A Brief Review of Quantum Cryptography

Richard Pawełkiewicz

Rensselaer Polytechnic Institute, Troy NY 12180, USA

1 Introduction

On November 9th, 2022, IBM announced they had created a 433 qubit processor, codenamed *Osprey* [17]. More than twice the scale of its predecessor, it now holds the record as the largest universal quantum processor. As if that wasn't enough, IBM also announced they have plans to break 1,000 qubits by 2023, and 4,000 by 2025. Albeit impressive and exciting, the rate of progress is also a serious cause for concern.

At this point, it is well known that quantum computers pose a threat to modern secure digital communications. Most modern cryptosystems rely on problems perceived to be intractable in the classical setting—RSA relies on factoring, and Diffie-Hellman relies on discrete log—yet, many of these problems can be solved efficiently in the quantum realm, as famously demonstrated by Shor in 1994 [25]. As of 2021, these algorithms, specifically, are the most common means of digital signature and key exchange in the TLS protocol, securing vital industry secrets, sensitive government data, as well as the entire web [15].

But, how close are we really to the doom prophesized by Peter Shor? Surely our primitive experiments are a long ways off from the capability of doing any real damage? In their 2021 paper, Gidney and Ekerå showed that a noisy universal quantum computer can factor a 2048-bit RSA prime in just 8 hours using 20 million qubits [12]. Now, that's a far cry from the 433 qubit record, but given our current rate of progress, it would only take about 20 years to reach. What's more, its been shown that, under certain circumstances, factoring can be achieved with considerably fewer bits. In 2017, Dridi and Alghassi successfully factored a 17-bit integer using an 1,152 qubit D-Wave quantum annealer [9]—a specialized type of quantum computer that is not universal but very good at solving particular optimization problems. In 2021, Karamlou et al. claimed to have factored a 40-bit integer with just 3 qubits using a classical-quantum hybrid algorithm called *Variational Quantum Factoring*, or VQF [18].

Yet, despite the writing on the wall, there is still hope. While some scientists have been trying to break current encryption schemes, others have been busy cooking up new algorithms based on even harder problems. These algorithms form the foundation of *post-quantum cryptography*. Ever since the malicious potential of quantum computing was realized, there has been a push to find quantum-resistant alternatives. In 2016, NIST launched a competition for post-quantum cryptographic algorithms [24]. While many submissions are still under review, some have already become standards. Among them are CRYSTALS-Kyber—a key exchange algorithm based on module lattices—and CRYSTALS-

Dilithium, Falcon, and SPHINCS+—digital signature algorithms based on module lattices, fast Forier lattices, and hashes, respectively. The question remains, however: Are these problems *hard enough*? The truth is, we don't know. There is good reason to believe they are, but it has not been proven. Despite the blessings of many credible scientists and mathematicians, it remains possible that a malicious actor with sufficient resources can break these post-quantum codes, just as it is with RSA and Diffie-Hellman.

A natural question to ask at this point is—if quantum computing can be used to attack secure communications, can it also be used to defend them? The answer, of course, is yes. Not only can quantum computing be used in cryptography, but it can be proven to provide so-called *unconditional security* [23,14], which means it will remain secure even if we grant our adversaries infinite time and resources. This is because, while classical cryptography relies on the assumption that problems are hard, quantum cryptography relies on physics, which cannot be broken [7].

The remainder of this paper will cover some basic types of quantum cryptography: Section 2 will discuss Quantum Key Exchange and the BB84 protocol, Section 3 will discuss Quantum Identity Authentication and the OT QIA protocol, Section 4 will discuss Quantum Secure Direct Communication and the ping-pong protocol, Section 5 will discuss Discrete Secure Quantum Communication and the modified ping-pong protocol with reordering, and Section 6 will conclude with a summary of the covered topics, an overview of the uncovered topics, and some recommendations for further reading.

2 Quantum Key Exchange

When Alice wants to send a private message to Bob, she generally has two options: She can use public-key/assymetric-key cryptography, or symmetric-key cryptography. In public-key cryptography, there are two keys: a public key, which is used to encrypt messages and can be shareed openly, and a private key which is used to decrypt messages and must be kept secret. This assymetry makes it easy for Alice to talk to Bob without any prior communications or secret sharing. However, it is slow. For this reason, it is generally prefferable to use symmetric-key cryptography, in which a single key is capable of both encryption and decryption. This key cannot be shared openly, which leads to the key distribution problem. Classically, to overcome this problem, either a public-key cryptosystem—such as RSA—is used to encrypt the key, or a key exchange algorithm—such as Diffie Helman—can be employed to generate a shared secret key. As previously mentioned, both of these algorithms rely on the difficuly of solving certain problems and are vulnerable to quantum computers.

Fortunately, there is a quantum analog to classical key exchange, appropriately termed *Quantum Key Exchange*, or QKE. Like classical key exchange, QKE allows Alice and Bob to generate a shared secret key. However, unlike its classical counterpart, QKE can be proven to be unconditinally secure [14]. QKE typically involves generating, sending, and measuring random quantum

states, taking advantage of the tendency of superposed states to decohere upon measurement in order to detect evesdroppers. A classical channel is used to help verify the integrity of the sent bits. After the key is generated, it can be employed in a symmetric-key cryptosystem—typically the one-time-pad (OTP), the only unconditionally secure classical symmetric cryptosystem [1].

2.1 BB84 Protocol

The first QKE protocol was proposed by Bennett and Brassard in 1984, now known as BB84 [10,14]. It as since been followed by some others, notably E91 by Ekert in 1991 [11] and B92 by Bennett in 1992 [2]. An outline of the BB84 protocol for generating n bit shared cryptographic keys is given in Algorithm 1. It assumes Alice and Bob each have access to at least n qubits—though, in principle, it could be modified to work with just 1—an open quantum channel between them, and an authenticated classical channel.

Algorithm 1 BB84

1. Alice chooses n initial qubit values from the set $\{0, 1\}$ uniformly at random. Assuming her initial state is all 0, she applies the NOT gate to obtain 1.
2. Alice chooses n bases from the set $\{X, Z\}$ uniformly at random. Assuming her initial state is all in the Z basis, then she applies the Hadamard gate to switch them to the X basis.
3. Alice sends all n qubits to Bob over a public quantum channel.
4. Bob does not know which bases Alice chose, so the best he can do is guess. He chooses n bases uniformly at random. Assuming he wants the final state to be in the Z basis, he applies the Hadamard to each qubit he believes to be in the X basis. He will get this right about 50% of the time.
5. Bob measures all n qubits, obtaining n potentially shared, secret classical bits.
6. *After* Bob measures, Alice sends Bob her chosen bases over an authenticated classical channel.
7. Bob discards all the qubits for which he guessed wrong, and tells Alice which ones he got right over the authenticated classical channel.
8. Alice discards the qubits Bob got wrong.
9. Alice and Bob choose $m < n$ bits each to compare in an attempt to detect an eavesdropper. They disclose their bits in the authenticated classical channel.
10. If any of their compared bits are off, they assume their quantum messages were intercepted and discard all of their remaining bits and quit. Otherwise, they use the remaining bits to form a key according to some well-defined public process.
11. Either separately, or in parallel, Bob and Alice switch roles and repeat, so that they both contribute equally to the shared keys.

Suppose an eavesdropper, Eve, is interested in intercepting the messages between Alice and Bob. If she wants to do a passive attack, then the best she can do is guess the bases and measure the qubits before forwarding them to Bob. However, for all the bases she chose wrong, the qubits will collapse, affecting

Bob's subsequent measuring. When Bob compares his qubits with Alice, they are highly likely to notice a large number of errors, revealing Eve's presence. Alice can also attempt a more active man-in-the-middle attack in which she pretends to be Bob talking to Alice and Alice talking to Bob. In doing so, she will try to trick Alice and Bob into generating two separate keys that she can use to communicate with them. Assuming the classical channel is authenticated, this faces the same limitation as the passive attack–Eve's presence will be revealed during the comparison step.

One major downside of the BB84 protocol is that it requires the classical channel to be authenticated. If it is not authenticated, then Eve can simply impersonate Alice and Bob during the comparison step and trick them into believing they share the same key. Alice and Bob can use encryption to authenticate each other, but this requires them to have some pre-shared key, which seems to defeat the purpose of the protocol in the first place. Despite this, there is still some merit in using BB84, and QKE in general—Suppose Eve isn't capable of breaking the encryption scheme right now, but she saves the intercepted messages for later in the hope that she will eventually be able to decipher them. If BB84 is used, then even if the authentication method eventually is cracked, and the messages exchanged in the classical channel are compromised, Eve will still learn nothing about the key that Alice and Bob exchanged in the quantum channel. Thus, if Alice and Bob used that key, all their future messages should remain secure. This is called *Perfect Forward Secrecy* (PFS).

To authenticate each other, Alice and Bob can make use of post-quantum cryptography. All of their messages will be secure as long as the post-quantum algorithm is *currently* secure. Thanks to PFS, if the algorithm is later found to be vulnerable, Alice and Bob's messages will not be compromised. This is somewhat of an unsatisfying answer. Presumably, the reader of this paper is expecting quantum solutions to classical problems, and not the other way around. Fortunately, as with key exchange, there are quantum techniques we can use for authentication.

3 Quantum Identity Authentication

Authentication often involves some form of *zero-knowledge proof*, in which the authenicatee proves they have knowledge of some secret without disclosing that secret. Using this ability, one can authenticate themselves without sharing that ability with a potential eavesdropper, even if their messages are not encrypted. Classically, asymmetric cryptography can be used for this purpose, such as RSA or or CRYSTAL-Kyber, but these are only conditionally secure. On the other hand, *Quantum Identity Authentication* (QIA) offers unconditional security.

3.1 QIA with Oblivious Transfer

There are many methods for QIA. Dutta and Pathak showed in 2021 that practically any quantum communication or secret sharing protocol can be used for

QIA, including QKE, QSDC, and DSQC [10]. The first QIA algorithm was proposed by Crépeau and Salvail in 1995 [10,8]. Zero knowledge is achieved by using a technique called *Oblivious Transfer* (OT), in which the sender shares one piece of information out of a set, without knowing which one. The method for Quantum OT is modified from the protocol by Bennett and Brassard [3]. To ensure the authenticatee cannot modify their message mid-protocol, they also employ a quantum bit commitment scheme by Brassard et al. [6]. The algorithm assumes Alice and Bob have access to n qubits each and a public Quantum channel between them. It also requires they have some pre-shared secrets, an unfortunate limitation that will be discussed later. An overview of the protocol is given in Algorithm 2.

Algorithm 2 QIA with OT

1. Alice chooses n pairs (r, s) of binary digits uniformly at random.
2. For each (r, s), Alice uses oblivious transfer [3] to send r or s to Bob, without knowing which one.
3. Bob chooses n pairs (x, y) of binary digits uniformly at random, sending them to Alice over a public classical or quantum channel.
4. Alice chooses a word c from a large, sparse set of pre-shared n-bit binary strings. She computes $u = (c \oplus r \oplus x, c \oplus s \oplus y)$, where $\oplus$ denotes bit-wise exclusive OR. She then encodes u using a pre-shared ordered list of n bases in the set $\{X, Z\}$, and sends the resulting string to Bob over the public quantum channel.
5. Bob decodes the string using the same pre-shared bases and computes $(u \oplus v \oplus x, u \oplus v \oplus y)$. One of the resulting words is in the pre-shared set, then he accepts.

Suppose Eve would like to impersonate Alice. Even if she has knowledge of the pre-shared set of strings, she cannot guess the bases with any significant probability. When she sends u to Bob, about half of the bits will be incorrect, and the authentication will fail. The most knowledge she gains from this transaction is that her chosen bases is incorrect. If Eve would like to impersonate Bob, she will only be able to decode about half of Alice's u, and she does not know which half are correct, thus she gains no knowledge of the word or the bases used.

The requirement that Alice and Bob have some pre-shared secrets is a little inconvenient. It turns out this is a requirement shared by most QIA protocols to date [10]. However, even classical algorithms demand some kind of preshared secrets, in the form of root certificates. The major problem is that it is not scalable to have every agent share unique secrets with every other agent—the number of secrets would be quadratic in the number of agents. To circumvent this limitation, each pair of agents can initiate their communication through a trusted hub. This way every agent only needs to share secrets with the hub, and the number of secrets scales linearly.

As it turns out, QIA with OT cannot actually be implemented for 2 agents in an unconditionally secure manner. This was proven by Lo [20] and Lo and

Chau [21] shortly after Crépeau and Salvail proposed their protocol. However, there are others that can [10].

4 Quantum Secure Direct Communication

Unconditionally secure communication is possible by combining QKE and QIA, however, requiring a separate step to generate keys is not very efficient. It turns out it is possible for Alice and Bob to communicate directly without this step. This is called *Quantum Secure Direct Communication* (QSDC).

4.1 Ping-pong Protocol

Perhaps the most well known QSDC protocol is the *ping-pong* protocol, proposed by Boström and Felbinger in 2002, which uses entangled pairs. A variation using pure states, called *LM05*, was created by Lucamarina and Mancini in 2005 [22]. An outline of ping-pong is given in Algorithm 3. It assumes Alice and Bob each have access to at least 2 qubits, a shared public quantum channel, an authenticated classical channel, and that Alice wants to send an n-bit classical message to Bob.

Suppose Eve wants to learn Alice's message. One option is she can measure Bob's travel qubit in the X basis before Alice receives it, then she returns it to the X basis and forwards it to Alice. If Alice responds with *send*, Eve measures again, before again putting it in the X basis and forwarding it to Bob. By comparing her measurements before and after Alice receives the qubit, Eve will learn whether or not Alice performed a phase flip, thereby revealing a bit of the message. However, if Alice chooses to *check* instead, the travel qubit is no longer entangled with the home qubit, so her measurement has a 50% chance of failure, in which case Eve's presence will be revealed. Note that Eve needs to measure the travel qubit before it gets to Alice because she doesn't know which qubit Bob chose to send, therefore she wouldn't know what value it started with. Also, Eve's chances of failure increase exponentially with the number of checks Alice performs. Thus, as long as Alice performs a sufficient number of checks, Eve is highly unlikely to pass undetected.

The efficiency gained in the ping-pong protocol compared to QKE is respectable, yet there is a glaring flaw—Eve is very likely to gain some parts of the message before she is detected. This is fine if the message hasn't yet been assigned any significance, such as if it is being used to exchange keys, but that is exactly what we were trying to avoid. In order to keep both the efficiency and security of ping-pong, we can use DSQC, as discussed below.

5 Discrete Secure Quantum Communication

Discrete Secure Quantum Communication (DSQC) is a form of QSDC[1] in which an authenticated classical channel is necessary to decrypt the message. At least

[1] The Q and D are switched in the acronyms, most likely for the purpose of confusing the reader

Algorithm 3 Ping-pong

1. For each bit x_i in Alice's message $(x_1, \cdots, x_n)$:
   (a) Bob uses 2 qubits to create the Bell state $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. He can do this by applying a Hadamard and a NOT gate to two zero qubits, respectively, followed by a controlled NOT on the result. These qubits are now random, yet guaranteed to be opposite.
   (b) He randomly chooses one qubit to be the *home* qubit, and the other to be the *travel* qubit, and sends the travel qubit to Alice over the public quantum channel.
   (c) Alice chooses one of two tasks—*check* or *send*—according to some pre-established probability.
   (d) If she chooses *check*:
      i. Alice measures the travel qubit in the Z basis. Since the qubit's value was originally in the X basis, Alice will be equally likely to measure a 0 or 1.
      ii. Alice sends Bob her measurement through the authenticated classical channel.
      iii. Bob measures his home qubit in the Z basis. Since they were supposed to be entangled, both measurements should result in the same value.
      iv. If the two measurements differ, Eve is detected and they abort the protocol. Otherwise, they both return to step 1a.
   (e) If Alice chooses *send*:
      i. If $x_i = 1$, Alice applies a phase flip to the travel qubit. This can be done with a Z gate.
      ii. Alice returns the travel qubit to Bob.
      iii. Bob measures both qubits in the X basis. This can be done by applying a Hadamard gate to both qubits, then measuring them in the Z basis.
      iv. If the qubits are equal, he determines that $x_i = 0$.
      v. Otherwise, they are opposite, so Alice must have applied a phase shift. He knows $x_i = 1$.
2. The message has successfully been sent.

one bit is sent over the channel per bit in the message. Compare this with ping-pong, in which the classical channel is only used for checking for the presence of Eve. One DSQC algorithm, proposed by Zhu et al. in 2006 [27], is detailed below.

5.1 Ping-pong with Reordering

Using DSQC we can solve the efficiency-security dilemma caused by ping-pong. This is done by modifying the original ping-pong protocol so the order of the qubits sent is random. Any bits Eve is able to decode will appear random and be useless to her. Alice keeps track of the order of the qubits until the end, after her and Bob are sure Eve was not listening. Then Alice shares the order of the qubits with Bob over authenticated public channel, and Bob is able to reorder them to read the message.

6 Conclusion

Advances in quantum computing pose a huge threat to the secure communications that underlie our modern world. Quantum cryptography is a useful means to combat this threat. Furthermore, the unconditional security it brings makes it a favorable choice as compared with post-quantum cryptography. We have seen that there are quantum analogs for key exchange [14,11,2]—which provide advantages over classical protocols even when classical authentication schemes are used—there are quantum algorithms for authentication[8,10], that QSDC can be used to send messages over a quantum channel without requiring a key exchange [4,22], and that DSQC can solve some of the limitations of QSDC [27].

Other classes of algorithms not discussed in this paper include Quantum Bit Commitment [6], Quantum Secret Sharing [16], Quantum Digital Signatures [13], and Quantum Private Comparison [19]. There are also many variations of these algorithms, using GHZ triplets, Bell states, or single qubits, with or without pre-shared secrets, trusted or untrusted third parties, or classical channels [10]. Some of the interesting examples use teleportation [26], and some are deniable schemes to keep interacting identities secret [**?**]. There are also semi-quantum approaches [5], which allow for some of the agents to participate even if they don't have direct access to a quantum computer. This will likely prove particularly useful because all current hardware necessary for effective quantum computers require prohibitively expensive equipment. Assuming there are no major improvements in this regard, direct access to quantum computers will not be possible for most. For further reading, I highly recommend a recent paper by Duta and Pathak [10], which offers a detailed review of QIA and how other quantum cryptographic algorithms can be used to implement it.

References

1. Bellovin, S.M.: Frank miller: Inventor of the one-time pad. Cryptologia **35**(3), 203–222 (2011). https://doi.org/10.1080/01611194.2011.583711
2. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (May 1992). https://doi.org/10.1103/PhysRevLett.68.3121, https://link.aps.org/doi/10.1103/PhysRevLett.68.3121
3. Bennett, C.H., Brassard, G., Crépeau, C., Skubiszewska, M.H.: Practical quantum oblivious transfer. In: Feigenbaum, J. (ed.) Advances in Cryptology — CRYPTO '91. pp. 351–366. Springer Berlin Heidelberg, Berlin, Heidelberg (1992)
4. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Physical Review Letters **89**, 187–902 (October 2002). https://doi.org/10.1103/PhysRevLett.89.187902, https://link.aps.org/doi/10.1103/PhysRevLett.89.187902
5. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical bob. Phys. Rev. Lett. **99**, 140–501 (October 2007). https://doi.org/10.1103/PhysRevLett.99.140501
6. Brassard, G., Crepeau, C., Jozsa, R., Langlois, D.: A quantum bit commitment scheme provably unbreakable by both parties. In: Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science. pp. 362–371 (1993). https://doi.org/10.1109/SFCS.1993.366851

7. Common Sense:
8. Crépeau, C., Salvail, L.: Quantum oblivious mutual identification. In: Guillou, L.C., Quisquater, J.J. (eds.) Advances in Cryptology — EUROCRYPT '95. pp. 133–146. Springer Berlin Heidelberg, Berlin, Heidelberg (1995)
9. Dridi, R., Alghassi, H.: Prime factorization using quantum annealing and computational algebraic geometry. Scientific Reports **7**(1), 43048 (February 2017). https://doi.org/10.1038/srep43048, https://doi.org/10.1038/srep43048
10. Dutta, A., Pathak, A.: A short review on quantum identity authentication protocols: how would Bob know that he is talking with Alice? Quantum Information Processing **21**, 369 (November 2022). https://doi.org/10.1007/s11128-022-03717-0
11. Ekert, A.K.: Quantum cryptography based on bell's theorem. Phys. Rev. Lett. **67**, 661–663 (August 1991). https://doi.org/10.1103/PhysRevLett.67.661, https://link.aps.org/doi/10.1103/PhysRevLett.67.661
12. Gidney, C., Ekerå, M.: How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits. Quantum **5**, 433 (April 2021). https://doi.org/10.22331/q-2021-04-15-433
13. Gottesman, D., Chuang, I.: Quantum digital signatures (May 2001). https://doi.org/10.48550/ARXIV.QUANT-PH/0105032
14. H. Bennett, C., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science **560**, 7–11 (December 2014). https://doi.org/10.1016/j.tcs.2014.05.025
15. Helme, S.: Top 1 million analysis—November 2021 (November 2021), https://scotthelme.co.uk/top-1-million-analysis-november-2021/, accessed: 2022-12-06
16. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (March 1999). https://doi.org/10.1103/PhysRevA.59.1829
17. IBM: IBM unveils 400 qubit-plus quantum processor and next-generation IBM quantum system two. IBM News (November 2022), https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two
18. Karamlou, A.H., Simon, W.A., Katabarwa, A., Scholten, T.L., Peropadre, B., Cao, Y.: Analyzing the performance of variational quantum factoring on a superconducting quantum processor. npj Quantum Information **7**(1), 156 (October 2021). https://doi.org/10.1038/s41534-021-00478-z, https://doi.org/10.1038/s41534-021-00478-z
19. Liu, W.J., Liu, C., Wang, H., Jia, T.: Quantum private comparison: A review. IETE Technical Review **30**, 439–445 (2013)
20. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**, 1154–1162 (August 1997). https://doi.org/10.1103/PhysRevA.56.1154
21. Lo, H.K., Chau, H.: Why quantum bit commitment and ideal quantum coin tossing are impossible. Physica D: Nonlinear Phenomena **120**(1), 177–187 (1998). https://doi.org/https://doi.org/10.1016/S0167-2789(98)00053-0, proceedings of the Fourth Workshop on Physics and Consumption
22. Lucamarini, M., Mancini, S.: Secure deterministic communication without entanglement. Phys. Rev. Lett. **94**, 140501 (April 2005). https://doi.org/10.1103/PhysRevLett.94.140501
23. Mayers, D.: Unconditional security in quantum cryptography. Journal of the ACM **48** (March 1998). https://doi.org/10.1145/382780.382781

24. National Institute of Standards and Technology: Status report on the third round of the NIST post-quantum cryptography standardization process. Tech. Rep. NIST Internal Report (IR) 8413, Includes updates as of September 26, 2022, U.S. Department of Commerce, Washington, D.C. (July 2022). https://doi.org/10.6028/NIST.IR.8413-upd1
25. Shor, P.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science. pp. 124–134. SFCS '94, IEEE Computer Society, USA (November 1994). https://doi.org/10.1109/SFCS.1994.365700
26. Zhou, N., Zeng, G., Zeng, W., Zhu, F.: Cross-center quantum identification scheme based on teleportation and entanglement swapping. Optics Communications **254**(4), 380–388 (2005). https://doi.org/https://doi.org/10.1016/j.optcom.2005.06.002
27. Zhu, A.D., Xia, Y., Fan, Q.B., Zhang, S.: Secure direct communication based on secret transmitting order of particles. Physical Review A **73**(2) (February 2006). https://doi.org/10.1103/physreva.73.022338