RIGA TECHNICAL UNIVERSITY

Information Technology and Management Science

ISSN 2255-9094 (online)
ISSN 2255-9086 (print)
December 2018, vol. 21, pp. 37–44
doi: 10.7250/itms-2018-0005
https://itms-journals.rtu.lv

An Overview of Quantum Key Distribution Protocols

Anastasija Trizna[1], Andris Ozols[2]
[1, 2] *Riga Technical University, Riga, Latvia*

***Abstract* – Quantum key distribution (QKD) is the objects of close attention and rapid progress due to the fact that once first quantum computers are available – classical cryptography systems will become partially or completely insecure. The potential threat to today's information security cannot be neglected, and efficient quantum computing algorithms already exist. Quantum cryptography brings a completely new level of security and is based on quantum physics principles, comparing with the classical systems that rely on hard mathematical problems. The aim of the article is to overview QKD and the most conspicuous and prominent QKD protocols, their workflow and security basement. The article covers 17 QKD protocols and each introduces novel ideas for further QKD system improvement.**

***Keywords* – CV-QKD, DI-QKD, DV-QKD, MDI-QKD, public cryptography QKD, QKD, quantum cryptography.**

I. Introduction

Current cryptography security relies on hard mathematical problems impossible to break nowadays on classical computer (CC) within a polynomial time. For example, public-key cryptography relies on the mathematical assumption that prime factorization is impossible to be solved by CC, due to computational power limitation and/or lack of efficient algorithm for solving a factorization problem.

However, with quantum computer (QC) the things change. Quantum physics has changed our view of nature fundamentally and widened technological horizons. Moreover, there is an efficient factorization algorithm on a QC [1]. This suggests that as soon as the first large-scale quantum computer switches on, most of today's crypto-graphic systems could collapse overnight [2]. Quantum key distribution will bring new levels of confidentiality and privacy of communication services [3].

In the present study, the most prominent quantum key distribution protocols are explained, and comparative summary is prepared.

The present paper covers the proved QC algorithms that will expose CC cryptography (Section 2). Brief introduction in quantum physics principles in the basement of quantum cryptography are covered in Section 3 and the notion of a qubit is introduced in Section 4. Section 5 provides a survey of quantum key distribution protocols. The comparison table of QKD protocols is prepared in Section 6, and Section 7 contains research findings.

II. Quantum Computing Impact on Cryptography

Currently, there are two efficient quantum algorithms that may impact classical cryptography: Grove's and Shor's algorithms. While Grover's algorithm does not provide as spectacular speedup as Shor's algorithms, the widespread applicability of search-based methodologies has excited considerable interest in Grover's algorithm [4].

A. Shor's Algorithm and Impact on Asymmetric Cryptography

P. Shor (1994) demonstrated [1] that two enormously important problems – the problem of finding the prime factors of an integer and discrete logarithm problem – could be solved efficiently on a quantum computer.

The factorization of large integers has always been a hard problem for classical computing and is used for the public key cryptography systems. Shor's algorithms and the progressing maturity of quantum computing makes ECC (Elliptic-Curve Crypto) and RSA (Rivest–Shamir–Adleman cryptosystem) increasingly vulnerable to quantum attacks over time. Present implementations of TLS/SSL (Transport Layer Security) rely upon RSA public keys for server authentication and Diffie-Hellman for key agreement, both of which are susceptible to attack by Shor's algorithm [3].

The time it takes for the classical algorithm to factor numbers goes up as 2n where n is the length of the number; this is exponential complexity. Shor's quantum factoring algorithm requires the time that goes up only as n3, i.e., a polynomial complexity rather than an exponential complexity.

B. Grove's Algorithm against Symmetric Cryptography

Further evidence for the power of quantum computers came in 1995 when L. Grover showed that the problem of conducting a search could be sped up by quantum computer [4].

The quantum search algorithm solves the following problem: Given a search space of size N, and no prior knowledge about the structure of the information in it (e.g., phone directory containing N names arranged in completely random order), we want to find an element of that search space satisfying a known property. How long does it take to find an element satisfying that property? Classically, this problem requires approximately N operations, but the quantum search algorithm allows it to be solved using approximately N operations [2]. Grover's search algorithm would allow for a quadratic speedup of quantum computers in brute force search, which means that the primitives need to double the key length to maintain the same level of security against a quantum computer [3].

C. ETSI (European Telecommunications Standards Institute) Post-Quantum Table

Based on the algorithms described above and studies performed over the years, the ETSI created a table comparison of conventional and quantum security levels of some popular ciphers in 2015 [3].

TABLE I

ETSI POST-QUANTUM TABLE [3]

Algorithm	**Key length**	**Effective key strength/Security level**	
		Conventional computing	**Quantum computing**
RSA-1024	1024 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-25	256 bits	128 bits	0 bits
ECC-3846	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

In Table I, effective key strength characterising the security level, for conventional computing (CC), is derived from NIST SP 800-57 "Recommendation for Key Management", evaluation based on GNFS (General Number Field Sieve) – the most efficient classical algorithm known for factoring integers larger than 10100. Time consumption of the classical computer scales with 2n (where n corresponds to key length in bits) attempts to determine the key.

III. QUANTUM PHYSICS PRINCIPLES IN THE BASEMENT OF CRYPTOGRAPHY

In quantum cryptography systems, the principles of quantum physics are applied to generate a secret data encryption key. The security of this key is guaranteed by the laws of quantum physics, and this distributed key can be used to encrypt data to enable secure communication on insecure channels. The major principles of quantum mechanics that allow us to build a security basement for quantum cryptography [5] are listed below:

Superposition. It states that, much like waves in classical physics, quantum states can be added together – superposed – to yield a new valid quantum state; and conversely, that every quantum state can be described as a linear combination, a sum of other distinct quantum states.

Heisenberg uncertainty principle. W. Heisenberg (1927) [6] performed a famous thought experiment measuring the position of an electron using a gamma-ray microscope. This experiment led to the concept of the position and momentum uncertainties of the electron under observation. Too much precision in q0 (initial position coordinate) produces great uncertainty in p0 (initial momentum). From Heisenberg uncertainty principle, the property follows that it is not possible to measure the quantum state of any quantum system without disturbing that system. Thus, the polarization of quantum particle can only be known at the point where it is measured.

Coherence. The coherence is a quantum particle ability to maintain superposition over time. It is the absence of "decoherence", which is any process that collapses the state into a classical state, for instance, by interaction with an environment or as a result of performed measurement.

Entanglement, EPR-correlations, Bell states. Entanglement is a connection between two quantum particles and an ability to keep this connection over a time and distance. When particles are measured in the same basis, they will always yield the same outcome. This outcome is not decided beforehand, but it is completely random and is decided when the measurement happens. If two particles are maximally entangled with each other, then no other party in the universe can have a share of this entanglement. This property is called the monogamy of entanglement.

The term "EPR correlations" was born by Einstein, Podolsky, and Rosen [7] while demonstrating the incompleteness of quantum mechanics using quantum entanglement.

J. Bell (1964) showed a discrepancy between predictions for the correlations between entangled spin particles given by quantum mechanics and local realistic theories. Bell's theorem is about checking non-local correlations and verifying entanglement.

No-cloning theorem. The no-cloning principle is a fundamental property of quantum mechanics, which states that given an unknown quantum state there is no way to produce copies of that state. It was discovered and announced by Wootters, Zurek, and Dieks (1982) [8], and it had profound implications in quantum computing and related fields. This also means that information encoded in quantum states is essentially unique.

IV. QUANTUM BIT – QUBIT

A qubit is a quantum system that can have only two orthogonal states, where one state will be defined to be zero and the other – to be one. According to quantum mechanics, a qubit can also be in any superposition of these two levels. It is possible for a quantum system to have multiple states [9]. Each qubit can be represented as a linear combination of $|0\rangle$ and $|1\rangle$ (braket Dirac notation):

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (1)$$

where α and β are complex probability amplitudes of qubit being 1 or 0. Single-qubit pure states can be represented as points/vectors on Bloch sphere, for example: $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ (see Fig. 1), where $|0\rangle$, $|1\rangle$ is equal to rectilinear (+) and $|+\rangle$, $|-\rangle$ to diagonal (×) particle polarization.

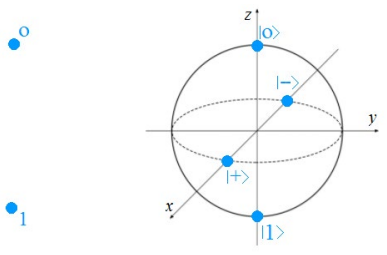

Fig. 1. Classical bits (left) and quantum bit (right). Single-qubit pure states can be represented as points on the surface of the Bloch sphere.

Quantum physic principles endow qubits with very peculiar properties. It is not possible to make copies of qubits recalling no-cloning theorem. Anybody who tries to detect/measure a qubit will disturb its state and force qubit to collapse into one of classical states (Decoherence); this makes channel eavesdropping impossible without disturbing the state. Heisenberg uncertainty principle plays a crucial role in thwarting the attempts of eavesdroppers in a cryptosystem based on quantum cryptography.

Each photon of the EPR pair is in a maximum mixed state (fully non-polarized), the eavesdropper cannot gain any information from the photon when it transmits from the EPR source to the user because there is no information encoded before the measurement is performed. The random bits are generated during the measurement processes.

V. Quantum Key Distribution Protocols and Classifications

Cryptography is a competitive game between the legitimate users and the eavesdropper.

There are conventionally three parties: Alice, Bob and Eve. Alice wants to share a secret message with Bob and at the same time, Eve tries to catch the secret bits without revealing her presence. Most quantum key distribution (QKD) protocols have a similar underlying structure (see Fig. 2). Subsequent steps take place over a classical channel – ordinary public communication channel, assumed to be susceptible to eavesdropping but not to the injection or alteration of messages.

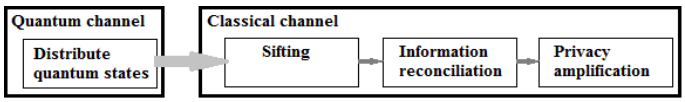

Fig. 2. The common underlying structure of QKD.

During quantum state distribution, a sender (Alice) will prepare and send qubits to a recipient (Bob) over a quantum channel and the recipient (Bob) will measure the income. In sifting or "basis-reconciliation", Alice and Bob analyze the result and discard all rounds where measurement results are not correct. For information reconciliation, Alice sends an error correction to Bob. Alice randomly chooses n of remaining bits to test and says to Bob which rounds are tested. Alice and Bob exchange bits, compare and compute a quantum bit error rate (QBER). Alice and Bob estimate the information gained by an eavesdropper (Eve) during the quantum transmission stage from the observed QBER. If an error rate exceeds the set threshold – they abort the protocol. If the threshold is not reached and no eavesdropper is determined, they will continue with a final round of privacy amplification – Alice and Bob now share a weak secret X, which may be correlated with an eavesdropper holding quantum side information E. Alice chooses a random seed Y for the extractor, and computes RA=Ext($X;Y$). She sends Y to Bob over a public communication channel. Upon receiving Y, Bob sets RB= Ext($X;Y$). Alice and Bob now share a uniformly random key.

A. Discrete Variable and Continuous Variable QKDs

Analogous to the particle-wave duality of light, these two approaches treat light as either particles or waves in order to provide the security.

In discrete variable QKD (DV-QKD), the particle nature of light is exploited to achieve secure key distribution. Information is encoded at the single photon state by a transmitter. Single photon detectors are used to measure the received quantum states.

In continuous variable QKD (CV-QKD), the wave nature of light is exploited to achieve secure key distribution. In this second approach, information is encoded onto the amplitude and phase or onto the corresponding quadrature components (carriers) of a coherent laser light by the transmitter, and the receiver measures the in-phase and quadrature components of light using balanced homodyne detectors [10].

B. Discrete Variable QKD Protocols

BB84

The idea of quantum cryptography appeared in the 1980s. C. H. Bennett and G. Brassard applied a "quantum multiplexing" channel theory to solve the key distribution problem in classical cryptography. In 1984, the well-known BB84 QKD protocol was published [11].

Alice chooses a random bit string and a random sequence of polarization bases (rectilinear or diagonal, see Fig. 3) and prepares qubits. She sends to Bob a train of photons, each representing one bit of the string in the basis chosen for that bit position.

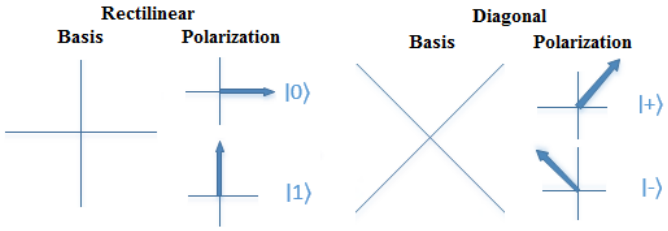

Fig. 3. Rectilinear |0⟩, |1⟩ and diagonal |+⟩, |-⟩ (|-⟩ standing for a binary 1 and |+⟩ standing for a binary 1) measurement bases and photon polarization states.

As Bob receives the photons, he decides randomly for each photon and independently of Alice, which basis he will use to measure the photon and interprets the result of the measurement as a binary 0 or 1. Random answer is produced, and all information is lost when one attempts to measure the rectilinear polarization of a diagonal photon, or vice versa. Thus, Bob obtains meaningful data from only half the photons he detects – those for which he guessed the correct polarization basis.

Bob and Alice first determine, by public exchange of messages, which photons were successfully received, and which measured on a correct basis. If the quantum transmission has been undisturbed, Alice and Bob should agree on the bits encoded by these photons, even though these data have never been discussed over the public channel. Alice and Bob can test for eavesdropping by publicly comparing some of the bits, though this sacrifices the secrecy of these bits. The bit positions used in this comparison should be a random subset of the

correctly received bits, so that eavesdropping on more than a few photons is unlikely to escape detection [11].

E91

QKD scheme, published by A. Ekert (1991), uses entangled pairs of photons [12] and relies on two properties of entanglement: perfect correlation of the results and any attempt at eavesdropping will collapse qubit and destroy EPR state. Alice, Bob or an intermediate transmitter prepares EPR pair of qubits, sends one to Alice and the second – to Bob. Since an entanglement property remains over the distance, once one of protocol parties measures their qubit – the second qubit will show a correlated result (EPR properties).

A. Ekert considered that if Alice and Bob were able to test entanglement between their qubits, then by the monogamy of entanglement they were able to certify that their systems were uncorrelated with Eve's [9]. By a statistical test that confirms the expected violations of Bell's inequality, they can verify the EPR pairs were not subjected to eavesdropping by Eve. After the transmission, they can announce in public the bases they have chosen for each measurement and divide the measurements into two groups: for which they used different bases, and for which they used the same bases. Then they can discard all measurements, in which they failed to register a particle at all [12].

BBM92

The protocol, published by C. H. Bennett el al. (1992) [13], uses weak coherent light and is the first experimental quantum key distribution.

After qubit transmission the same as in BB84, but with very dim light pulses instead of single photons, Alice and Bob exchanged public messages to reconcile the differences between their data. Comparing with BB84, an effective way for Alice and Bob to perform reconciliation is first to agree on a random permutation of their strings (to randomize the locations of errors), then separate strings into blocks of size k and calculate and compare block parities. Blocks with matching parity are accepted as correct, while those of discordant parity are subject to a bisective search, disclosing log(k) further parities of sub-blocks, until the error is found and corrected. To avoid leaking information to Eve during the reconciliation process, Alice and Bob agree to discard the last bit of each block or sub-block whose parity they have disclosed. As a result, Eve has information only about parity bits. Next stage is hash computation and comparison: hash function has the property that if Eve's knowledge of x before privacy amplification was strictly in the form of parity bits, then such is also the case about her knowledge of h(x) [13].

BB92

BB92 protocol, published by C. Bennett (1992), uses two non-orthogonal low-intensity coherent states [14]. The signal pulse is phase shifted 0 or 180 degrees $\{0, \pi\}$ to encode the bits 0 and 1. Alice sends two sequential coherent pulses: a weak signal pulse and a bright reference pulse. The brighter reference pulse is not phase shifted but is delayed by a fixed time and then launched into a fiber. The weak pulse is randomly phase-modulated by $\{0, \pi\}$. Bob measures the signal and reference on a random basis $\{0, \pi\}$. When the phase modulation is matched between Alice and Bob, Bob can count a photon from which they create a secret key [15]. The signal pulse undergoes constructive or destructive interference with the attenuated reference pulse before entering the detector. Eve cannot suppress the reference or signal pulses without being caught [14].

Six-State Protocol (SSP)

The six-state or three bases cryptographic BB84 scheme with an additional basis. SSP was proposed by H. Bechmann-Pasquinucci and N. Gisin (1999) [16]. The six-state or three bases cryptographic scheme is nothing but a well-known BB84 four-state scheme with an additional basis. However, this scheme does hold an advantage compared to the BB84 protocol – higher symmetry. The symmetry of this protocol simplifies considerably the security analysis (compared to the four-state protocol), it reduces the number of parameters necessary to describe general strategies [16].

DPS

Differential-phase-shift was proposed by K. Inoue et al. (2003) [15]. It is based on two non-orthogonal states.

Alice phase-modulates a pulse train of weak coherent states by $\{0, \pi\}$ for each pulse and sends it to Bob. Bob divides each incoming pulse into two paths and recombines them by 50:50 photon beam splitters. Photon detectors are placed at the two outputs of the recombining beam splitter. At the detectors, the partial wave functions of two sequential pulses interfere with each other. With an appropriate phase in the interferometer, Bob's 1st detector clicks for 0 phase difference between the two consecutive pulses and the 2nd detector clicks for π phase difference. After transmission, Bob tells Alice the time instances at which a photon is counted. Under the agreement that the click by detector 1 denotes '0' and the click by detector 2 denotes '1', Alice and Bob obtain an identical bit string. They can find the existence of eavesdropping from this error rate. DPS system utilises all photons for creating the key; thus, the key creation efficiency is n [15].

BB84 Decoy State

In 2003, a decoy idea was proposed by W.-Y. Hwang [17] to address PNS (Photon Number Splitting) attack.

In PNS attack, Eve performs a special measurement to learn the photon number information of laser pulse without disturbing the encoded quantum information. If the laser pulse contains one photon, Eve simply blocks it and Bob will not receive anything. If the laser pulse contains more than one photon, Eve splits out one photon and sends the rest to Bob through a lossless channel. Eve stores the intercepted photons until Bob announces measurement bases. Then she measures her photons in the same bases as Bob. In the end, Eve has an exact copy of a bit.

The insight of the decoy idea is that the PNS attack can be detected by testing the quantum channel during the QKD process. Decoy state helps Alice and Bob to estimate the amount of multi-photon pulses Eve is attaching and the information she is getting.

Alice and Bob conduct QKD with laser pulses having different average photon numbers and evaluate their transmittances and quantum bit error rates (QBERs) separately.

A PNS attack by Eve will inevitably result in different transmittances for signal state and decoy states and thus can be detected [2].

SARG04

Protocol was proposed by V. Scarani el al. (2004) [18]. The basic idea is that Alice should encode each bit into a pair of non-orthogonal states belonging to two or more suitable sets. By encoding a classical bit in sets of non-orthogonal qubit states, a system gains significant robust against PNS attack.

At the 'quantum' level, the protocol is identical to BB84. However, instead of revealing the basis, Alice announces publicly one of the four pairs of non-orthogonal states [17] in which bit might be encoded: s1 = (|1⟩, |+⟩), s2 = (|1⟩, |−⟩), s3 = (|0⟩, |+⟩) and s4 = (|0⟩, |−⟩). If Bob measured the qubit on a correct basis, he would see that he used one of these two non-orthogonal states, and if no – discarded this bit. In PNS attack on SARG04, Eve gets no information which bases to use when measuring her photon even after Alice and Bob agree on the bases used. However, after this sifting procedure Bob is left with 1/4 of the raw list of bits, compared to the 1/2 of the original BB84 protocol.

KMB09

KMB09 [19] was designed by M. M. Khanet et al. (2009).

Alice and Bob use two mutually unbiased bases with one of them encoding a '0' and the other one encoding '1'. The security of the scheme is due to a minimum index transmission error rate (ITER) introduced by an eavesdropper that increases significantly for higher dimensional photon states.

Alice and Bob use two orthogonal bases e and f with all states of 'e' encoding a '0' and all states of 'f' encoding a '1'. All vectors of the same basis encode the same bit. Bit can be transmitted only when Alice and Bob use different bases.

Protocol requires Alice only to share the index of the respective basis state 'i = 1' or 'i = 2' (for N=2). This does not reveal any information about the key if states |eij⟩ and |fij⟩ with the same index i encode different bits. Bob interprets his measurement outcomes after Alice shares the index i of her basis state. He does this by using a pre-defined table. Bob always knows which key bit the photon encodes in this case [19].

The novelty of this protocol is the introduction of an index transmission error rate (ITER) along with the qubit error rate (QBER) as a performance parameter. ITER increases significantly for higher dimensional photon states. This allows for more noise tolerance in the transmission line, thereby increasing the possible QKD distance [20].

Alice should randomly select some photons that should not be used to obtain key bits. For these photons, she tells Bob exactly which states she prepared. Comparing this information with his own measurement outcomes, Bob can then easily calculate the ITER [18]. Alice and Bob can also detect an eavesdropper by calculating the QBER.

T12

Protocol was created by Toshiba Research Europe Ltd. engineers (2013) [21] by analyzing the finite-size security of the efficient BB84 protocol implemented with decoy states and applying the results to a gigahertz-clocked quantum key distribution system.

The light pulses are modulated both in intensity and in another degree of freedom, which is used to encode the quantum information. It can be the polarization, or the relative phase. For the intensity, Alice chooses among three possible values: u (signal), v (decoy1) and w (decoy2). The values are selected with probabilities $pu >> pv > pw$.

For encoding, Alice randomly selects one of four possible states, as in the standard BB84 protocol. Rectilinear (+) is the majority basis, selected most often, and diagonal (x) is the minority basis. When $p+ > px$, there is an increase of efficiency with respect to the standard BB84 protocol, in which $p+ = px$ [21].

In a single key session, N pulses are sent by the transmitter to Bob. A software program controls all the equipment continuously, calculates the QBER for the fiber-stretcher to counteract any drift in the phase and corrects the detector gate delay and polarization to maximize the count rate [21]. Advanced data analysis of QBER (detector losses, non-empty counts, number of transmission errors) keeps the system secure.

EPR Authentication-Based QKD (AE17)

A. A. Abushgra and K.M. Elleithy (2017) presented an improved QKD scheme that was designed to include user's authentication within an entangled channel [22]. QKD algorithm is technically processed into two quantum channels; one channel is an EPR channel, and the second is a quantum channel (qubit channel in superposition). The reconciliation phase in the proposed protocol is also included in the first phase of the communication, not as a separate phase.

Alice converts plaintext key bits into qubits and fills the designed matrix [22] with converted qubits, decoy states and parity bits. Then she prepares the EPR string that contains encoded parameters, which are considered an open key for the whole QKD scheme. The encoded parameters are sent by one designed string (package) that includes: initiation time, the number of matrices, matrix size, parity bits, state dimension, matrix indices, and termination time.

The presented QKD algorithm is essentially initiated by creating an EPR communication and sending an EPR string with a parameter. After ensuring that Bob has received an EPR string, exchange of the prepared qubits (data) in the designed matrix starts. The submitted qubits will be created in one string by two bases, rectilinear or diagonal, and four states (|0⟩, |1⟩, |+⟩, |−⟩). Each row of a matrix indicates one string of qubits. The string of qubits will be emitted into a quantum channel, where each prepared qubit will be polarized into a superposition state. When Bob receives the upcoming qubits, he will insert the qubits to a matrix and then recover it using information obtained from EPR string [22].

C. Continuous Variable Protocols

MSZ96

Y. Mu et al. (1996) proposed QKD without using polarized photons [23]. System is based on the optical coupler and four non-orthogonal states modelled by using quantized arguments:

quadrature phase amplitudes of light field. Two orthogonal squeezed states are used by Bob as input to the optical coupler.

Alice has a signal generator, which can produce four non-orthogonal states and Bob measures the signal states by means of an optical coupler and can independently choose his own squeezed input source for it. To achieve perfect coupling for measuring the signal, Alice and Bob choose a phase reference before communication starts.

During the information reconciliation stage, to correct bits, Alice secretly divides all remaining bits related to each four states into N groups (N≥100). Each group involves only one signal state but both binary bits. Alice publicly announces the grouping result. Nobody knows which group belongs to which state, except Alice herself. Since each Bob's detection vector has been used to two non-orthogonal states, knowing the detection vector of each group releases no encoding information of the group. Bob calculates the number of 0 or 1 bits in each group. The encoding of the majority bits will represent the encoding of all bits in the group. This allows correcting all mistakes caused by the overlap. Bob tells Alice the positions of all useful bits; Alice knows the full information of these bits, and they use these bits as a secret key [23].

COW

Coherent one-way protocol was created by N. Gisin et al. (2004) [23]. The information is encoded in time.

Alice sends coherent pulses that are either empty or have a mean photon number μ<1, typically μ=0.5 (μ-pulse). Each bit is encoded by sequences of two pulses, μ-0 for "0" or 0-μ for "1". Alice can also send decoy sequences μ-μ. Bob measures the time-of-arrival of the photons on his data-line, detector DB. To ensure the security, Bob randomly measures the coherence between successive non-empty pulses, bit sequences "1–0" or decoy sequences, with the detectors DM1 and DM2 [20].

With the idea of a simple data line for key creation, and 'complementary' line for monitoring, one may implement a version of the BB84 protocol: Alice and Bob agree to produce the key using only the rectilinear basis; sometimes Alice prepares one of the eigenstates of the diagonal basis that acts as a decoy state [24].

D. Device Independence

The security of QKD protocols is based on the fundamental laws of physics and certain assumptions, such as 'perfect' and trusted equipment (sources and detectors) and secure environment. The solution for this limitation is device independence.

DI

D. Mayers (1998) proposed and gave a concrete design [25] for a new concept, self-checking source, which required the manufacturer of the photon source to provide certain tests; these tests were designed such that, if passed, the source was guaranteed to be adequate for the security of the quantum key distribution protocol, even though the testing devices might not be built to the original specification.

Unfortunately, the first DI-QKD is highly impractical because it needs near unity detection efficiency together with a qubit amplifier or a quantum non-demolition (QND) measurement of the number of photons in a pulse, and even then generates an extremely low key rate (of order 10^{-10} bits per pulse) at practical distances [26].

MDI

H.-K. Lo et al. (2012) proposed measurement device independent QKD [26].

Alice and Bob prepare phase randomized weak coherent pulses in the four possible BB84 polarization states and send them to an untrusted relay called Charlie (measurement device) located in the middle that performs a Bell state measurement and projects the incoming signals into a Bell state.

Inside the measurement device, signals from Alice and Bob interfere and project the input photons into either horizontal (H) or vertical (V) polarization states [26]. This stage is based on Hong-Ou-Mandel effect: when two identical single-photon waves enter a 50:50 beam splitter, they extinguish each other. If they become more distinguishable, the probability of detection increases.

After quantum state distribution, Charles publicly announces the events where a successful outcome has been obtained, including measurement results (Bell states). Alice and Bob keep the data that correspond to these instances and discard the rest. They post-select the events where they use the same basis in the authenticated public channel. Afterwards, either Alice or Bob has to apply a bit flip to her/his data, except for the cases where both of them select the diagonal basis and Charles obtains a successful measurement outcome corresponding to a triplet state [26].

E. Public Key Cryptography QKD

S09

It is based on public key cryptography combinations and private key cryptography presented by E. H. Serna (2012) [27]. Unlike the BB84 protocol, Bob knows the key to transmit; the qubits are transmitted in only one direction and classical information exchanged thereafter, and the communication in the proposed protocol remains quantum in each stage.

In the preparation phase, Alice prepares qubits by transforming bits into elements of secret bases and sends the qubits to Bob. Bob applies unitary secret operation to the qubits and they return to Alice over a quantum channel. Alice measures the qubits in the initial base and obtains a value sent by Bob. Eavesdropper gains no information about bases or unitary operations applied.

S13

QKD protocol, designed by E. H. Serna (2013) [28], generates various secure keys of the same size of the transmitted qubits, implying zero information losses between the interlocutors. Besides, it generates key swapping between the two recipients of photons, without even sharing a past between them. This protocol differs from BB84 just in the classic procedures, using a random seed and asymmetric cryptography. It demonstrates that using a random seed over a set of photons and asymmetric cryptography over the encoded bits, the QKD becomes a process of zero information losses, where the percentage of coincidence of the reconciliated key against the

size of the raw key is 100 % unlike the BB84, in which the expected result is 50 % [28].

VI. Comparison Table of QKD Protocols

To summarize the covered QKD protocols, we can denote the criteria for comparison:

- Protocol name;
- Authors, year of initial publication, reference;
- Type: discrete variable or continuous variable;
- Photon number splitting attack vulnerability (PNS attack described in Section 4.1.1: BB84 Decoy state);
- Efficiency: the proportion of remaining key bits from initial N bit string after sifting and information reconciliation phases (in no-noise channel);
- Characteristic features: highlighting the uniqueness and the novel idea introduced by each protocol.

Table II summarizes the described QKD protocols to bring a convenient overview, including publication details, protocol type, safety against source-hacking and key rate efficiency.

TABLE II

Comparison Results of Described OKD Protocols

Protocol Name	Authors; year; reference	Type	Principles	PNS safe	Efficiency	Specialty
BB84	C. H. Bennett and G. Brassard; 1984 [11]	DV	Uncertainty	No	~N/4	First in the history QKD.
E91	A. Ekert; 1991 [12]	DV	Entanglement	Yes	~N/2	First in the history EPR-based QKD.
BBM92	C. H. Bennett, G.Brassard and N. D. Mermin; 1992 [13]	DV	Uncertainty	No	~N/3	First experimental QKD. Introduced parity check and hashing methods during information reconciliation.
BB92	C. H. Bennett; 1992 [14]	DV	Uncertainty	No	~N/2	Uses two non-orthogonal low-intensity coherent states.
MSZ96	Yi Mu, Jennifer Seberry, Yuliang Zheng; 1996 [22]	CV	Uncertainty	N/A	~N/2	No units polarized photons, bit encoded in four non-orthogonal states described by quadrature phase amplitudes of a weak optical field.
DI	D.Mayers and A.Yao; 1998 [25]	DV	Uncertainty	N/A	Extremely low [26]	First device independent QKD.
SSP	H. Bechmann-Pasquinucci and N. Gisin; 1999 [16]	DV	Uncertainty	No	~N/3	The symmetry of this protocol simplifies considerably the security analysis.
DPS	K.Inoue, E.Waks and Y.Yamanoto; 2003 [15]	DV	Uncertainty	Yes	~N [15]	Utilises all photons for creating the key, simple configuration, efficient time domain use.
BB84 decoy state	W.-Y. Hwang; 2003 [17]	DV	Uncertainty	Yes	~N/2	First proposed a decoy-state method to overcome the PNS attack in the presence of high loss.
SARG04	V. Scarani, A. Acin, G.Ribordy and N. Gisin; 2004 [18]	DV	Uncertainty	No [28]	~N/6	Encoding classical bit in sets of non-orthogonal states, made significant robust against PNS attack.
COW	N.Gisin, G. Ribordy, H.Zbinden, D. Stucki, N. Brunner, V.Scarani; 2004 [24]	CV	Uncertainty	Yes	~N, decreases linearly	The information is encoded in time. Additional communication line allows monitoring the presence of a spy.
KMB09	M. M. Khan, M. Murphy, and A. Beige; 2009 [19]	DV	Uncertainty	Yes	~N/4	Two mutually unbiased bases used. Index transmission error rate was introduced.
S09	E. H. Serna; 2012 [27]	DV	Uncertainty	N/A	~N	Public crypto QKD. Can be implemented for more than two parties. One-photon protocol version persists.
MDI	H.-K. Lo, M. Curty and B. Qi; 2012 [26]	DV	Uncertainty	Yes	~N/6	Works even when Alice and Bob's preparation processes are imperfect.
S13	E. H. Serna; 2013 [28]	DV	Uncertainty	N/A	~N, ~4N [28]	Public crypto QKD. Generates various secret keys of the transmitted qubits, implying zero information losses between the interlocutors.
T12	Toshiba Research Europe; 2013 [21]	DV	Uncertainty	Yes	~N	Rectilinear (+) is the majority basis. Three intensity values are used. Equipment controls QBER continuously.
AE17	A. A. Abushgra and K. M. Elleithy; 2017 [22]	DV	Uncertainty, Entanglement	Yes	~N	Designed matrix that includes decoy states and parity check. EPR authentication phase, where EPR string is used as a key for the whole system.

VI. Conclusion

BB84 is the first QKD protocol that has become the basis of many further QKDs and nowadays a variety of protocols are based on it. Every protocol, described in this overview paper, introduces novel ideas for further QKD system improvement.

In DV-QKD protocols, it is required that Bob randomly switches measurement basis. However, counter intuitively, with CV-QKD protocols it is not only possible to simultaneously encode information onto amplitude and phase or onto the corresponding quadrature carriers of the coherent laser light, but also to simultaneously measure both the amplitude and phase or in-phase and quadrature carriers (or components) of the light. This so-called "no-switching" protocol not only vastly simplifies the implementation of CV-QKD protocols, but also enables higher secret key transmission rates [29].

Unfortunately, there is a big gap between the theory and practice of QKD. In principle, QKD offers unconditional security guaranteed by the laws of physics. However, real-life implementations of QKD rarely conform to the assumptions in idealized models used in security proofs. The classical BB84 quality-control in the basic quantum key distribution protocol is inadequate in practice for two reasons: realistic detectors have some noise; therefore, Alice and Bob's data will differ even in the absence of eavesdropping; and it is technically difficult to produce a light pulse containing exactly one photon [13].

MDI QKD was proposed as a solution to remove all (existing and yet to be discovered) detector side channels, arguably the most critical part of the implementation. It has both excellent security and performance [26]. DI helps address the E91 problem – assuming the detector efficiency, which if not 100 % can be exploited to produce detection loopholes.

There are a variety of theoretical attacks on QKD systems, such as detector side channel attacks, beam splitter attack, intercept-resend, PNS, unambiguous discriminations, external control, Trojan horse, collective attack etc. To address all of them without affecting protocol efficiency from the perspective of key generation and keeping setup simple is an inspiring challenge on way to the safest cryptographic system.

References

[1] P. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", *Proc. 35th Annu. Symp. on Foundations of Computer Science*, Santa Fe, NM, USA, 1994. https://doi.org/10.1109/sfcs.1994.365700

[2] B. Qi, L. Qian, H-K. Lo, "A brief introduction of quantum cryptography for engineers", 2010.

[3] ETSI, "Quantum Safe Cryptography and Security", White Paper No. 8, June 2015.

[4] L. Grover, "A fast quantum mechanical algorithm fordatabase search," *Proc. 28th ACM Symposium on Theory of Computing*, ACM Press, New York, NY, 1996, pp. 212–219. https://doi.org/10.1145/237814.237866

[5] DelftX, "The Quantum Internet and Quantum Computers: How Will They Change the World", QTM1x Lecture notes, 2018.

[6] W. Heisenberg, "The Physical Content of Quantum Kinematics and Mechanics," in J. A. Wheeler, and W. H. Zurek, Eds., Quantum Theory and Measurement, Princeton, Princeton University Press, 1927, pp. 62–84.

[7] A. Einstein, B. Podolsky, N. Rosen, "Can Quantum-Mechanical Description of Physical Reality Be considered Complete?", *Phys. Rev.* vol. 47, May 1935. https://doi.org/10.1103/PhysRev.47.777

[8] W. K. Wootters, W. H. Zurek, "A Single Quantum Cannot Be Cloned", *Nature*, vol. 299, pp. 802–803, 1982. https://doi.org/10.1038/299802a0

[9] D. Wang, J. Wu, X. Yi, "Optical Quantum Computing", *11th International Conference on Natural Computation (ICNC)*, Zhangjiajie, China, 2015. https://doi.org/10.1109/ICNC.2015.7378022

[10] Quintessence labs, "Quantum Key Distribution Systems Compared", White Paper #2, December 2014.

[11] C. H. Bennett, and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, 10–12 December, 1984, pp. 175–179.

[12] A. K. Ekert, "Quantum cryptography based on Bell's theorem", Physical *Review Letters*, vol. 67, August 1991. https://doi.org/10.1103/PhysRevLett.67.661

[13] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental Quantum Cryptography", *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992. https://doi.org/10.1007/BF00191318

[14] C. H. Bennett, "Quantum cryptography using any two non-orthogonal states", *Phys. Rev*. vol. 68, pp. 3121–3124, 1992.

[15] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light", *Physical Review A*., vol. 68, 2003. https://doi.org/10.1103/PhysRevA.68.022317

[16] H. Bechmann-Pasquinucci, N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography", *Phys. Rev*. A. vol. 59, no. 6, pp. 4238–4248, 1999. https://doi.org/10.1103/PhysRevA.59.4238

[17] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication", *Physical Review Letters*, vol. 91, 2003. https://doi.org/10.1103/PhysRevLett.91.057901

[18] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations", *Phys. Rev. Lett*., vol. 92, 057901, 2002. https://doi.org/10.1103/PhysRevLett.92.057901

[19] M. M. Khan, M. Murphy, and A. Beige, "High error-rate quantum key distribution for long distance communication", *New J. Phys*., vol. 11, 2009. https://doi.org/10.1088/1367-2630/11/6/063043

[20] D. Stucki, S. Fasel, N. Gisin, Y. Thoma, and H. Zbinden, "Coherent one-way quantum key distribution", 2007.

[21] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Efficient decoy-state quantum key distribution with quantified security", *Optics Express*, vol. 21, no. 21, pp. 24550–24565, 2013. https://doi.org/10.1364/OE.21.024550

[22] A. A. Abushgra and K. M. Elleithy, "A Shared Secret Key Initiated by EPR Authentication and Qubit Transmission Channels", *IEEE Access*, vol. 5, pp. 17753–17763, 2017. https://doi.org/10.1109/ACCESS.2017.2741899

[23] Y. Mu, J. Seberry, and Y. Zheng, "Shared Cryptographic Bits Via Quantized Quadrature Phase Amplitudes of Light", *Optical Communications*, vol. 123, pp. 344–352, 1996. https://doi.org/10.1016/0030-4018(95)00688-5

[24] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, "Towards practical and fast quantum cryptography", 2004.

[25] D. Mayers, A. Yao, "Quantum Cryptography with Imperfect Apparatus", in *Proc. of the 39th Annual Symposium on Foundations of Computer Science*, 1998, pp. 503–509. https://doi.org/10.1109/sfcs.1998.743501

[26] H.-K. Lo, M. Curty, and B. Qi, "Measurement device independent quantum key distribution", 2012.

[27] E. Esteban, E. H. Serna, "Quantum Key Distribution protocol with private-public key", May 2012

[28] E. H. Serna, "Quantum Key Distribution from a random seed", Nov. 2013.

[29] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, "Security of two quantum cryptography protocols using the same four qubit states", *Phys. Rev. A*., vol. 72, no. 3, 2005. https://doi.org/10.1103/physreva.72.032301

Anastasija Trizna obtained his Bachelor's degree (Telecommunications Engineering) in 2013. She is a second-year student of the professional Master study programme "Information Technology". Current research topic – Measurement Device Independent Quantum Key Distribution.
E-mail: Anastasija.Trizna@edu.rtu.lv

Andris Ozols, Professor, *Dr. habil. phys.* (Institute of Technical Physics), Head of Optics Department at Riga Technical University.
E-mail: aozols@latnet.lv
ORCID iD: https://orcid.org/0000-0002-0221-4892