Demonstration of quantum-digital payments

Peter Schiansky   Julia Kalb   Esther Sztatecsny
Marie-Christine Roehsner [*]   Tobias Guggemos
Alessandro Trenti [†]   Mathieu Bozzio
Philip Walther

University of Vienna, Faculty of Physics,
Vienna Center for Quantum Science and Technology (VCQ),
1090 Vienna, Austria
Christian Doppler Laboratory for Photonic Quantum Computer,
Faculty of Physics, University of Vienna,
1090 Vienna, Austria

35th Crypto Day, 25/26 May 2023

Digital contactless payments have replaced physical banknotes in many aspects of our daily lives. Similarly to banknotes, they are easy to use, unique, tamper-resistant and untraceable, but additionally have to withstand attackers and data breaches in the digital world. Current technology substitutes customers' sensitive data by randomized tokens, and secures the uniqueness of each digital purchase with a cryptographic function, called a cryptogram. However, computationally powerful attacks violate the security of these functions. Quantum technology, on the other hand, has the unique potential to guarantee payment protection even in the presence of infinite computational power. Here, we show how quantum light can secure daily digital payments in a practical manner by generating inherently unforgeable quantum-cryptograms. We implement the full scheme over an urban optical fiber link, and show its robustness to noise and loss-dependent attacks. Unlike previously proposed quantum-security protocols, our solution does not depend on challenging long-term quantum storage or a network of trusted agents and authenticated channels. The envisioned scenario is practical with near-term technology and has the potential to herald a new era of real-world, quantum-enabled security.

1 Paper Summary

In the modern era of digital payments ranging from contactless purchases to online banking, a plethora of new security threats arise. One significant threat

[*]Current address: QuTech & Kavli Institute of Nanoscience, Delft University of Technology, 2628 CJ Delft, The Netherlands.

[†]Current address: Security and Communication Technologies, Center for Digital Safety and Security, AIT Austrian Institute of Technology GmbH, Giefinggasse 4, 1210 Vienna, Austria.

crypto day matters 35 (2023)
Beiträge vom 35. Kryptotag, 25.-26. Juni 2023, Regensburg.
doi:10.18420/cdm-2023-35-01

occurs when customers interact with untrusted merchants, who may not have sufficient means to protect against external fraud, or may be malicious themselves.

Motivated by the no-cloning property of quantum mechanics, previous works have investigated the potentials and drawbacks of using quantum light in the prevention of banknote counterfeiting [1] and double-spending with tokens or credit cards [2]. Introducing this fundamentally new type of money to everyday scenarios is, however, technologically challenging: quantum states must be stored over days or months to ensure flexible spending. This is far beyond state-of-the-art quantum storage times, which range from a few microseconds to a few minutes [3]. Recently, an interesting alternative was proposed, replacing quantum storage by a network of trusted agents and authenticated channels, positioned at precise spatial locations with respect to the spending points [4]. From a practical standpoint, this approach presents new drawbacks, as customers and online shoppers do not have the means to securely set up complex trust networks for everyday transactions.

In this work, we show how quantum light can provide practical security advantages over classical methods in everyday digital payments. As shown in Figure 1, we generate and verify i.t.-secure quantum cryptograms, in such a way that the unforgeability and user privacy properties from previous experimental works holds [5], but all intermediate channels, networks and parties are untrusted, thus significantly loosening the security assumptions. Only one authenticated communication (between the client and their payment provider) has to take place at an arbitrary prior point in time. The concealment of the customers' sensitive information is guaranteed by an information-theoretic secure (i.t.-secure) function, and the commitment to the purchase is guaranteed by the laws of quantum mechanics. Additionally, no cross-communication is required to validate the transaction in the case of multiple verifier branches. Our implementation is performed over a 641m urban fiber link, and can withstand the full spectrum of noise and loss-dependent attacks, including those exploiting reporting strategies [6].

References

Scott Aaronson & Paul Christiano (2012). Quantum Money from Hidden Subspaces. *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing* 41–60. URL https://doi.org/10.1145/2213977.2213983.

K. Bartkiewicz, A. Černoch, G. Chimczak, K. Lemr, A. Miranowicz & F. Nori (2017). Experimental quantum forgery of quantum op-

[1] Wiesner (1983); Aaronson & Christiano (2012); Bartkiewicz, Černoch, Chimczak, Lemr, Miranowicz & Nori (2017)

[2] Pastawski, Yao, Jiang, Lukin & Cirac (2012); Bozzio, Orieux, Trigo Vidarte, Zaquine, Kerenidis & Diamanti (2018); Guan, Arrazola, Amiri, Zhang, Li, You, Wang, Zhang & Pan (2018); Bozzio, Diamanti & Grosshans (2019); Horodecki & Stankiewicz (2020)

[3] Ma, Ma, Zhou, Li & Guo (2021); Vernaz-Gris, Huang, Cao, Sheremet & Laurat (2018); Heshami, England, Humphreys, Bustard, Acosta, Nunn & Sussman (2016)

[4] Kent & Pitalúa-García (2020); Kent, Lowndes, Pitalúa-García & Rarity (2022)

[5] Kent *et al.* (2022)

[6] Bozzio, Cavaillès, Diamanti, Kent & Pitalúa-García (2021)

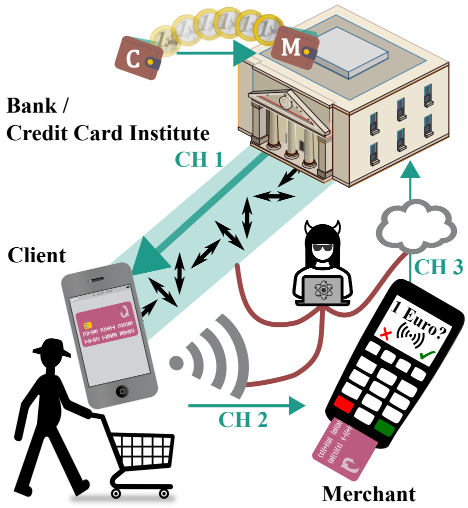

Figure 1: **Simplified representation of quantum-digital payments.** As in classical payments, we consider three parties: a Client, a Merchant and a Bank/Creditcard institute. We do not assume any quantum or classical communication channel to be trusted (i.e. CH 1, CH 2 and CH 3 are insecure), except an initial prior step between the Bank and Client for an account creation. All parties involved apart from the Bank can also act maliciously. During a payment, the Bank sends a set of quantum states to the Client's device (e.g. phone, computer, etc.), who measures them and transforms them into a quantum-secured payment token – *cryptogram* – which we display here as a one-time credit card. The Client uses this classical token for paying at the Merchant, who then contacts the Bank for payment verification. If the payment is accepted, the bank transfers the money from the Client's account to the Merchant's.

tical money. *npj Quantum Inf.* **3**, 7. URL `https://doi.org/10.1038/s41534-017-0010-x`.

Mathieu Bozzio, Adrien Cavaillès, Eleni Diamanti, Adrian Kent & Damián Pitalúa-García (2021). Multiphoton and Side-Channel Attacks in Mistrustful Quantum Cryptography. *PRX Quantum* **2**, 030 338. URL `https://link.aps.org/doi/10.1103/PRXQuantum.2.030338`.

Mathieu Bozzio, Eleni Diamanti & Frédéric Grosshans (2019). Semi-device-independent quantum money with coherent states. *Physical Review A: General Physics* **99**(2), 022336. URL `https://doi.org/10.1103/PhysRevA.99.022336`.

Mathieu Bozzio, Adeline Orieux, Luis Trigo Vidarte, Isabelle Zaquine, Iordanis Kerenidis & Eleni Diamanti (2018). Experimental investigation of practical unforgeable quantum money. *npj Quantum Inf.* **4**, 5. URL `https://doi.org/10.1038/s41534-018-0058-2`.

J-Y. Guan, J-M. Arrazola, R. Amiri, W. Zhang, H. Li, L. You, Z. Wang, Q. Zhang & J-W. Pan (2018). Experimental preparation and verification of quantum money. *Phys. Rev. A* **97**, 032 338. URL https://doi.org/10.1103/PhysRevA.97.032338.

Khabat Heshami, Duncan G. England, Peter C. Humphreys, Philip J. Bustard, Victor M. Acosta, Joshua Nunn & Benjamin J. Sussman (2016). Quantum memories: emerging applications and recent advances. *J. Mod. Opt.* **63**(20), 2005–2028. URL https://doi.org/10.1080/09500340.2016.1148212.

Karol Horodecki & Maciej Stankiewicz (2020). Semi-device-independent quantum money. *New J. Phys.* **22**(2), 023 007. URL https://doi.org/10.1088/1367-2630/ab6872.

Adrian Kent, David Lowndes, Damián Pitalúa-García & John Rarity (2022). Practical quantum tokens without quantum memories and experimental tests. *npj Quantum Inf.* **8**, 28. URL https://doi.org/10.1038/s41534-022-00524-4.

Adrian Kent & Damián Pitalúa-García (2020). Flexible quantum tokens in spacetime. *Physical Review A: General Physics* **101**(2), 022309. URL https://doi.org/10.1103/PhysRevA.101.022309.

Yu Ma, You-Zhi Ma, Zong-Quan Zhou, Chuan-Feng Li & Guang-Can Guo (2021). One-hour coherent optical storage in an atomic frequency comb memory. *Nat. Commun.* **12**, 2381. URL https://doi.org/10.1038/s41467-021-22706-y.

F. Pastawski, N. Y. Yao, L. Jiang, M. D. Lukin & J. I. Cirac (2012). Unforgeable noise-tolerant quantum tokens. *PNAS* **109**(40), 16 079–16 082. URL https://doi.org/10.1073/pnas.1203552109.

Pierre Vernaz-Gris, Kun Huang, Mingtao Cao, Alexandra S. Sheremet & Julien Laurat (2018). Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble. *Nat. Commun.* **9**, 363. URL https://doi.org/10.1038/s41467-017-02775-8.

S. Wiesner (1983). Conjugate coding. *ACM Sigact News* **15**, 78. URL https://doi.org/10.1145/1008908.1008920.