Strategic Interaction Over Pump Power for Fidelity in Spontaneous Parametric Down-Conversion

Hilal Sultan Duranoglu Tunc*, Leonardo Badia*†, Riccardo Bassoli*, Frank H. P. Fitzek*
* Deutsche Telekom Chair of Communication Networks, TU Dresden, Germany
† Dept. of Information Engineering, University of Padova, Italy
{hilal_sultan.duranoglu_tunc,riccardo.bassoli,frank.fitzek}@tu-dresden.de, badia@dei.unipd.it

***Abstract*—We consider a scenario of spontaneous parametric down-conversion to generate entangled states that are used for quantum communications. Such a mechanism is vulnerable to attacks caused by an adversary that may inject power to the nonlinear crystal to drive the operating point away from maximum fidelity. We devise a low-cost strategic mechanism to counteract this attack, which corresponds to lowering the injected power anticipating the attack. If the attacker is also rational, this leads to a strategic interaction that can be studied with game theory. We show how the strategic response of the transmitter can mitigate the extent of the attack when it is not too strong.**

***Index Terms*—SPDC, fidelity, pump power, pair generation probability, game theory.**

I. Introduction

Many quantum information processing techniques, such as quantum key distribution [1], quantum teleportation [2], entanglement swapping [3], quantum relays [4], quantum memory and repeaters [5], and the general exchange of confidential information [6], depend on entanglement as a valuable resource. In nonlinear crystals, spontaneous parametric down-conversion (SPDC), is the most common method used in optics to create entangled states [7]. SPDC sources provide a number of benefits, including the ability to be integrated into optical circuits and being small, resilient, affordable, and room temperature operating systems.

If we briefly summarize the process dynamics of SPDC, when a pump photon enters the nonlinear crystal, it can spontaneously split into two photons (signal and idler) due to the crystal's nonlinear properties. These photons are generated in such a way that both energy and momentum are conserved. The spatial and spectral characteristics of the emitted photons are dictated by the phase-matching conditions in the crystal. In summary, SPDC is a fundamental process in quantum optics, enabling the creation of entangled photon pairs essential for numerous applications in quantum information science and fundamental physics research [8].

The fidelity of the entangled states generated by the SPDC source is a crucial characteristic for all the above stated applications, since it has a significant impact on the protocol's performance and success rate. The entanglement fidelity of photons produced through SPDC is influenced by several factors such as the choice of crystal, pump laser properties, mode matching, filtering, and multiphoton events. Balancing pump power to maximize pair production without increasing multipair events is crucial for maintaining high fidelity. Increasing the pump power enhances the rate of SPDC, resulting in a higher number of photon pairs. This is beneficial for applications requiring high photon flux, such as quantum communication and quantum computing. Higher pump power also increases the probability of multi-pair events. When multiple pairs are generated simultaneously, distinguishing between the pairs becomes challenging, introducing noise and reducing the entanglement fidelity. Multi-pair events can lead to false coincidences and degrade the purity of the entangled state. For these reasons, finding and applying the optimal power is of great importance for SPDC. If the pump power is too low, it causes insufficient photon pair production, leading to low signal rates and inefficient quantum information processing. If the pump power is too high, it causes increased multi pair production, degrading the fidelity of the entangled states [9].

Two particles that have never interacted or exchanged any history can become entangled through the use of a quantum communication technique called entanglement swapping. By using two particles that are entangled with one of the two target particles, this is accomplished. For quantum communication networks to operate at a greater range, quantum repeaters—which are critical to the process—are required [10]. In our study, we assume that the entanglement photons generated by SPDC are distributed in the network by entanglement swapping.

For this type of network, changing the SPDC pump power causes the generation of entangled states to work off the optimal range [11], which in turn makes this technology vulnerable to external attackers that would like this to happen. In particular, a malicious advrersary can intentionally increase the pump power so as to decrease fidelity.

However, in this paper we are interested in countering this kind of threat. We assume that the transmitter is aware of this risk and enacts a countermeasure through game theory [12]. The resulting scenario corresponds to a strategic interaction of two players, the legitimate transmitter and the adversary, that regulate the pump power in opposite directions, within an adversarial setup [13]. The possible countermeasure enacted by the transmitter to respond to the attacker is to reduce the pump power, anticipating that the attacker will increase it. We will show how, in a certain range of realistic scenarios, such a countermeasure is effective in decreasing the impact of the attacker.

Formally, this results in a zero-sum static game of complete information [14]. We derive the formal conditions where the solution is known to be found in a mixed strategy (therefore implying that the attacker is not always attacking, but does so with a certain probability), which corresponds to a benefit for the network management. This procedure is actually successful only if the attacking strategy is not strictly dominant, which happens when the extra injected pump power is very high. If the power applied by the attacker is high, it becomes easier to detect the attack. In such a scenario, the connection with the affected node or link can be severed, then

- rerouting can be implemented ;
- more advanced hardware can be used to tolerate this situation (e.g., using single-photon sources instead of weak coherent sources);
- extra optical components can be added (such as incorporating spectral or spatial filters) ;
- a new protocol can be implemented (e.g., applying device-independent protocols) .

When the attack strategy is strictly dominant, this actually leads to a pure strategy Nash equilibrium (NE) that does not impede the attacker from disrupting the communication significantly lowering fidelity.

However, one can argue that this situation corresponds to the general scenario of an unbeatable adversary (as present in every security problem, when the attacker is all-powerful [15]), and is likely to be unrealistic in that such an attacker would be easily detected, whereas a malicious adversary prefers to act inconspicuously. As such, in a more reasonable scenario where the injected power is limited, the resulting outcome would correspond to a mixed strategy equilibrium that can be found in closed form [16]. Under this condition, the countermeasure applied by the transmitter can be effective in reducing the damage caused of the adversary.

Although SPDC and game theory have been considered separately in previous studies, to our knowledge, there is not many papers studying SPDC and game theory together. By merging SPDC with game theory, the study provides a new theoretical framework that can be used for future research and practical applications.

The rest of this paper is organized as follows. In Section II, we review the quantum technology that is the focus of our analysis. Section III presents the game theoretic analysis. In Section IV, we show some numerical results, and we finally conclude in Section V.

II. Methodology

In quantum optics, the powerful and popular SPDC approach allows for the creation of entangled photons, which are essential for many quantum technologies. Fig. 1 shows a schematic representation of the SPDC experimental setup that generates entangled photons.

In our analysis, we consider that that we are using a pulsed pumped collinear quasi-degenerate down-conversion type 1 (or 2) non-linear crystals. We assume that the used filter has a

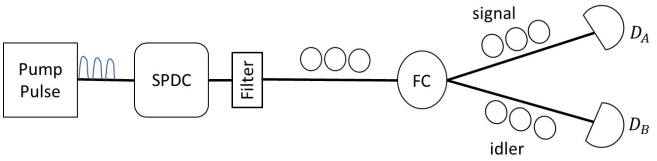

Fig. 1. Schematic setup of SPDC

bandwidth greater than the bandwidth of the pump beam's. The filter separates the two photons, which are then coupled into the same optical fiber. In Fig. 1, FC represents the fiber-coupler, which splits the photon pair into signal and idler. At the end of each channel, photo diodes, called D_{A} and D_{B}, respectively, are present. The transmission for channels A and B is represented as $X_{\mathrm{A,B}}$ and calculated as

$$X_{\mathrm{A,B}} = R_{\mathrm{A,B}} T_{\mathrm{A,B}} \eta_{\mathrm{A,B}} \tag{1}$$

The output ratio of the fiber coupler is denoted by $R_{\mathrm{A,B}}$ in the transmission equation, the losses are denoted by $T_{\mathrm{A,B}}$, and the quantum efficiency of the detectors for channels A and B is represented by $\eta_{\mathrm{A,B}}$.

In the $D_{\mathrm{A,B}}$ detector inside the gate time, the probability of receiving one count is

$$P_{\mathrm{A,B}} = 2 p_0 I_1 X_{\mathrm{A,B}} K_{\mathrm{T}} + P_{N_{\mathrm{A,B}}} \tag{2}$$

where the probability of the dark count on detector $D_{\mathrm{A,B}}$ is $P_{N_{\mathrm{A,B}}}$, the gate duration is T, and the peak spectral probability density is p_0.

The probability of true coincidences arising from the idler photon and signal is

$$P_{\mathrm{TC}} = 2 p_0 I_2 X_{\mathrm{A}} X_{\mathrm{B}} K_{\mathrm{T}} \,. \tag{3}$$

Then, this further formula is used to determine the probability of accidental events:

$$P_{\mathrm{AC}} = 4 (p_0 I_1)^2 X_{\mathrm{A}} X_{\mathrm{B}} (K_{\mathrm{T}})^2 \tag{4}$$

The symbol for the likelihood of coincidences associated with noise is $P_{N_{\mathrm{AB}}}$, where

$$P_{N_{\mathrm{AB}}} = (P_{\mathrm{A}} - P_{N_{\mathrm{A}}}) P_{N_{\mathrm{B}}} + (P_{\mathrm{B}} - P_{N_{\mathrm{B}}}) P_{N_{\mathrm{A}}} + P_{N_{\mathrm{A}}} P_{N_{\mathrm{B}}} \,. \tag{5}$$

The probability of coincidence (P_{C}) between the counts on detectors D_{A} and D_{B} can therefore be computed as

$$P_{\mathrm{C}} = P_{\mathrm{TC}} + P_{\mathrm{AC}} + P_{N_{\mathrm{AB}}} \tag{6}$$

With the analysis of coincidence rates, we obtained the formula of visibility. In [17], system fidelity is assumped as visibility.

$$F_{\mathrm{sys}} = \frac{1}{1 + 2 \frac{P_{\mathrm{AC}} + P_{N_{\mathrm{AB}}}}{P_{\mathrm{TC}}}} \,. \tag{7}$$

The graph in Fig. 2 is what we get when we use (7) to investigate the link between fidelity and pair generation probability for every quantum node.

The relationship between accidental coincidences and the square of pair creation probability can be understood from

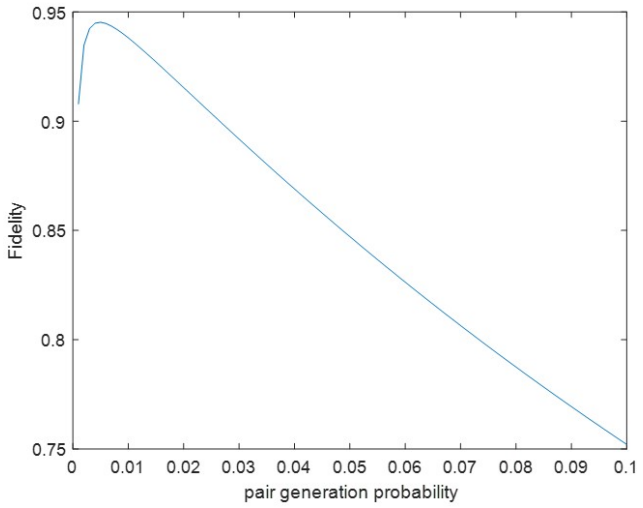

Fig. 2. Fidelity vs Pair generation probability

(3). As the probability of pair production rises, this results in a decrease in fidelity. It is clear from Fig. 2 that we gain lesser fidelity for increasing pair generation probability. The SPDC pump peak power is shown to be directly related to the photon pair probability per pulse in [18].

III. Game Theoretic model

We consider a scenario where a malicious attacker is able to increase the pump power, so as to decrease fidelity. However, the transmitter is also able to anticipate this move and may think of decreasing the pump power to contrast this attack [13].

This can be formalized by including the attacker A and the transmitter T as players in a static game of complete information, implying that both players are aware of each other's options but make their decision without telling each other what they will actually do, which makes sense in this setup that involves security [19]–[21].

The game is ultimately modeled as a zero-sum [14], whose normal form $\mathcal{G} = (\mathcal{P}, \mathcal{A}, \mathcal{U})$ includes the set of players $\mathcal{P} = \{\mathrm{A}, \mathrm{T}\}$, the set $\mathcal{A} = \{\mathcal{A}_\mathrm{A}, \mathcal{A}_\mathrm{T}\}$ of actions available to the players, and the resulting utilities of the players in set $\mathcal{U}$. For the sake of simplicity, the actions in set $\mathcal{A}_\mathrm{A}$ available to the attacker are assumed to increase the pump power by a certain amount Δ_P or do nothing, denoted as P and N, respectively. Conversely, the actions available to the transmitter are to use the pump power that is supposedly optimal in the absence of an attacker, P_opt, or to decrease it by a certain amount Δ_d so that the power injected by the transmitter is $P_\mathrm{opt} - \Delta_\mathrm{d}$. These two actions are referred to as N and D, respectively. Notice that, if T decides to decrease the pump power and the attacker increases it as well, the resulting injected value will be $P_\mathrm{opt} - \Delta_\mathrm{d} + \Delta_\mathrm{p}$.

Finally, the utilities are evaluated as the resulting system fidelity from (7). Since the game is zero-sum, the attacker acts as a minimizer of this utility (i.e., it tries to minimize the fidelity), whereas the transmitter is obviously a maximizer. For a zero-sum game, there is no need to display both utility values in the normal form. According to the common game theoretic convention, we only consider the utility of the maximizer as the fidelity F from (7), whereas the objective value for the minimizer is numerically computed as $-F$.

TABLE I
Normal form of the zero-sum game

		Attacker A	
		N	P
Transmitter T	N	F_max	F_sub
	D	F_att	F_def

Combining all the possible outcomes and the zero-sum convention, the normal form of game $\mathcal{G}$ results as shown in Table I. When neither of the players changes action from the regular power pump injection (i.e., their joint strategy corresponds to N,N), the system fidelity F_opt is the one maximizing (7). If the attacker increases the pump power, the fidelity of the system under attack becomes F_att. If the transmitter contextually decreases the pump power as well, the fidelity becomes F_def. Finally, if the transmitter unnecessarily decreases the injected power, but the attacker was actually not increasing the pump power, the sub-optimal fidelity of the system is denoted by F_sub. Notice that $F_\mathrm{att} < F_\mathrm{def}$, $F_\mathrm{opt} > F_\mathrm{att}$, and $F_\mathrm{opt} > F_\mathrm{sub}$. Depending on what further relationship is established, the game obtains different NEs [22].

In particular, if $F_\mathrm{def} < F_\mathrm{sub}$, implying that the transmitter cannot successfully defend from an attack, not even decreasing the pump power, then playing P is a *strictly dominant strategy* for player A. This means that the attacker is guaranteed to attack and, while the transmitter can anticipate this, the only countermeasure is to decrease the pump power, and the NE of the game will be (D,P). The interaction results in a fidelity value F_def that is lower than F_opt. However, one can argue that such a situation only happens if Δ_P is very high, which corresponds to the typical security scenario where there is no countermeasure available against a very powerful attacker [15]. Beyond being theoretically impossible to defeat, this situation will likely correspond to a detectable attack that goes against the principle that the adversary prefers to go unnoticed [23].

Conversely, when the power that can be injected by an attacker is relatively limited, the game does not admit a pure strategy NE and the scenario becomes a more interesting zero-sum game (akin to rock-paper-scissors or similar games) where the solution can only be found in mixed strategies. To find the NE, one can simply leverage the *indifference theorem* [16] that gives a probabilistic interpretation of either side attacking/defending, or not.

The numerical solution is found in an intermediate value between all the entries in Table I, but can correspond to an

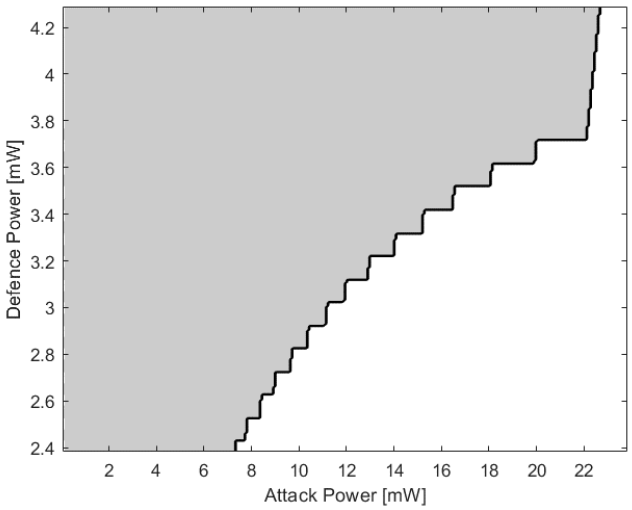

Fig. 3. Diagram of the meaningful NEs. The dark area corresponds to the values where a mixed NE exists.

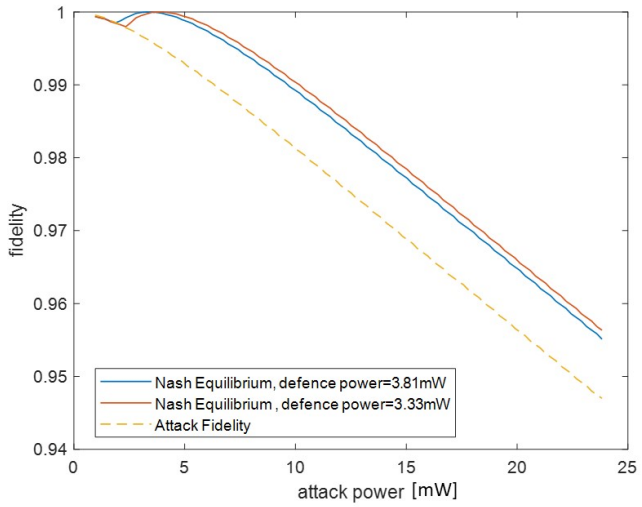

Fig. 4. Fidelity at NE obtained under strategic defense.

effective defense mechanism for the transmitter, as will be argued in the next section.

IV. Results

In this study, it is assumed that the used SPDC is a pulsed pumped collinear quasi-degenerate down conversion in type I (or II) nonlinear crystals. Signal and idler photons are filtered by the same filter which has a bandwidth much larger than that of the pump beam. By using a fiber coupler the signal and idler photons are splitted and by using single photon avalanche photodiodes they are detected. Finally the fidelity is calculated via (7).

We present some numerical values related to the problem at hand, to better capture the physical meaning and quantify the numerical values of the parameter. Fig. 3 shows the different regions of the NEs, and the dark area corresponds to the more interesting case where the equilibrium is found in mixed strategies. It is also visible that, as the attack power grows, it becomes increasingly difficult to counteract this attack, and beyond a certain point the attack power is so strong that this kind of power injection becomes impossible to mitigate. This result can serve as a practical guideline to establish when the attacker can be countered, and what kind of power reduction is necessary to accomplish this [13].

It is also worth mentioning that the best operating region would be the one close to the border between the regions, since this corresponds to an equilibrium point that is not too far from the best fidelity value F_{opt}. If the defence power is too high compared to the attack power, it means that the transmitter can achieve a successful damage reduction by decreasing the pump power, but the strategic outcome of the game will sometimes result in (D,N). This outcome implies that the transmitter is reducing power when it is not necessary, as the attacker is not injecting, and therefore the achieved value is F_{sub}.

Fig. 4 shows the results of the mixed strategy NE that is obtained for different values of the attack power Δ_{P} and defensive power reduction Δ_{d}. These are compared with the reference scenario where no strategic countermeasure is adopted and the adversary is just performing an undisturbed attack to the system.

This figure also confirms that for high values of Δ_{P} the attacker cannot be effectively counteracted, the only impact of the defensive power reduction being a constant positive offset in the achieved fidelity. However, if the attack power is moderate, a consistent damage reduction can be obtained by simply decreasing the injected power in a strategic way, restoring the fidelity of SPDC to high levels.

To sum up, these numerical results can serve as practical guidelines to identify the options for a strategic defense against an attacker that injects extra power with the objective to decrease the system fidelity. They can both identify when it makes sense to enact a power reduction mechanism, and how strong, and also what resulting improvement it can bring over a lack of reaction to the attack.

V. Conclusions and Future Directions

We presented a game theoretic analysis of an adversarial interaction between a quantum transmitter and an attacker, over the pump power in SPDC, contending for the achieved fidelity [7], [9].

If the transmitter does not take any countermeasure, an attacker can reduce the system fidelity by injecting extra power. However, a simple contrasting action would be to decrease the injected power in return, especially when this results in a mixed strategy NE, whose value can be compensating the attack to a variable extent. This scenario was analyzed through game theory, as a static game of complete information, and we computed the NE discussing whether it is in pure or mixed strategies [19].

There are a number of possible extensions to this kind of study. First of all, the choice of a static game of complete information is made, since this is possibly the simplest kind of game theoretic scenario that can convey meaningful results, and it makes sense in an adversarial game. However, if the transmitter is able to anticipate and prevent the presence of the attacker in the game beforehand, or anyways to take actions in response to the attacker, a dynamic game setup could also be envisioned [24].

Moreover, the nature of the attacker can be uncertain, which would extend to the case of incomplete information, or Bayesian games [25]. This would lead to a more general scenario where the values of the injected power, but possibly also the model itself of the interaction, are blurred. Also in this context, game theory can illuminate the interactions between strategic agents and enhance the security of quantum communication systems.

ACKNOWLEDGMENT

The authors acknowledge the financial support by the German Research Foundation (DFG, Deutsche Forschungsgemeinschaft) as part of Germany's Excellence Strategy – EXC 2050/1 – Project ID 390696704 – Cluster of Excellence 'Centre for Tactile Internet with Human-in-the-Loop' (CeTI) of Technische Universität Dresden , Federal Ministry of Education and Research of Germany in the project Q-TREX with project identification number of 16KISR027 .

REFERENCES

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, p. 145, 2002.

[2] Y.-H. Kim, S. P. Kulik, and Y. Shih, "Quantum teleportation of a polarization state with a complete Bell state measurement," *Phys. Rev. Lett.*, vol. 86, no. 7, p. 1370, 2001.

[3] M. Halder, A. Beveratos, N. Gisin, V. Scarani, C. Simon, and H. Zbinden, "Entangling independent photons by time measurement," *Nat. Phys.*, vol. 3, no. 10, pp. 692–695, 2007.

[4] D. Collins, N. Gisin, and H. De Riedmatten, "Quantum relays for long distance quantum cryptography," *J. Mod. Opt.*, vol. 52, no. 5, pp. 735–753, 2005.

[5] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, no. 26, p. 5932, 1998.

[6] L. Badia, H. S. Duranoglu Tunc, A. C. Aka, R. Bassoli, and F. H. Fitzek, "Strategic interaction over age of information on a quantum wiretap channel," in *Proc. European Wireless Conf.*, 2023, pp. 388–394.

[7] Y. Shih, A. Sergienko, M. H. Rubin, T. Kiess, and C. Alley, "Two-photon entanglement in type-II parametric down-conversion," *Phys. Rev. A*, vol. 50, no. 1, p. 23, 1994.

[8] L. Caspani, C. Xiong, B. J. Eggleton, D. Bajoni, M. Liscidini, M. Galli, R. Morandotti, and D. J. Moss, "Integrated sources of photon quantum states based on nonlinear optics," *Light: Science & Applications*, vol. 6, no. 11, pp. e17 100–e17 100, 2017.

[9] G. Kulkarni, J. Rioux, B. Braverman, M. V. Chekhova, and R. W. Boyd, "Classical model of spontaneous parametric down-conversion," *Phys. Rev. Res.*, vol. 4, no. 3, p. 033098, 2022.

[10] T. Satoh, S. Nagayama, S. Suzuki, T. Matsuo, M. Hajdušek, and R. Van Meter, "Attacking the quantum internet," *IEEE Trans. Quantum Engin.*, vol. 2, pp. 1–17, 2021.

[11] R. Hošák, I. Straka, A. Predojević, R. Filip, and M. Ježek, "Effect of source statistics on utilizing photon entanglement in quantum key distribution," *Phys. Rev. A*, vol. 103, no. 4, p. 042411, 2021.

[12] L. Badia, "Age of information from two strategic sources analyzed via game theory," in *Proc. IEEE Int. Wkshp Comput. Aided Model. Design Commun. Links Netw. (CAMAD)*, 2021.

[13] V. Bonagura, S. Panzieri, F. Pascucci, and L. Badia, "A game of age of incorrect information against an adversary injecting false data," in *Proc. IEEE Int. Conf. Cyber Security Resil. (CSR)*, 2023, pp. 347–352.

[14] M. Scalabrin, V. Vadori, A. V. Guglielmi, and L. Badia, "A zero-sum jamming game with incomplete position information in wireless scenarios," in *Proc. European Wireless Conf.* VDE, 2015.

[15] C. Portmann and R. Renner, "Security in quantum cryptography," *Rev. Mod. Phys.*, vol. 94, no. 2, p. 025008, 2022.

[16] C. K. Sheemar, L. Badia, and S. Tomasin, "Game-theoretic mode scheduling for dynamic TDD in 5G systems," *IEEE Commun. Lett.*, vol. 25, no. 7, pp. 2425–2429, 2021.

[17] J.-L. Smirr, S. Guilbaud, J. Ghalbouni, R. Frey, E. Diamanti, R. Alléaume, and I. Zaquine, "Simple performance evaluation of pulsed spontaneous parametric down-conversion sources for quantum communications," *Opt. Exp.*, vol. 19, no. 2, pp. 616–627, 2011.

[18] Y. M. Sua, H. Fan, A. Shahverdi, J.-Y. Chen, and Y.-P. Huang, "Direct generation and detection of quantum correlated photons with 3.2 um wavelength spacing," *Scient. Rep.*, vol. 7, no. 1, p. 17494, 2017.

[19] M. Borgo, B. Principe, L. Spina, L. Crosara, L. Badia, and E. Gindullina, "Attack strategies among prosumers in smart grids: A game-theoretic approach," in *Proc. IEEE icSmartGrid*, 2023, pp. 01–06.

[20] V. K. Singh and M. S. Kankanhalli, "Adversary aware surveillance systems," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 552–563, 2009.

[21] L. Badia, A. Baiocchi, A. Todini, S. Merlin, S. Pupolin, A. Zanella, and M. Zorzi, "On the impact of physical layer awareness on scheduling and resource allocation in broadband multicellular IEEE 802.16 systems," *IEEE Wireless Commun.*, vol. 14, no. 1, pp. 36–43, 2007.

[22] F. Brandt, F. Fischer, and Y. Shoham, "On strictly competitive multi-player games," in *Proc. Nat. Conf. Artif. Intell.*, vol. 21, no. 1, 2006, p. 605.

[23] A. V. Guglielmi and L. Badia, "Analysis of strategic security through game theory for mobile social networks," in *Proc. Int. Wkshp Comput. Aided Model. Design Commun. Links Netw. (CAMAD)*, 2017.

[24] L. Canzian, L. Badia, and M. Zorzi, "Promoting cooperation in wireless relay networks through Stackelberg dynamic scheduling," *IEEE Trans. Commun.*, vol. 61, no. 2, pp. 700–711, 2012.

[25] A. Tolio, D. Boem, T. Marchioro, and L. Badia, "A Bayesian game framework for a semi-supervised allocation of the spreading factors in LoRa networks," in *Proc. IEEE UEMCON*, 2020, pp. 0434–0439.