Software tool for the performance evaluation of satellite quantum key distribution links

Andrea Stanco [1,*], Giulio Foletto [1], Alessia Scriminich [1], Lorenzo Dal Corso [2], Luca Canzian [2], Francesco Petroni [3,†], Giuseppe Piscopiello [3], Gilles Mariotti [4], Luca De Filippis [3],Giuseppe Vallone [1,5], and Paolo Villoresi [1]

[1] Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Padova, Italy
[2] Qascom S.r.l., via Orazio Marinali 87, 36061 Bassano del Grappa (VI), Italy
[3] Sitael S.p.A., via San Sabino 21, 70042 Mola di Bari (BA), Italy
[4] Sitael S.p.A., via Filippo Guarini 13, 47121 Forlì, Italy
[5] Dipartimento di Fisica e Astronomia, Università degli Studi di Padova, via Marzolo 8, 35131 Padova, Italy
[†] Present address: Aerospazio Tecnologie S.r.l., 1ª Strada 5, 57017 Guasticce (Collesalvetti, LI), Italy

SUMMARY

Here we present a software tool developed under an 18-month project called **PROtocols for Space sEcure Quantum cOmmunication (PROSEQO)**, funded by the European Space Agency and coordinated by the University of Padova with Sitael and Qascom as industrial partners. The scope of the project was to assess the protocols feasible for Satellite QKD and then realize an analytical model to describe all the elements that contribute to the Secret Key Rate (SKR). The analytical model was integrated in a dedicated software able to get several input parameters and orbit descriptions and calculate the final SKR [1]. The software was tested in 10 different case studies. Therefore, this can be a useful tool for future Satellite QKD missions as a preliminary step to evaluate mission feasibility. It could also be the starting point for a numerical overview on the practicability of a satellite QKD infrastructure.

TASK 1 – REVIEW & ASSESSMENT

- Review of State-of-the-art QKD protocols
- Assessment of suitable protocols for Satellite QKD links
  - Efficient BB84 [2]
  - BB84 without announcement of bases [3]
  - 4-D Time Bin BB84 like protocol [4]
  - BBM92 protocol [5]
  - E91 protocol [6]
  - CV no switching and heterodyne detection protocol [7]

TASK 2 – BUILD ANALYTICAL MODEL

- Analysis of every contribution
  - Transmitter
    - Source Repetition Rate, Time Jitter, …
  - Channel
    - Channel Transmittivity, Telescope size, Turbulence, Background Light,…
  - Receiver
    - Detector Efficiency , Afterpulses, States per Detector,…
  - Others
    - Finite Key Effects, Coding Error, Error Correction inefficiency, …

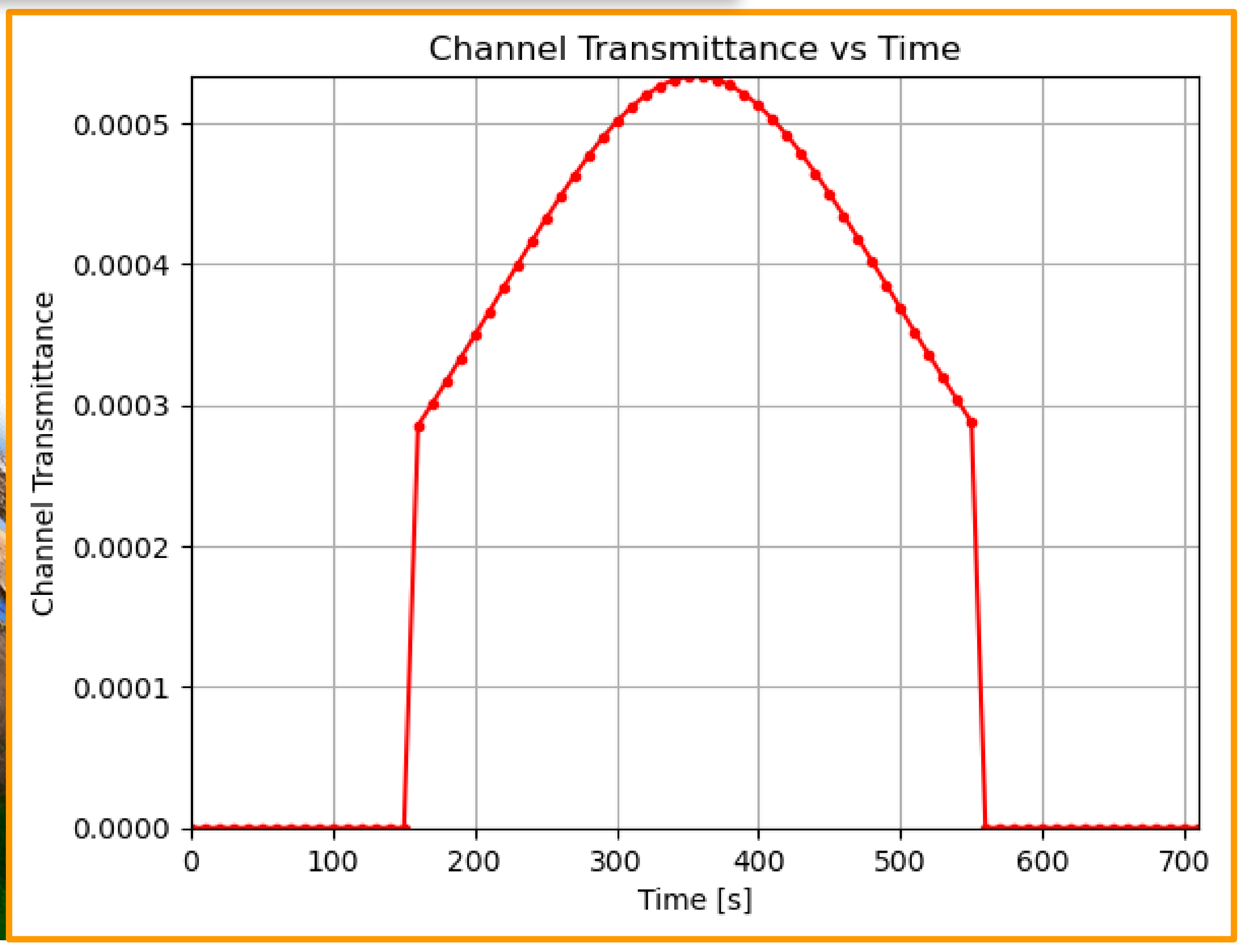
TASK 3 – SOFTWARE

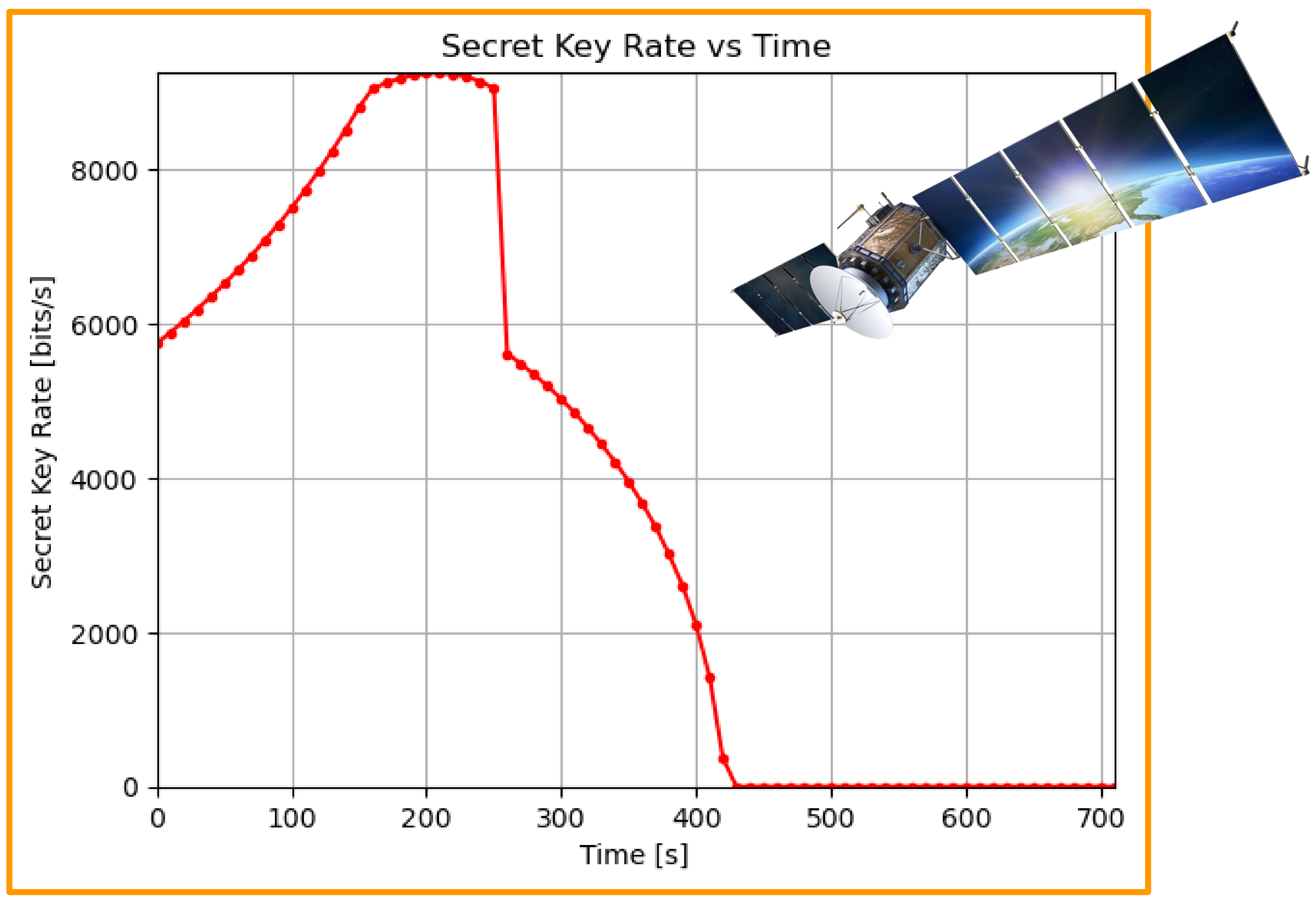
- Scenario Definition
  - Orbit and fixed-point simulations
- Protocol selections + parameters
- Prepare and measure
  - Select to share detector among different states + decoy [8]
- Entanglement based
  - Two separated channels simulation
  - CV protocol
    - Possibility to switch between heterodyne and homodyne

Fixed-point simulations

CS	Protocol	Source rate [MHz]	Detector	Wavelength [nm]	Time of day	Altitude	Channel Transmittance	SKR
1	BB84	1000	SPAD	1550	Day	LEO	0.003	19 kbps
2	BB84	5000	SNSPD	800	Night	MEO	0.0001	32 kbps
3	BB84	1000	SNSPD	1550	Night	GEO	0.0002	16 kbps
4	BB84	1000	SPAD	800	Day	LEO	0.01	0
5	BB84-WBA	100	SPAD	800	Night	MEO	0.0001	1 kbps
6	BB84-TB	1000	SNSPD	1550	Day	LEO	0.003	225 kbps
7	BB84-TB	1000	SNSPD	800	Night	MEO	0.0001	11 kbps
8	BBM92	1	SNSPD	1550	Night	GEO	2E-8	0.006 bps
9	E91	1	SPAD	1550	Night	GEO	2E-8	0
10	BBM92	1	SPAD	800	Night	LEO	3E-5	4.4 bps

Orbit simulations





RESULTS

Results from orbit case study with efficient BB84, LEO orbit, 1 GHz source repetition rate, 1550 nm wavelength and night pass. The figure on the left shows the Channel Transmittance: before and after specific point of the orbit the transmittance has zero value because of the application of a visibility mask. In the right figure it is possible to see the Secret Key Rate. Each point marks the moment when a key block starts to be accumulated. Due to finite-size effects, ~300 s are needed to generate a key block. Thus, the drop around 250 s is caused by the end of the visibility mask at 550 s, after which the key block can no longer be completed. This plot-visualization was chosen because it straightforwardly indicates the best moment when to start a key block, around 200 s in this case.

REFERENCES

[1] A. Stanco, G. Foletto, A. Scriminich, et al., *in preparation*.
[2] H. K. Lo, H. F. Chau, and M. Ardehali, "*Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security*", J Cryptology 18, 133–165 (2005).
[3] W. L. Hwang, I. G. Koh, and Y. D. Han, "*Quantum cryptography without public announcement of bases*", Physics Letters A, Volume 244, Issue 6, Pages 489-494 (1998).
[4] L. Sheridan and V. Scarani, "*Security proof for quantum key distribution using qudit systems*", Phys. Rev. A - At. Mol. Opt. Phys., vol. 82, no. 3 (2010).
[5] C. H. Bennett et al., "*Quantum cryptography without Bell's theorem*", Phys. Rev. Lett. 68, 557-559 (1992).
[6] A. K. Ekert, "*Quantum cryptography based on Bell's theorem*", Phys. Rev. Lett., vol. 67, no. 6, pp. 661–663 (1991).
[7] D. Dequal et al., "*Feasibility of satellite-to-ground continuous-variable quantum key distribution*", npj Quantum Inf 7, 3 (2021).
[8] D. Rusca et al., "*Finite-key analysis for the 1-decoy state QKD protocol*", Appl. Phys. Lett., vol. 112, no. 17 (2018).

Acknowledgment and disclaimer

This work was funded by the European Space Agency (ESA) within the ARTES Scylight programme under contract n. 4000127700/19/UK/AB. The views expressed herein can in no way be taken to reflect the official opinion of the European Space Agency.

QuantumFuture
The shift in the communication paradigm

quantumfuture.dei.unipd.it

*andrea.stanco@unipd.it