quantum reports

MDPI

Article

Entropic DDoS Detection for Quantum Networks

Del Rajan

HSBC Lab, 8 Canada Square, London E14 5HQ, UK; del.rajan@hsbc.com

Abstract: Distributed Denial-of-Service (DDoS) attacks are a significant issue in classical networks. These attacks have been shown to impact the critical infrastructure of a nation, such as its major financial institutions. The possibility of DDoS attacks has also been identified for quantum networks. In this theoretical work, we introduce a quantum analogue of classical entropic DDoS detection systems 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 results extend the applicability of quantum information from the domain of data security to the area of network security.

Keywords: quantum networks; quantum DDoS; DDoS; Distributed Denial-of-Service

check for updates

Citation: Rajan, D. Entropic DDoS Detection for Quantum Networks. *Quantum Rep.* **2022**, *4*, 604–615. https://doi.org/10.3390/quantum4040044

Academic Editor: Antonio Manzalini

Received: 4 November 2022
Accepted: 10 December 2022
Published: 13 December 2022

1. Introduction

A central aim of quantum information science is to design quantum systems that perform information tasks [1]. Prominent examples of such work involved deriving quantum analogues of classical information technologies and demonstrating an advantage by utilizing the quantum resource. For instance, the property of superposition is used by quantum models of computation to drastically outperform the best classical supercomputers on certain tasks [2,3]. Another example is the quantum analogues of classical communication networks which are simply referred to as quantum networks [4]. In such networks, quantum information can be teleported [5], notably to distances exceeding 1000 km [6]. Further protocols include secure key distribution which are predicated on the impossibility to copy quantum information [7].

Beyond this established work, a direction ahead is to design novel quantum information technologies by harnessing our understanding of the classical case. Our main result is to demonstrate progress in this area.

Distributed Denial-of-Service (DDoS) attacks are a significant issue in network security [8,9], and various methods have been developed to detect the attacks in classical networks. The possibility of DDoS attacks has also been identified for quantum networks [7,10–12]. In our theoretical work, we designed a detection system for such attacks that occur in this quantum setting.

2. Classical DDoS

In classical networks, information is transmitted in the form of data packets, and the role of directing this traffic is performed by routers. To initiate a DDoS flooding attack, many routers would direct packets from multiple attack nodes to a victim node. The intent behind this flood of traffic is to overload the victim node so that it becomes unresponsive to legitimate traffic.

DDoS attacks are rather frequent events [8,9], and their reach can extend into the critical infrastructure of a nation [13]. These include attacks on major financial institutions, such as banks [14,15] and exchanges [16].

Preventing a DDoS attack requires most essentially the ability to identify the attack traffic as early as possible [17]. To achieve this capability, detection systems have been designed using the Shannon entropy:

$$H(X) \equiv -\sum_i p_i \log p_i, \tag{1}$$

where p_i are the probabilities associated with random variable X, and logarithms are taken to base 2.

Reviews of such entropic approaches can be found in [9,17,18]. We briefly outline one of these methods [19].

A flow at a router is group of packets categorized as

$$f_{ij}(u_i, d_j, t) \equiv \{< u_i, d_j, t > | u_i \in U, d_j \in D\}, \tag{2}$$

where $i, j \in \mathbb{Z}^+$, U is the set of the upstream routers, D denotes the set of destination addresses from the router, and t is the time stamp. Let $|f_{ij}(u_i, d_j, t)|$ represent the number of packets of flow f_{ij} at time t. For a given time interval ΔT, the variation of the number of packets for a given flow is defined as

$$N_{ij}(u_i, d_j, t + \Delta t) \equiv |f_{ij}(u_i, d_j, t + \Delta T)| - |f_{ij}(u_i, d_j, t)|. \tag{3}$$

If $|f_{ij}(u_i, d_j, t)| = 0$, then $N_{ij}(u_i, d_j, t + \Delta T)$ is the number of packets of flow f_{ij} that went through the router during time interval ΔT. The quantity

$$p_{ij}(u_i, d_j, t + \Delta T) = \frac{N_{ij}(u_i, d_j, t + \Delta T)}{\sum_{i=1}^{\infty} \sum_{j=1}^{\infty} N_{ij}(u_i, d_j, t + \Delta T)}, \tag{4}$$

gives the probability of the flow f_{ij} over all flows at the router with

$$\sum_{i=1}^{\infty} \sum_{j=1}^{\infty} p_{ij}(u_i, d_j, t + \Delta T) = 1. \tag{5}$$

The computation of the Shannon entropy (1) at the router is obtained through

$$H(F) = -\sum_{i,j} p_{ij}(u_i, d_j, t + \Delta T) \log p_{ij}(u_i, d_j, t + \Delta T), \tag{6}$$

where F is the associated random variable with respect to flows during ΔT. If the total number of flows is constrained to N, then (6) is rather simply

$$H(F) = H(p_1, p_2, \ldots, p_N) = -\sum_{i=1}^{N} p_i \log p_i, \tag{7}$$

with $0 \leq H(F) \leq \log N$. The lower bound occurs when there is only one flow.

In order to model a DDoS attack, a number of assumptions are made. These are that there is no extraordinary change of traffic in a very short time for the non-attack case, the number of attack packets is at least an order of magnitude higher than that of normal flows, there is only one attack ongoing at a time, and the number of flows is stable for both non-attack and attack cases.

Suppose attack flows start passing through the router at $t = (n + 1)\tau$; hence, $t = n\tau$ signifies the time at the router just before the attack. The respective distributions are

$$\{p_1^{(n+1)\tau}, p_2^{(n+1)\tau}, \ldots, p_N^{(n+1)\tau}\}, \tag{8}$$

$$\{p_1^{n\tau}, p_2^{n\tau}, \ldots, p_N^{n\tau}\}. \tag{9}$$

A consequence of the assumptions is that $p_k^{n\tau} \ll p_k^{(n+1)\tau}$ for some k. Further reasoning with Jensen's inequality leads to

$$-\sum_{i=1}^{N} p_i^{n\tau} \log p_i^{n\tau} \gg -\sum_{i=1}^{N} p_i^{(n+1)\tau} \log p_i^{(n+1)\tau}. \tag{10}$$

Expressing this in terms of the entropy (7) gives

$$H(F^{n\tau}) \gg H(F^{(n+1)\tau}). \tag{11}$$

The entropy at the router drops dramatically as soon as attack flows are passing through, thereby allowing for an ability to detect an attack as early as possible.

3. Quantum Networks

Quantum networks [4] generate entanglement over long distances. These entanglement flows are routed through devices known as repeaters [20,21], which perform entanglement swapping to connect two spatially entangled links into a longer entangled link.

To illustrate an instantiation of this task, we will utilize Bell states

$$|\beta_{xy}\rangle = \frac{|0\rangle \otimes |y\rangle + (-1)^x |1\rangle \otimes |\bar{y}\rangle}{\sqrt{2}}, \tag{12}$$

where the bar denotes negation and we have a choice between $xy = 00, 01, 10$, or 11. With respect to the computational basis states, the quantum information in the Bell state (12) takes the form

$$\left(\frac{\bar{y}}{\sqrt{2}}, \frac{y}{\sqrt{2}}, \frac{(-1)^x y}{\sqrt{2}}, \frac{(-1)^x \bar{y}}{\sqrt{2}}\right). \tag{13}$$

Consider a quantum network which has to perform a routing task between two nodes. A request node needs to share a Bell state with a receiver node, with the constraint that the request node is unable to directly communicate with the receiver node. Despite the apparent difficulty, this task can be accomplished through the use of a quantum repeater located at another node.

We start by generating Bell pairs at both the request node (qubits A and B) and the repeater node (qubits C and D). One qubit (B) of the request pair reaches the repeater to be Bell projected with a qubit (C) at the repeater.

The joint state can be written as

$$\begin{aligned} |\text{Request}\rangle \otimes |\text{Repeater}\rangle &\equiv |\beta_{00}\rangle_{A,B} \otimes |\beta_{xy}\rangle_{C,D} \\ &= \tfrac{1}{2}(|\beta_{xy}\rangle_{A,D} \otimes |\beta_{00}\rangle_{B,C}) \\ &\quad + |\beta_{\bar{x}y}\rangle_{A,D} \otimes |\beta_{10}\rangle_{B,C} \\ &\quad + (-1)^x |\beta_{x\bar{y}}\rangle_{A,D} \otimes |\beta_{01}\rangle_{B,C} \\ &\quad + (-1)^x |\beta_{\bar{x}\bar{y}}\rangle_{A,D} \otimes |\beta_{11}\rangle_{B,C}\,. \end{aligned} \tag{14}$$

The repeater performs a Bell state projection on BC. This returns one of four possible outcomes with consequences for AD:

$$\begin{aligned} |\beta_{00}\rangle_{B,C} &\rightarrow |\beta_{xy}\rangle_{A,D} \\ |\beta_{01}\rangle_{B,C} &\rightarrow (-1)^x |\beta_{x\bar{y}}\rangle_{A,D} \\ |\beta_{10}\rangle_{B,C} &\rightarrow |\beta_{\bar{x}y}\rangle_{A,D} \\ |\beta_{11}\rangle_{B,C} &\rightarrow (-1)^x |\beta_{\bar{x}\bar{y}}\rangle\,. \end{aligned} \tag{15}$$

Depending on the outcome, the repeater applies a particular unitary operator to qubit D:

$$\begin{gathered}(\mathbb{I}\otimes\mathbb{I})\left|\beta_{xy}\right\rangle_{A,D},\\ (\mathbb{I}\otimes(-1)^{x}\hat{\sigma}_1)(-1)^{x}\left|\beta_{x\bar{y}}\right\rangle_{A,D},\\ (\mathbb{I}\otimes(-1)^{y}\hat{\sigma}_3)\left|\beta_{\bar{x}y}\right\rangle_{A,D},\\ (\mathbb{I}\otimes(-1)^{x+y}\hat{\sigma}_3\hat{\sigma}_1)(-1)^{x}\left|\beta_{\bar{x}\bar{y}}\right\rangle_{A,D},\end{gathered} \tag{16}$$

where $\hat{\sigma}_1 = |0\rangle\langle 1| + |1\rangle\langle 0|$, $\hat{\sigma}_2 = -i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0|$ and $\hat{\sigma}_3 = |0\rangle\langle 0| - |1\rangle\langle 1|$. Afterwards, the non-projected qubit (D) of the repeater pair leaves towards the destination node. This results in the desired output of having state $\left|\beta_{xy}\right\rangle_{A,D}$ shared between the request node and receiver.

We want to view this procedure in terms of the von Neumann quantum entropy [1], which is defined as

$$S(\rho) \equiv -\mathrm{Tr}(\rho\log\rho), \tag{17}$$

where ρ is a density operator. The entropy is zero if and only if it is a pure state. For an arbitrary composite system with subsystems K and L, the joint and conditional entropy are

$$S(\rho_{KL}) \equiv -\mathrm{Tr}(\rho_{KL}\log\rho_{LK}), \tag{18}$$

$$S(\rho_K|\rho_L) \equiv S(\rho_{KL}) - S(\rho_L), \tag{19}$$

where $\rho_K = \mathrm{Tr}_L(\rho_{KL})$ and $\rho_L = \mathrm{Tr}_K(\rho_{KL})$. Suppose ρ_{KL} is a pure state; then, ρ_{KL} is entangled if and only if

$$S(\rho_K|\rho_L) < 0. \tag{20}$$

In this case, the entropy of either subsystem, $S(\rho_K)$ or $S(\rho_L)$, is referred to as the entanglement entropy.

In the repeater, the density operator is

$$\rho_{C,D} = \left|\beta_{xy}\right\rangle_{B,C}\left\langle\beta_{xy}\right|_{B,C}, \tag{21}$$

and the associated conditional entropy is

$$S(\rho_C|\rho_D) = S(\rho_{C,D}) - S(\rho_D) = 0 - 1 = -1, \tag{22}$$

which indicates entanglement (20) as expected. Note that at the time before projection, qubits A and D are not entangled

$$S(\rho_A|\rho_D) = S(\rho_{A,D}) - S(\rho_D) = 2 - 1 = 1. \tag{23}$$

For the output state, the density operator takes the form

$$\rho_{A,D} = \left|\beta_{xy}\right\rangle_{A,D}\left\langle\beta_{xy}\right|_{A,D}, \tag{24}$$

and the associated conditional entropy is

$$\begin{aligned} S(\rho_A|\rho_D) &= S(\rho_{A,D}) - S(\rho_D)\\ &= 0 - 1 = -1, \end{aligned} \tag{25}$$

signifying entanglement, with a loss of it in

$$\begin{aligned} S(\rho_C|\rho_D) &= S(\rho_{C,D}) - S(\rho_D)\\ &= 2 - 1 = 1. \end{aligned} \tag{26}$$

In terms of the joint entropy, just before projection (22), we see that $S(\rho_{C,D}) = 0$, which specifies a pure state. After projection (26), we have that $S(\rho_{C,D}) = 2$, which signifies missing information in CD. Part of that missing information moved, as described by the updated entropy $S(\rho_{A,D}) = 0$ in the output $|\beta_{xy}\rangle_{A,D}$.

4. Quantum DDoS

Quantum networks can also experience DDoS attacks [10,22], which poses a significant threat to its quantum key distribution protocols [7,11]. Given that quantum repeaters have a maximum session capacity [23], we consider DDoS attacks on a repeater where service requests exceed that maximum capacity.

The entanglement entropy will be used to formulate a DDoS detection system analogous to the classical case (11). To derive this, we utilize various aspects of the material in [24] towards our specific application.

Our model starts with the request node generating $|\beta_{00}\rangle_{A,B}$, with qubit B being sent to the repeater. The repeater generates $|\beta_{00}\rangle_{C,D}$, which can be viewed as an instantiation of $|\beta_{xy}\rangle_{C,D}$.

We consider the quantities before the projection. The total system is $\rho_{A,B,C,D}$, which denotes

$$|\beta_{00}\rangle_{A,B} |\beta_{00}\rangle_{C,D} \langle\beta_{00}|_{A,B} \langle\beta_{00}|_{C,D}, \tag{27}$$

and the subsystem held at the repeater is $\rho_{B,C,D}$, as it excludes ρ_A. Given qubits C and D are jointly in a pure state, we have that

$$S(\rho_{B,C,D}) = S(\rho_B) = 1. \tag{28}$$

The qubit B is maximally mixed, since it is entangled with qubit A in a Bell state. Thus, the entanglement entropy of qubit A before the projection equates to

$$S(\rho_A) = S(\rho_{B,C,D}). \tag{29}$$

We take the partial trace to obtain the density operator for qubit D

$$\rho_D = \mathrm{Tr}_{ABC}(\rho_{A,B,C,D}). \tag{30}$$

We have that $S(\rho_D) = 1$, since it is entangled with ρ_C.

The entanglement entropy forms a crucial role for a repeater session. A successful session occurs when the entanglement is swapped (15). The swapping is successful only if the repeater uses some rank-one orthogonal projectors Π_i such that no matter what outcome occurs at the repeater on qubits B and C, the value of the entanglement entropy of ρ_A before projection must equal the value of the entanglement entropy of ρ_A after projection.

We proceed to examine the quantities after the projection. If the repeater obtains outcome i, then the density operator of D is

$$\rho_{D_i} = \frac{1}{p_i}\mathrm{Tr}_{ABC}(\Pi_i \rho_{A,B,C,D}), \tag{31}$$

where p_i is the associated Born probability. Given

$$\sum_i \Pi_i = \mathbb{I}, \tag{32}$$

we have that

$$\rho_D = \sum_i p_i \rho_{D_i}. \tag{33}$$

After measurement, qubits A and D are in a pure entangled state. The entanglement entropy of D equates to the entanglement entropy of A after projection

$$S(\rho_{D_i}) = S(\rho_A). \tag{34}$$

Using the crucial condition that a successful session requires the entropy before projection and entropy after projection of ρ_A to equate, we can formulate relationships between the quantities before and after projection. Specifically, using (29) and (34), we obtain

$$S(\rho_{D_i}) = S(\rho_{B,C,D}), \tag{35}$$

and furthermore

$$S(\rho_{B,C,D}) = S(\rho_{D_i}) = \sum_i p_i S(\rho_{D_i}). \tag{36}$$

Applying the concavity inequality [24] to (33) results in

$$S(\rho_D) \geq \sum_i p_i S(\rho_{D_i}). \tag{37}$$

Combining (36) and (37) gives

$$S(\rho_{B,C,D}) = \sum_i p_i S(\rho_{D_i}) \leq S(\rho_D). \tag{38}$$

Therefore, before the projection, one can predict that a successful session is possible when and only when

$$S(\rho_{B,C}|\rho_D) = S(\rho_{B,C,D}) - S(\rho_D) \leq 0. \tag{39}$$

A failed session will occur when $S(\rho_{B,C}|\rho_D) > 0$. For our specific case (27), we have that $S(\rho_{B,C}|\rho_D) = 0$, which implies a successful session ahead.

The capacity of the repeater is defined as the maximum number of sessions it can facilitate simultaneously, and this is directly related to the number of Bell pairs that can be stored in memory [23]. In our case, this would be the maximum number of copies of $\rho_{C,D}$ generated at a time to keep the service at full capacity. After that time, any unused Bell pairs get destroyed, and the system regenerates to full capacity at the next time point.

With respect to capacity, we modify our previous analysis to N copies of system $\rho_{A,B,C,D}$ for a large N. The repeater would perform a complete projective measurement on $(\rho_{B,C})^{\otimes N}$. In this case, all the entropies are multiplied by N. Hence, the condition (39) for sessions is maintained, and we can interpret it in terms of capacity.

In [24], it was shown that a negative conditional entropy in an entanglement-swapping protocol equals the number of left Bell pairs. Harnessing this reasoning in our quantum repeater scenario implies that if we have $S(\rho_{B,C}|\rho_D) < 0$ before the projection, then $-S(\rho_{B,C}|\rho_D)$ is the number of Bell pairs left afterwards in the memory. It can be viewed as quantifying the unused capacity after the session requests have been fulfilled. If $S(\rho_{B,C}|\rho_D) > 0$, it not possible to carry out a session to begin with, and the system predicts an unresponsive service due to requests exceeding the capacity. Therefore, (39) can be used to model a DDoS attack.

To design a detection system, suppose a flood of attack requests reaches a repeater at specific time $t = (n+1)\tau$. We make the same assumptions about the network traffic of the attack requests as in the previous classical case. For example, here we also assume the number of attack requests is at least an order of magnitude higher than that of normal requests. The entropy of the requests at the repeater is quantified as

$$S(\rho_B^{n\tau}) \ll S(\sigma_B^{(n+1)\tau}), \tag{40}$$

where ρ is used to label the systems involved prior to attack, and σ denotes the systems involved in the attack (the superscripts signify the respective times). The repeater generates the same full capacity at each time point; hence,

$$S(\rho_{C,D}^{n\tau,n\tau}) = S(\sigma_{C,D}^{(n+1)\tau,(n+1)\tau}), \tag{41}$$

and with (40), we obtain

$$S(\rho_{B,C,D}^{n\tau,n\tau,n\tau}) \ll S(\sigma_{B,C,D}^{(n+1)\tau,(n+1)\tau,(n+1)\tau}). \tag{42}$$

From (41), we have that

$$S(\rho_{D}^{n\tau}) = S(\sigma_{D}^{(n+1)\tau}). \tag{43}$$

Combining this with (42) produces an entropic DDoS detection formula at the repeater

$$S(\rho_{B,C}^{n\tau,n\tau}|\rho_{D}^{n\tau}) \ll S(\sigma_{B,C}^{(n+1)\tau,(n+1)\tau}|\sigma_{D}^{(n+1)\tau}). \tag{44}$$

The conditional entropies in (44) encode both the requests and the capacity, thereby providing a mechanism for early detection of a DDoS attack. In an attack, this entropy increases dramatically at the repeater, signifying a drastic reduction in capacity.

It is important to note that in this attack scenario, the capacity for service may still be available, in that (39) is still satisfied. What is of importance to the detection system (for early detection) is that there has been a drastic change in capacity, as expressed through (44). Hence, we use (44) to detect the attack. This line of reasoning follows from the classical system, and thus, in this work we have provided a quantum DDoS detection system that is analogous to the classical case (11).

5. Discussion

To address implementation, a large number of low-level design features need to be addressed. One issue is for the node to compute the quantum entropy using some subset of the network traffic. Various quantum algorithms for calculating entropy have been developed [25–27], and future work would involve integrating these methods for a refined detection system.

In classical networks, after detecting a DDoS attack, it is common to employ a mitigation method [8]. As a result, the service capacity is unaffected, leaving service available to legitimate traffic. Future work on our quantum DDoS case could involve developing mitigation methods based on quantum resources.

We illustrate this with a simple method that could be used to develop a more sophisticated strategy. Suppose we have attack Bell states $|\beta_{00}\rangle_{A_1B_1}^{(n+1)\tau,(n+1)\tau}$ and $|\beta_{00}\rangle_{A_2B_2}^{(n+1)\tau,(n+1)\tau}$. The labels A_1 and A_2 refer to the qubits at the respective attack nodes, and labels B_1 and B_2 are the qubits that reach the repeater at $t = (n+1)\tau$ (see Appendix A). Under normal conditions, the repeater would perform a projection with the Bell pairs generated at the repeater.

Given that the attack has been detected, the repeater performs a joint projective measurement on the attack qubits themselves, B_1 and B_2 at $t = (n+1)\tau$. We can write this as

$$|\beta_{00}\rangle_{A_1B_1}^{(n+1)\tau,(n+1)\tau} \otimes |\beta_{00}\rangle_{A_2B_2}^{(n+1)\tau,(n+1)\tau} \tag{45}$$

$$\begin{aligned} &= \tfrac{1}{2}(|\beta_{00}\rangle_{A_1A_2}^{(n+1)\tau,(n+1)\tau} \otimes |\beta_{00}\rangle_{B_1B_2}^{(n+1)\tau,(n+1)\tau}) \\ &+ |\beta_{01}\rangle_{A_1A_2}^{(n+1)\tau,(n+1)\tau} \otimes |\beta_{01}\rangle_{B_1B_2}^{(n+1)\tau,(n+1)\tau} \\ &+ |\beta_{10}\rangle_{A_1A_2}^{(n+1)\tau,(n+1)\tau} \otimes |\beta_{10}\rangle_{B_1B_2}^{(n+1)\tau,(n+1)\tau} \\ &+ |\beta_{11}\rangle_{A_1A_2}^{(n+1)\tau,(n+1)\tau} \otimes |\beta_{11}\rangle_{B_1B_2}^{(n+1)\tau,(n+1)\tau}. \end{aligned} \tag{46}$$

This joint measurement would swap the entanglement to qubits A_1 and A_2, which are at the attack nodes. Consequently, the Bell pairs generated at the repeater are not used, thereby leaving the repeater's capacity available for legitimate traffic.

In a large classical network, it is advantageous to devise a traceback method [19] so to identify the source of the attack. Both classical and quantum networks can be modelled as a directed acyclic graphs, where the upstream routers could be viewed as parent nodes and the downstream routes as children nodes. Hence, an interesting direction would be to employ quantum causal models [28] to provide a traceback model for DDoS attacks on a quantum network. The attacks could be formulated in terms of do-interventions and would allow the ability to apply a quantum do-calculus or a quantum causal discovery algorithm to carry out successful traceback for a DDoS attack on a quantum network.

There are a number of ways in which this research could be extended for more practical scenarios. One direction would be to investigate how this entropic detection system could be modified for near-term quantum networks, such as trusted relay networks.

Another research direction would be to explore how this work translates into repeater scenarios involving mixed states. Such cases are of practical importance for quantum networks given channel noise and the imperfections of local devices. One possibility for such modeling is to utilize Werner states for the entanglement swapping protocol and to derive analogous results.

Furthermore, one can consider cases involving multiple repeaters to generate entanglement over farther and farther distances. For such practical cases and where mixed states are employed, the entanglement decreases exponentially with the number of swappings. Finding potential DDoS attacks within such scenarios and designing the associated entropic DDoS detection systems is left for future work.

6. Conclusions

DDoS attacks are a central topic in classical network security and have been identified to be significant threat tp quantum networks. In this work, we designed a quantum analogue of a classical DDoS detection system and applied it in the context of a quantum network. We hope that our design contributes to extending the applicability of quantum information from the domain of data security to area of network security.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: The author thanks Winston Seah (Victoria University of Wellington) for helpful discussions.

Conflicts of Interest: The author declares no conflict of interest. This paper was prepared for informative purposes and is not a product of HSBC Bank Plc. or its affiliates. Neither HSBC Bank Plc. nor any of its affiliates make any explicit or implied representation or warranty, and none of them accept any liability in connection with this paper, including, but limited to, the completeness, accuracy, and reliability of information contained herein and the potential legal, compliance, tax, or accounting effects thereof. This document is not intended as investment research or investment advice; or a recommendation, offer, or solicitation for the purchase or sale of any security, financial instrument, financial product, or service; or to be used in any way for evaluating the merits of participating in any transaction.

Abbreviations

The following abbreviations are used in this manuscript:

DDoS Distributed Denial-of-Service

Appendix A

Derivation of equations in main text:

$$
\begin{aligned}
|\beta_{00}\rangle_{A,B}\,|\beta_{xy}\rangle_{C,D} &= \left(\frac{|00\rangle_{A,B}+|11\rangle_{A,B}}{\sqrt{2}}\right)\otimes\left(\frac{|0y\rangle_{C,D}+(-1)^x\,|1\bar{y}\rangle_{C,D}}{\sqrt{2}}\right) && \text{(A1)}\\
&= \frac{1}{2}(|00\rangle_{A,B}\,|0y\rangle_{C,D}+(-1)^x\,|00\rangle_{A,B}\,|1\bar{y}\rangle_{C,D} && \text{(A2)}\\
&+ |11\rangle_{A,B}\,|0y\rangle_{C,D}+(-1)^x\,|11\rangle_{A,B}\,|1\bar{y}\rangle_{C,D}) && \text{(A3)}\\
&= \frac{1}{2}(|0y\rangle_{A,D}\,|00\rangle_{B,C}+(-1)^x\,|0\bar{y}\rangle_{A,D}\,|01\rangle_{B,C} && \text{(A4)}\\
&+ |1y\rangle_{A,D}\,|10\rangle_{B,C}+(-1)^x\,|1\bar{y}\rangle_{A,D}\,|11\rangle_{B,C}) && \text{(A5)}\\
&= \frac{1}{4}\Big[2\,|0y\rangle_{A,D}\,|00\rangle_{B,C}+2(-1)^x\,|1\bar{y}\rangle_{A,D}\,|11\rangle_{B,C} && \text{(A6)}\\
&+ 2(-1)^x\,|0\bar{y}\rangle_{A,D}\,|01\rangle_{B,C}+2\,|1y\rangle_{A,D}\,|10\rangle_{B,C}\Big] && \text{(A7)}\\
&= \frac{1}{2}\Big[\frac{1}{2}(|0y\rangle_{A,D}\,|00\rangle_{B,C}+|0y\rangle_{A,D}\,|11\rangle_{B,C} && \text{(A8)}\\
&+ (-1)^x\,|1\bar{y}\rangle_{A,D}\,|00\rangle_{B,C}+(-1)^x\,|1\bar{y}\rangle_{A,D}\,|11\rangle_{B,C}) && \text{(A9)}\\
&+ \frac{1}{2}(|0y\rangle_{A,D}\,|00\rangle_{B,C}-|0y\rangle_{A,D}\,|11\rangle_{B,C} && \text{(A10)}\\
&+ (-1)^{\bar{x}}\,|1\bar{y}\rangle_{A,D}\,|00\rangle_{B,C}-(-1)^{\bar{x}}\,|1\bar{y}\rangle_{A,D}\,|11\rangle_{B,C}) && \text{(A11)}\\
&+ \frac{1}{2}((-1)^x\,|0\bar{y}\rangle_{A,D}\,|01\rangle_{B,C}+(-1)^x\,|0\bar{y}\rangle_{A,D}\,|10\rangle_{B,C} && \text{(A12)}\\
&+ |1y\rangle_{A,D}\,|01\rangle_{B,C}+|1y\rangle_{A,D}\,|10\rangle_{B,C}) && \text{(A13)}\\
&+ \frac{1}{2}((-1)^x\,|0\bar{y}\rangle_{A,D}\,|01\rangle_{B,C}-(-1)^x\,|0\bar{y}\rangle_{A,D}\,|10\rangle_{B,C} && \text{(A14)}\\
&- |1y\rangle_{A,D}\,|01\rangle_{B,C}+|1y\rangle_{A,D}\,|10\rangle_{B,C})\Big] && \text{(A15)}\\
&= \frac{1}{2}\Bigg[\left(\frac{|0y\rangle_{A,D}+(-1)^x\,|1\bar{y}\rangle_{A,D}}{\sqrt{2}}\right)\left(\frac{|00\rangle_{B,C}+|11\rangle_{B,C}}{\sqrt{2}}\right) && \text{(A16)}\\
&+ \left(\frac{|0y\rangle_{A,D}+(-1)^{\bar{x}}\,|1\bar{y}\rangle_{A,D}}{\sqrt{2}}\right)\left(\frac{|00\rangle_{B,C}-|11\rangle_{B,C}}{\sqrt{2}}\right) && \text{(A17)}\\
&+ \left(\frac{(-1)^x\,|0\bar{y}\rangle_{A,D}+(-1)^{2x}\,|1y\rangle_{A,D}}{\sqrt{2}}\right)\left(\frac{|01\rangle_{B,C}+|10\rangle_{B,C}}{\sqrt{2}}\right) && \text{(A18)}\\
&+ \left(\frac{(-1)^x\,|0\bar{y}\rangle_{A,D}+(-1)^{x+\bar{x}}\,|1y\rangle_{A,D}}{\sqrt{2}}\right)\left(\frac{|01\rangle_{B,C}-|10\rangle_{B,C}}{\sqrt{2}}\right)\Bigg] && \text{(A19)}\\
&= \frac{1}{2}(|\beta_{xy}\rangle_{A,D}\otimes|\beta_{00}\rangle_{B,C}+|\beta_{\bar{x}y}\rangle_{A,D}\otimes|\beta_{10}\rangle_{B,C}) && \text{(A20)}\\
&+ (-1)^x\,|\beta_{x\bar{y}}\rangle_{A,D}\otimes|\beta_{01}\rangle_{B,C}+(-1)^x\,|\beta_{\bar{x}\bar{y}}\rangle_{A,D}\otimes|\beta_{11}\rangle_{B,C}\,.
\end{aligned}
$$

We also applied the following operators to the respective states to obtain the outcome $|\beta_{xy}\rangle_{A,D}$:

$$
\begin{aligned}
(\mathbb{I}\otimes(-1)^x\hat{\sigma}_1)(-1)^x\left|\beta_{x\bar{y}}\right\rangle_{A,D} &= (\mathbb{I}\otimes(-1)^x\hat{\sigma}_1)\left(\frac{(-1)^x\left|0\bar{y}\right\rangle_{A,D}+\left|1y\right\rangle_{A,D}}{\sqrt{2}}\right) && \text{(A21)}\\
&= \frac{1}{\sqrt{2}}(\left|0\right\rangle_A\otimes(-1)^x(-1)^x\hat{\sigma}_1\left|\bar{y}\right\rangle_D) && \text{(A22)}\\
&+ \frac{1}{\sqrt{2}}(\left|1\right\rangle_A\otimes(-1)^x\hat{\sigma}_1\left|y\right\rangle_D) && \text{(A23)}\\
&= \frac{1}{\sqrt{2}}(\left|0\right\rangle_A\otimes(-1)^{x+x}\left|y\right\rangle_D) && \text{(A24)}\\
&+ \frac{1}{\sqrt{2}}(\left|1\right\rangle_A\otimes(-1)^x\left|\bar{y}\right\rangle_D) && \text{(A25)}\\
&= \frac{1}{\sqrt{2}}(\left|0\right\rangle_A\otimes\left|y\right\rangle_D) && \text{(A26)}\\
&+ \frac{1}{\sqrt{2}}((-1)^x\left|1\right\rangle_A\otimes\left|\bar{y}\right\rangle_D) && \text{(A27)}\\
&= \left(\frac{\left|0y\right\rangle_{A,D}+(-1)^x\left|1\bar{y}\right\rangle_{A,D}}{\sqrt{2}}\right) && \text{(A28)}\\
&= \left|\beta_{xy}\right\rangle_{A,D} && \text{(A29)}
\end{aligned}
$$

$$
\begin{aligned}
(\mathbb{I}\otimes(-1)^y\hat{\sigma}_3)\left|\beta_{\bar{x}y}\right\rangle_{A,D} &= (\mathbb{I}\otimes(-1)^y\hat{\sigma}_3)\left(\frac{\left|0y\right\rangle_{A,D}+(-1)^{\bar{x}}\left|1\bar{y}\right\rangle_{A,D}}{\sqrt{2}}\right) && \text{(A30)}\\
&= \frac{1}{\sqrt{2}}(\left|0\right\rangle_A\otimes(-1)^y\hat{\sigma}_3\left|y\right\rangle_D) && \text{(A31)}\\
&+ \frac{1}{\sqrt{2}}(\left|1\right\rangle_A\otimes(-1)^y(-1)^{\bar{x}}\hat{\sigma}_3\left|\bar{y}\right\rangle_D) && \text{(A32)}\\
&= \frac{1}{\sqrt{2}}(\left|0\right\rangle_A\otimes(-1)^y(-1)^y\left|y\right\rangle_D) && \text{(A33)}\\
&+ \frac{1}{\sqrt{2}}(\left|1\right\rangle_A\otimes(-1)^y(-1)^{\bar{x}}(-1)^{\bar{y}}\left|\bar{y}\right\rangle_D) && \text{(A34)}\\
&= \frac{1}{\sqrt{2}}(\left|0\right\rangle_A\otimes(-1)^{y+y}\left|y\right\rangle_D) && \text{(A35)}\\
&+ \frac{1}{\sqrt{2}}(\left|1\right\rangle_A\otimes(-1)^{y+\bar{y}}(-1)^{\bar{x}}\left|\bar{y}\right\rangle_D) && \text{(A36)}\\
&= \frac{1}{\sqrt{2}}(\left|0\right\rangle_A\otimes\left|y\right\rangle_D) && \text{(A37)}\\
&+ \frac{1}{\sqrt{2}}(\left|1\right\rangle_A\otimes(-1)(-1)^{\bar{x}}\left|\bar{y}\right\rangle_D) && \text{(A38)}\\
&= \frac{1}{\sqrt{2}}(\left|0\right\rangle_A\otimes\left|y\right\rangle_D) && \text{(A39)}\\
&+ \frac{1}{\sqrt{2}}(\left|1\right\rangle_A\otimes(-1)^x\left|\bar{y}\right\rangle_D) && \text{(A40)}\\
&= \left(\frac{\left|0y\right\rangle_{A,D}+(-1)^x\left|1\bar{y}\right\rangle_{A,D}}{\sqrt{2}}\right) && \text{(A41)}\\
&= \left|\beta_{xy}\right\rangle_{A,D} && \text{(A42)}
\end{aligned}
$$

$$
\begin{aligned}
(\mathbb{I} \otimes (-1)^{x+y}\hat{\sigma}_3\hat{\sigma}_1)(-1)^x \left|\beta_{\bar{x}\bar{y}}\right\rangle_{A,D} &= (\mathbb{I} \otimes (-1)^{x+y}\hat{\sigma}_3\hat{\sigma}_1)\left(\frac{(-1)^x \left|0\bar{y}\right\rangle_{A,D} - \left|1y\right\rangle_{A,D}}{\sqrt{2}}\right) && \text{(A43)}\\
&= \frac{1}{\sqrt{2}}(\left|0\right\rangle_A \otimes (-1)^x(-1)^{x+y}\hat{\sigma}_3\hat{\sigma}_1 \left|\bar{y}\right\rangle_D) && \text{(A44)}\\
&- \left|1\right\rangle_A \otimes (-1)^{x+y}\hat{\sigma}_3\hat{\sigma}_1 \left|y\right\rangle_D) && \text{(A45)}\\
&= \frac{1}{\sqrt{2}}(\left|0\right\rangle_A \otimes (-1)^x(-1)^{x+y}(-1)^y \left|y\right\rangle_D) && \text{(A46)}\\
&- \left|1\right\rangle_A \otimes (-1)^{x+y}(-1)^{\bar{y}} \left|\bar{y}\right\rangle_D) && \text{(A47)}\\
&= \frac{1}{\sqrt{2}}(\left|0\right\rangle_A \otimes (-1)^{x+y+x+y} \left|y\right\rangle_D) && \text{(A48)}\\
&- \left|1\right\rangle_A \otimes (-1)^{x+y+\bar{y}} \left|\bar{y}\right\rangle_D) && \text{(A49)}\\
&= \frac{1}{\sqrt{2}}(\left|0\right\rangle_A \otimes \left|y\right\rangle_D) && \text{(A50)}\\
&- \left|1\right\rangle_A \otimes -(-1)^x \left|\bar{y}\right\rangle_D) && \text{(A51)}\\
&= \frac{1}{\sqrt{2}}(\left|0\right\rangle_A \otimes \left|y\right\rangle_D) && \text{(A52)}\\
&+ (-1)^x \left|1\right\rangle_A \otimes \left|\bar{y}\right\rangle_D) && \text{(A53)}\\
&= \left(\frac{\left|0y\right\rangle_{A,D} + (-1)^x \left|1\bar{y}\right\rangle_{A,D}}{\sqrt{2}}\right) && \text{(A54)}\\
&= \left|\beta_{xy}\right\rangle_{A,D} && \text{(A55)}
\end{aligned}
$$

References

1. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2010.
2. Arute, F.; Arya, K.; Babbush, R.; Bacon, D.; Bardin, J.C.; Barends, R.; Biswas, R.; Boixo, S.; Brandao, F.G.S.L.; Buell, D.A.; et al. Quantum supremacy using a programmable superconducting processor. *Nature* **2019**, *574*, 505–510. [CrossRef] [PubMed]
3. Wu, Y.; Bao, W.S.; Cao, S.; Chen, F.; Chen, M.C.; Chen, X. Strong quantum computational advantage using a superconducting quantum processor. *Phys. Rev. Lett.* **2021**, *127*, 180501. [CrossRef] [PubMed]
4. Wehner, S.; Elkouss, D.; Hanson, R. Quantum internet: A vision for the road ahead. *Science* **2018**, *362*, 6412. [CrossRef] [PubMed]
5. Bennett, C.H.; Brassard, G.; Crepeau, C.; Jozsa, R.; Peres, A.; Wootters, W.K. Teleporting an unknown quantum state via dual classical and Einstein–Podolsky-Rosen channels. *Phys. Rev. Lett.* **1993**, *70*, 1895–1899. [CrossRef]
6. Ren, J.G.; Xu, P.; Yong, H.L.; Zhang, L.; Liao, S.K.; Yin, J.; Liu, W.; Cai, W.; Yang, M.; Li, L.; et al. Ground-to-satellite quantum teleportation. *Nature* **2017**, *549*, 70–73. [CrossRef]
7. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]
8. Osterweil, E.; Stavrou, A.; Zhang, L. 21 years of distributed denial-of-service: A call to action. *Computer* **2020**, *53*, 94–99. [CrossRef]
9. Mahjabin, T.; Xiao, Y.; Sun, G.; Jiang, W. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1550147717741463. [CrossRef]
10. Satoh, T.; Nagayama, S.; Suzuki, S.; Matsuo, T.; Hajdušek, M.; Meter, R.V. Attacking the quantum internet. *IEEE Trans. Quantum Eng.* **2021**, *2*, 1–17. [CrossRef]
11. Clark, R.; Bartlett, S.; Bremner, M.; Lam, P.K.; Ralph, T. *The Impact of Quantum Technologies on Secure Communications*; Australian Strategic Policy Institute: Canberra, Australia, 2021; pp. 1–47.
12. Price, A.B.; Rarity, J.G.; Erven, C. A quantum key distribution protocol for rapid denial of service detection. *EPJ Quantum Technol.* **2020**, *7*, 8. [CrossRef]
13. Lesk, M. The new front line: Estonia under cyberassault. *IEEE Secur. Priv.* **2007**, *5*, 76–79. [CrossRef]
14. Mansfield-Devine, S. The growth and evolution of DDoS. *Netw. Secur.* **2015**, 13–20. [CrossRef]
15. Kathirkamanathan, N.; Thevarasa, B.; Mahadevan, G.; Skandhakumar, N.; Kuruwitaarachchi, N. Prevention of DDoS attacks targeting financial services using supervised machine learning and stacked LSTM. In Proceedings of the IEEE 7th International Conference for Convergence in Technology, Mumbai, India, 7–9 April 2022; pp. 1–5.
16. Financial Markets Authority. *Market Operator Obligations Targeted Review–NZX*; Financial Markets Authority New Zealand: Wellington, New Zealand, 2021; pp. 1–19.

17. Koay, A. Detecting High and Low Intensity Distributed Denial of Service (DDoS) Attacks. Ph.D. Thesis, Victoria University of Wellington, Wellington, New Zealand, 2019.
18. Özçelik, İ.; Brooks, R.R. Deceiving entropy based DoS detection. *Comput. Secur.* **2015**, *48*, 234–245. [CrossRef]
19. Yu, S.; Zhou, W.; Doss, R.; Jia, W. Traceback of DDoS attacks using entropy variations. *IEEE Trans. Parallel Distrib. Syst.* **2010**, *22*, 412–425. [CrossRef]
20. Pant, M.; Krovi, H.; Towsley, D.; Tassiulas, L.; Jiang, L.; Basu, P.; Englund, D.; Guha, S. Routing entanglement in the quantum internet. *NPJ Quantum Inf.* **2019**, *5*, 1–9. [CrossRef]
21. Lee, Y.; Bersin, E.; Dahlberg, A.; Wehner, S.; Englund, D. A quantum router architecture for high-fidelity entanglement flows in quantum networks. *NPJ Quantum Inf.* **2022**, *8*, 1–8. [CrossRef]
22. Dai, E.; Huang, D.; Zhang, L. Low-rate denial-of-service attack detection: defense strategy based on spectral estimation for CV-QKD. *Photonics* **2022**, *9*, 365. [CrossRef]
23. Rabbie, J.; Chakraborty, K.; Avis, G.; Wehner, S. Designing quantum networks using preexisting infrastructure. *NPJ Quantum Inf.* **2022**, *8*, 1–12. [CrossRef]
24. Witten, E. A mini-introduction to information theory. *La Riv. del Nuovo C.* **2020**, *43*, 187–227. [CrossRef]
25. Acharya, J.; Issa, I.; Shende, N.V.; Wagner, A.B. Measuring quantum entropy. In Proceedings of the 2019 IEEE International Symposium on Information Theory, Paris, France, 7–12 July 2019; pp. 3012–3016.
26. Wang, Y.; Zhao, B.; Wang, X. Quantum algorithms for estimating quantum entropies. *arXiv* **2022**, arXiv:2203.02386.
27. Wang, Q.; Guan, J.; Liu, J.; Zhang, Z.; Ying, M. New quantum algorithms for computing quantum entropies and distances. *arXiv* **2022**, arXiv:2203.13522.
28. Barrett, J.; Lorenz, R.; Oreshkov, O. Cyclic quantum causal models. *Nat. Commun.* **2021**, *12*, 1–15. [CrossRef] [PubMed]