Proceedings of the Estonian Academy of Sciences
2025, **74**, 2, 175–180

https://doi.org/10.3176/proc.2025.2.17

www.eap.ee/proceedings
Estonian Academy Publishers

QUANTUM TECHNOLOGIES

RESEARCH ARTICLE

Received 16 January 2025
Accepted 28 February 2025
Available online 29 April 2025

Keywords:
QKD distribution, Industry 4.0, quantum technologies

Corresponding author:
Fabio Auriemma
fabio.auriemma@spin.cnr.it

Citation:
Auriemma, F. and Ejrnaes, M. 2025. Addressing security issues in Industry 4.0 through quantum key distribution. *Proceedings of the Estonian Academy of Sciences*, **74**(2), 175–180. https://doi.org/10.3176/proc.2025.2.17

Addressing security issues in Industry 4.0 through quantum key distribution

Fabio Auriemma[a,b] and Mikkel Ejrnaes[b]

[a] Institute for SuPerconductors, INnovative materials, and devices (SPIN), National Research Council (CNR), Via Campi Flegrei 34, I-80078 Pozzuoli, Napoli, Italy

[b] Department of Mechanical and Industrial Engineering, Tallinn University of Technology, Ehitajate tee 5, 19086 Tallinn, Estonia

ABSTRACT

Industry 4.0 is a recent manufacturing paradigm based on the automation and digitalization of industrial processes, leveraging the interconnection of systems and processes through automation and data exchange. Despite the fact that the fourth "industrial revolution" has not yet reached its maturity and is not being widely implemented, engineers have already outlined the characteristics and goals of the upcoming fifth one. On the other hand, quantum technologies – quantum computing, sensing and communication – will soon become another point of rupture for society and industry, with a quantum-driven technological revolution expected in the next two decades. In this paper, we show that quantum key distribution, an emerging technique for secure communication, can be readily employed in Industry 4.0 to address a number of safety and privacy issues. In fact, due to the reliance of this industrial model on interconnectivity and data, cyberattacks can pose threats to production systems and infrastructures such as power grids or water treatment facilities. This threat also increases with the level of automation, digitalization, and remote control. Moreover, data can be stolen and misused both at a personal level and for collective exploitation. We simulate the transmission of sensitive data within a power plant, encryption through quantum key distribution and tentative eavesdropping, to demonstrate that this approach ensures theoretically complete security in data transmission.

Introduction

The German government introduced the term Industry 4.0 in 2011 as part of a high-tech strategy to enhance digitalization in manufacturing [1]. Since then, engineers and policymakers have used this term to refer to the current stage of innovation of modern manufacturing systems that leverage interconnectivity and "smart systems" (such as the Internet of Things (IoT), cloud computing, and artificial intelligence (AI)). Due to recent global crises – global warming, pandemics, wars – policymakers, stakeholders and technological innovators are already looking ahead to Industry 5.0. This new phase aims to create a sustainable, resilient, human-centric manufacturing system that enables interaction and collaboration between humans and machines [2,3]. These two industrial models rely heavily on interconnectivity and smart systems as a fundamental part of the manufacturing model. Cyber-physical systems (CPSs) – smart grids, autonomous vehicles, industrial control systems, etc. – are digital apparatuses that monitor and control physical systems in real time by means of distributed and interconnected devices. Introduced by Industry 4.0, CPSs will also be a fundamental pillar in Industry 5.0. In addition to positively impacting the manufacturing process in terms of production efficiency, flexibility and sustainability, they also present important safety and privacy issues in highly interconnected digital systems [4].

In this paper, we describe how modern industrial models can benefit from quantum key distribution (QKD) – currently one of the most mature quantum technologies – to ensure secure communication of sensitive data. In fact, even when endpoints are secured (e.g. by applying the principles of least privilege, strong privilege user management and identity authentication), credentials can be stolen, and privilege escalation can be actuated to access sensitive data and systems.

The second generation of quantum technologies – quantum computing, sensing and communication – represents an emerging technological shift of potentially epochal proportions [5]. Although its adoption on a wide scale is still at least a decade

away, this paper explores a possible application of QKD in modern industrial scenarios. Section 2 provides a historical framework for the industrial, digital and quantum revolutions. Section 3 explains the basic functioning of a QKD system, while Section 4 proposes an information communication scheme within Industry 4.0 where sensitive industrial data can be secured using a QKD system.

Industrial models and "industrial revolution"

"Industrial revolutions" have resulted from breakthrough technological advances that have irreversibly transformed production methods, reshaped entire economic systems and originated profound socio-cultural changes. Historians have traditionally distinguished two stages of the "industrial revolution" within the modern era, commonly referred to as the first and the second "industrial revolutions" [1]. In the late 1970s, the so-called digital revolution or information age prompted traditional manufacturing economies to transition toward economic systems centered on information technology.

The term "Industry 4.0" rapidly gained widespread acceptance among engineers and policymakers – to refer to the industrial models of the first and second "industrial revolutions", as well as to the production models of the information age, Industry 1.0, 2.0 and 3.0. This also set the stage for referring to the current and upcoming stages as Industry 4.0 and 5.0 [2,4]. In reality, digitalization has been the root cause of the profound and irreversible socio-cultural changes that have characterized the last fifty years, and in the last two decades, it is the pervasive use of smart systems and AI. Thus, the shift in the industrial models which has occurred since then is a consequence – not a cause – of the revolution, which is ultimately of a digital rather than industrial nature.

Currently, the advent of the new generation of quantum technologies is a potential cause for another radical shift in the social, political and technological development of humanity, which could be the transition into a radically different epoch [6]. It is important to distinguish between two quantum revolutions and two generations of quantum technologies. The first quantum revolution started at the beginning of the previous century and is mainly scientific and conceptual in nature [6,7]. The standard formulation of atomic physics was conceptualized based on quantum mechanics, which was unified and formalized by D. Hilbert [8]. The first quantum revolution also produced, between the 1960s and 1990s, several quantum technologies which are currently in use in many sectors of our society (e.g. medicine, research and industry). Examples include nuclear magnetic resonance (manipulation of nuclear spins), magnetic resonance imaging, spin electronics and new electronic devices (e.g. magnetoresistive heads for hard drives, magnetoresistive RAM, etc.).

The second quantum revolution mainly has the features of a technological revolution and originates with the development of the second generation of quantum technologies. This is the result of the technical ability of modern quantum engineering not only to manipulate single atoms and spins but also to isolate and control quantum states. In this way, these new technologies can exploit unique properties of quantum-mechanical systems, such as quantum superposition and entanglement [8]. In fact, a quantum system lives in a superposition of states until a measurement is performed that provides a probabilistic – thus, non-deterministic – result. Two quantum systems may also have intertwined properties, so that the measurement of an observable on one of them instantly affects the other, irrespective of their distance. The superposition of quantum states decays when a measurement is performed on the quantum system and the result of the measurement is completely random. These properties can be used for quantum teleportation and cryptography, as well as quantum sensing [8].

This conference paper aims to provide an overview of QKD to conceptualize a communication architecture in which QKD is used to overcome the information security issues that inherently affect modern industrial paradigms (i.e. Industry 4.0 and 5.0). Although this second-generation quantum technology has reached maturity for practical applications, the industrial engineering community is still relatively new to it.

Quantum key distribution

In cryptography, the key distribution problem involves finding a string of information that can be safely shared between two distant parties, conventionally called Alice and Bob, through a communication channel. This enables private communication even in the presence of an eavesdropper, typically referred to as Eve [9,10]. All key distribution schemes that use logic and signals based on the principles of classical physics guarantee only computational security, because theoretically nothing – except computational limitations – prevents Eve from copying the key and successfully decrypting the message received by Bob, even at later time. In public-key cryptography, two keys are generated: a public key that allows anyone, including Alice, to encrypt a plain text message; and a private key that only Alice and Bob own, which allows decryption of the message to recover the plain text. With only the public key, there is no efficient algorithm for Eve to decipher the encrypted message. The privacy solely relies on this inefficiency, but in principle, Eve could discover – by leveraging computational power – how to hack the private key.

There exists a number of different quantum protocols developed for secure communication. In this section, we briefly introduce the Bennet and Brassard 1984 (BB84) protocol, which is among the simplest and most popular protocols, aiming to provide an overview of the basics of QKD [10]. In BB84, one can encode binary information (0 or 1) by leveraging the polarization of a single photon: each photon is in a polarization state $|\psi\rangle$ that can be described as a linear combination of horizontal polarization (1,0) and vertical polarization (0,1), described in a normalized form as $|\psi\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle + |\uparrow\rangle)$. In this two-dimensional space, one can use an alternative reference system, where the axes are rotated by an angle of $\pi/4$, thus formed by the orthogonal vectors $(\sqrt{2}, \sqrt{2})$ and $(\sqrt{2},-\sqrt{2})$, i.e. $|\psi\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle + |\nwarrow\rangle)$. The first reference basis is called the rectilinear (or Z-) basis, and the second one is the diagonal (or X-) basis; the two will be symbolized here as $\llcorner$ and $\vee$, respectively. In order to

transmit binary information (0 or 1), Alice assigns 0 to a certain polarization in either basis. For instance, 0 can be associated with horizontal polarization in the rectilinear basis, 0: = (↑, ∟), and with π/4 rad polarization in the diagonal basis, 0: = (↗, ∨). In this case, 1 will be encoded as 1: = (→, ∟) and 1: = (↖, ∨), i.e. with an orthogonal type of polarization in the respective basis. Whenever Alice transmits a string of bits, she randomly chooses a basis per each bit and emits a single photon polarized according to the value of the bit and the chosen basis. On the other side, Bob performs a quantum measurement on the polarization of the photon received, randomly choosing his reference basis, either the rectilinear or the diagonal one. Unlike the measurement of a macroscopic physical system acting in a classical way, quantum measurements are not deterministic but probabilistic in nature [8]. The possible outcomes result from the interaction between the measurement system and the quantum object: in a bi-dimensional space, the measurement performed by Bob on the photon's polarization will be either $|\rightarrow\rangle$ or $|\uparrow\rangle$ if he measures in the rectilinear reference basis, ∟, and either $|\nearrow\rangle$ or $|\nwarrow\rangle$ if he measures in the diagonal one, ∨. The probabilities of these outcomes depend on the measurement basis and the initial state of the photon due to the collapse of the wavefunction $|\psi\rangle$, a fundamental principle of quantum mechanics. In fact, if the photon sent by Alice has vertical polarization $|\uparrow\rangle$, there is a 100% probability that Bob measures $|\uparrow\rangle$ if he has picked the orthogonal polarization, and this measurement will not alter the polarization state of the photon. However, Bob will have a 50% probability of measuring $|\nearrow\rangle$ and a 50% probability of measuring $|\nwarrow\rangle$ if he has picked the "wrong" reference basis (in this example, the diagonal one, ∨). Most importantly, this measurement will alter the polarization of the photon, forcing it to be either $|\nearrow\rangle$ or $|\nwarrow\rangle$ with 50% probabilities. As a result, Bob can detect the same bit sent by Alice only when he (randomly) picks the same basis as the one used by Alice to encrypt that bit. Thus, only half of the bits sent by Alice are read correctly by Bob. In reality, the communication line is also affected by intrinsic losses, reducing this percentage even further. Once Bob has performed these measurements and stored the results, Alice communicates through a public channel (e.g. a classical optical fiber) the sequence of the basis type she has used for each photon sent (e.g. ∨, ∨, ∟, ∨, ∟, ∨, ∨, ∟,…), representing the public key. Bob can then discard the readings obtained when he has used a different basis (e.g. if Bob has picked ∟, ∨, ∟, ∟, ∨, ∨, ∟, ∟,…, he will discard the 1st, 4th, 5th and 7th readings). If an eavesdropper, Eve, wants to gain information from this communication, she also has to choose a reference basis (e.g. ∨, ∟, ∨, ∟, ∟, ∨, ∟, ∟,…), with a 50% probability of picking the same basis as Alice, and thus with a 50% probability of altering the polarization state of the photons sent by Alice. When Bob measures the polarization state after Eve's intervention, his probability of correctly detecting the information sent by Alice will now drop to 25%. In this example, due to Eve's intervention, the polarization of the 2nd, 3rd, 4th and 7th photons transmitted by Alice will be altered because of the different basis used. As a result, Bob will "wrongly" read not only the 1st, 4th and 5th bits, but also the 2nd and 3rd bits, which were altered by Eve. After a public comparison, Alice and Bob will notice a drop in the success rate of detection, and Alice can decide to discard the current key and use another channel or another key. In QKD, the collapse of the wavefunction implies the quantum no-cloning theorem, which regulates the process described above: an unknown quantum state cannot be cloned reliably [8,10]. Therefore, once a QKD session is over, the information transferred is secure forever. At this point, the secret key can be used to encrypt the sender's message and decrypt the receiver's message using classical algorithms (e.g. Ascon).

QKD in Industry 4.0

Over the past five years, cyberattacks have escalated in frequency, sophistication and impact. In the sole year 2024, fifty-nine events, including cyberattacks and economic crimes targeting governmental agencies, defense and high-tech companies – with losses exceeding one million dollars – were reported by international security agencies [11]. Cyberattacks cost British businesses $55 billion in the past five years, and attacks on critical infrastructures (e.g. energy, healthcare, and transportation) accounted for $500 billion in losses globally, in 2023 alone [11].

Figure 1 reports a typical configuration used in industrial plants (e.g. energy generation plants, water treatment plants, manufacturing plants, etc.) implementing Industry 4.0, where the supervisory control and data acquisition (SCADA) system "dialogues" with a cloud system as well as with the gateway of remote terminal units (RTUs) connected to IoT devices operating at the field level [12,13,14]. SCADA systems are vulnerable to both traditional and post-quantum cyberattacks [5]: in Fig. 1, straight lines indicate communication channels that are susceptible to cyberattacks. Three main issues may arise from these attacks: loss of confidentiality (data theft), loss of integrity (data tampering) and loss of authentication (illegitimate use of control systems) [15]. For this reason, we have included in the scheme of Fig. 1 the use of a QKD system, where the key is generated at the SCADA level by means of an Alice unit and shared at vulnerable points where Bob units are installed. Once a uniformly random quantum (sifted) key is distributed between Alice and one of the Bobs, it is used to encode information, such as a control command over the temperature settings, provided at supervisory level and destined for one of the RTUs.

The secure quantum key is used by ciphers/deciphers at the sender and receiver points to encrypt the message by using an authenticated cipher (e.g. the classical Ascon algorithm). Once the message is encrypted, the only way to decrypt it is by using the same algorithm knowing the secret key, which is owned by Alice and Bob only. If an intruder, Eve, with some uncertainty regarding the uniformly random key, attempts to intercept the key, it is irreversibly modified according to the no-cloning theorem of quantum information [15]. Alice and Bob will measure an increase in the quantum bit error rate (QBER) and decide to discard the sifted key, generate a new one, and change the communication channel [10].

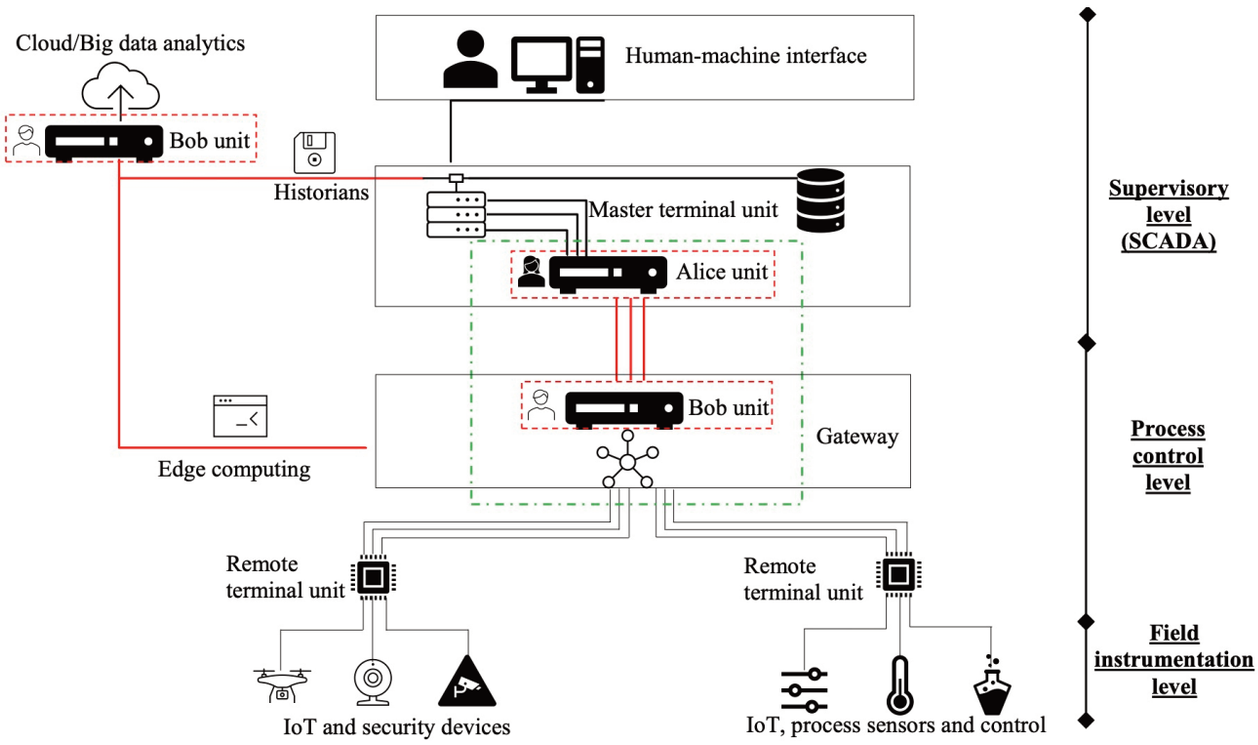

Fig. 1. Integration of QKD into a typical Industry 4.0 scenario, including SCADA and IoT systems.

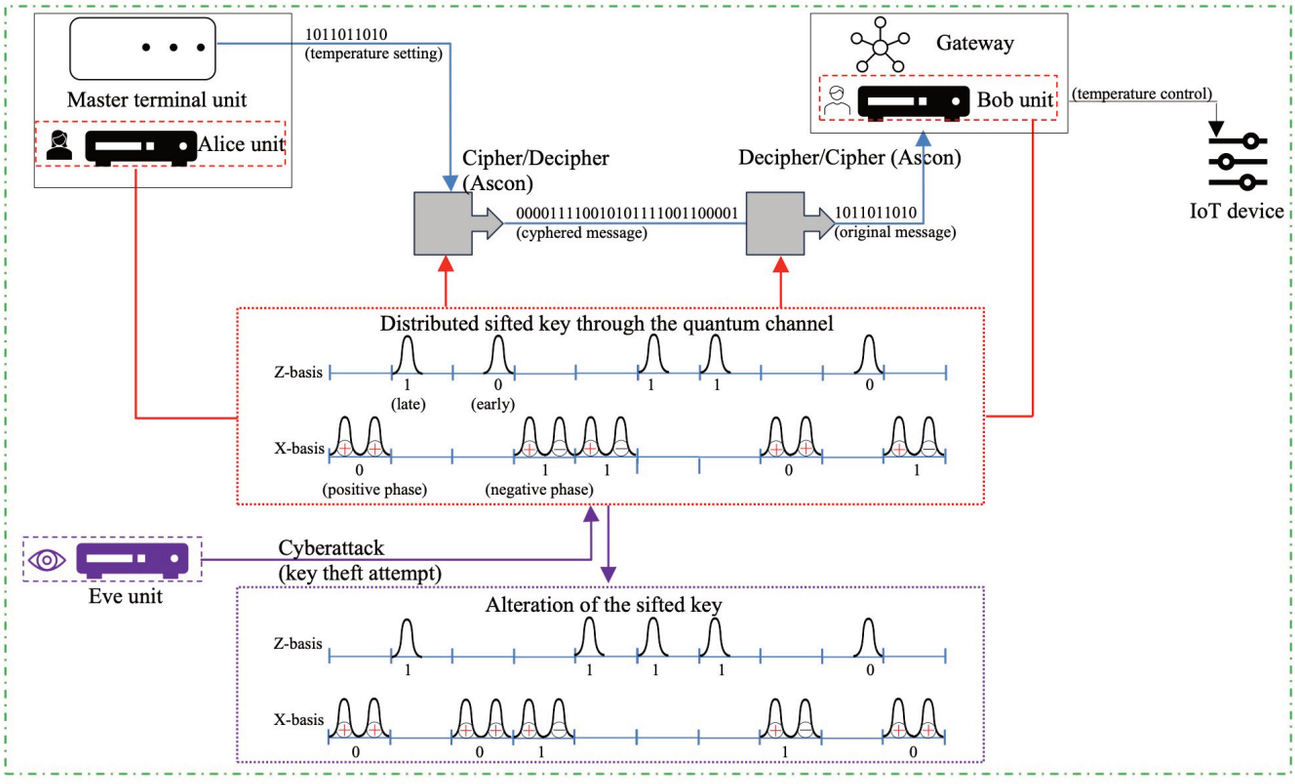

Fig. 2. Schematic of QKD-secured communication between a master terminal unit and a gateway of IoT devices. Temperature settings are encrypted using a quantum key, and an attempt by Eve to copy the sifted key results in a modification of the key that can be easily detected by the Alice and Bob units.

Unlike classical protocols, even an unsuccessful attempt at eavesdropping alters permanently the shared key, alerting both Alice and Bob.

The classical QKD protocol BB84 has been described in the previous section with the aim of providing a general overview of quantum secure communication. However, for practical implementation in an industrial context, a polarization encoding protocol of this type may lack robustness, as casual movement of the optical fibers in the communication channel could alter the polarization of light, resulting in a large increase in communication errors in polarization-based encryption. For this reason, the scheme suggested in Fig. 2

uses time-bin encoding, where the two encoding bases (referred to as the Z- and the X-basis) are obtained by considering the photon's arrival time and the relative phase between two pulses, respectively [16,17], instead of orthogonal and rectilinear polarizations. In this way, Alice and Bob account for synchronized time slots (e.g. 1.68 ns long) and can either generate/receive an early or a late pulse (e.g. 800 ps long), which in the Z-basis encode bit 0 and bit 1, or generate/receive two pulses whose relative phase ($+\pi$ or $-\pi$) encodes bit 0 and bit 1 in the X-basis. The main advantage of using a non-polarization encoding protocol is greater robustness of the system, as casual movement of the optical fibers in the communication channel alters the polarization of light, resulting in a large increase in communication errors in polarization-based encryption. Obviously, a number of factors affect transmission through the quantum channel (e.g. photons can be lost, especially in long optical fibers), preventing Alice and Bob from obtaining the identical quantum key. However, as long as the QBER is kept below 11%, ad-hoc classical post-processing procedures can be used to recover the correctness of the key (information reconciliation) as well as its secrecy (privacy amplification), by sacrificing part of the key. Moreover, in time-bin encoding protocols, perfect encoding is possible only for single-photon emission sources, which are difficult to achieve in practice because the information is encoded on multiple photons simultaneously, and one of the photons could be detected by Eve without altering the information transmitted by Alice to Bob. To circumvent this problem, decoy state techniques can be utilized, where light intensity is varied and modulated at different levels, known by Alice and Bob, so that the presence of Eve would result in an evident change in the expected photon statistics [16,17].

Conclusions

The vulnerability to traditional and post-quantum cyberattacks in SCADA/IoT-integrated systems represents a significant issue in modern industrial systems that leverage the interconnection of systems and processes. For this reason, we have provided an overview of the fundamental principles of QKD for the industrial engineering community to become familiar with these relatively new concepts. We have also conceptualized the use of a time-bin-based QKD protocol as a potential means of tackling information security issues within Industry 4.0. Furthermore, we have proposed a communication architecture that includes an Alice unit placed at the SCADA point and one or more Bob units at critical points where sensitive data is generated and/or stored and/or sensitive instructions can be received. As information encoded in a non-classical state is irreversibly affected by measurement, the action of an eavesdropper can be detected and the attack thwarted. Since this approach is new in the context of Industry 4.0, further research is needed to provide details and troubleshooting for practical implementation in a real-case scenario.

Data availability statement

All research data are contained within the article and can be shared upon request from the authors.

Acknowledgments

This work was partially funded by the project "Partenariato Esteso NQSTI, Spoke 4 CUPB53C22004180005". The publication costs of this article were partially covered by the Estonian Academy of Sciences.

References

1. Stearns, P. N. *The Industrial Revolution in World History.* 5th ed. Routledge, New York, 2021.
2. Kagermann, H., Wahlster, W. and Helbig, J. *Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0*. Acatech, Munich, 2013.
3. Mourtzis, D., Angelopoulos, J., Panopoulos, N. A literature review of the challenges and opportunities of the transition from Industry 4.0 to Society 5.0. *Energies*, 2022, **15**, 6276.
4. Golovianko, M., Terziyan, V., Branytskyi, V. and Malyk, D. Industry 4.0 vs. Industry 5.0: co-existence, transition, or a hybrid. *Procedia Comput. Sci.*, 2022, **217**(4), 102–113.
5. Alabdulatif, A., Thilakarathne, N. N. and Lawal, Z. K. A review on security and privacy issues pertaining to cyber-physical systems in the Industry 5.0 era. *Comput. Mater. Contin.*, 2024, **80**(3), 3917–3943.
6. Calzati, S. and de Kerckhove, D. *Quantum Ecology*. The MIT Press, Cambridge, MA, London, 2024.
7. Georgescu, I. and Nori, F. Quantum technologies: an old new story. *Phys. World*, 2012, **25**(05), 16–17.
8. Cohen-Tannoudji, C., Diu, B. and Laloë, F. *Quantum Mechanics*. John Wiley and Sons, New York, 1977.
9. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. and Pan, J.-W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.*, 2020, **92**, 025002.
10. Bruscino, C. *SNSPDs for QKD applications*. MS thesis. Università degli Studi di Napoli Federico II, Italy, 2022.
11. Center for Strategic and International Studies (SCIS). *Significant Cyber Incidents*. https://www.csis.org/ (accessed 2025-03-01).
12. Bellini, P., Cenni, D., Mitolo, N., Nesi, P., Pantaleo, G. and Soderi, M. High level control of chemical plant by Industry 4.0 solutions. *J. Ind. Inf. Integr.*, 2022, **26**, 100276.
13. Nechibvute, A. and Mafukidze, H. D. Integration of SCADA and Industrial IoT: opportunities and challenges. *IETE Tech. Rev.*, 2024, **41**(3), 312–325.
14. Umbrello, S. Quantum technologies in Industry 4.0: navigating the ethical frontier with value-sensitive design. *Procedia Comp. Sci.*, 2024, **232**, 1654–1662.
15. Guarda, G., Ribezzo, D., Salvoni, D., Bruscino, C., Ercolano, P., Ejrnaes, M. et al. BB84 decoy-state QKD protocol over long-distance optical fiber. In *2023 23rd International Conference on Transparent Optical Networks (ICTON 2023), Bucharest, Romania, 2–6 July 2023*. IEEE, 2024, 654–658.
16. Ghosh, S., Zaman, M., Joshi, R. and Sampalli, S. Multi-phase quantum resistant framework for secure communication in SCADA systems. *IEEE Trans. Dependable Secure Comput.*, 2024, **21**, 5461–5478.
17. Boaron, A., Boso, G., Rusca, D., Vulliez, C., Autebert, C., Caloz, M. et al. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.*, 2018, **121**(19), 190502.

Tööstus 4.0 turbeprobleemide lahendamine kvantvõtmete jaotamise abil

Fabio Auriemma ja Mikkel Ejrnaes

Tööstus 4.0 on hiljutine tootmisparadigma, mis põhineb tööstusprotsesside automatiseerimisel ja digitaliseerimisel, võimaldades süsteemide ja protsesside omavahelist ühendamist automatiseerimise ja andmevahetuse kaudu. Kuigi neljas „tööstusrevolutsioon“ ei ole veel täielikult küps ja seda ei rakendata laialdaselt, on insenerid juba välja toonud eelseisva viienda omadused ja eesmärgid, mis kasutavad ära Tööstus 4.0 arendatud tööriistu, pannes samal ajal rõhku protsesside jätkusuutlikkusele nii keskkonna kui inimese vaatenurgast. Teisest küljest kujutavad kvanttehnoloogiad kvantarvutuse, -anduri ja -kommunikatsiooni kujul peagi ühiskonnale ja tööstusele järjekordset murdepunkti ning järgmise kahe aastakümne jooksul on oodata kvantpõhist tehnoloogilist revolutsiooni. Artiklis näitame, et kvantvõtmete jaotust, mis on arenev turvalise side tehnika, saab hõlpsasti kasutada mitme ohutus- ja privaatsusprobleemi lahendamiseks. Simuleerime tundlike andmete edastamist elektrijaamas, krüpteerimist kvantvõtme jaotuse kaudu ja pealtkuulamist, et näidata, kuidas see lähenemine tagab teoreetiliselt täieliku ohutuse andmeedastuses.