakis G, Maglogiannis I, Rouskas A. PKI-based secure mobile access to electronic health services and data. Technol Health Care 2005;13(6):511–526. PMID: 16340094.
56. Naresh VS, Nasralla MM, Reddi S, et al. Quantum Diffie–Hellman extended to dynamic quantum group key agreement for e-healthcare multi-agent systems in smart cities. Sensors (Basel) 2020;20(14): 3940. DOI: 10.3390/s20143940.
57. Sheng Y, Xin Z, Alam MS, et al. Information hiding based on double random-phase encoding and public–key cryptography. Opt Express 2009;17(5):3270-84. DOI: 10.1364/oe.17.003270.
58. Zhang L, Tang S, Luo H. Elliptic curve cryptography-based authentication with identity protection for smart grids. PLoS One 2016;11(3):e0151253. DOI: 10.1371/journal.pone.0151253.
59. Bhowmik A, Menon U. An adaptive cryptosystem on a finite field. Peer J Comput Sci 2021;7:e637. DOI: 10.7717/peerj-cs.637.
60. Calkavur S. Public–Key cryptosystems and bounded distance decoding of linear codes. Entropy (Basel) 2022;24(4):498. DOI: 10.3390/e24040498.
61. Nechvatal J, Barker E, Bassham L, et al. Report on the development of the advanced encryption standard (AES). J Res Natl Inst Stand Technol 2001;106(3):511–577. DOI: 10.6028/jres.106.023.
62. Radwan AG, AbdElHaleem SH, Abd-El-Hafiz SK. Symmetric encryption algorithms using chaotic and non-chaotic generators: A review. J Adv Res 2016;7(2):193–208. DOI: 10.1016/j.jare.2015.07.002.
63. Dworak K, Boryczka U. Breaking data encryption standard with a reduced number of rounds using metaheuristics differential cryptanalysis. Entropy (Basel) 2021;23(12):1697. DOI: 10.3390/e23121697.
64. Shin SH, Yoo WS, Choi H. Development of modified RSA algorithm using fixed Mersenne prime numbers for medical ultrasound imaging instrumentation. Comput Assist Surg (Abingdon) 2019;24(Suppl. 2):73–78. DOI: 10.1080/24699322.2019.1649070.
65. Giri D, Maitra T, Amin R, et al. An efficient and robust RSA-based remote user authentication for telecare medical information systems. J Med Syst 2015;39(1):145. DOI: 10.1007/s10916-014-0145-7.
66. Hayat U, Ullah I, Azam NA, et al. A novel image encryption scheme based on elliptic curves over finite rings. Entropy (Basel) 2022;24(5):571. DOI: 10.3390/e24050571.
67. Burg D, Ausubel JH. Moore's law revisited through Intel chip density. PLoS One 2021;16(8):e0256245. DOI: 10.1371/journal.pone.0256245.
68. Lim MH, Teoh AB, Toh KA. Dynamic detection-rate-based bit allocation with genuine interval concealment for binary biometric representation. IEEE Trans Cybern 2013;43(3):843–857. DOI: 10.1109/TSMCB.2012.2217127.
69. Bordg A, Lachnitt H, He Y. Certified quantum computation in Isabelle/HOL. J Autom Reason 2021;65(5):691–709. DOI: 10.1007/s10817-020-09584-7.
70. Kendon V. Quantum computing using continuous-time evolution. Interface Focus 2020;10(6):20190143. DOI: 10.1098/rsfs.2019.0143.
71. Chen Y, Neill C, Roushan P, et al. Qubit architecture with high coherence and fast tunable coupling. Phys Rev Lett 2014;113(22):220502. DOI: 10.1103/PhysRevLett.113.220502.
72. Kranz L, Gorman SK, Thorgrimsson B, et al. The use of exchange coupled atom qubits as atomic-scale magnetic field sensors. Adv Mater 2022:e2201625. DOI: 10.1002/adma.202201625.
73. Chinnamsetty SR, Espig M, Khoromskij BN, et al. Tensor product approximation with optimal rank in quantum chemistry. J Chem Phys 2007;127(8):084110. DOI: 10.1063/1.2761871.
74. Huang R, Tan X, Xu Q. Learning to learn variational quantum algorithm. IEEE Trans Neural Netw Learn Syst 2022;PP. DOI: 10.1109/TNNLS.2022.3151127.
75. Fickler R, Krenn M, Lapkiewicz R, et al. Real-time imaging of quantum entanglement. Sci Rep 2013;3:1914. DOI: 10.1038/srep01914.
76. Paneru D, Cohen E, Fickler R, et al. Entanglement: Quantum or classical? Rep Prog Phys 2020;83(6):064001. DOI: 10.1088/1361-6633/ab85b9.
77. Leggett AJ. The quantum measurement problem. Science 2005;307(5711):871–872. DOI: 10.1126/science.1109541.
78. Lazarovici D, Hubert M. How quantum mechanics can consistently describe the use of itself. Sci Rep 2019;9(1):470. DOI: 10.1038/s41598-018-37535-1.
79. Daffertshofer A, Plastino AR, Plastino A. Classical no-cloning theorem. Phys Rev Lett 2002;88(21):210601. DOI: 10.1103/PhysRevLett.88.210601.
80. Bauer B, Bravyi S, Motta M, et al. Quantum algorithms for quantum chemistry and quantum materials science. Chem Rev 2020;120(22):12685–12717. DOI: 10.1021/acs.chemrev.9b00829.
81. Ahnefeld F, Theurer T, Egloff D, et al. Coherence as a resource for Shor's algorithm. Phys Rev Lett 2022;129(12):120501. DOI: 10.1103/PhysRevLett.129.120501.
82. Gebhart V, Pezze L, Smerzi A. Quantifying computational advantage of Grover's algorithm with the trace speed. Sci Rep 2021;11(1):1288. DOI: 10.1038/s41598-020-80153-z.
83. Godfrin C, Ferhat A, Ballou R, et al. Operating quantum states in single magnetic molecules: Implementation of Grover's quantum algorithm. Phys Rev Lett 2017;119(18):187702. DOI: 10.1103/PhysRevLett.119.187702.
84. Scully MO, Zubairy MS. Quantum optical implementation of Grover's algorithm. Proc Natl Acad Sci U S A 2001;98(17):9490–9493. DOI: 10.1073/pnas.171317798.
85. Wright K, Beck KM, Debnath S, et al. Benchmarking an 11-qubit quantum computer. Nat Commun 2019;10(1):5464–5472. DOI: 10.1038/s41467-019-13534-2.
86. Chen A. Implementation of Deutsch–Jozsa algorithm and determination of value of function via Rydberg blockade. Opt Express 2011;19(3):2037–2045. DOI: 10.1364/OE.19.002037.
87. Ampatzis M, Andronikos T. QKD based on symmetric entangled Bernstein–Vazirani. Entropy (Basel) 2021;23(7):870. DOI: 10.3390/e23070870.
88. Dixit V, Jian S. Quantum Fourier transform to estimate drive cycles. Sci Rep 2022;12(1):654. DOI: 10.1038/s41598-021-04639-0.
89. Kang C, Bauman NP, Krishnamoorthy S, et al. Optimized quantum phase estimation for simulating electronic states in various energy regimes. J Chem Theory Comput 2022;18(11):6567–6576. DOI: 10.1021/acs.jctc.2c00577.
90. Chakraborty S, Novo L, Ambainis A, et al. Spatial search by quantum walk is optimal for almost all graphs. Phys Rev Lett 2016;116(10):100501. DOI: 10.1103/PhysRevLett.116.100501.
91. Wang Y, Hu ML. Quantum teleportation and dense coding in multiple bosonic reservoirs. Entropy (Basel) 2022;24(8):1114. DOI: 10.3390/e24081114.
92. Yang YH, Li PY, Ma SZ, et al. All optical metropolitan quantum key distribution network with post-quantum cryptography

authentication. Opt Express 2021;29(16):25859–25867. DOI: 10.1364/OE.432944.
93. Anusuya Devi V, Kalaivani V. Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications. Pers Ubiquitous Comput 2021:1–11. DOI: 10.1007/s00779-021-01546-z.
94. Fujiwara M, Yoshino K, Nambu Y, et al. Modified E91 protocol demonstration with hybrid entanglement photon source. Opt Express 2014;22(11):13616–13624. DOI: 10.1364/OE.22.013616.
95. Neeley M, Bialczak RC, Lenander M, et al. Generation of three-qubit entangled states using superconducting phase qubits. Nature 2010;467(7315):570–573. DOI: 10.1038/nature09418.
96. Skosana U, Tame M. Demonstration of Shor's factoring algorithm for N [Formula: see text] 21 on IBM quantum processors. Sci Rep 2021;11(1):16599. DOI: 10.1038/s41598-021-95973-w.
97. Ducas L, Kiltz E, Lepoint T, et al. CRYSTALS-Dilithium: A lattice-based digital signature scheme. IACR Trans Cryptogr Hardw Embed Syst 2018;2018(1):238–268. DOI: 10.13154/tches.v2018.i1.238-268.
98. Lizama–Perez LA, Lopez RJ. Non-invertible public key certificates. Entropy (Basel) 2021;23(2). DOI: 10.3390/e23020226.
99. Septien–Hernandez JA, Arellano–Vazquez M, Contreras–Cruz MA, et al. A comparative study of post-quantum cryptosystems for Internet-of-things applications. Sensors (Basel) 2022;22(2):489. DOI: 10.3390/s22020489.
100. Ortiz JN, de Araujo RR, Aranha DF, et al. The ring-LWE problem in lattice-based cryptography: The case of twisted embeddings. Entropy (Basel) 2021;23(9):1108. DOI: 10.3390/e23091108.
101. Dai S. Quantum cryptanalysis on a multivariate cryptosystem based on clipped Hopfield neural network. IEEE Trans Neural Netw Learn Syst 2022;33(9):5080–5084. DOI: 10.1109/TNNLS.2021.3059434.
102. Ren L, Zhang D. A QR code-based user-friendly visual cryptography scheme. Sci Rep 2022;12(1):7667. DOI: 10.1038/s41598-022-11871-9.
103. Rani R, Kumar S, Kaiwartya O, et al. Towards green computing oriented security: A lightweight postquantum signature for IoE. Sensors (Basel) 2021;21(5). DOI: 10.3390/s21051883.
104. McGoldrick LK, Weiss EA, Halamek J. Symmetric-key encryption based on bioaffinity interactions. ACS Synth Biol 2019;8(7):1655–1662. DOI: 10.1021/acssynbio.9b00164.
105. Campagna M. Preparing today for a post-quantum cryptographic future. Available at: https://www.amazon.science/blog/preparing-today-for-a-post-quantum-cryptographic-future 2022. Accessed date: 31 October 2022.
106. Gambetta JM, Chow JM, Steffen M. Building logical qubits in a superconducting quantum computing system. npj Quantum Inf 2017;3(2):7. DOI: 10.1038/s41534-016-0004-0.
107. Landig AJ, Koski JV, Scarlino P, et al. Virtual-photon-mediated spin–qubit–transmon coupling. Nat Commun 2019;10(1):5037. DOI: 10.1038/s41467-019-13000-z.
108. Zhang Q, Xu F, Li L, et al. Quantum information research in China. Quantum Sci Technol 2019;4(4). DOI: 10.1088/2058-9565/ab4bea.