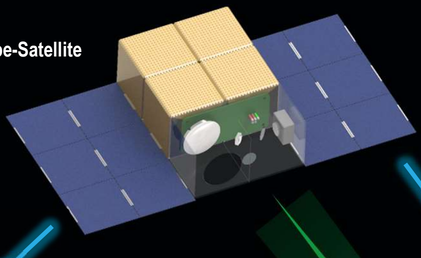
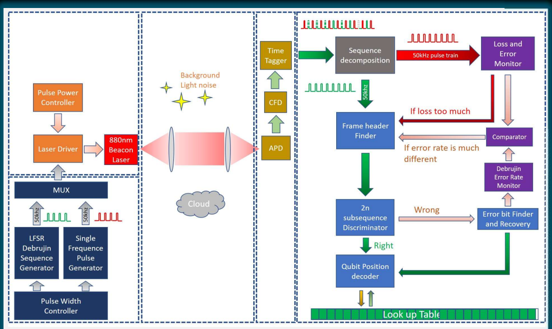
Timing and Noise Tolerant Absolute Pulse Numbering for CubeSat QKD

Zhang, P.[1], Hastings, E.[1], Lowndes, D.[1], Joshi, S,[1], Rarity, J.[1], Oi, D.[2], Mercury, C.[3], Sidhu, J.[2], Greenland, S.[3], Mazzarella, L.[4], McNeil, D.[3], Mohapatra, S[3].

1. Quantum Engineering Technology Labs, University of Bristol, Bristol, UK
2. SUPA Department of Physics, University of Strathclyde, Glasgow G4 0NG, UK
3. Craft Prospect Ltd, Glasgow, G1 5ES, UK
4. NASA, Jet Propulsion Laboratory, 4800 Oak Grove Dr, Pasadena, CA 91109, USA

6U Cube-Satellite





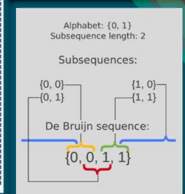


Fig 3. Beacon laser encode and decode diagram; Fig 4. De Bruijn sequence encode diagram [5]

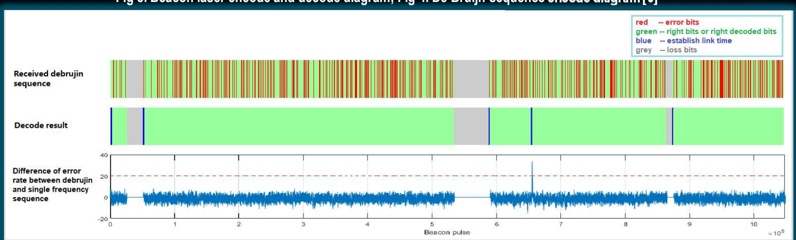
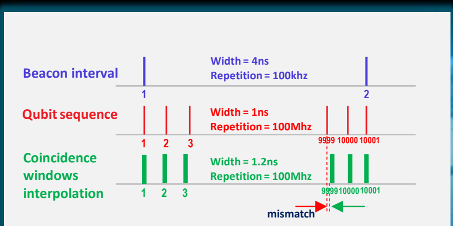


Fig 5. de Bruijn decode simulation result with noise. The simulation error ratio = 5%, fatal error threshold = 20, decode length = 40

Advantages

a. This solution don't need to explicitly synchronise clocks, can simply post-process the time-tagged data.
b. De Bruijn codes are the optimum encoding, that n-bits of signal are required to unambiguously determine the position within a 2^n long bit sequence Utilize de Bruijn sequence to encode the index of beacon pulse reliably on the satellite in real time [3].
c. The sequence position of each pulse only depends on the n pulses adjacent to it, which provides a basis for fast link reconstruction after technology or object occlusion. Error correction module provides the function of identifying and correcting errors caused by noise.
d. Low duty cycle provides a low average power (important for CubeSats) but high peak powers by using short pulses increases the receiver signal to noise and reduces jitter; For flexibility, pulse width, repetition frequency, amplitude of beacon are all adjustable online, which provide a possibility of parameters influence test on sync quality as well.
e. Interleaved de Bruijn code every second pulse means that there are no long sequences of no pulses that could occur using a simple on-off pseudorandom bit sequence, hence the largest gap to interpolate is only 20 microseconds at 100kHz.



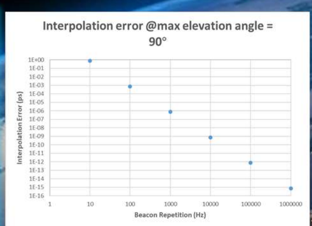


Fig 6. Coincidence windows interpolation diagram; Fig 7. Simulation of non-linear doppler effect on uniform interpolation. Due to the non-linear part of doppler effect caused by jerk of satellite, the uniform interpolation between the two signals will bring nonlinear drift. In this regard, we calculate and compensate the offset according to the corresponding orbit position [4].

Reference
[1] Alberto Carrasco-Casado, Hideki Takenaka, Mikio Fujiwara, Mitsuo Kitamura, Masahide Sasaki, and Morio Toyoshima "QKD from a microsatellite: the SOTA experience", Proc. SPIE 10660, Quantum Information Science, Sensing, and Computation X, 106600B (14 May 2018);
[2] Mazzarella L. et al., QUARC: Quantum Research Cubesat—A Constellation for Quantum Communication. Cryptography 4, 7 (2020)
[3] Chang, Z., Ezerman, M.F., Ling, S. et al. On binary de Bruijn sequences from LFSRs with arbitrary characteristic polynomials. Des. Codes Cryptogr. 87, 1137–1160 (2019).
[4] I. Ali, N. Al-Dhahir and J. E. Hershey, "Doppler characterization for LEO satellites," in IEEE Transactions on Communications, vol. 46, no. 3, pp. 309-313, March 1998, doi: 10.1109/26.662636.
[5] https://en.wikipedia.org/wiki/De_Bruijn_sequence

Introduction

Space-based quantum key distribution (QKD) overcomes the limits of distance between terrestrial users caused by losses in optical fibre [1]. To further promote the commercial application, we present our Cube-Sat payload design which has a more economically viable key-rate [2]. The system is designed for polarisation based BB84/Decoy-State protocol with 100Mhz key transmission rate. In order to avoid the light pollution near the metropolitan centres and provide flexibility, we present our progress towards a mobile OGS which will be able to act as a receiver for the quantum signal. The payload is only 2U installed in a 6U Cube Satellite.

Challenge.

The quantum source is sending out 1ns long pulses with fewer than 1 photon per pulse on average. A LEO satellite will suffer a 30-50dB loss in the channel which means only 1 in 1000-100000 photons could arrives at the detector while the beacon loss is approximately 20dB greater than the quantum signal (i.e. 50-70dB). The raw key is determined from received photons and the main source of errors is spurious detections arising from background light and dark counts. If we can precisely determine short time windows in which the single photons should be arriving, we can reject most of the errors caused by spurious signals. To do this we need very accurate time synchronisation providing accurate timing of the arriving pulses to better than 1ns. When using a beacon pulse it is the time jitter in the rising edge that introduces an uncertainty to synchronization. To solve this a stable transmitter with sufficient peak power needs to be developed within the constraints of minimizing satellite power consumption and cost. We also need to determine the absolute pulse position number of detected events to allow sifting of the raw key using the basis information. This can be done by interspersing our timing pulses with a pseudo-random code that uniquely determines the absolute time from transmission start. Here we investigate the de Bruijn codes

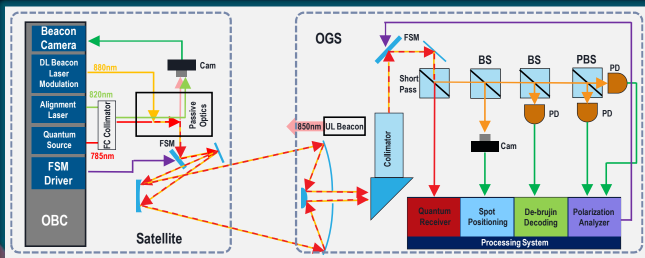


Fig 1. Timing and Sync System Diagram. A downlink beacon pulsed at 100kHz is used to convey both the coincidence window timing as well as encode the pulse position information. The rising edge of the beacon pulse defines a periodic reference time that the receiver can use in decoding time and pulse number. A beacon pulse is sent every 1000 quantum signal, hence the intermediate quantum signal arrival times need to be interpolated precisely. The beacon pulse characteristics such as peak power, risetimes, signal to noise, propagation characteristics etc. need to be studied to achieve the timing signal's jitter lower than 100ps, and a robust way of encoding and decoding pulse number need to be implemented as well.

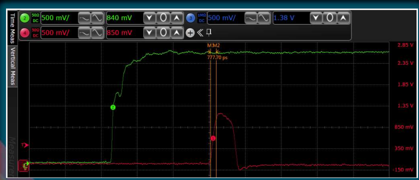


Fig 2. Controllable short beacon pulse with rise time of 777ps. The red pulse is the beacon optical pulse received by detector while the green one is the trigger signal. This is generated with the conditions of pulse width = 3.1ns, repetition = 100khz, average transmit power = 34.7uW, attenuator = 40dB, expected received peak power = 8.9uW

Mobile Optic Ground Station (MOGS)

Summary.

Based on the decode module, a beacon pulse numbering has been simulated with 5% error bits. The result shows that the module could detect the error accurately and resume the link quickly after an interruption. A preliminary experimental result of beacon pulses has been performed which shows that the requirement should be achievable. The interpolation error introduced by doppler effect with different beacon period has been simulated. The result shows that a repetition down to 10hz don't have significant error on interpolation. In the future, the analysis of beacon power and receiver performance will be completed; A experimental encode and decode test will be conducted in the practical system to further verify the reliability. A lower beacon repetition will be considered to further increase the peak power for a better SNR. Finally, a km range free-space system will be demonstrated experimentally and will be integrated into a full QKD system.