Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 3, pp. 851–860
DOI : 10.47974/JIOS-1942

Exploring the untapped potential of digital lending through the power of quantum computing

Asamani Akhileshwari *
Jayavani Majumdar †
Department of Management
Koneru Lakshmaiah Education Foundation
Hyderabad 500075
Telangana
India

Abstract

The advent of digital disruption in lending has yielded many advantages for both borrowers and lenders. Simultaneously, it has also generated apprehensions over regulation and risks. Like conventional lending, digital lending should possess qualities such as user-friendliness, distinctiveness, resistance to tampering, and being untraceable. However, it is vital for it to possess the capability to endure assaults from digital adversaries and safeguard against breaches of data. Contemporary technologies substitutes clients' sensitive information with randomised tokens and guarantees the distinctiveness of payments by employing a cryptographic function called a cryptogram. Nevertheless, attacks utilising substantial computational resources undermine the security of these functions. Quantum technology can offer safeguards against the limitless computational capabilities. This work showcases the capacity of quantum light to augment the security of common digital lending systems by generating quantum cryptograms that are virtually impervious to counterfeiting. Our technique is distinct from previous protocols in that it is not contingent upon the presence of reliable agents and authenticated channels, nor does it rely on long-term quantum storage. Considering the present technological advancements, this is not only feasible but also possesses the potential to usher in a new epoch of security augmented by quantum capabilities.

Subject Classification: *81P10, 81V80.*

Keywords: *Digital lending, Quantum computing, TTP, Client, Lenders.*

* *ORCID-ID:* **0000-0002-7639-2376**
† *ORCID-ID:* **0009-0000-0741-6672**

* *E-mail:* **2002550003@kluniversity.in (Corresponding Author)**
† *E-mail:* **vani@klh.edu.in**

© Taru Publications

Introduction

Global research endeavours have been initiated in response to the development of quantum computation algorithms that weaken current encryption methods, with the aim of improving security standards [1] [2]. The current cryptographic schemes rely on mathematically complex problems that are computationally difficult to solve (referred to as computational security), and these should be replaced with schemes that are resistant to quantum attacks. Although there is ongoing research and standardisation efforts for quantum-resistant technologies, several solutions have already been compromised by computational attackers [3].

Quantum-mechanical rules can provide defence against attackers that have unlimited processing power for certain tasks. i.t.-security, is a type of security that is driving the development of a quantum internet [4]. Currently, to provide secure communication between two trusted parties across a publicly available channel, the most cutting-edge and widely used quantum technique is 'Quantum Key Distribution (QKD)'. By employing 'quantum key distribution (QKD)', it is possible to create links that are secure from an information-theoretic perspective for distances of up to 500 km with optical fibre and up to 1000 km when using satellites in free space [5]. In the contemporary era of digital lending, which encompasses many forms such as bank lending, peer-to-peer lending, and pay later services, a multitude of new security risks emerge. A major risk arises when clients engage with untrustworthy merchants, who may lack adequate safeguards against external hackers or may have harmful intentions themselves [6]. Therefore, to ensure the legitimacy of a transaction, a binding agreement must be established among the consumer, the merchant, and the bank or lending network [7] [8]. A bond of this sort often manifests as a cryptogram [9] [10], which is the result of a hash function that ensures the uniqueness of each borrowing. Due to the lack of trust among all parties involved, Quantum Key Distribution (QKD) is not a feasible option for providing information technology security in this scenario. Because of this, it is necessary to employ alternative quantum approaches. Variants of QKD that do not rely on particular equipment, such as quantum sources or detectors, are also unsuitable due to the fact that the untrusted parties themselves are in charge of the cryptogram, which is the ultimate classical output. Previous research has investigated the pros and cons of employing quantum light for the reproduction of expenditures using tokens or credit cards, due to its non-cloning characteristic [11][12]. The implementation of a novel currency in daily

contexts poses considerable technological obstacles. More precisely, it necessitates keeping track of quantum states over prolonged durations, spanning from days to months, to provide convenient and flexible use. These quantum storage periods greatly exceed the current state-of-the-art range of a few microseconds to a few minutes [13][14]. A proposal has been made to substitute quantum storage with an infrastructure of trustworthy operators and verified methods, which would be strategically positioned in relation to the locations where expenditures are made [15]. Practically, this technique has additional disadvantages since clients and online shoppers lack the ability to establish secure and intricate trust networks for their regular credit transactions. Furthermore, the accurate monitoring of the verifiers' geographical and chronological whereabouts necessitates a dependable Global Positioning System (GPS), which regrettably renders them susceptible to undesired spoofing endeavours [16]. This study demonstrates the practical security benefits of quantum light compared to conventional approaches in typical digital lending [17]. We produce and authenticate quantum cryptograms that are secure against information-theoretic attacks. These cryptograms preserve the qualities of being unable to be forged and ensuring the anonymity of the user, as demonstrated in prior experimental research. Nevertheless, the security assumptions are loosened as all intermediary channels, networks, and parties are regarded as untrustworthy. Only a single verified communication needs to occur between the customer and their loan service provider at any given moment in time. An i.t.-secure function ensures the protection of consumers' sensitive information, while the commitment to the transaction is assured by the rules of quantum physics. In the event of numerous verifier branches, there is no need for cross-communication to validate the loan transaction [18].

Methodology

Digital lending

We intend to provide an overview of the fundamental security concepts that are utilised in modern online lending (the exact implementation may vary) [19], through the process by which each Client creates a profile with a Trusted Token Provider (TTP) through the use of an encrypted communication channel. The acronym "TTP" commonly refers to the lender or credit issuer of the client, or a trusted third-party entity. The initial part of the process involves the provision of a one-of-a-

kind identifying token, which is symbolised by the letter C. This token is then kept in a safe manner on the devices belonging to both the 'Client' and 'TTP'. The information that is held on the Client's device may include a virtual credit card or an electronic wallet that is kept on a smartphone, watch, or other similar devices. In case the borrower desires to obtain a loan from a certain Lender Li, it is of the utmost importance to make certain that dishonest organisations, such as lenders who are not dependable, are unable to lend money in the name of the Client at a different location or at a different time. There is a single-use payment token, designated by the letter P, that is issued to the Client by the Lender or the Trusted Third Party (TTP). A cryptogram is the result of a function that includes the Client's secret token C, the 'Lender's public ID Li', and the 'one-time payment token P'. This token is used to generate a 'cryptogram', which is the output of the function. The function is producing the result, which is the cryptogram that is being computed. It cannot be overstated how important it is to emphasise that the Lender identification, also known as Li, must be genuine and trustworthy in order to be regarded valid. It is highly recommended to obtain information from a trustworthy source, such as a Public Key Infrastructure or a localised maintained database that is pre-shared and inaccessible to unauthorised individuals. The message that is encrypted, which is denoted by the symbol κ (C, Li, P), is sent to the Lender. In order to authenticate the borrower, the lender then transmits the information to the Trusted Third Party (TTP). As a result of the fact that it is in possession of the pertinent information connected with all three inputs, which are C, Li, and P, the TTP is able to validate the encryption key and validate that the cryptogram is original. This can be done since the TTP is enabled to validate the encryption key. In practical situations, the term "cryptogram" typically refers to the output of a cryptographic hashing or encrypting operation that possesses a high level of computational security. Nevertheless, this would make it possible for a malicious entity that possessed a large amount of computing power to conduct a comprehensive examination of every conceivable combination of C, P, and Li as input until they were able to effectively identify the particular combination that matches to the initial cryptogram without any problems. Under those conditions, the client's identification and the information about their borrowing are completely exposed.

Quantum advantage

Previous quantum-digital signature schemes have demonstrated the ability to provide i.t. security when considering these attacks exclusively [20][21]. The study presents a quantum-based method employing a

singular Quantum Key Distribution (QKD) for the preliminary phase of connecting the Client and Trusted Third Party (TTP) to guarantee the efficient functioning of QKD systems.

Step 1: Quantum lending is a variation of classical digital lending where the conventional loan token P is substituted by a sequence $|P\rangle$ of quantum states. In other words, the notation κ (C, L_i, P) is modified to κ (C, L_i, $|P\rangle$).

Step 2: The TTP is responsible for the generation of a bitstring, which is indicated as b, and a conjugate basis-string, which is designated as B, both of which are created randomly and have a length of λ. An encoded quantum state is formed in Bj, where j is a member of the set of integers ranging from 1 to λ. Every single bit 'bj' is encoded onto this quantum state. The TTP maintains the traditional representation (b, B) of the quantum token $|P\rangle$ associated with the Client's ID CID. This description is preserved in the TTP. For example, when λ equals 4, and the basis Bj is selected from the set {+/-; 0/1}, with (b, B) being (0101, 0011), the expression "$|P\rangle$" can be expressed as "$|+\rangle|-\rangle|0\rangle|1\rangle$". The duration of λ is influenced by two key factors: the anticipated probability of an assault and the availability of lenders in the market.

Step 3: After receiving $|P\rangle$, the Client selects the Lender L_i from a database that was securely provided in advance with the Trusted Third Party (TTP). Afterwards, they compute $l_i = MAC(C, L_i)$, where l_i represents the output tag of 'Message Authentication Code (MAC)' that is i.t.-secure. The MAC function employs a confidential token C and a public ID Li from a selected Lender, with the user regarding "mi" as a basic string and confidentially assessing the 'sequence $|P\rangle$'. It is the accumulation of the outcomes of the measurements that makes up the cryptogram.

Step 4: The Client transmits κi and their ID C_{ID} to the lender, who then sends this information, together with its L_i, as {κ_i, L_i, C_{ID}}, to the TTP for authentication.

Step 5: In order to provide permission for borrowing, the Trusted Third Party (TTP) retrieves information about C and (b,B), and computes l_i by applying the Message Authentication Code (MAC) function to C and L_i, which represents the Client's ID. The TTP approves the transaction only if $(\kappa_i)_j$ is equal to b_j when $(l_i)_j$ is equal to B_j. The TTP refuses any other options.

The security of the protocol is dependent on the maximum probability of generating two unique and legitimate cryptograms '$\kappa_{i'}$ and '$\kappa_{j'}$ for two different Lenders L_i and L_j. This is referred to as p_d in the subsequent two sections. Another potential method of attack involves the creation of a

counterfeit output tag, resulting in the equation 'MAC(C, L_i) = MAC(C, L_j) $\Leftrightarrow l_i = l_j \Leftrightarrow \kappa_i = \kappa_j$'. This probability is referred to as p_t.

In a secure information technology (IT) environment, the equation "pt = 1/|l| = |L|/|C| = 1/√|C|" is accurate. In this framework, the symbols |l|, |L|, and |C| represent the cardinality of the MAC, the Lender ID, and the secret token of the Client, respectively. We will posit that the magnitude of l is equivalent to the magnitude of L, which is likewise equal to the square root of the magnitude of C.

For the sake of consistency, we select p_d and p_t to have about the same magnitude, specifically $p_d \approx p_t = 1 = \sqrt{|C|}$. As a consequence of this, the number N of quantum states that are necessary to validate a single bit of the cryptogram will be determined. According to the logarithm of the size of the message, which is indicated as log2(|m|), the bit length of every MAC is defined by the logarithm of base 2. The entire length of the quantum token may be determined by analysing the equation $\lambda = N. \log2(|l|) = N \log2(\sqrt{|C|})$. It is possible to integrate as an input to the MAC function any supplemental parameter that is required to be included in the transaction. For example, the payment amount is one example of such a parameter.

Similar to how Quantum Key Distribution (QKD) ensures information security for key exchanges like [22], Our technique ensures the confidentiality of information by utilising cryptograms that can only be used a single time. The i.t. secure Messages Authentication Code safeguards C's concealment, despite the impossibility theory's limitation on quantum commitment, and the irreversible nature of quantum measurements guarantees that commitment to Mi is never violated [23] [24], this allows for the possibility that one of both parties may purposefully delay their quantum measurements. This is due to the fact that our protocol is based on the presumption that one of the parties involved, who is referred to as the Trusted Third Party (TTP), is trustworthy and behaves in an honest manner.

In two distinct ways, our technique is distinct from the QKD approaches that are commonly used. To begin, the selection of the measurement foundation utilises determinism rather than randomness as the underlying principle. An effective association between the purchase and a particular Client token and Lender is established during this phase. As an additional benefit, the measurement bases are always concealed, which offers the intriguing advantage of concealing the name of the Lender that the Client has selected until verification is necessary.

Loss-contingent security

While the theoretical rules of quantum physics provide the security of commitment, actual settings need careful consideration of specific factors. Certain 'quantum states' will deviate from their ideal classical descriptions on account of the inherent defects of actual devices, such as faulty state preparation, noisy quantum channels, and non-unit detecting efficacy. Additionally, certain quantum states will be lost along the process. It is possible that specific components in step 5 will be different, despite the fact that they will be evaluated using the same criteria. (i.e., '$(\kappa_i)_j \neq b_j$ when $(l_i)_j = B_j$'). Consequently, the protocol would terminate prematurely, even if it was executed faithfully. It is necessary to account for mistakes and losses throughout the verification stage. Consequently, a malevolent entity can take use of this newly granted permission to bypass the obligation or duplicate the cryptogram's spending. Consider, for example, the possibility that the TTP is able to sustain a loss of up to fifty percent. To generate two tokens that have been successfully committed, a malicious client may thereafter measure fifty percent of the quantum token $|P\rangle$ in the M0 basis and the remaining fifty percent in the M1 basis. This results in the generation of two tokens. Despite the fact that double-spending is conceivable with a loss rate of fifty percent that is authorised, we used semidefinite programming to determine the exact mistake and loss rate combinations that may still be recognised in an attack. This was done in spite of the fact that the loss rate was permitted. Derivation in quantum tokens entails recognising deceptive tactics to reduce errors and losses caused by malicious entities. Previous implementations failed to account for high-intensity attacks reliant on loss, making it imperative to rectify this concern in future endeavours.

Discussion

Quantum lending is a mechanism that we give and evaluate, which guarantees the unique occurrence of transactions while maintaining the confidentiality of information technology networks. It is possible to dramatically reduce the possibility of cheating in the presence of experimental faults such as noise and losses by increasing the length of the quantum token. With the exception of single-photon detection, the implementation does not need any complicated technology on the part of the Client organisation.

The typical timeframe for borrowing and lending is in the range of seconds. However, our quantum communication and verification technique provide information technology security within a few tens of minutes. Nevertheless, the cited limits are exclusively of a technical nature. In order to improve the speed of quantum communication, one can employ more potent quantum sources. However, the verification delay occurs due to the necessity of correcting discrepancies in time-tagging between the two buildings. It has been demonstrated that there are brighter sources of entangled photon pairs, which might possibly decrease the time it takes to transmit quantum tokens to less than one second.

It is crucial to guarantee that practical digital lending systems can process borrowing requests without jeopardising the client's sensitive data. Within our method, the adversary has the ability to compromise either the payment token $|P\rangle$ transmitted over the quantum channel, the cryptogram transmitted through the conventional channel, or the Client's selection of L_i.

In the first two scenarios, quantum mechanics will guarantee that the Trusted Third Party (TTP) will identify the incorrectly generated cryptogram and decline the payment with a probability that can be arbitrarily close to 100%. The transaction can be resumed. However, in order to ensure the security of i.t. system, it is important to avoid reusing the key C. Therefore, we suggest using an n-time-secure Message Authentication Code (MAC) as a solution to this challenge. This enables the reuse of C as an input for subsequent borrowings, so imposing a definite and arbitrary limit on the amount of loan that may be obtained [25].

Upon consumption of C, a novel C must be produced, which will be shared by both the Client and TTP. We may modify our protocol to remove the restriction on the loan amount imposed by the MAC function [26]. This can be achieved by increasing the value of C during the lending process. When the Client gets a new quantum token $|P\rangle$, we add more quantum states for QKD and utilise the cryptogram κ for authentication. In order to safeguard against the third scenario, it is imperative to guarantee that the Client's selection of Mi is completely unaffected by any external prejudice. For instance, this can be achieved by initially distributing a secure database of Lenders in conjunction with C and enabling the Client to select without any prior communication with the Lender. Alternatively, the Lender can choose to send their identify to the Client, who then uses the local database to provide an additional degree of authentication [27]. The streamlined implementation requirements of our protocol, together with its ability to

tolerate errors, make it well-suited for deployment in intermediate quantum networks. Classical networks facilitate the provision of hosting services for applications that extend beyond basic communication functionalities [28]. Moreover, the progress in creating other quantum building blocks and using them for purposes other than Quantum Key Distribution (QKD) would be essential for the progress of a prospective quantum internet. Our approach propels the area of quantum payment systems towards practical relevance in the medium term [29].

References

[1] N. S. Elie Gouzien, "Factoring 2048-bit RSA Integers in 177 Days with 13,436 Qubits and a Multimode Memory," *Physical Review Letters* (2021).

[2] E. M. Lopez, "Experimental Realization of Shor's Quantum Factoring Algorithm Using Qubit Recycling," *Nature* (2012).

[3] T. D. Wouter Castryck, "An Efficient Key Recovery Attack on SIDH," *Cryptology ePrint Archive* (2022).

[4] D. E. a. R. H. Stephanie Wehner, "Quantum Internet: A Vision for the Road Ahead," *Science* (2018).

[5] Y. H. L. Juan Yin, "Entanglement-Based Secure Quantum Cryptography Over 1,120 Kilometres," *Nature* (2020).

[6] PCI Security Standards Council, "PCI Security Standards Council," [Online]. Available: https://www.pcisecuritystandards.org/.

[7] EMVCo LLC, "Interpreting the EMV Tokenisation Specification," [Online]. Available: https://www.emvco.com/specifications/.

[8] K. L. Francisco Corella, "Interpreting the EMV Tokenisation Specification," *White Paper* (2014).

[9] T. v. L. Wei Zhang, "A Device-Independent Quantum Key Distribution System for Distant Users," *Nature* (2022).

[10] Y. Z. Z. Wen Zhao Liu, "Toward a Photonic Demonstration of Device-Independent Quantum Key Distribution," *Physical Review Letters* (2022).

[11] E. D. F. G. Mathieu Bozzio, "Semi-Device-Independent Quantum Money with Coherent States," *Physical Review A* (2023).

[12] J. M. A. Jian-Yu Guan, "Experimental Preparation and Verification of Quantum Money," *Physical Review A* (2018).

[13] Y. Z. M. Yu Ma, "One-Hour Coherent Optical Storage in an Atomic Frequency Comb Memory," *Nature Communications* (2021).

[14] D. G. E. Khabat Heshami, "Quantum Memories: Emerging Applications and Recent Advances," *Journal of Modern Optics* (2016).

[15] D. L. Adrian Kent, "Practical Quantum Tokens Without Quantum Memories and Experimental Tests," *Nature* (2021).

[16] C. P. Nils Ole Tippenhauer, "On the Requirements for Successful GPS Spoofing Attacks," in *Proceedings of the 18th ACM Conference on Computer and Communications Security* (2011).

[17] A. O. Mathieu Bozzio, "Experimental Investigation of Practical Unforgeable Quantum Money," *Nature* (2018).

[18] K. M. Danushka Jayasinghe, "Enhancing EMV Tokenisation with Dynamic Transaction Tokens," in *Radio Frequency Identification and IoT Security* (2017).

[19] P. W. Ryan Amiri, "Secure Quantum Signatures Using Insecure Quantum Channels," *Physical Review A* (2016).

[20] Y. F. Hua Lei Yin, "Experimental Quantum Secure Network with Digital Signatures and Encryption," *National Science Review* (2021).

[21] H. F. C. Hoi Kwong Lo, "Is Quantum Bit Commitment Really Possible?," *Physical Review Letters* (1997).

[22] D. W. and H. M., "New Directions in Cryptography," *IEEE* (1976).

[23] Fak, "Repeated Use of Codes Which Detect Deception (Corresp.)," *IEEE* (1979).

[24] S. I. Laszlo Gyongyosi, "Advances in the Quantum Internet," *Communications of the ACM* (2022).

[25] A. C. Mathieu Bozzio, "Multiphoton and Side-Channel Attacks in Mistrustful Quantum Cryptography," *PRX Quantum* (2021).

[26] G. E. N. and M. F. K., "Codes Which Detect Deception," *IEEE* (1974).

[27] S. G. and P. Sarkar, "Variants of Wegman-Carter Message Authentication Code Supporting Variable Tag Lengths," *Designs, Codes and Cryptography* (2021).

[28] J. A. K. Marie Christine Roehsner, "Probabilistic One-Time Programs Using Quantum Entanglement," *Nature* (2021).

[29] D. C. Paul Skrzypczyk, *Semidefinite Programming in Quantum Information Science* (2023).

Received August, 2024