Daily Quantum Cryptography Snacks

Everyone

March 29, 2022

0.1 Deploying an inter-European quantum network

Domenico Ribezzo, Mujtaba Zahidy, Ilaria Vagniluca, Nicola Biagi, Saverio Francesconi, Tommaso Occhipinti, Leif K. Oxenløwe, Martin Lončarić, Ivan Cvitić, Mario Stipčević, Žiga Pušavec, Rainer Kaltenbaek, Anton Ramšak, Francesco Cesa, Giorgio Giorgetti, Francesco Scazza, Angelo Bassi, Paolo De Natale, Francesco Saverio Cataliotti, Massimo Inguscio, Davide Bacco, Alessandro ZavattaAround forty years have passed since the first pioneering works have introduced the possibility of using quantum physics to strongly enhance communications safety. Nowadays Quantum Cryptography, and in particular, Quantum Key Distribution (QKD) exited the physics laboratories to become commercial technologies that increasingly trigger the attention of States, military forces, banks, and private corporations. This work takes on the challenge of bringing QKD closer to a consumer technology: optical fibers deployed and used by telecommunication companies of different States have been used to realize a quantum network, the first-ever connecting three different countries. This pushes towards the necessary coexistence of QKD and classical communications on the same infrastructure, which currently represents a main limit of this technology. Our network connects Trieste to Rijeka and Ljubljana via a trusted node in Postojna; a key rate of over 3 kbps has been achieved in the shortest link, and a 7-hour long measurement has demonstrated the system stability and reliability. Finally, the network has been used for a public demonstration of QKD at the G20 Digital Ministers' Meeting in Trieste. The reported experimental results, together with the significant interest that one of the most important events of international politics has attracted, showcase the maturity of the QKD technology bundle, placing it in the spotlight for consumer applications in the near term.

0.2 Proposal for Quantum Ciphertext-Policy Attribute-Based Encryption

Asmita Samanta, Arpita Maitra, Shion Samadder ChaudhuryA Quantum Ciphertext-Policy Attribute-Based Encryption scheme (QCP-ABE) has been presented. In classical domain, most of the popular ABE schemes are based on the hardness of the Bilinear Diffie-Hellman Exponent problem, which has been

proven to be vulnerable against Shor's algorithm. Recently, some quantum safe ABE schemes have been proposed exploiting the Lattice problem. However, no efficient Quantum Attribute-Based Encryption scheme has been reported till date. In this backdrop, in the present initiative, we propose a quantum CP-ABE scheme exploiting Quantum Key Distribution (QKD) and Quantum Error Correcting code. A Semi Quantum version of the scheme has also been considered. Finally, we introduced dynamic access structure in our proposed protocols.

0.3 Device-independent quantum key distribution from computational assumptions

Tony Metger, Yfke Dulek, Andrea Coladangelo, Rotem Arnon-FriedmanIn device-independent quantum key distribution (DIQKD), an adversary prepares a device consisting of two components, distributed to Alice and Bob, who use the device to generate a secure key. The security of existing DIQKD schemes holds under the assumption that the two components of the device cannot communicate with one another during the protocol execution. This is called the no-communication assumption in DIQKD. Here, we show how to replace this assumption, which can be hard to enforce in practice, by a standard computational assumption from post-quantum cryptography: we give a protocol that produces secure keys even when the components of an adversarial device can exchange arbitrary quantum communication, assuming the device is computationally bounded. Importantly, the computational assumption only needs to hold during the protocol execution – the keys generated at the end of the protocol are information-theoretically secure as in standard DIQKD protocols.

0.4 Quantum Analogue of Entropy Based DDoS Detection

Del RajanDistributed Denial-of-Service (DDoS) attacks can occur in quantum networks, which can pose a significant threat to its key distribution protocols. We introduce a quantum analogue of a classical entropic DDoS detection system, and apply it in the context of detecting an attack on a quantum network. In particular, we examine DDoS attacks on a quantum repeater and harness the associated entanglement entropy for the detection system. Our method contributes to the applicability of quantum information from the domain of data security to the area of network security.

0.5 Quantum Computing and the Future Internet

Tajdar JawaidOne of the biggest concerns among cybersecurity professionals these days is the hype around quantum computing, its incomprehensible power, and its implications. The advancement in quantum computing has the potential to revolutionize our daily lives, but it can also completely break down the Internet as we know it. Mathematicians and physicists have developed algorithms based on quantum computing, which can change the Internet security paradigm.

This article discusses quantum computing key concepts, with a special focus on quantum Internet, quantum key distribution, and related challenges.

0.6 Experimental Semi-quantum Key Distribution With Classical Users

Francesco Massa, Preeti Yadav, Amir Moqanaki, Walter O. Krawec, Paulo Mateus, Nikola Paunković, André Souto, Philip WaltherQuantum key distribution, which allows two distant parties to share a perfectly secure cryptographic key, promises to play an important role in the future of communication. For this reason such technique has attracted many theoretical and experimental efforts, thus becoming one of the most prominent quantum technologies of the last decades. The security of the key relies on quantum mechanics and therefore requires the users to be capable of performing quantum operations, such as state preparation or measurements in multiple bases. A natural question is whether and to what extent these requirements can be relaxed and the quantum capabilities of the users reduced. Here we demonstrate a novel quantum key distribution scheme, where users are fully classical. In our protocol, the quantum operations are performed by an untrusted third party acting as a server, which gives the users access to a superimposed single photon, and the key exchange is achieved via interaction-free measurements on the shared state. We also provide a full security proof of the protocol by computing the secret key rate in the realistic scenario of finite-resources, as well as practical experimental conditions of imperfect photon source and detectors. Our approach deepens the understanding of the fundamental principles underlying quantum key distribution and, at the same time, opens up new interesting possibilities for quantum cryptography networks

0.7 Quantum Proofs of Deletion for Learning with Errors

Alexander PorembaQuantum information has the property that measurement is an inherently destructive process. This feature is most apparent in the principle of complementarity, which states that mutually incompatible observables cannot be measured at the same time. Recent work by Broadbent and Islam (TCC 2020) builds on this aspect of quantum mechanics to realize a cryptographic notion called certified deletion. While this remarkable notion enables a classical verifier to be convinced that a (private-key) quantum ciphertext has been deleted by an untrusted party, it offers no additional layer of functionality. In this work, we augment the proof-of-deletion paradigm with fully homomorphic encryption (FHE). This results in a new and powerful cryptographic notion called fully homomorphic encryption with certified deletion – an interactive protocol which enables an untrusted quantum server to compute on encrypted data and, if requested, to simultaneously prove data deletion to a client. Our main technical ingredient is an interactive protocol by which a quantum prover can convince a classical verifier that a sample from the Learning with Errors (LWE) distribution in the form of a quantum state was deleted. We introduce an

encoding based on Gaussian coset states which is highly generic and suggests that essentially any LWE-based cryptographic primitive admits a classically-verifiable quantum proof of deletion. As an application of our protocol, we construct a Dual-Regev public-key encryption scheme with certified deletion, which we then extend towards a (leveled) FHE scheme of the same type. Our construction achieves indistinguishable ciphertexts in the semi-honest adversarial model, even if the secret key is later revealed after deletion has taken place.

0.8 Breaking the Rate-Loss Bound of Quantum Key Distribution with Asynchronous Two-Photon Interference

Yuan-Mei Xie, Yu-Shuo Lu, Chen-Xun Weng, Xiao-Yu Cao, Zhao-Ying Jia, Yu Bao, Yang Wang, Yao Fu, Hua-Lei Yin, Zeng-Bing ChenTwin-field quantum key distribution can overcome the secret key capacity of repeaterless quantum key distribution via single-photon interference. However, to compensate for the channel fluctuations and lock the laser fluctuations, the techniques of phase tracking and phase locking are indispensable in experiment, which drastically increase experimental complexity and hinder free-space realization. Inspired by the duality in entanglement, we herein present an asynchronous measurement-device-independent quantum key distribution protocol that can surpass the secret key capacity even without phase tracking and phase locking. Leveraging the concept of time multiplexing, asynchronous two-photon Bell-state measurement is realized by postmatching two interference detection events. For a 1 GHz system, the new protocol reaches a transmission distance of 450 km without phase tracking. After further removing phase locking, our protocol is still capable of breaking the capacity at 270 km. Intriguingly, when using the same experimental techniques, our protocol has a higher key rate than the phase-matching-type twin-field protocol. In the presence of imperfect intensity modulation, it also has a significant advantage in terms of the transmission distance over the sending-or-not-sending type twin-field protocol. With high key rates and accessible technology, our work provides a promising candidate for practical scalable quantum communication networks.

0.9 Secure Software Leasing from Standard Assumptions

Fuyuki Kitagawa, Ryo Nishimaki, Takashi YamakawaSecure software leasing (SSL) is a quantum cryptographic primitive that enables users to execute software only during the software is leased. It prevents users from executing leased software after they return the leased software to its owner. SSL can make software distribution more flexible and controllable. Although SSL is an attractive cryptographic primitive, the existing SSL scheme is based on public key quantum money, which is not instantiated with standard cryptographic assumptions so far. Moreover, the existing SSL scheme only supports a subclass of evasive functions. In this work, we present SSL schemes based on the learning with errors assumption (LWE). Specifically, our contributions

consist of the following. - We construct an SSL scheme for pseudorandom functions from the LWE assumption against quantum adversaries. - We construct an SSL scheme for a subclass of evasive functions from the LWE assumption against sub-exponential quantum adversaries. - We construct SSL schemes for the functionalities above with classical communication from the LWE assumption against (sub-exponential) quantum adversaries. SSL with classical communication means that entities exchange only classical information though they run quantum computation locally. Our crucial tool is two-tier quantum lightning, which is introduced in this work and a relaxed version of quantum lighting. In two-tier quantum lightning schemes, we have a public verification algorithm called semi-verification and a private verification algorithm called full-verification. An adversary cannot generate possibly entangled two quantum states whose serial numbers are the same such that one passes the semi-verification, and the other also passes the full-verification. We show that we can construct a two-tier quantum lightning scheme from the LWE assumption.

0.10 Paving the Way towards 800 Gbps Quantum-Secured Optical Channel Deployment in Mission-Critical Environments

Farzam Toudeh-Fallah, Marco Pistoia, Yasushi Kawakura, Navid Moazzami, David H. Kramer, Robert I. Woodward, Greg Sysak, Benny John, Omar Amer, Antigoni O. Polychroniadou, Jeffrey Lyon, Suresh Shetty, Tulasi D. Movva, Sudhir Upadhyay, Monik R. Behera, Joseph A. Dolphin, Paul A. Haigh, James F. Dynes, Andrew J. ShieldsThis article describes experimental research studies conducted towards understanding the implementation aspects of high-capacity quantum-secured optical channels in mission-critical metro-scale operational environments based on Quantum Key Distribution (QKD) technology. The test bed for this research study was carefully designed to mimic such environments. To the best of our knowledge, this is the first time that an 800 Gbps quantum-secured optical channel–along with several other Dense Wavelength Division Multiplexed (DWDM) channels on the C-band and multiplexed with the QKD channel on the O-band–was established at distances up to 100 km, with secure-key rates relevant for practical industry use cases. In addition, during the course of these trials, transporting a blockchain application over this established channel was utilized as a demonstration of securing a financial transaction in transit over a quantum-secured optical channel. In a real-world operational environment, deployment of such high-capacity quantum-secured optical channels multiplexed with the quantum channel will inevitably introduce challenges due to their strict requirements, such as high launch powers and polarization fluctuations. Therefore, in the course of this research, experimental studies were conducted on the impact on the system performance–and specifically on the quantum channel–of several degradation factors present in real-world operational environments, including inter-channel interference (due to Raman scattering and nonlinear effects), attenuation, polarization fluctuations and distance

dependency. The findings of this research pave the way towards the deployment of QKD-secured optical channels in high-capacity, metro-scale, mission-critical operational environments, such as Inter-Data Center Interconnects.