Scientific and Social Research, 2024, Volume 6, Issue 11
https://ojs.bbwpublisher.com/index.php/SSR
Online ISSN: 2981-9946
Print ISSN: 2661-4332

The Fascinating Evolution of Quantum Cryptography: The Modern Information Maginot Line

Shaohan Qin*

The Experimental High School Attached to Beijing Normal University, Beijing, China

Corresponding author: Shaohan Qin, qinshaohan2007@163.com

Abstract: During the Cold War, a revolutionary cryptographic method, quantum cryptography, emerged. Grounded in the laws of quantum physics, quantum cryptography ensures absolute security using quantum principles. Stephen Wiesner introduced the concept in 1983, but initially received little attention, as technology at the time did not allow the encryption method to be put into practice. The field of quantum cryptography began to take shape with the arrival of two more researchers, Giles Brassard and Charles Bennett. The development of quantum cryptography accelerated dramatically after Artur Ekert proposed the application of Bell's theorem in this field. Afterwards, more researchers got involved and new theorems and applications were developed, leading the field to become a major subject at the forefront of physics research. This paper explores why quantum cryptography is exceptionally secure and the steps that brought this idea to practice. The paper looks into the intriguing concept of quantum cryptography and the stimulating stories surrounding its progress. From Stephen Wiesner's original proposal through Brassard and Bennett's persistent efforts to the exciting debates between Ekert and Brassard and Bennett. This paper highlights the significant milestones and achievements that have positioned quantum cryptography at the forefront of physics research.

Keywords: Cryptography; Quantum physics; BB84 scheme; Bell's theorem

Online publication: November 29, 2024

1. Introduction

On April 21, 2004, in Vienna, the world's first bank transfer via quantum cryptography took place [1]. The significance of the event was apparent, as those in attendance included not only bankers, physicists, and bank staff, but also the mayor. A commercially viable encryption technology based on the theory of quantum mechanics has been created. Unlike traditional cryptography methods, which are based on mathematics, this new encryption method relies on physics, and by transmitting photons—individual particles of light—information could be

encoded with an unbreakable code. When using quantum cryptography, any attempt at eavesdropping can easily be detected, as any such attempt changes the quantum state of the dispatched information. Not only does this alternation destroy the message, but it also serves to identify the eavesdropper. With such a secure encryption system to safeguard the process, the mayor was able to transfer electronic funds quickly and securely. What chain of events led to this first transfer? What is quantum cryptography, why is it so secure, and what makes it impossible to break?

In 1983, Stephen Wiesner proposed a groundbreaking idea: quantum cryptography. This form of encoding could serve as the basis for a completely secure system of encryption. What sets this new encryption method apart from the rest is that it relied not on mathematics or information theory, but on the fundamental laws of physics—specifically those of quantum mechanics. These laws impose restrictions on the information an observer can know at any one time, with the uncertainty principle dictating that one cannot simultaneously ascertain both the position and momentum of a particle. Using the protection provided by the laws of physics, Wiesner claimed, a new form of cryptography could be designed and applied to real-life situations. Despite the potential for unbreakable encryption, little attention was directed toward Wiesner's idea initially.

In the following decade, various groups of researchers made their contributions to the development of quantum cryptography—sometimes working independently, at others collaboratively, and occasionally even against one another. This paper tells the story of two decades of scientific effort that led to the commercially viable quantum cryptographic solutions people know today. It starts with Wiesner's 1983 paper and continues with Charles H. Bennett and Gilles Brassard's development and elaboration of Wiesner's ideas, which ultimately attracted the attention of the scholarly community to this new field of quantum cryptography. The narrative then advances to the seminal 1991 contribution of Artur Ekert, which set off a debate that thrust the discipline into the spotlight and contributed to its burgeoning success.

2. Social and historical background of the development of quantum cryptography

Attempts to encrypt information can be traced back to the ancient Romans [2]. In the time of Julius Caesar, people made use of a simple method now known as the "Caesar Cipher." This method involved shifting letters backward or forwards by a set amount of places (as illustrated in **Figure 1**), thereby creating a seemingly meaningless message. While this code was effective and easy to implement, it could also be broken with minimal analysis.

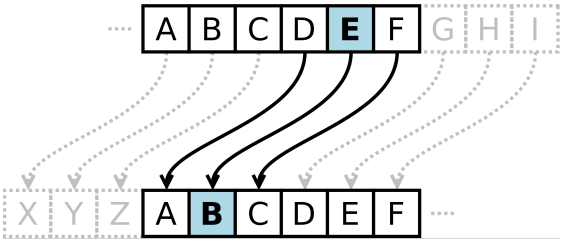

Figure 1. Caesar code

For the next two millennia, the complexity of encryption systems remained largely stagnant. It was only in the 1940s that cryptography evolved substantially [3]. This change was spurred by the outbreak of World War II, which stimulated research and the development of new and better systems of encryption through the utilization of mathematics and information theory. A famous instance of decipherment in this pivotal time is the breaking of the Enigma code, used by the Germans during World War II, through the ingenious work of mathematicians such as

the brilliant Alan Turing.

The most notable breakthrough in that era was Shannon's formulation of information theory, which he outlined in a seminal 1949 paper. In the following decades, emerged encryption schemes such as the Data Encryption Standard (DES) in 1977; Rivest, Shamir, and Adleman (RSA) in 1978; and many others. The Cold War, with its constant threat of hostile surveillance, called for a way to send information with guaranteed protection. Yet none of the aforementioned theories and schemes, all derived from mathematics and information theory (the RSA method, for example, makes use of the multiplication of very large prime numbers, with its security depending on the relative complexity of factorization) were up to the task. While they enabled encryption strong enough to fend off any attempt at decipherment relying on human computing power, they were not unbreakable, and with the advancement of computing technology, the protection they afforded became increasingly weaker. A cryptographical breakthrough was needed, and urgently. This is where quantum cryptography comes in.

3. Early theoretical foundations: Wiesner's ideas and proposal

The path to Vienna began in the 1960s and 1970s when Stephen Wiesner formulated the principles of quantum conjugate coding at Columbia University. Wiesner hypothesized that the principles of quantum physics could be used to revolutionize information transmission and the world of finance. Using mathematical tools, he was able to demonstrate the validity of this theory.

Wiesner argued that a cryptographic system could be created based on the principles of quantum physics—specifically those related to the "spin" of photons. Each photon can spin either clockwise or counterclockwise, designated as "up" or "down", as shown in **Figure 2**.

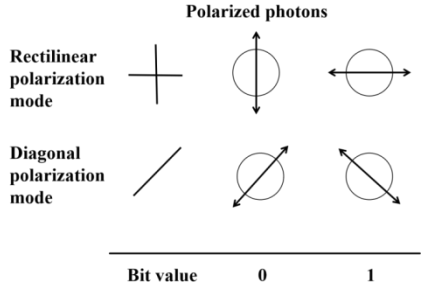

Figure 2. Different polarization of photons

Wiesner proposed that by sending polarized photons through special tubes and then analyzing the spin of these photons with special detectors and algorithms, information could be sent and received in a completely secure way. He also proposed the creation of a currency system based on quantum mechanics. This currency, which he called "quantum money", would, he argued, be nearly impossible to counterfeit.

Despite the novelty of Wiesner's ideas and their enormous practical potential, it took many years for his work on quantum cryptography to find publication. His original paper on the subject, Conjugate Coding, was published in 1983, more than ten years after it was written—and even then, not in a prestigious scientific journal, but as a conference paper in the lesser-known SIGACT News [3–4].

Why did the paper receive so little attention? A possible explanation may be that not only were Wiesner's ideas far ahead of their time, but also that the technology of the day was not sufficiently advanced to realize them. His proposed application of quantum physics for the rehauling of cryptography required further mathematical

proof for validation, and the implementation of his ideas, as described in the paper, would necessitate complex engineering work. Without a channel successfully transferring individual polarized photons, it would be impossible to implement quantum information transmission. Countless difficulties arise in the process of producing polarized photons, to begin with, sending the photons without disturbing them with background noise, and, finally, receiving the photons and taking in the information. It would have been impossible at that time to build equipment to overcome these difficulties, and thus to enable the execution of Wiesner's proposed experiments.

Fortunately, despite not being able to publish his proposal for quantum cryptography until more than a decade after he first formulated it, Wiesner did not lose faith in its viability. He shared his ideas with his long-time friend Charles Bennett, who had studied alongside Wiesner when the two were undergraduates. Upon learning of Wiesner's hypothesis that one could use quantum mechanics to produce banknotes that are impossible to counterfeit, and even to create a completely secure communication channel, Bennett's interest in quantum cryptography was ignited. He decided to take Wiesner's ideas a step further. In 1979, another important member of this groundbreaking group of researchers joined: Giles Brassard, whom Bennett had met while swimming, after which the two discussed Wiesner's proposals and embarked on their journey into quantum cryptography.

4. Continual advancement: The BB84 scheme and the efforts by Brassard and Bennett

In 1984, Bennett and Brassard published Public Key Distribution and Coin Tossing, a key paper that would become the foundation for all further developments in quantum cryptography. In this paper, the two formulated a cryptographic scheme later known as the BB84 (that is, Brassard and Bennett 1984) scheme. To understand this scheme, it is necessary to introduce the concept of public-key cryptography.

Public-key cryptography involves the use of asymmetric keys, a public key, which, as its name suggests, is open to the public; and a private key, which is kept to oneself. In this method, messages are encrypted using public keys but can only be decrypted with the aid of private keys. This means that even if a message is intercepted, the eavesdropper cannot hope to decode it. Drawing on this method, Brassard and Bennett developed a cryptographic scheme utilizing quantum mechanics. The paper uses the term "quantum coding" to describe a communication channel that could "distribute random key information between users with the assurance of keeping the information unknown to others, guaranteed by fundamental quantum mechanical principles and phenomena like the uncertainty principle and the Einstein-Poldosky-Rosen (EPR) paradox" [5]. The paper proposes a radically different approach to encryption compared to contemporaneous cryptosystems such as Enigma or DES. Bennett and Brassard argue that even without the sender and the receiver sharing any secret information, they can measure disturbances of quantum information to assess whether messages between them can be exchanged securely and defer communication until such time as it can be. They illustrate their proposed scheme by referencing how coin flipping by telephone can take place. In their game, the receiver must guess which basis the sender is using to encode photons. Given the difficulty of falsifying a table on an alternate basis, "because the table is the result of probabilistic behavior of the photons after they left her hands", the sender cannot reliably cheat using traditional methods.

What was the scientific community's response to this new groundbreaking scheme? At first, Bennett and Brassard met with little additional success than Wiesner did with his original paper. In the first few years after publication, no one referenced the paper other than the authors themselves. Yet, as can be seen in later works by

subsequent researchers, BB84 was the basis for all the developments that followed.

After completing the BB84 paper, Bennett and Brassard continued to write on the topic, quantum cryptography was far from complete, and there were new issues to tackle. In 1986, the two sought a way to address the disclosure of information during transmission. In a paper from that year, they used the example of two people seeking to exchange secrets. Bob wants to know Alice's secrets, but Alice is only willing to share one of her secrets and does not want Bob to gain more information than that single secret. Alice agrees to let Bob choose the secret, but Bob does not want to reveal which secret he wants. Through theoretical analysis, they were able to apply quantum cryptography to information theory, then the main theory of encryption, thereby solving this problem. The field's response improved only slightly but remained relatively muted. Out of the five papers citing this research, two were written by Brassard himself, and one more by Bennett.

Later in 1986, Bennett and Brassard published a book entitled "Modern Cryptography: A Tutorial" [6]. Aimed at college students, it contains six chapters outlining the development of cryptosystems from ancient times to the present day. It offers information on the historical context in which cryptography emerged and discusses recent breakthroughs in the field of cryptography—including Shannon's information theory, mathematical and computational methods, and quantum cryptography.

The textbook also offered an innovative way for Bennett and Brassard to assert the importance and potential of quantum cryptography to a new, less specialized audience. The textbook also enabled professors elsewhere to apply and disseminate their insights into this new topic. Without a formal textbook, it was hard for the subject to gain popularity among undergraduate students. Only when students began to read original papers in graduate school could they truly understand this topic.

The first researcher to publish a serious paper on quantum cryptography was Wiedemann. Surprisingly, he had not even heard of Bennett and Brassard's work. In his 1986 paper, "Quantum Cryptography", Wiedemann explicitly referenced Wiesner's work in the development of "a method of public key distribution which is provably secure under quantum mechanics" [7]. He raised the same concept of performing cryptography using quantum mechanical principles, proposed a protocol identical to that of Bennett and Brassard, and claimed to have come up with the idea of quantum cryptography independently of Stephen Wiesner. Awkwardly, Bennett and Brassard responded by pointing out that they had already come up with the same proposal and also addressed some of the difficulties mentioned in Wiedemann's paper. Yet this demonstrated that more scholars were beginning to be interested in the topic.

Brassard continued to publish, writing Minimum Disclosure Proofs of Knowledge. Here, he sought to resolve the question of how to minimize the amount of information needed to convince others that one's own knowledge of something is verifiable and true. He explains the issue regarding two fictional people, Peggy and Vic. It is assumed that Peggy knows some verifiable information. To convince Vic that the information is true, Peggy can reveal it to Vic himself—which would be a "maximum disclosure" proof. Alternatively, she can develop a protocol to convince Vic that she possesses information that would pass the certifying procedure, but in a way that does not help him determine the information.

As a recap, from 1983 onwards, Brassard and Bennett published numerous papers aimed at advancing quantum cryptography theoretically and spreading its ideas. From their first paper establishing a cryptographic protocol, Public Key Distribution and Coin Tossing, to the college textbook they prepared, Modern Cryptography, and the regular advancements pushing the development of the field forward, Brassard and Bennett ensured that quantum cryptography remained at the forefront of the conversation. This was critical because of the funding

required to make more substantial experimental advancements. Without an increase in popularity, this significant field might not yield any promising results.

5. Beginning of breakthrough: The introduction of Bell's theorem and entanglement

The next giant leap forward for quantum cryptography was the application of entanglement and Bell's theorem, after which the idea of quantum cryptography really took off. Bell's theorem, proposed by John Bell, addresses the problem of locality in quantum mechanics. Quantum physics often describes phenomena and their states using a probabilistic function, which can lead to results that seem to contradict common sense. Einstein and his colleagues produced a thought experiment attempting to point out the flaw in quantum theory. If two particles were to be created from the splitting of a single particle with each carrying a definite spin, then according to the law of the conservation of energy, whatever the individual spin of each particle, the two must have opposite spin—one upward and one downward. Before measuring either one, the state of both remains unknown to the observer, with the two particles being in a state of entanglement. This means that their states are opposite, but people do not know the exact state of each.

However, if the two particles were to be separated a great distance from each other, and the spin of one particle is measured, then the spin of the other particle would be instantaneously known, even if it might be light years away. This is equivalent to sending a message with a speed faster than light, violating one of physics' fundamental tenets. Locality, which holds that objects are only directly influenced by their immediate surroundings, would be disproven. This famous paradox is called the EPR (Einstein, Podolsky, Rosen) paradox. Bell's theorem focuses on this issue. By deriving an inequality, Bell proposed a possible method to prove which opinion was correct—locality or quantum mechanics.

Bell's theorem attracted the interest of many researchers, which included a very special group of people, the Fundamental Fysiks Group.

6. Sparking insights: The Fundamental Fysiks Group's contribution

The Fundamental Fysiks Group was unique, as it consisted of researchers passionate about physics yet not in academia. As described by David Kaiser in the book How the Hippies Saved Physics, the group was started by Nick Herbert, Jack Sarfatti, and others in Berkeley, California. Unlike academic physics, which seemed caught up in minute mathematical calculations, the group comprised physics lovers who wanted to find answers to the profound interpretative questions behind quantum physics. They delved into the philosophical aspects of things, relating physics to the perception of the world.

Bell's theorem is something that they were extremely passionate about, as it completely contradicts the view of the world. Do things not actually have locality, and do statistical results truly dominate a multitude of the phenomena observed? Does the non-locality, or "spooky action at a distance" as coined by Einstein himself, allow for the transmission of information faster than the speed of light?

To test whether superluminal teleportation—the sending of information at speeds faster than light is possible, Nick Herbert devised an experiment that he coined the QUICK apparatus. In this experiment, two experimenters measure the polarization of light coming their way. There are two kinds of polarization that the experimenters can try to measure: linear and circular. Two pairs of entangled photons are sent to A and B. At A's end, if the experimenter decides to measure the linear polarization of photons, then this measurement collapses the

entanglement, and the twin photons at B's end would immediately enter the same state of polarization. Thus, A can send a message to B immediately through B's measurement.

The initial design was impossible to realize. To get the result on the single photon level, the test plate would need to be infinitely large yet still sensitive to the slightest perturbation. Nevertheless, Herbert did not abandon this idea and improved his design into a new system called First Laser-Amplified Superluminal Hookup (FLASH). The correction was that before arriving at B's end, photons would go into a laser tube, making them coherent. With this design, Herbert and his colleagues were confident that it could be successful, but this was not the case. Critics were still able to spot a fatal mechanical flaw in the scheme, the improbable nature of creating the ideal laser tube required for it.

Despite the failure of superluminal teleportation, the Fundamental Fysiks Group garnered great attention from both the scientific community and the general public. Physicists like Dennis Dieks, Giancarlo Ghiradi, and Wojciech Zurek all became involved with the group's design—although they opposed its proposals. Dieks, a young physicist then based in Utrecht, pondered over the FLASH design and pointed out its flaws in his research paper. However, he credited many of his reflections to Herbert's paper. Ghirardi, a physicist at the International Centre for Theoretical Physics, firmly opposed Herbert's every design, clearly stating his opinion when Foundations of Physics consulted him on whether or not to accept Herbert's paper. It was Ghirardi who spotted the mistake in Herbert's design, a flaw that most did not see. Even famous physicist Richard Feynman could not identify the flaw upon first reading Herbert's paper. It was Zurek, who would later be known for his work on the no-cloning theorem, who pointed out the mistake in the design to Feynman. This shows how widespread Herbert's ideas had become, attracting the attention of many prestigious physicists.

Although the design did not have many supporters after its flaws were revealed, it still caused quite a commotion. Their fascination with almost fictional technology like superluminal communication was something truly unique at that time. At a time when mainstream physics focused on progress and looked down upon interpretation and philosophical thinking, the group emphasized the fundamental meanings of modern physics. Ironically, even John Bell's research and ideas were initially ignored by his professors and contemporaries due to their deviation from the mainstream, and it was only after some time that people became interested in the topic. Similarly, the topics that the Fundamental Fysiks Group worked on were far from trivial. The FLASH design attracted wide discussion, and the basic logic and design were related to the BB84 design in quantum cryptography. They all used polarized photons, but entanglement was not yet included in quantum cryptography, an intervention that would require Artur Ekert.

7. Big evolution: Debate about entanglement

Despite Bennett and Brassard's continued efforts, quantum cryptography was still struggling. Enter quantum entanglement. Between 1991 and 1992, two papers revolutionized the field of quantum cryptography [8]. The first was "Quantum Cryptography Based on Bell's Theorem", published in 1991 by Artur Ekert, still a graduate student at Oxford [9]. It presented an approach to solving the problem of quantum key distribution different from that put forward by Brassard and Bennett: offering an alternative to their 1984 original key distribution scheme (BB84), Ekert's own scheme made use of Bell's theorem and entanglement rather than the uncertainty principle.

Ekert proposed a key distribution process whose security depends on the completeness of quantum mechanics. As Bennett and Brassard summarized in their later response, two separated observers perform

measurements on a sequence of EPR-correlated pairs of particles to generate identical random numbers. The scheme introduces two novelties. First, it uses entangled pairs of photons, whereas the scheme by Bennett and Brassard only used polarized photons. Second, it makes use of entanglement to refine the process by which eavesdropping is detected while at the same time being able to test whether the photon's polarization has been affected by outside measurement. By observing whether the photon's state has been altered, people can now detect whether the information sent has been tampered with.

This new approach presents a theoretical extension of Bennett and Brassard's original idea and realizes a small change to experiments. Part of the force of Ekert's intervention is that it presented the mathematics underpinning this. Ekert was able to prove in this paper how this scheme could be used to transfer information securely, protected by the laws of physics. However, perhaps the greatest significance of this intervention was that it rendered the encryption process more practicable with the application of entanglement, proposing a way to ensure the safety of information sent and received.

Shortly after the publication of Ekert's paper, Bennett and Brassard published a rebuttal: the 1992 "Quantum Cryptography without Bell's Theorem", which appeared in Physical Review Letters [10]. Defending their own scheme, Bennett and Brassard responded to Ekert by claiming that quantum cryptography did not require Bell's theorem. They noted that a sophisticated attack is possible on the system, due to the entangled nature of the pairs. An alternative central body, they argued, could introduce a station that produces three correlated particles, allowing an eavesdropper to take control of the system. This exploit ("source substitution") undermines the security of the system. For this reason, they suggested that Bell's theorem is unlikely to prove important in quantum key distribution and that Ekert's new scheme was, in fact, equivalent, in essence, to their original scheme, BB84. On the other hand, Bennett and Brassard claimed, that their own refined and demonstrably simpler scheme was provably secure against all known sources of attack in quantum cryptography.

Crucial to this debate was the security of different key distribution protocols. Compared to the original paper by Wiesner, this marked a significant development in the discipline. Yet, Ekert's 1991 paper is best considered as an extension rather than a challenge to Bennett and Brassard's idea, for it did not point out any theoretical weaknesses in their proposal, but only presented an alternative protocol for key distribution (as well as directly connecting the process with current experimental research). In contrast, the 1992 paper by Bennett and Brassard pointed out flaws in Ekert's 1991 contribution.

The debate quickly drew great attention. This is perhaps due both to the addition of Bell's theorem, a prominent topic of research at that time, and to the fast development of information technology. In the 1990s, computer science was developing rapidly with the advent of major software and systems like Microsoft Windows, Linux, and Adobe. People were gradually entering the digital age, with MP3s, portable computers, and internet browsers appearing and spreading. Online information security was becoming increasingly a pressing problem.

Ekert's paper was cited nearly a hundred times within a few years of its publication (it currently has more than 13,000 citations). This marked a significant departure from the work of Bennett and Brassard, whose previous attempts at popularizing quantum cryptography had been only sporadically cited. The increased attention drawn by quantum cryptography at that time can also be glimpsed from the increasing citations of Wiesner's Conjugate Coding, which was initially neglected despite Bennett and Brassard's joint efforts for nearly a decade. After the duo of papers, quantum cryptography became a hot topic of discussion, with increasing numbers of people entering this field of research. Overall, "Quantum Cryptography Based on Bell's Theorem" opened a new page in quantum cryptography.

How would things develop after the debate? Would quantum cryptography continue down its path as before, or would it adopt Ekert's new scheme?

The following year, Bennett, Brassard, and Crepeau published their latest findings in a paper titled "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels" [11]. This was the first time that Bennett, Brassard, and their colleagues had considered the application of entanglement in their theory, signaling the impact of Ekert's paper on their research, as they attempted to establish an application of Wiesner's work on transporting information.

This paper applied Wiesner's original paper, which focused on purely theoretical calculations, to the problem of teleportation of the Einstein-Podolsky-Rosen (EPR) pairs of particles, which they suggest might allow people to send information over long distances securely and quickly. By prearranging the sharing of an EPR-correlated pair of particles, Alice and Bob can transfer information and replicate the unknown state that Alice had destroyed with her measurement. The instantaneous transfer of information by EPR was seemingly impossible. However, EPR particles can assist in the teleportation of "an intact quantum state from one place to another." To transfer the information to Bob, Alice can send the particle herself, or she can make it "interact unitarily with another system, or an 'ancilla'". When Bob receives the ancilla, he can reverse her actions to replicate the original state. Through this process, teleportation of a quantum state can be achieved.

Ekert, after the 1992 rebuttal from Bennett and Brassard saying that Ekert's 1991 scheme was flawed, published "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels" in 1996 as a defense of Ekert's claim of quantum cryptography using Bell's theorem [12]. The paper introduced a new concept called Quantum privacy amplification (QPA). The same year another paper was published by Bennett and Brassard, "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels" [13]. This paper presented another technology that was newly developed. Together, these two papers marked the continued development of Ekert's initial innovative use of entanglement, pushing forward the advancement of quantum cryptography.

In their discussion of quantum privacy amplification, Ekert and his fellow researchers described how Alice and Bob detect eavesdropping by "performing certain quantum measurements on transmitted batches of qubits", which had been mentioned in previous papers. However, this leads to the problem that it is impossible to distinguish between noise from eavesdroppers and noise from the environment. It was likely that all current protocols were inoperable in the presence of noise. Existing schemes which aimed to fix this issue had not yet been proven to be secure. This paper presented a protocol that was safe in the presence of noise and eavesdroppers. By applying Bell's theorem, also called entanglement-based cryptography, plus an entanglement purification procedure, the protocol was able to allow the people transporting information to generate a maximally entangled state that has low entanglement with the outside system. The procedure, called a quantum privacy amplification algorithm, can be performed with a series of operations by the two individuals sending information. This paper therefore provided theoretical support for the possibility of the scheme set out in Ekert's 1991 paper, boosting Ekert's proposal of entanglement-based quantum cryptography.

Bennett and Brassard first introduced quantum teleportation and quantum data compression in their 1992 paper. Quantum data compression, like classical data compression techniques, allows data to be transmitted with perfect fidelity using qubits (quantum bits). Quantum teleportation achieved faithful transmission differently, substituting classical communication and previous entanglement for a quantum channel. Similarly, the two methods were all noiseless channels. Although it was plausible to use current technologies to correct errors in

the transmission process, there was another way to deal with the problem. Their 1996 paper outlined a method in which the noisy channel "is not used to transmit the source states directly." By performing unitary operations and measurements on the entangled pairs, the two people transporting information could purify the pairs first, and then use them for teleportation. The result was an almost perfectly pure pair of entangled states that could be used to teleport information from sender to receiver. A noisy channel can simulate a noiseless one, leading to faithful teleportation. Thus, if a purification of noise could be achieved, Ekert's proposal could be further developed.

The two back-to-back papers in 1996 provided theoretical groundwork for quantum cryptography in noisy channels, applying Ekert's claim to real world situations. Unlike past research by Bennett and Brassard, these papers were increasingly oriented toward application. Technologies like quantum privacy amplification are necessary to realize the cryptographic protocols in real life, as noise during transmission was a significant hindrance to the accomplishment of Bennett and Brassard's scheme. As Brassard himself put it, "The idea (Ekert's scheme in 1991) proved to be very fertile, particularly after the invention of entanglement distillation and quantum privacy amplification" [14]. In conclusion, the two papers helped Ekert defend his scheme using Bell's theorem and led to the development of quantum cryptography based on Ekert's entanglement-based cryptography instead of the BB84 scheme by Bennett and Brassard.

Although Ekert's scheme was still "technically more challenging to implement" because it required the transmission of photon pairs and difficulties still hindered its rapid development, the value of Ekert's claim was evident, because it provided a convenient handle for proving quantum key distribution schemes secure against general attacks [15]. It constituted a necessary addition to the BB84 scheme that brought the realization of quantum cryptography closer.

The debate brought quantum cryptography to the forefront. It was after this period that the subject took off, transforming from a mere vision by Wiesner to a mature and ready-to-go state.

8. The story continues

Following the publication of Ekert's 1991 paper, an increasing number of people began to take notice of quantum cryptography. Yet it was only in 1995 that quantum cryptography suddenly took off. Papers on the subject increased dramatically, and new names appeared; new theories were proposed, old theories were proven, and experiments were conducted all over the world. Before looking into the field's application in the information era, people should ask why it suddenly became popular: was it merely because of Ekert's paper, or were there more factors at play?

The general interest of the public was greatly ignited after the appearance of Ekert's paper on quantum cryptography based on Bell's theorem in 1991. Appearing as it did, not in a journal dedicated to cryptography but one dedicated to physics, it stood out as a rare application of a groundbreaking theorem in physics to the relatively less well-known subject of quantum cryptography. This shocked many researchers, regardless of their previous experience with quantum cryptography. For researchers in quantum cryptography, it was surprising to see a newcomer propose a completely new approach to public key distribution. Ekert had raised a new, more workable approach to an existing problem, challenging the primacy of the well-established scheme of Bennett and Brassard. For those outside cryptography, it drew their attention to this new field. This is apparent in the wide range of people participating in the theoretical research of quantum cryptography. It was no longer Bennett and Brassard, along with a few of their colleagues, pushing their way forward into the unknown realm of quantum cryptography

without any support and attention from the outside. Their attempts to promote Wiesner's original ideas had nearly all fallen short, but, through the publication of Ekert's paper and the conversation that emerged around it, quantum cryptography was finally able to move forward with the joint efforts of researchers. Undoubtedly, this popularity was also influenced by the development of computer science and the internet, which led to rising pressure for a secure encryption system to guard everyone's information.

As quantum cryptography became more popular, many new names emerged [15]. The focus of these researchers can broadly be divided into two categories: experimental and theoretical. Some researchers worked on theories within cryptography, such as establishing flawless mathematical proofs for key distribution schemes and demonstrating their security under general cases of attack. Huttner, Ekert, Massimo Palma, and Asher Peres researched eavesdropping in cryptography in 1994 [16]. Norbert Lutkenhaus also studied the problem of security against eavesdropping in 1996 [17]. In particular, in 1996, the BB84 was at last validated theoretically when Dominic Mayers proved the scheme consistent with quantum mechanics, which drew on Andrew C-C Yao's work on the proof of quantum protocols in 1995 and his earlier study in 1996 on the transfer of information in noisy channels [18–20]. These studies aimed to improve the safety of transporting information against attacks or in noisy channels, which was a major problem in quantum cryptography. With a sound theoretical analysis and corresponding experimental validation, quantum cryptography soon became a more standardized and organized field of research.

Besides improving upon Bennett and Brassard's scheme, many researchers worked on establishing different protocols. Ekert's famous 1991 proposal is perhaps the most prominent of these, having brought entanglement into the mix. After this, many others followed. Wiesner himself proposed a quantum cryptographic system with bright light in 1993 [21]. Matsueda described a system that uses spontaneous photon emissions in 1995 [22]. All of these protocols, though some may not be used, still push forward advancements in the field as new ideas and innovations are generated.

Experimental implementation is also crucial to the realization of quantum cryptography. Remember, a significant reason why the subject started slowly was due to the difficulties in experimental implementation. The first experiment to prove the feasibility of quantum key distribution was done by Bennett, Brassard, and three other researchers in Experimental Quantum Cryptography [23]. Then in 1997, researchers Gisin, Ribordy, Gautier, and Zbinden proposed a setup for quantum cryptography based on photon pairs, a setup that could be carried out in a laboratory experiment [24]. The results made it clear that quantum cryptography was no longer something purely theoretical. They demonstrated that the theories could be applied to the real world, showcasing the practicality and potential of the field. It is precisely this work that turned quantum cryptography from a mere imagination to a real technology.

The potential applications of quantum cryptography, once its feasibility had been demonstrated, were enormous. Jaroslav Hruby worked on implementing a quantum smart card for identification, proposing to use quantum key distribution, and publishing his results in 1995 [25]. Townsend and his colleagues developed a method for securing a communication network with quantum cryptography in 1996 [26]. Richard Hughes and fellow collaborators considered quantum cryptography through satellites after having implemented long-distance experiments on it [27]. The list goes on and on.

The productivity of this period can be seen by the sheer variety and number of papers published. The flurry of discoveries and achievements has even been the subject of personal memoirs, for example in Brassard's 2006 Brief History of Quantum Cryptography: A Personal Perspective. From Ekert to Mayers, from Yao to Huttner, it

was the convergence of leading minds on the subject that marked the real turning point for quantum cryptography.

9. Conclusion

Returning to 2004, the first electric transfer in Vienna, developed by Anton Zeilinger of the University of Vienna, marked a significant milestone in quantum cryptography. The transfer involved transmitting pairs of entangled photons between Bank Austria Creditanstalt and Vienna City Hall using optical fiber, demonstrating the practical application of quantum cryptography. Observing their polarization confirms the validity of the transaction. Zeilinger's work built directly on the progressive developments in the field. Notice that the starting point of this experiment was not with the single photon envisaged by Wiesner, or Brassard and Bennett, but with entangled pairs of photons as suggested by Ekert using Bell's theorem and the EPR paradox, as indeed Brassard and Bennett's later research also demonstrates.

The event, attended by the mayor, scientists, and various bankers, highlighted the collaborative nature of scientific progress. While Wiesner's initial concept laid the foundation, it was the collaboration between Bennett, Brassard, Ekert, and their contemporaries that propelled the field forward. The story shows the cumulative effort required for scientific advancement. Without Bell's theorem, the rapid advancements leading to the realization of quantum cryptography would never have taken place. Bell's theorem itself exists because of Einstein's mistaken conjectures about apparent flaws in quantum mechanics, illustrating that even perceived failures can contribute to significant scientific progress. Without the Fundamental Fysiks Group's impassioned exploration of Bell's theorem and the philosophical conundrums posed by physics' thought experiments, the notion of entanglement cryptography probably would not have developed so rapidly and been accepted so readily. From this whole process, people can see that science is never the story of one person or even a single group. Rather, it is the collective efforts of many, the combined force of repeated experimentation and conjecture, each result building upon the last.

Disclosure statement

The author declares no conflict of interest.

References

[1] Kaiser D, 2011, How the Hippies Saved Physics: Science, Counterculture, and the Quantum Revival. W.W. Norton & Company, New York.

[2] Churchhouse RF, 2002, Codes and Ciphers: Julius Caesar, the Enigma, and the Internet. Cambridge University Press, Cambridge.

[3] Bennett CH, Brassard G, 1984, An Update on Quantum Cryptography, in Workshop on the Theory and Application of Cryptographic Techniques. Springer Berlin Heidelberg, Berlin, 475–477.

[4] Wiesner S, 1983, Conjugate Coding. ACM Sigact News, 15(1): 78–88.

[5] Bennett CH, Brassard G, 1984, Public Key Distribution and Coin Tossing. IEEE International Conference on Computer System and Application, Bangalore, India, 175–179.

[6] Brassard G, 1988, Quantum Cryptography, in Modern Cryptography: A Tutorial. Springer, Heidelberg, 79–90.

[7] Wiedemann D, 1986, Quantum Cryptography, ACM Sigact News, 18(2): 48–51.

[8] Brassard G, 2005, Brief History of Quantum Cryptography: A Personal Perspective, in IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 19–23.

[9] Ekert AK, 1991, Quantum Cryptography Based on Bell's Theorem. Physical Review Letters, 67(6): 661–663.

[10] Bennett CH, Brassard G, Mermin ND, 1992, Quantum Cryptography without Bell's Theorem. Physical Review Letters, 68(5): 557–559.

[11] Bennett CH, Brassard G, Crepeau C, et al., 1993, Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. Physical Review Letters, 70(13): 1895–1899.

[12] Deutsch D, Ekert A, Jozsa R, et al., 1996, Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels. Physical Review Letters, 77(13): 2818–2821.

[13] Bennett CH, Brassard G, Popescu S, et al., 1996, Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. Physical Review Letters, 76(5): 722–725.

[14] Brassard G, 2005, Brief History of Quantum Cryptography: A Personal Perspective, in IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 19–23.

[15] Brassard G, Crepeau C, 1996, 25 Years of Quantum Cryptography. ACM Sigact News, 27(3): 13–24.

[16] Ekert AK, Huttner B, Palma GM, et al., 1994, Eavesdropping on Quantum-Cryptographical Systems. Physical Review A, 50(2): 1047–1056.

[17] Lutkenhaus N, 1996, Security against Eavesdropping in Quantum Cryptography. Physical Review A, 54(1): 97–111.

[18] Dominic M, 1996, Quantum Key Distribution and String Oblivious Transfer in Noisy Channels, in Annual International Cryptology Conference. Springer, Berlin, 343–357.

[19] Dominic M, Salvail L, 1994, Quantum Oblivious Transfer is Secure against All Individual Measurements, in Proceedings Workshop on Physics and Computation. PhysComp'94 IEEE, 69–77.

[20] Yao ACC, 1995, Security of Quantum Protocols against Coherent Measurements, in Proceedings of the Twenty-seventh Annual ACM Symposium on Theory of Computing, 67–75.

[21] Wiesner S, 1993, Quantum Cryptography with Bright Light, manuscript.

[22] Matsueda H, 1995, Quantum Cryptography by Modulating Spontaneous Photon Emissions. Conference on Lasers and Electro-Optics, Pacific Rim.

[23] Bennett CH, Bessette F, Brassard G, et al., 1992, Experimental Quantum Cryptography. Journal of Cryptology, 1992(5): 3–28.

[24] Ribordy G, Brendel J, Gautier JD, et al., 2000, Long-distance Entanglement-based Quantum Key Distribution. Physical Review A, 63(1): 012309.

[25] Hruby J, 1995, Smart-card with Interferometric Quantum Cryptography Device, in International Conference on Cryptography: Policy and Algorithms. Springer Berlin Heidelberg, Berlin, 282–289.

[26] Townsend PD, Marand C, Phoenix SJD, et al., 1996, Secure Optical Communications Systems Using Quantum Cryptography, in Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 354(1708): 805–817.

[27] Hughes RJ, Buttler WT, Kwiat PG, et al., 1998, Practical Free-space Quantum Cryptography, in NASA International Conference on Quantum Computing and Quantum Communications. Springer Berlin Heidelberg, Berlin, 200–213.