Doctoral Dissertation Final Review

Research on Satellite-Based Free-Space Optical Quantum Key Distribution Systems for Multiple Wireless Users

Vu Quang Minh, 3rd year Ph.D. student

The University of Aizu

Supervisor: Prof. Anh T. Pham

Contents

1. Research Background

1.1. Future Wireless Networks and Security Threats

- Next-generation wireless networks are envisioned to revolutionize customer services and applications via the Internet of Things (IoT)

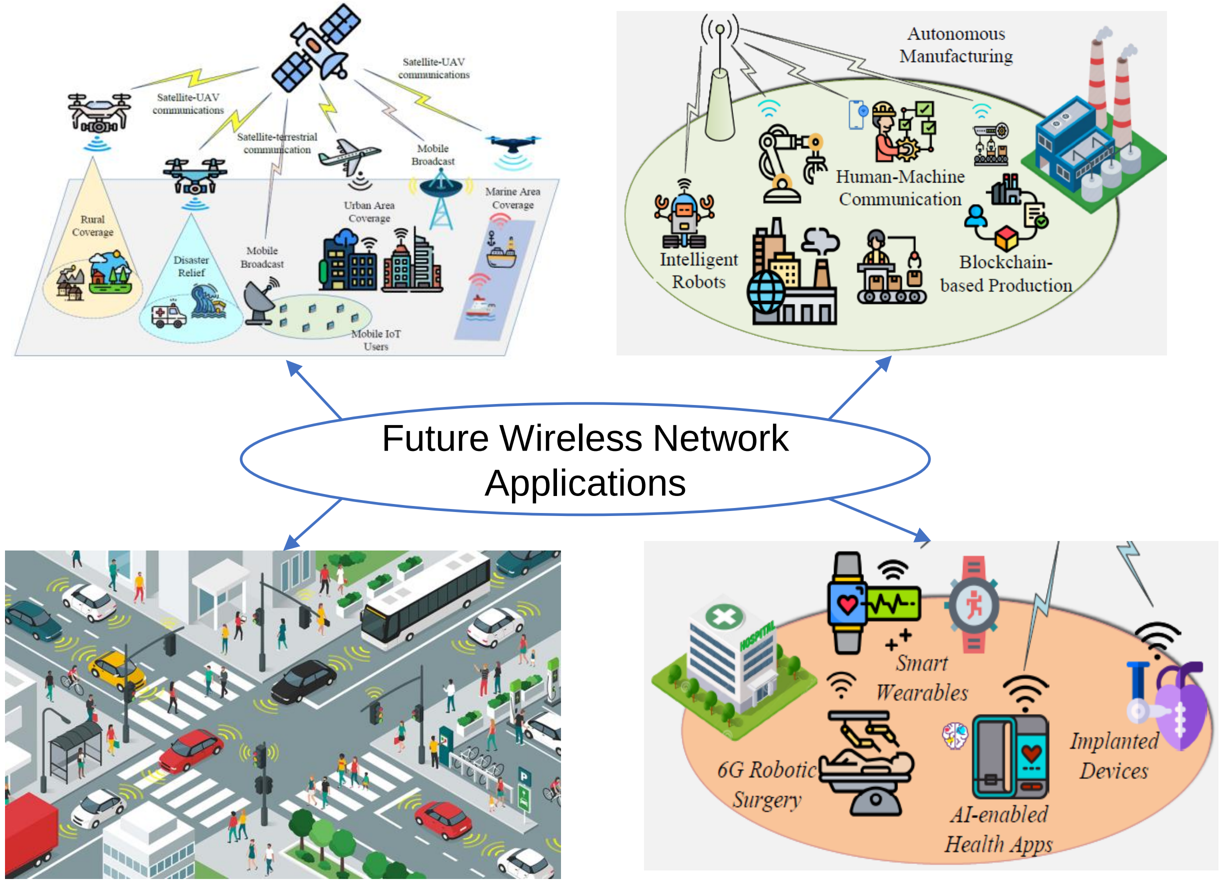
→ Future of fully intelligent and autonomous networks

- Security becomes even more concerning issues with such applications: related to
  - Human health
  - Human safety
  - Economy
  - Environment

→ Network security becomes more and more important in future networks

Satellite Internet of Things [1]

Industrial Internet of Things [1]

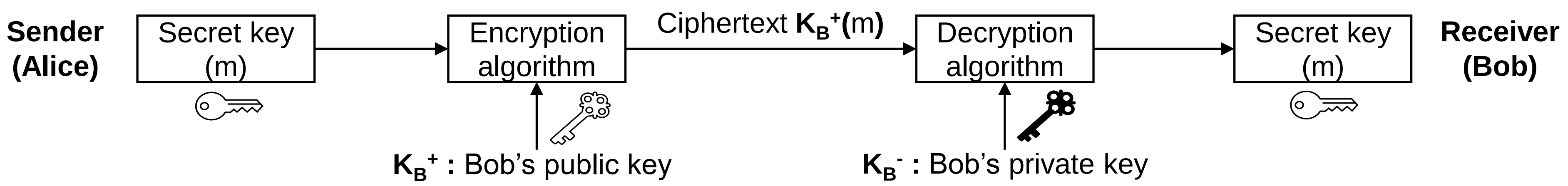


Vehicular Internet of Things and Autonomous Vehicle [2]

Internet of Healthcare Things [1]

1.2. QKD: Motivation (1)

- How is network security implemented to protect information?
  - Basically, based on symmetric cryptography (Secret keys are needed and shared with legitimate parties)
- How can secret keys be shared?
  - Manually: e.g., private meetings → impractical
  - Key distribution system (KDS)
    - ❑ The present KDS is based on public-key cryptography (PKC)

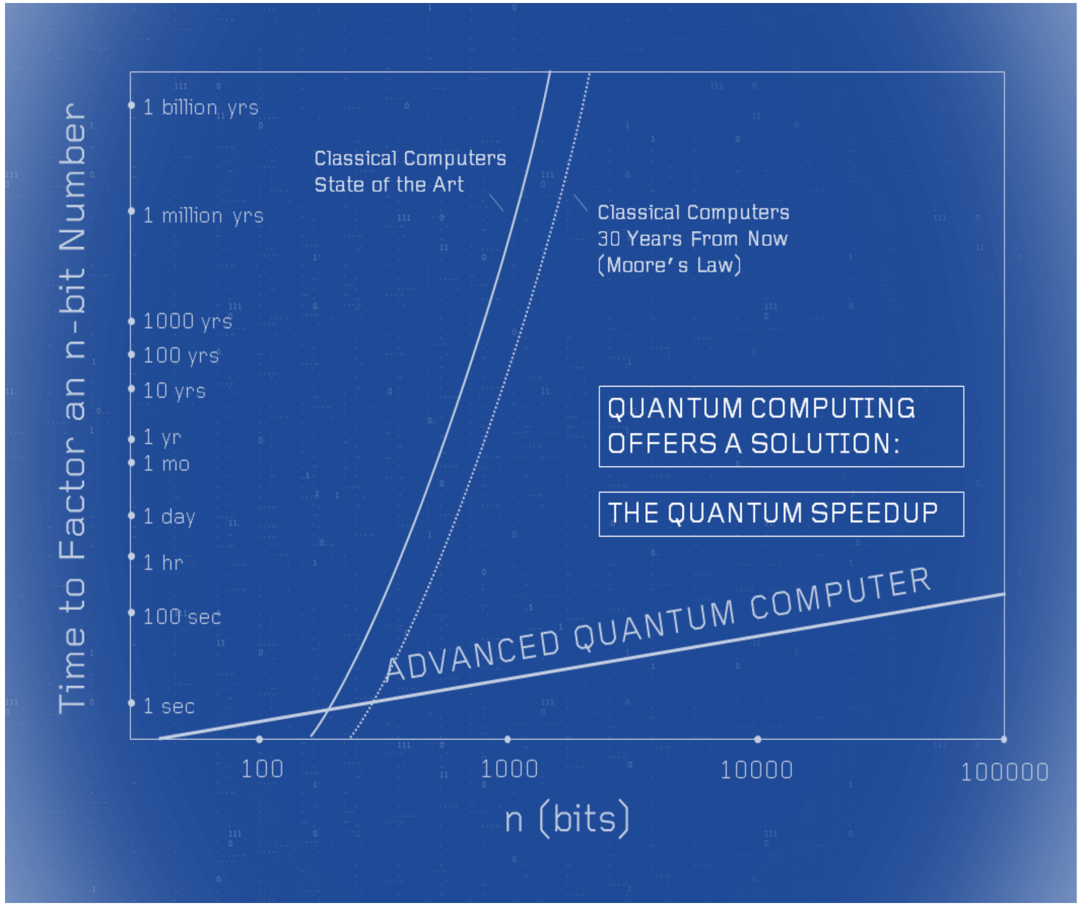


- ❑ Security of PKC is based on the mathematical complexity (Factoring problem)
  - $n = p \times q$ (p, q: two large prime numbers) is known (in the public key) → need to find p and q to break the private key
  - Difficult to find p and q when both are prime number
  - With classical computers, the computational time is exponentially increased as p and q increased

1.2. QKD: Motivation (2)

- Issues with PKC-based KDS
  - With classical computer → no problem
    - ❑ Time to factoring is up to 10,000s years as number of bits → 1000
  - Recent advances in computing (e.g., quantum computers)

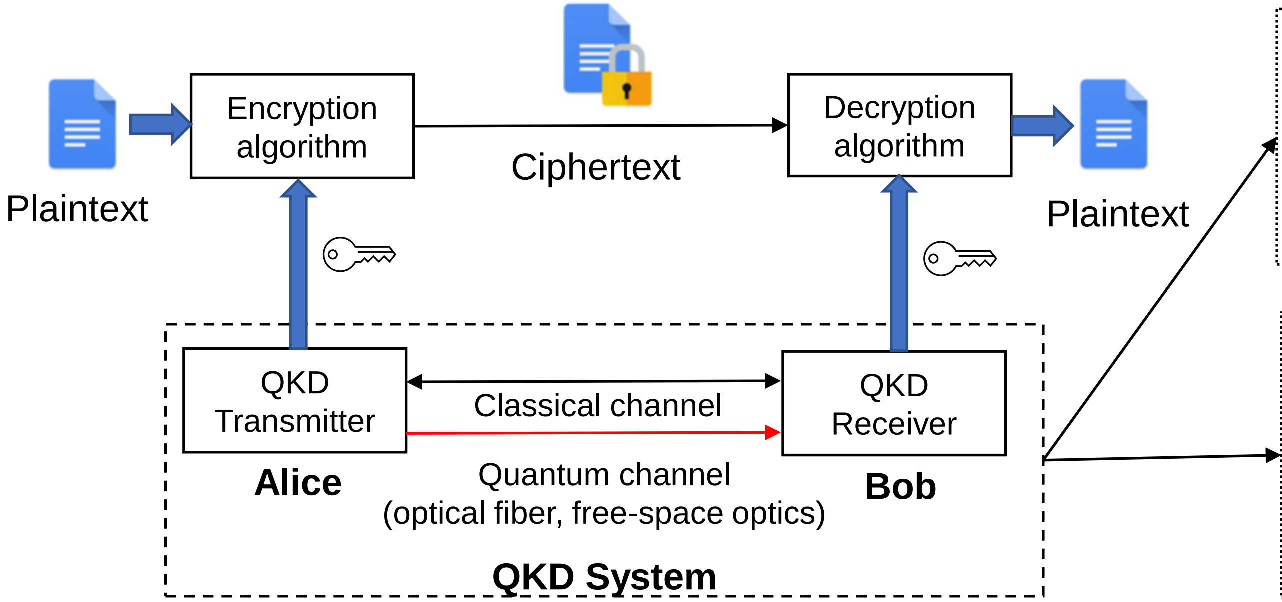
  → computational power can be exponentially increased
  - PKC can be broken in a much shorter time (a few minutes)



https://www.nea.com/blog/quantum-computing-time-for-venture-capitalists-to-put-chips-on-the-table

1.3. QKD: Implementation (1)

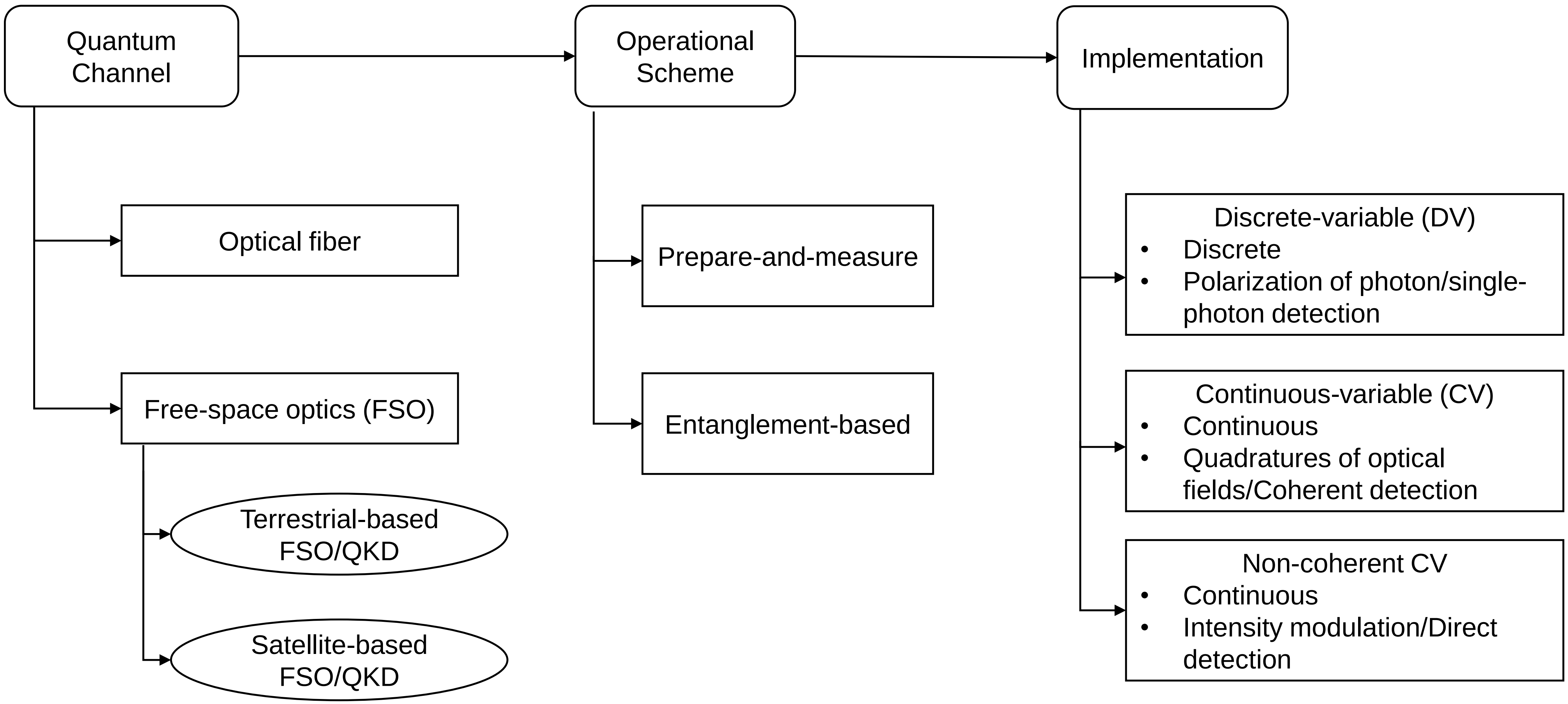
- New Key Distribution Systems Needed
  - Quantum key distribution (QKD)
    - ❑ QKD is being considered a promising method to distribute secure keys secretly
    - ❑ Key distribution based on the laws of physics (not by the complexity of mathematics)
    - ❑ First proposed by C. Bennett and G. Brassard in 1984



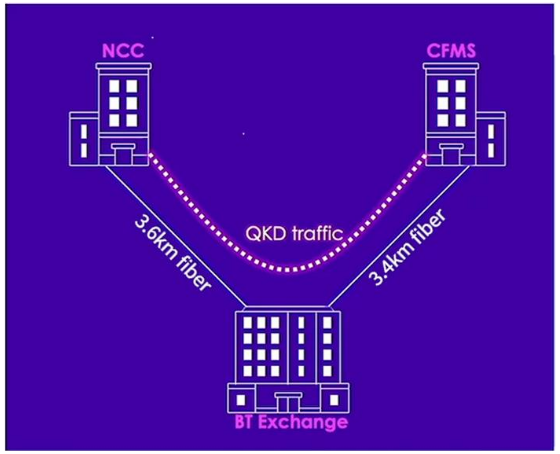
Stage 1: Using quantum channel
- Distribution of quantum states (e.g., photons, optical beams)
- Measurements

Stage 2: Using classical channel
- Comparing measurement methods to derived *sifted key*
- Error correction
- Privacy amplification

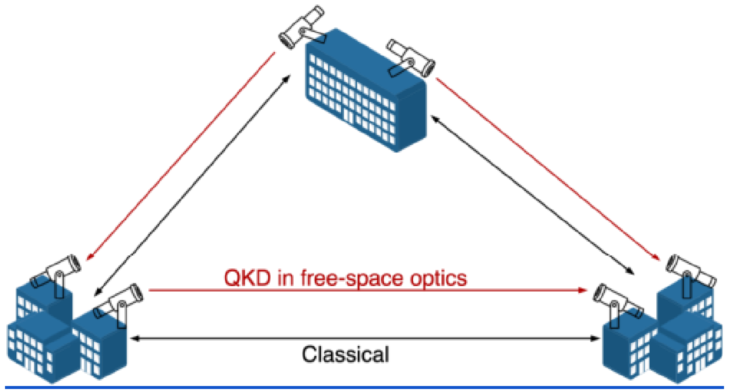
1.3. QKD: Implementation (2)



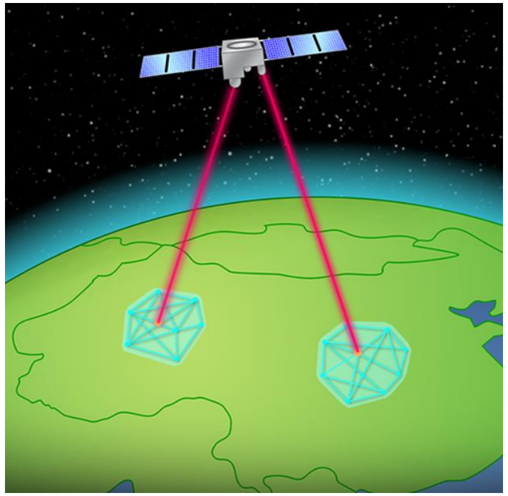
1.3. QKD: Implementation (3)



[3]



[4]



[5]

Optical Fiber

- The most common channel
- High stability
- High cost, difficulty in installing
- Only suitable for fixed users

Terrestrial Free-space Optics (FSO)

- Wireless solution for QKD
- Flexibility & cost-effectiveness (Infrastructure deployment)
- Block by physical objects (high-rise buildings, trees,…)

Satellite-based FSO

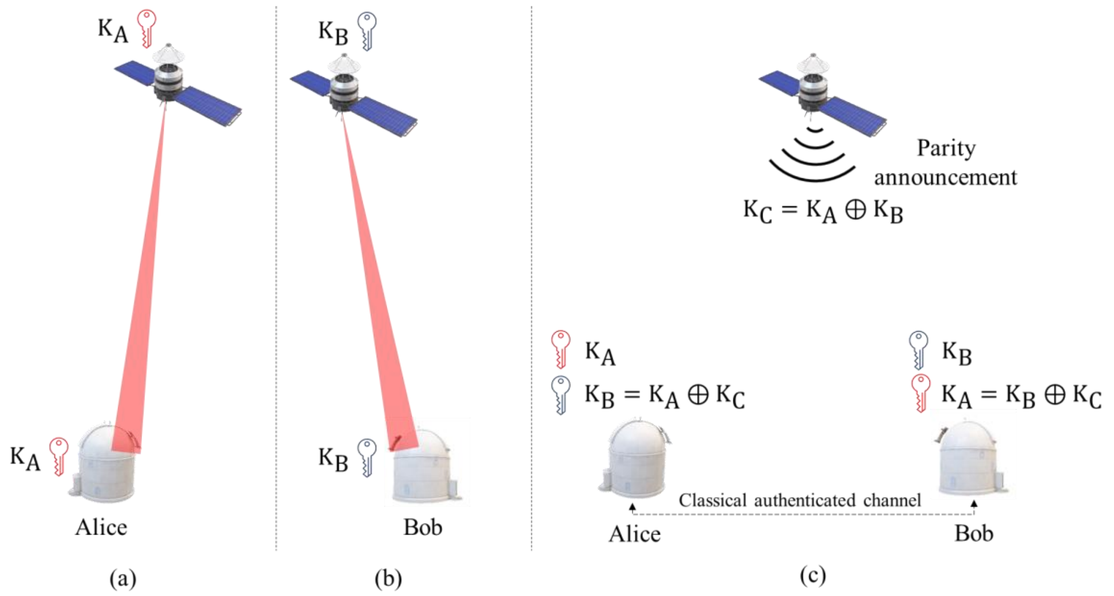
- Enable the possibility the global-scale quantum networks for both fixed and mobile users

Significant limitations in terms of **bridging larger geographical distances**

Solution

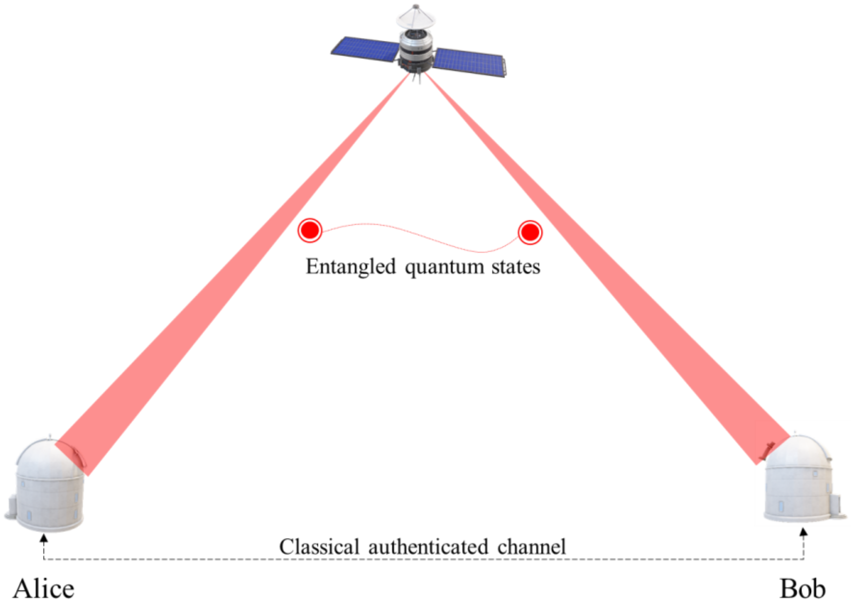
1.4. Satellite-based FSO/QKD: Operating Scheme

Prepare-and-measure (PM) scheme



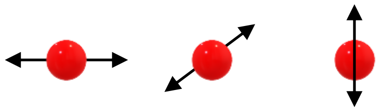
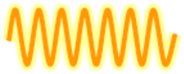
- More than one phase is needed to distribute a key from Alice to Bob ultimately → inefficiency
- The satellite must be trusted

Entanglement-based (EB) scheme



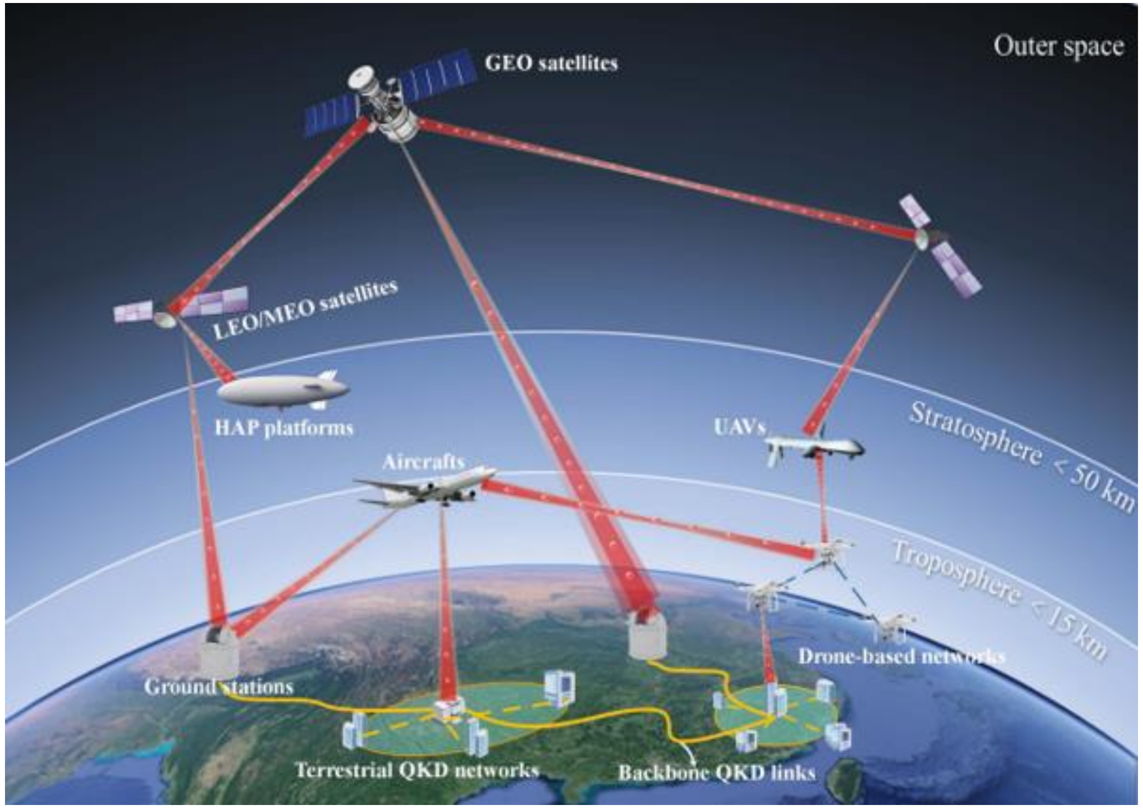
- The trust requirement of the satellite can be relaxed
- **Suitable for implementing a global-scale QKD network**

1.5. Satellite-based FSO/QKD: Implementation

	Discrete-variable QKD (DV-QKD) [6]	Continuous-variable QKD (CV-QKD) [7]	Non-coherent CV-QKD [8]
Source	Weak laser pulse (single-photon)	Laser	Laser
Modulation	Polarization of photons 	Amplitude and phase or quadrature of optical fields 	Intensity
Measurement	Single-photon detector	Coherent detection (homodyne or heterodyne detector)	Direct detection (using dual-threshold)
Compatibility with existing communication infrastructure	☒	☑	☑
Challenging issues	- Low key rate - Bulky and expensive receiver devices	Require a sophisticated phase-stabilized local light for coherent detection → High cost at receivers	Imitating DV and CV-QKD → Need a proper design for the transmitter and receivers

2. Scope of Study

2.1. Future of Global-scale QKD Network



[9]

- **Goal**: Implement a global-scale QKD network for a wide range of applications, including fixed and mobile users (e.g., autonomous vehicles, HAP, UAVs…)
- **Requirements**:
  - Simplicity, cost-efficiency, compatibility with current technologies
  - Capability of supporting multiple legitimate users

2.2. Scope of Study

- Present state-of-the-art
  - Optical fiber-based QKD, PM, non-coherent CV proposed by [10]
  - Terrestrial-based FSO/QKD, PM, non-coherent CV proposed by [7]
  - Satellite-based FSO/QKD, PM, non-coherent CV proposed by [11]
- To achieve the global-scale QKD network, in this study, we consider
  - Satellite-based FSO/QKD system
  - EB scheme
  - Non-coherent CV
  - Capability of supporting multiple legitimate users

3. Contributions of This Dissertation

Contributions: Overview

To implement practical satellite-based FSO/QKD systems towards the global-scale QKD network

1. How to implement practical satellite-based FSO/QKD systems with ***simplicity, cost-effectiveness, and compatibility with standard communication technologies***?

   → Proposal of a new design concept by applying *non-coherent CV-QKD* in the *EB scheme* using *LEO satellite* in [C1], [J1]

2. How to ***extend the coverage area*** of satellite-based FSO/QKD systems?

   → Proposal of a FSO/QKD system that uses LEO and GEO satellites in [J2],[J3]

3. If there are ***multiple users*** on Alice's and Bob's sides, can ***secret keys be distributed*** to them ***simultaneously***?

   → Proposal of a novel satellite-based FSO/QKD system for multiple users in [J2],[J3]

3.1. Practical Satellite-Based FSO/QKD Systems

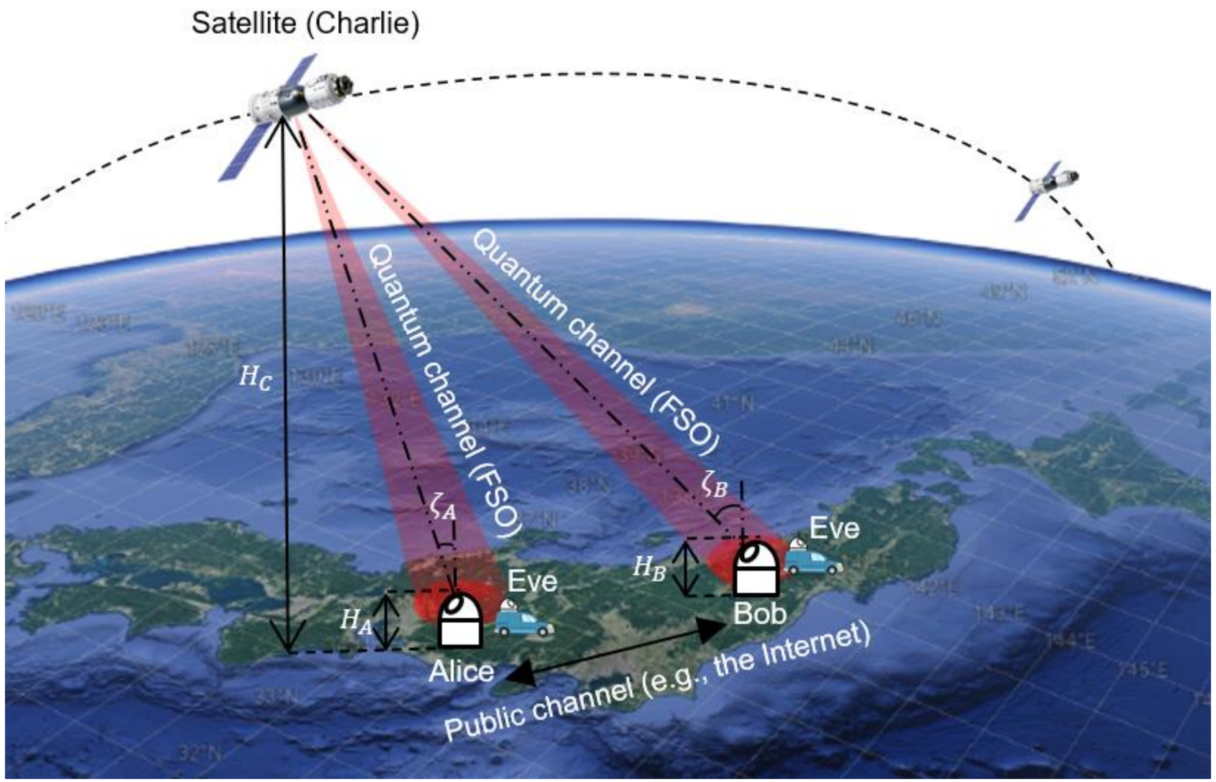
The content of this contribution was published in

[C1] Minh Q. Vu *et al.,* “Entanglement-based satellite FSO/QKD system using dual-threshold/direct detection,” ICC 2022 - IEEE International Conference on Communications, Seoul, Korea, Republic of, 2022, pp. 3245-3250.

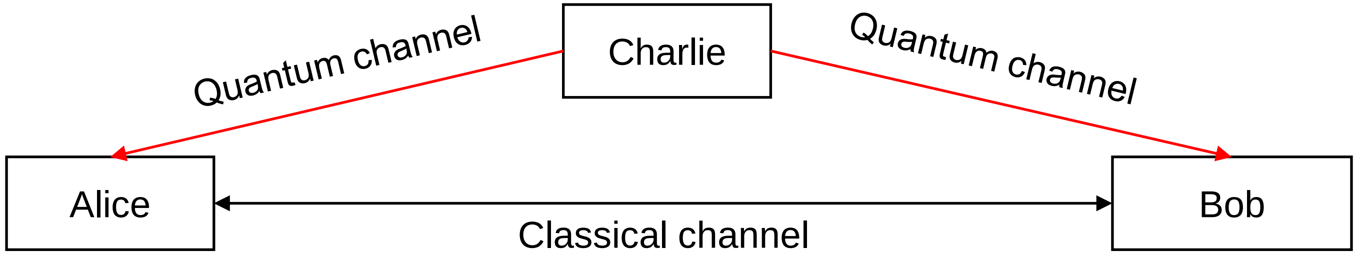
[J1] Minh Q. Vu *et al.,* “Toward practical entanglement-based satellite FSO/QKD systems using dual-threshold/ direct detection,” in IEEE Access, vol. 10, pp. 113260-113274, 2022.

3.1.1. Considered Scenario

- Entanglement-based QKD
- LEO satellite (Charlie): a key source
  - H_c: the altitude of Charlie
- Alice and Bob: two legitimate users
  - H_A: the altitude of Alice
  - H_B: the altitude of Bob
  - ζ_A: the zenith angle between Charlie and Alice
  - $\frac{\pi}{2} - \zeta_A$: the elevation angle between Charlie and Alice
  - ζ_B: the zenith angle between Charlie and Bob
  - $\frac{\pi}{2} - \zeta_B$: the elevation angle between Charlie and Bob
- Eve: eavesdroppers perform unauthorized receiver attack (URA)
- Channel model: geometric spreading loss, atmospheric attenuation, and atmospheric turbulence-induced fading



3.1.2. Conventional EB QKD Scheme (BBM92)



Basic setting of the BBM92 protocol (Alice, Bob: legitimate parties, Charlie: entangled source) [12]

Satellite (Charlie)		**Alice**				**Bob**				Sifted key
Time	Entangled photon pairs state	Time	Basis	Measured state	Bit	Time	Basis	Measured state	Bit (inverted)	
t_0	$1/\sqrt{2}(\lvert 01\rangle + \lvert 10\rangle)$	t_0	$\oplus$	$0°$	0	t_0	$\oplus$	$90°$	0	0
t_1	$1/\sqrt{2}(\lvert 01\rangle + \lvert 10\rangle)$	t_1	$\oplus$	$0°$	–	t_1	$\otimes$	$45°$	–	*discarded*
t_2	$1/\sqrt{2}(\lvert 01\rangle + \lvert 10\rangle)$	t_2	$\otimes$	$45°$	1	t_2	$\otimes$	$-45°$	1	1
t_3	$1/\sqrt{2}(\lvert 01\rangle + \lvert 10\rangle)$	t_3	$\otimes$	$-45°$	–	t_3	$\oplus$	$90°$	–	*discarded*

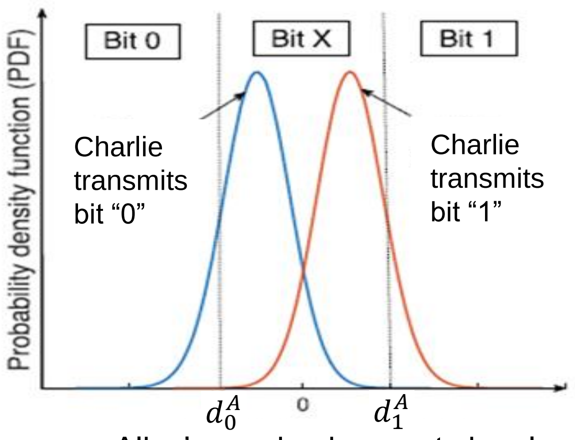
BBM92 Protocol: Example

3.1.3. Proposed EB QKD Scheme (1)

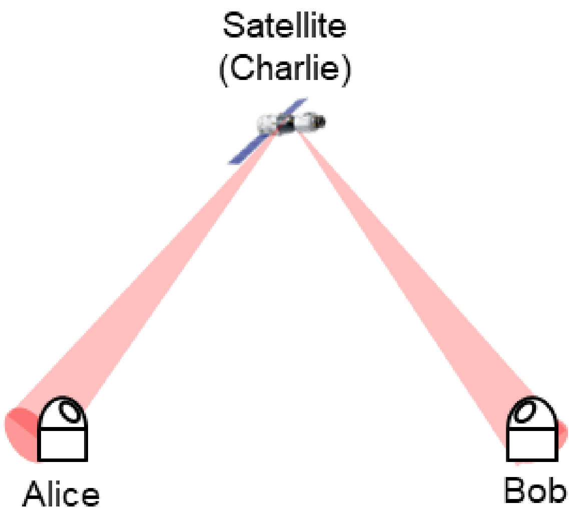
- We proposes non-coherent CV-QKD for satellite-based FSO/QKD in the ***EB scheme***
  - Motivation: To achieve QKD function with simple configuration (intensity modulation/direct detection) and overcome the challenging issue of DV, CV-QKD
  - Try to **mimic** the sifting process of the conventional EB QKD scheme by adjusting two thresholds at high and low levels of two intensity-modulated signals at the receiver
    - ❑ The random fluctuations in the received signals over the atmospheric channel result in random detection results
    - ❑ When the detect values of the received signal are in the middle of two thresholds, the coherent states are indistinguishable, and Eve unavoidably introduces errors by randomly guessing the states

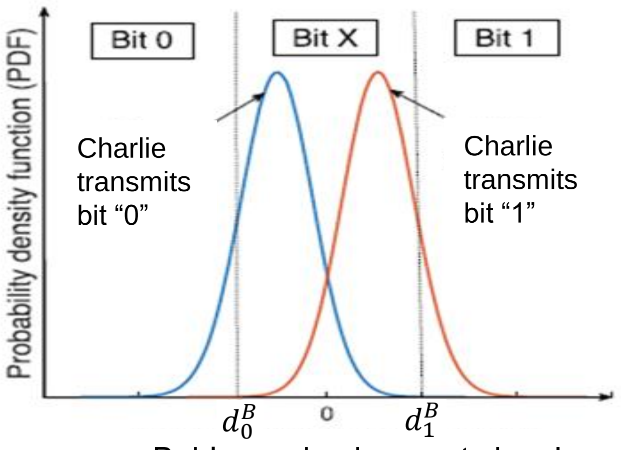
3.1.3. Proposed EB QKD Scheme (2)

- How to prepare transmitting signal for non-coherent CV-QKD in EB scheme?
  - Charlie transmits SIM/BPSK modulated signal to Alice and Bob
  - Purpose: The receivers can not fully distinguish transmitted bits “0” or “1”
  - How: Choose a small modulation depth (0<δ<1)
- How to detect signal?
  - The receivers use two thresholds (dual-threshold) to detect the received signal (direct detection)
  - Purposes:
    - ❑ To control the number of bits the receiver will detect
    - ❑ To control the error rate: not get the high error rate



Alice’s received current signal





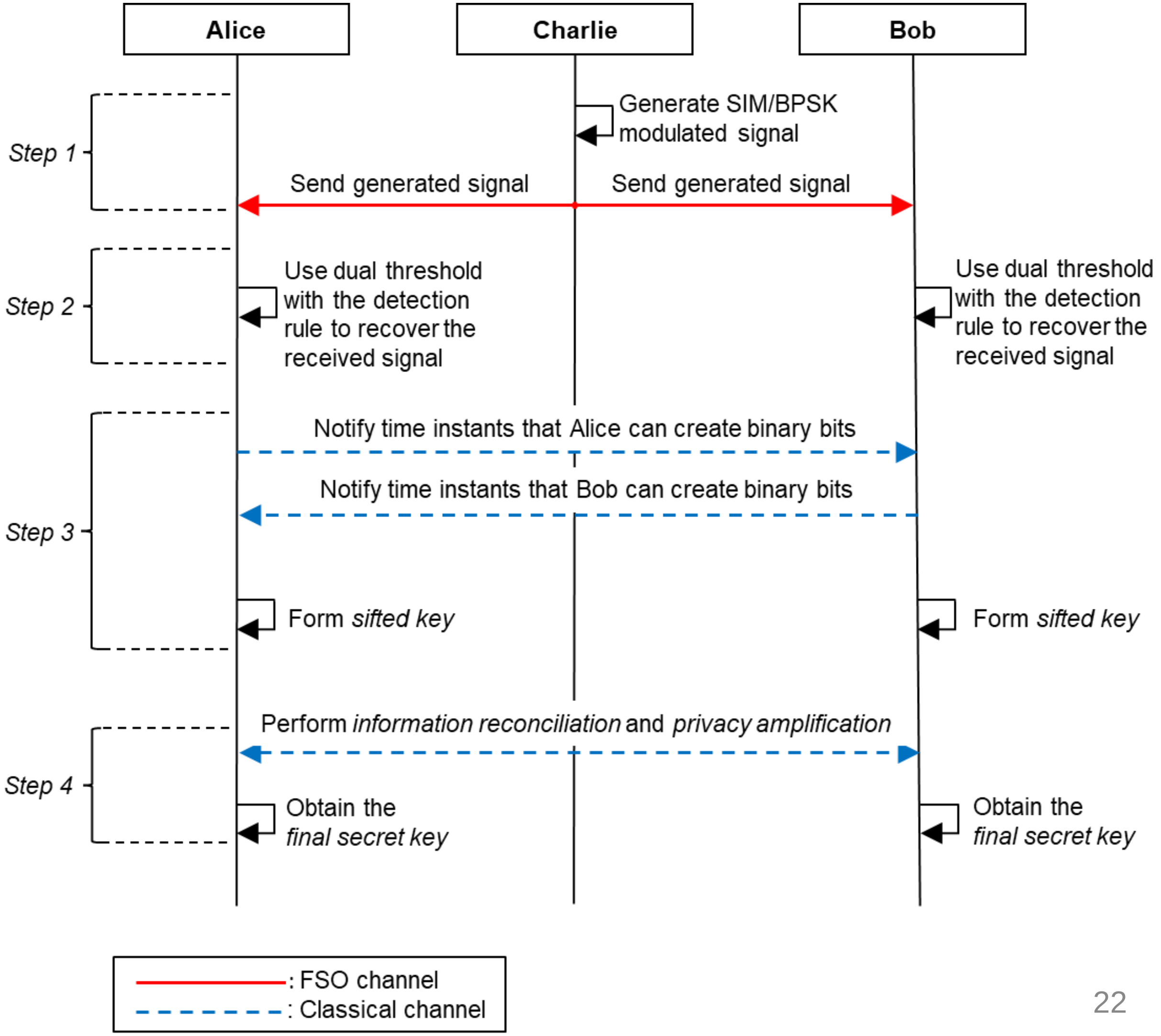
Bob’s received current signal

3.1.3. Proposed EB QKD Scheme (3)

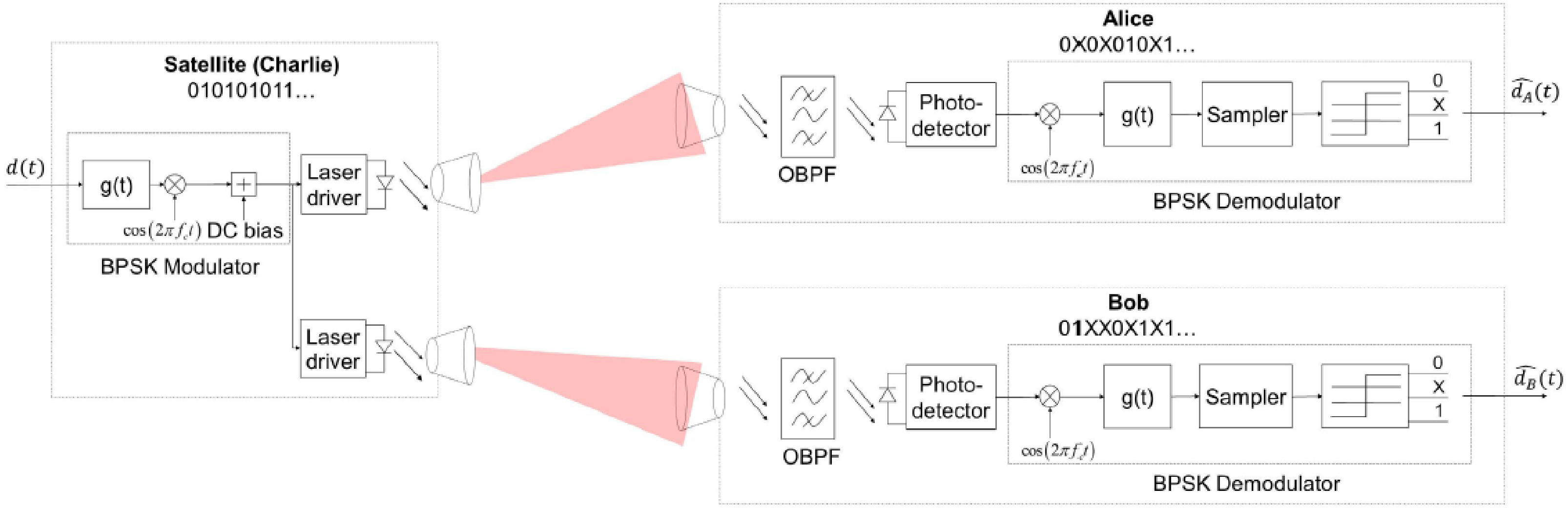
- Flowchart of the proposed protocol

The proposed protocol includes 4 steps

The key issue for simple and cost-effective implementation comes from *the non-coherent detection (realized by dual-threshold/direct detection)*



3.1.3. Proposed EB QKD Scheme (4): System Model and Example



The block diagram of the proposed satellite FSO/QKD system using SIM/BPSK and dual-threshold/direct detection (DT/DD) receiver

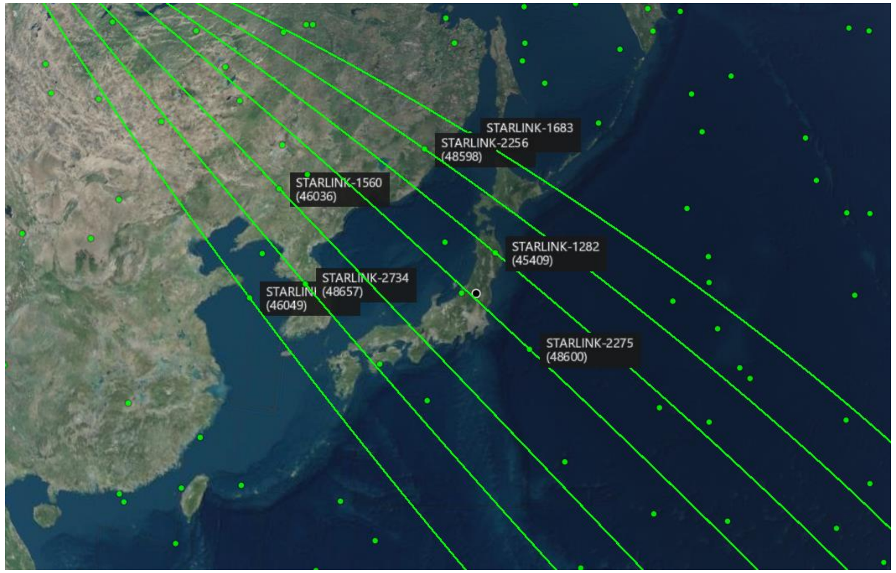
- Example of the proposed protocol

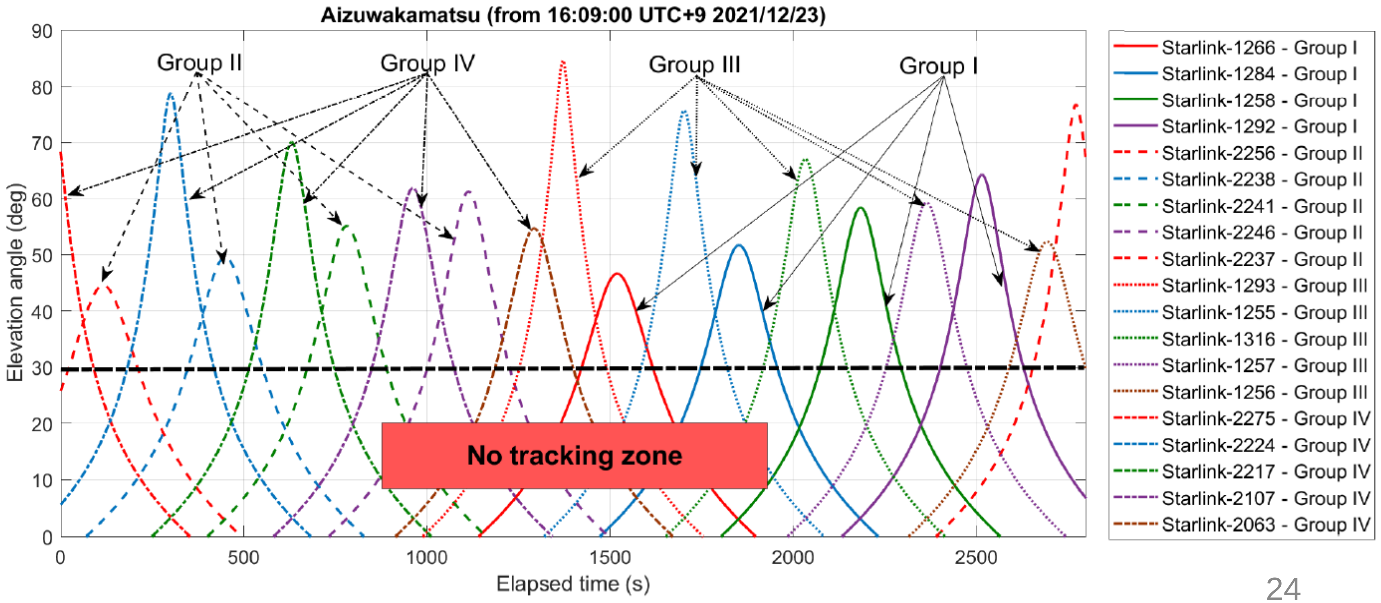
Satellite (Charlie)			Alice			Bob			Sifted key
Time	Bit	Signal	Time	Threshold	Bit	Time	Threshold	Bit	
t_0	0	i_0	t_0	d_0^A	0	t_0	d_0^B	X	*discarded*
t_2	1	i_1	t_2	d_1^A	X	t_2	d_1^B	X	*discarded*
t_3	0	i_0	t_3	d_0^A	0	t_3	d_0^B	0	0
t_4	1	i_1	t_4	d_1^A	1	t_4	d_1^B	1	1
t_5	0	i_0	t_5	d_0^A	X	t_5	d_0^B	0	*discarded*

3.1.4. Practical Satellite Selections

- Investigating the feasibility of the proposed satellite FSO/QKD system in a case study for the Japan QKD network using the existing Starlink LEO satellite constellation
  - Alice is assumed to locate in Aizuwakamatsu City, Fukushima, Japan
  - LEO satellites in the Starlink constellation play a role as Charlie
  - These satellites are supposed to equip with optical transmitters for FSO downlink transmission

→We design the transmitter's (Charlie) and receiver's (Alice & Bob) parameters (intensity modulation depth and dual threshold) for EB non-coherent CV

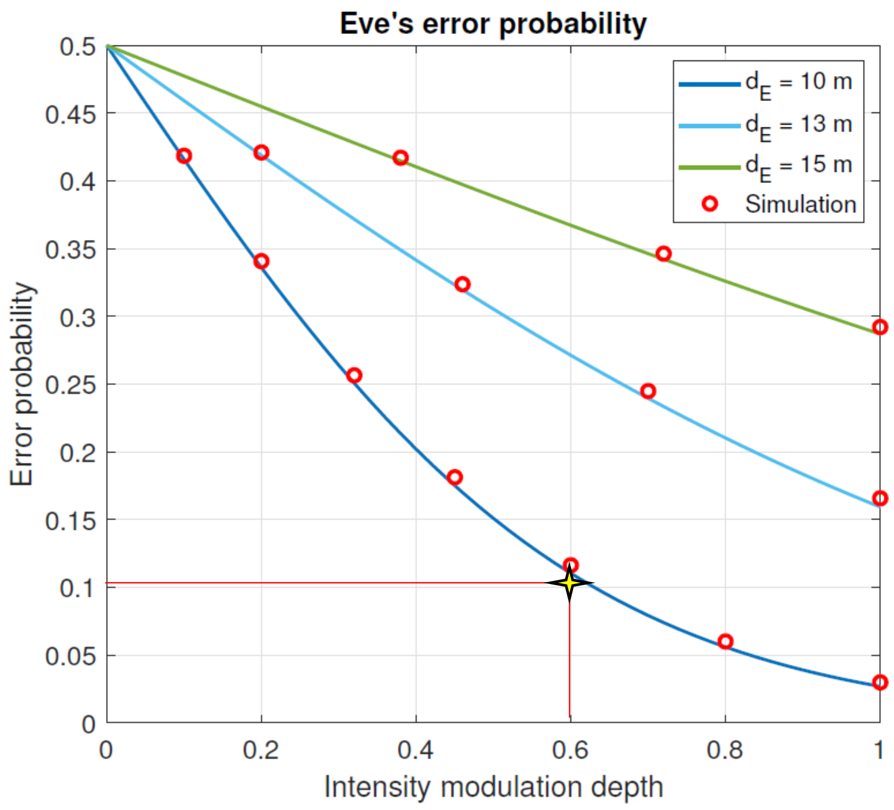




System Parameters

Name	Symbol	Value
LEO Satellite (Charlie)		
Wavelength	λ	1550 nm
Bit rate	R_{b}	1 Gbps
Altitude	H_{C}	550 km
Divergence angle	θ_C	50 μrad
Transmitted power	P	30 dBm
FSO Channel		
Sun's spectral irradiance from above the Earth	Ω_{v}	$0.2\ \mathrm{kW/m^2 \cdot \mu m}$
Wind speed	w	21 m/s
The refractive index structure parameter at the ground level	$C_n^2(0)$	$10^{-15}\mathrm{m}^{-2/3}$
Visibility	V	30 km
Alice/Bob/Eve		
Altitude	H_{U}	2 m
Aperture radius	a_{U}	5 cm
Optical bandwidth	B_0	250 GHz
Responsivity	R_e	0.9 A/W
Effective noise bandwidth	Δf	0.5 GHz
Temperature	T	298 K
Load resistor	R_{L}	1 kΩ
Amplifier noise figure	F_{n}	2

3.1.5. Charlie's Design



Eve's error probability versus intensity modulation depth of Charlie

- The intensity modulation depth of Charlie is designed to prevent unauthorized receiver attack (URA) which is the most popular attacking strategy of eavesdroppers (Eve)
  - Eve tries to tap the transmitted signal from Charlie by locating their receivers within the beam footprint near legitimate users at a distance d_E m
- To prevent URA, we need to select a small value of σ
  - Eve suffers from a high error rate when she tries to detect the received signal by the optimal threshold d_t^E = 0 to get as much information as possible
- We consider the worst-case scenario (i.e., the propagation distance from Charlie to legitimate users is minimal)
  - To make sure that Eve's error probability (P_{error}^E) is sufficiently high (e.g.,P_{error}^E>0.1), σ should be chosen ≤ 0.6

$\delta \downarrow$ => $P_{\text{error}}^E \uparrow$ & Bit error rate at Alice and Bob $\uparrow$
=> We use δ = 0.6 for Charlie's design

3.1.6. Alice's Design: Sift Probability and QBER

P_{sift} between Charlie and Alice: the probability that Alice is able to decode bits using DT

QBER between Charlie and Alice: the fraction of the probability that Alice mistakenly detects the transmitted bits and P_{sift} between Charlie and Alice

$$P_{CA}^{\text{sift}} = P_{CA}(0,0) + P_{CA}(0,1) + P_{CA}(1,0) + P_C(1,1)$$

$P_{CA}(x, y)$ with $(x, y) \in \{0,1\}$: the probability that Alice's detected bit "x" coincides with Charlie transmitted bit "y"

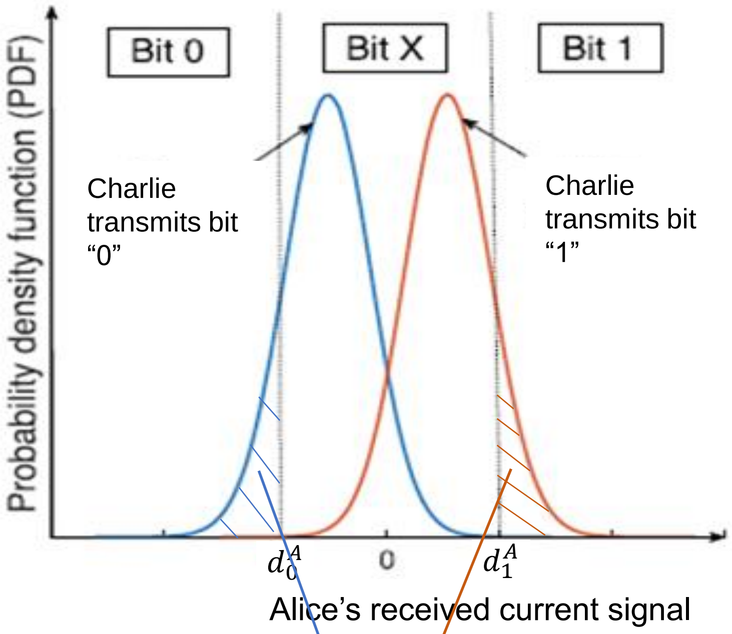
$$QBER = \frac{P_{CA}^{\text{error}}}{P_{CA}^{\text{sift}}} = \frac{P_{CA}(0,1) + P_{CA}(1,0)}{P_{CA}(0,0) + P_{CA}(0,1) + P_{CA}(1,0) + P_C(1,1)}$$

3.1.7. Alice's Design: Dual-Threshold Setting (1)

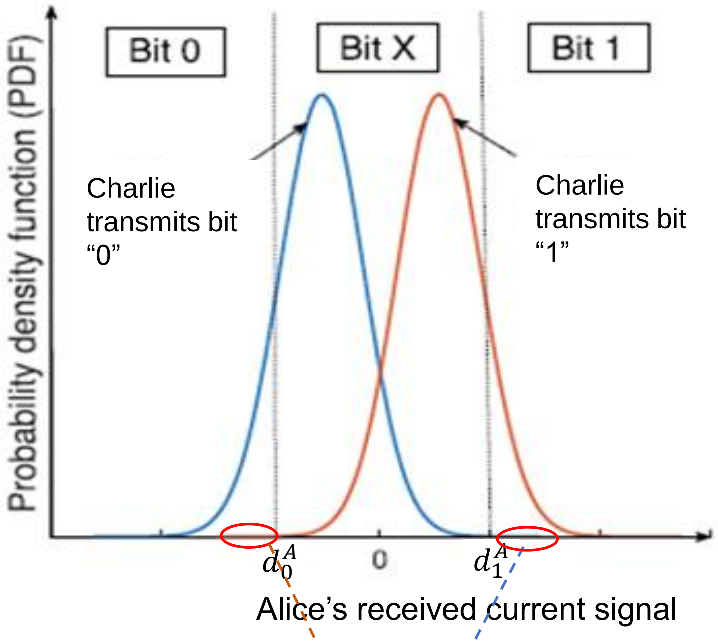
- Dual-threshold:
  - Determined by adjusting dual-threshold scale coefficient (ς_A)

$\varsigma_A \uparrow$ => $d_0^A \downarrow$ & $d_1^A \uparrow$ => $P_{CA}^{\text{sift}} \downarrow$, $P_{CA}^{\text{error}} \downarrow$

$\varsigma_A \downarrow$ => $d_0^A \uparrow$ & $d_1^A \downarrow$ => $P_{CA}^{\text{sift}} \uparrow$, $P_{CA}^{\text{error}} \uparrow$



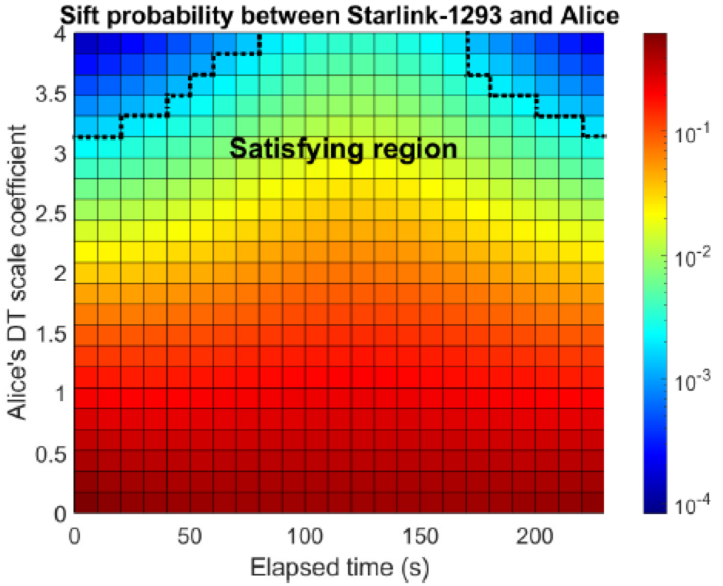
P_{CA}^{sift} between Charlie and Alice



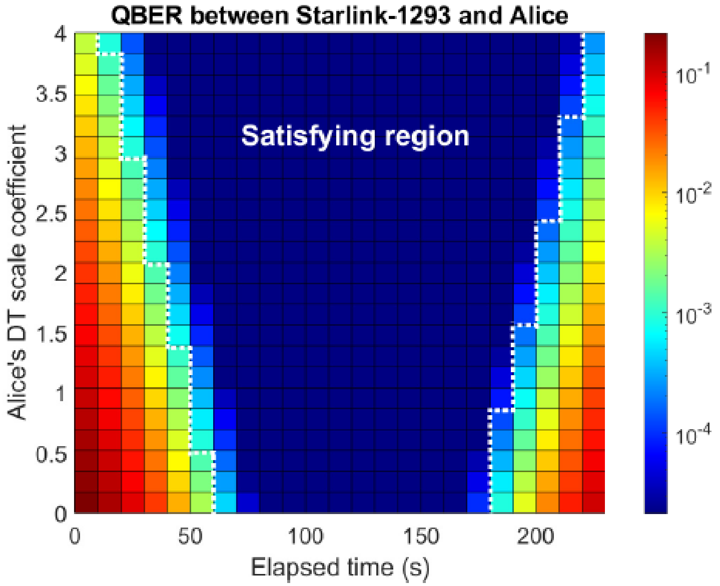
P_{CA}^{error} between Charlie and Alice

3.1.7. Alice's Design: Dual-Threshold Setting (2)

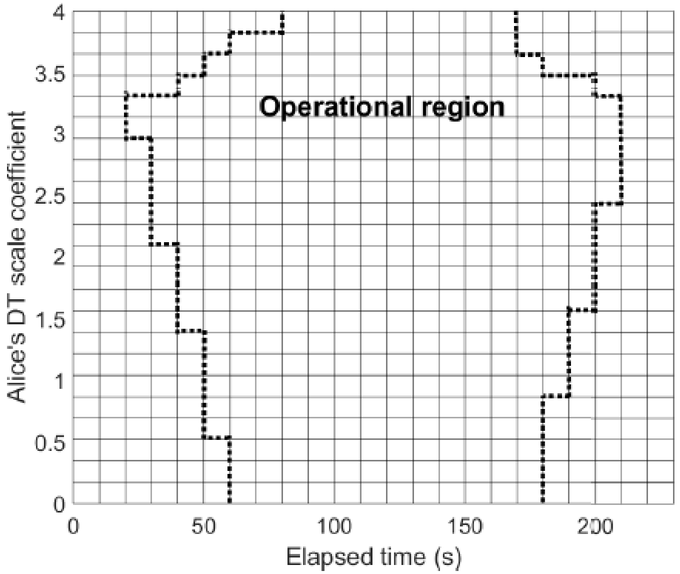
- Our main target is to control
  - P_{sift} between Charlie and Alice needs to be at least 10^{-3} → Alice receives sufficient information
  - QBER between Charlie and Alice needs to be less than 10^{-3} → Errors can be efficiently corrected



(a) $P_{\text{sift}} \geq 10^{-3}$



(b) QBER$\leq 10^{-3}$



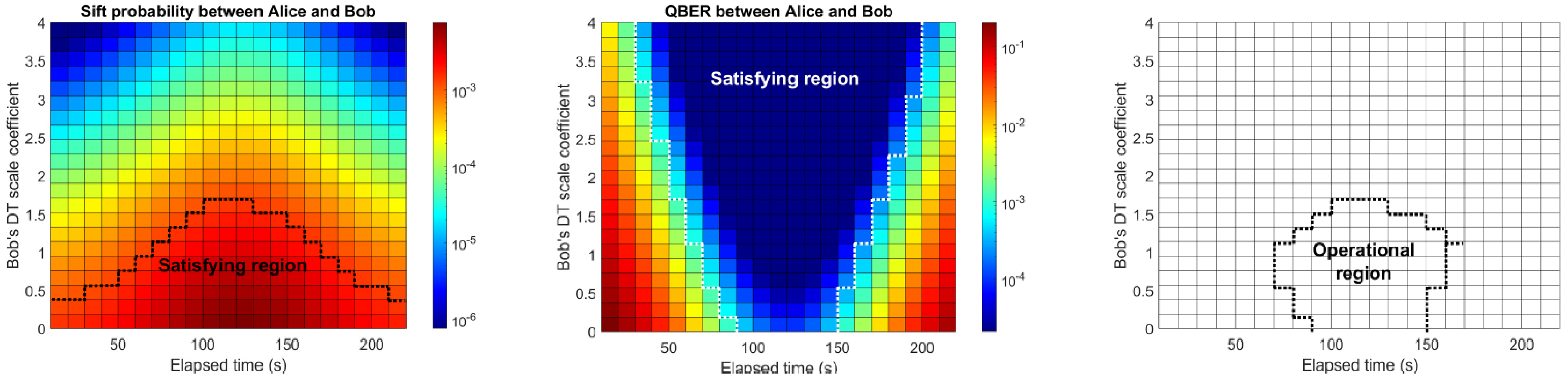
(c) $P_{\text{sift}} \geq 10^{-3}$, QBER$\leq 10^{-3}$

3.1.8. Bob's Design: Dual-Threshold Setting

P_{sift} between Alice and Bob: the probability that both Alice & Bob are able to decode bits using DT

QBER between Alice & Bob: the fraction of the probability that the detected bits at Alice & Bob are not the same and P_{sift} between Alice and Bob

- Alice & Bob can operate when
  - P_{sift} between Alice and Bob needs to be at least 10^{-3} → Alice & Bob receive sufficient information
  - QBER between Alice and Bob needs to be less than 10^{-3} → Errors can be efficiently corrected

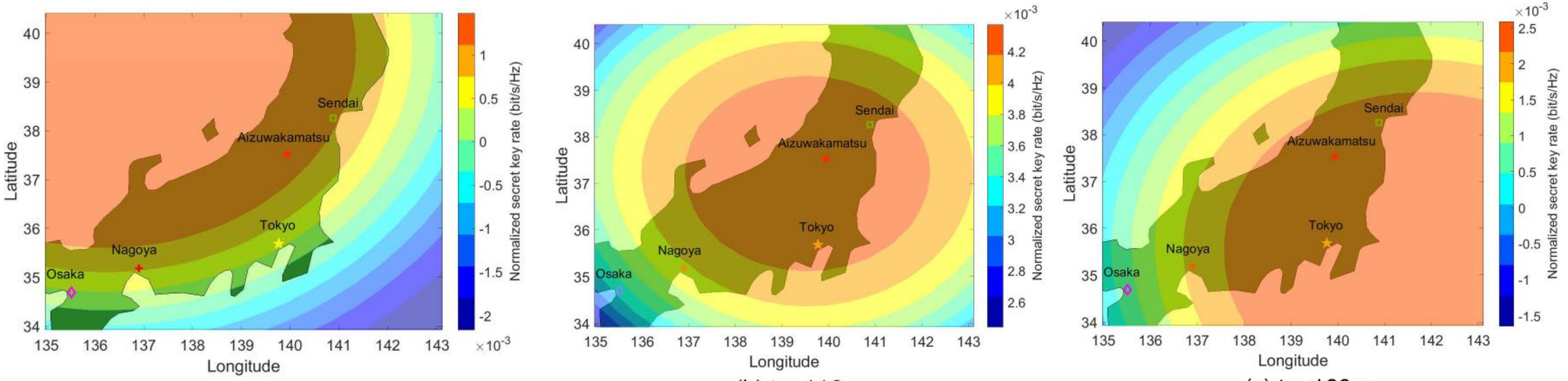


(a) $P_{sift} \geq 10^{-3}$ (b) QBER$\leq 10^{-3}$ (c) $P_{sift} \geq 10^{-3}$, QBER$\leq 10^{-3}$

P_{sift} and QBER between Alice and Bob versus Bob's DT scale coefficient and the elapsed time in seconds with $\varsigma_A = 3$

3.1.9. Secret Key Rate Performance

- The spatial distribution of normalized secret key rate (SKR) of the proposed system



(a) t = 60 s

(b) t = 116 s

(c) t = 160 s

The time that Alice and Bob start receiving secret keys via the quantum channel

The time that the elevation angle between Alice and the satellite is maximum (i.e., the shortest slant path between Alice and the satellite)

The time that the key transmission over the quantum channel from the satellite terminates

3.2. Satellite-Based FSO/QKD Systems using GEO/LEOs for Multiple Wireless Users

The content of this contribution was published in

[C2] Minh Q. Vu *et al.,* “A proposal of satellite-based FSO/QKD system for multiple wireless users,” IEICE International Conference on Emerging Technologies for Communications (ICETC), Waseda, Japan, Nov. 2022.

[J2] Minh Q. Vu *et al.,* “Entanglement-based FSO/QKD systems using GEO/LEOs for multiple users,” in IEEE Photonics Journal, Accepted with Minor Revisions

3.2.1. Motivation for Two-layer GEO/LEO Satellite FSO/QKD

- LEO satellite: limited coverage and flyover time

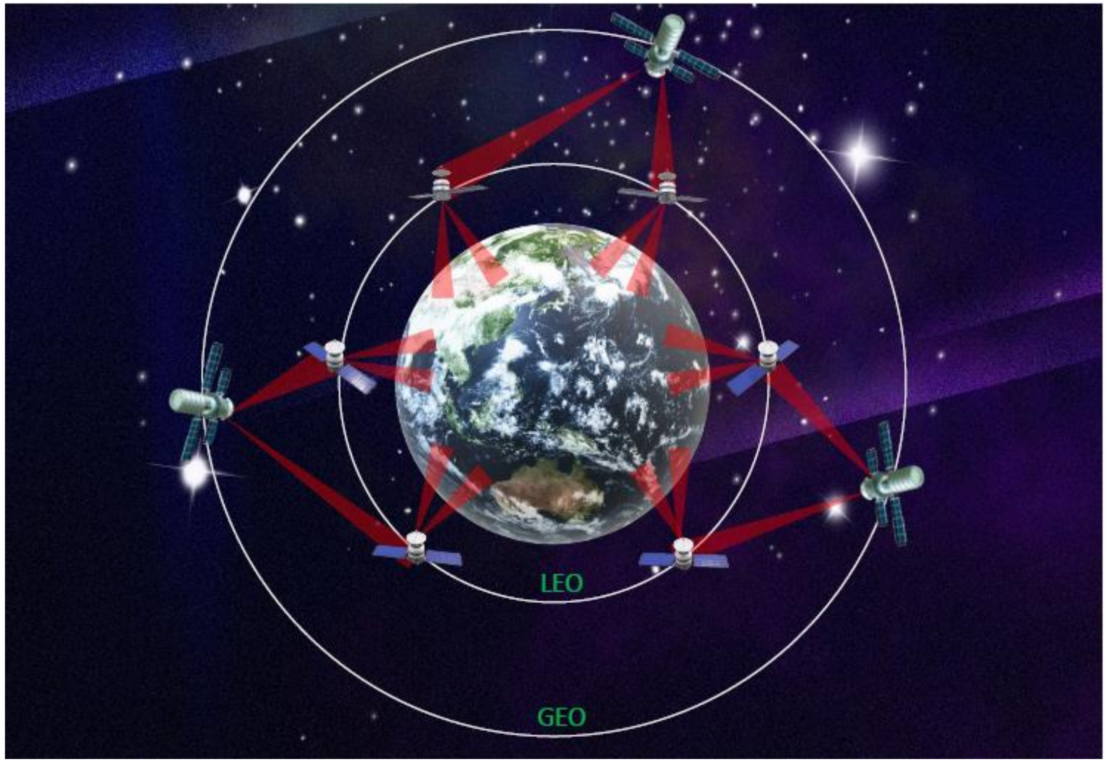
→ Establishing the constellation of LEO satellites

- Nevertheless, the key relaying/routing in the network among LEO satellites

→ New security concerns while QKD is performed for two distant ground stations

- GEO satellites: a broad coverage, accessing ground stations continuously.
    - However, the signal can suffer from high channel loss and limited key generation rates

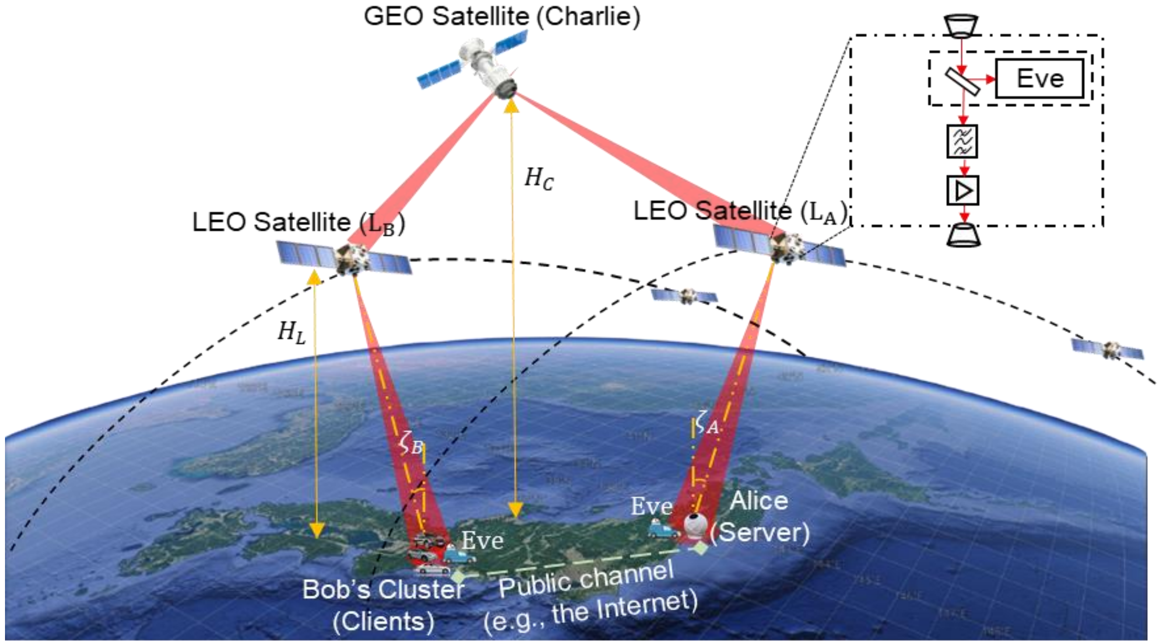
→ **Combining both GEO and LEO satellites** to build QKD networks is a research direction worth exploring

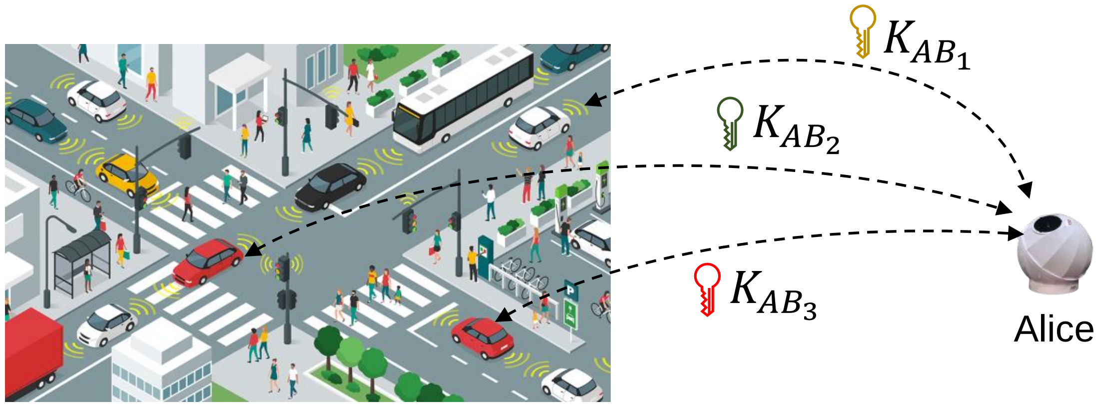


A global-scale QKD network
using LEO satellite and GEO satellites

3.2.2. Considered scenario of satellite FSO/QKD Systems using GEO/LEOs

- GEO satellite (Charlie): a key source
  - ❑ H_c: the altitude of Charlie
- LEO satellites (L_A and L_B): relay nodes (optical amplify and forward)
  - ❑ H_c: the altitude of Charlie
- Alice: a server that agrees on the secret key with each user Bob_i
- Bob's cluster: multiple legitimate users Bob_i
- Eve: eavesdroppers
- Channel model:
  - ❑ GEO-LEO: geometric spreading loss
  - ❑ LEO-users: geometric spreading loss, atmospheric attenuation, and atmospheric turbulence-induced fading



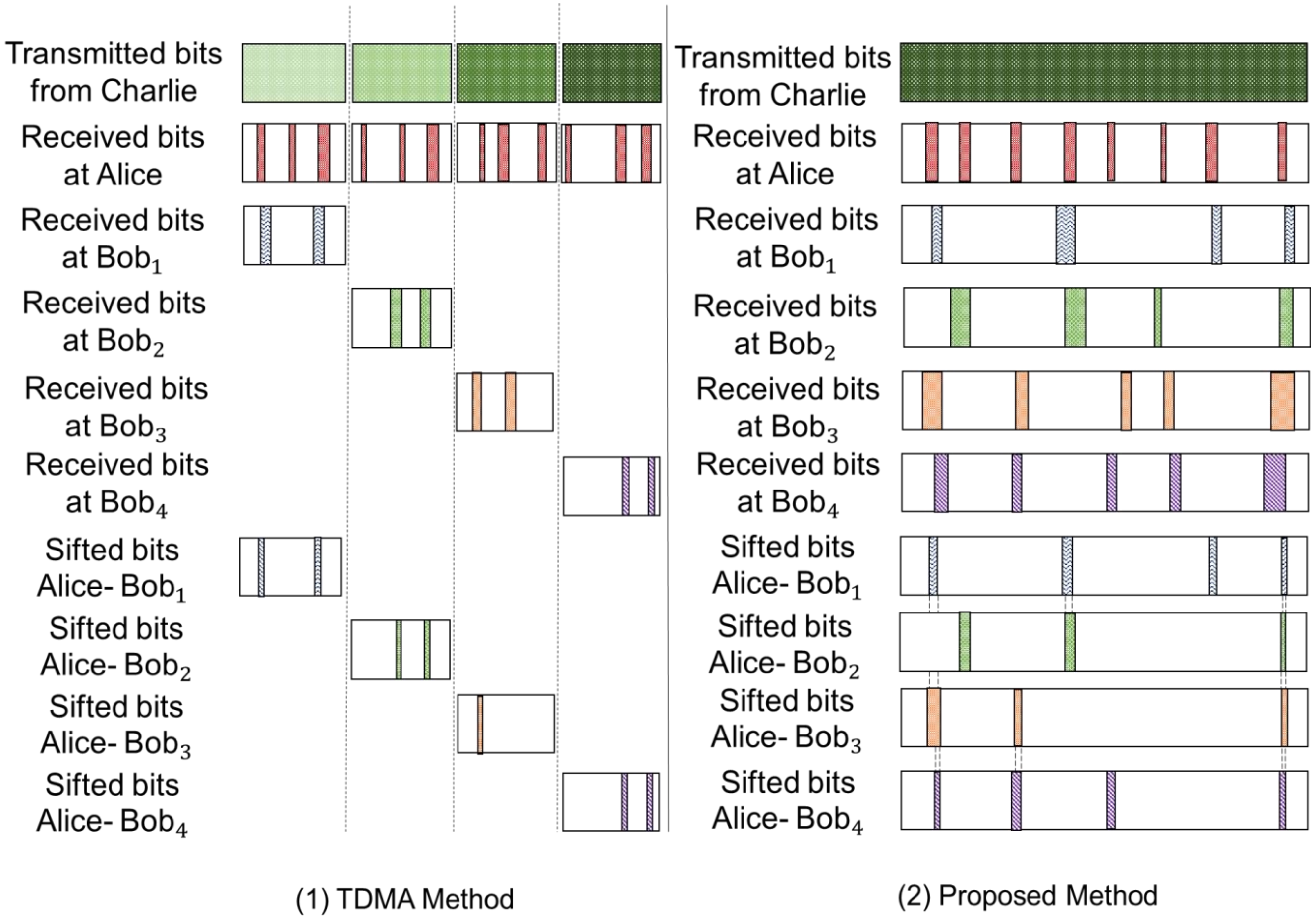


3.2.3. Multiple Access Method

- TDMA:
  - Charlie sends the signal to each user Bob_i within specified time slots
  - Alice and each user Bob_i receive independent binary bit sequences from Charlie

  → The key rate will be decreased proportionally to the number of users

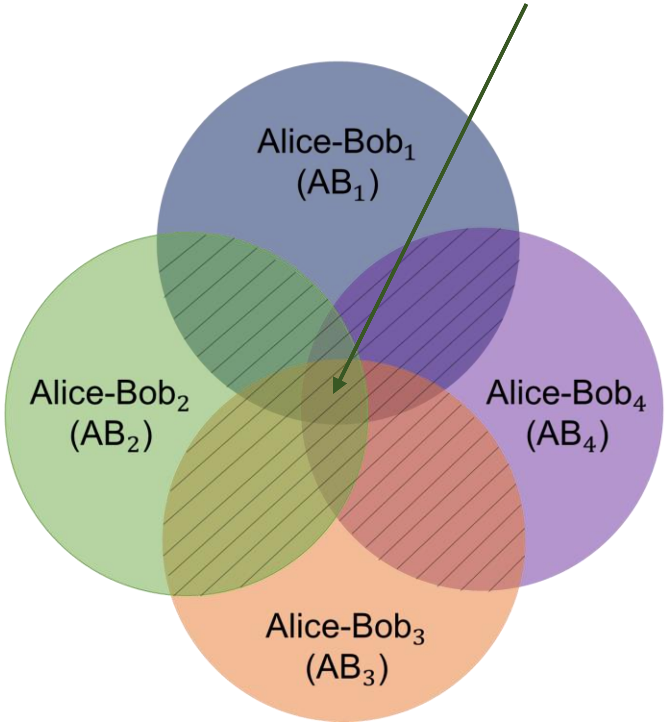
- Proposed method:
  - Charlie send the same bit sequence to Alice and all users Bob_i
  - We expect each pair of Alice and Bob to achieve a secret key with a minimum, unknown overlapped with others



Time Division Multiplexing Access (TDMA) vs. the proposed method for key distribution with the number of users at Bob's site = 4

3.2.4. Sift Probability

The overlapping region: shows the probabilities that Alice, Bob_i, and Bob_j, $j≠i$, $j \in \{1, 2, 3, 4\}$ can decode bits at the same time instant



Visualization for the relationship of sift probabilities between Alice and Bob_i , $i \in \{1, 2, 3, 4\}$

- In TDMA system:

$$P_{AB_i}^{\text{sift}} = P_{AB_i}(0,0) + P_{AB_i}(0,1) + P_{AB_i}(1,0) + P_{AB_i}(1,1)$$

$P_{AB_i}(x, y)$ with $(x, y) \in \{0,1\}$: the probability that Alice's detected bit "x" coincides with Bob's detected bit "y"

- In the proposed system:

$$P_{AB_i}^{\text{sift}-\text{excl}} = P_{AB_i}^{\text{sift}} - \varepsilon P_{AB_i}^{\text{excl}}$$

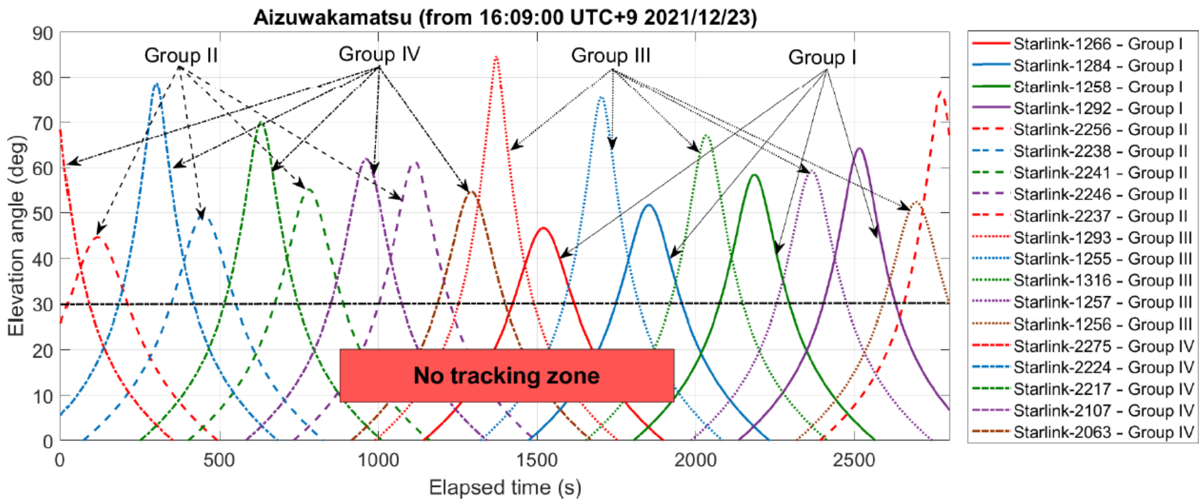
$P_{AB_i}^{\text{excl}}$: the mutual sift probability with other users Bob_j

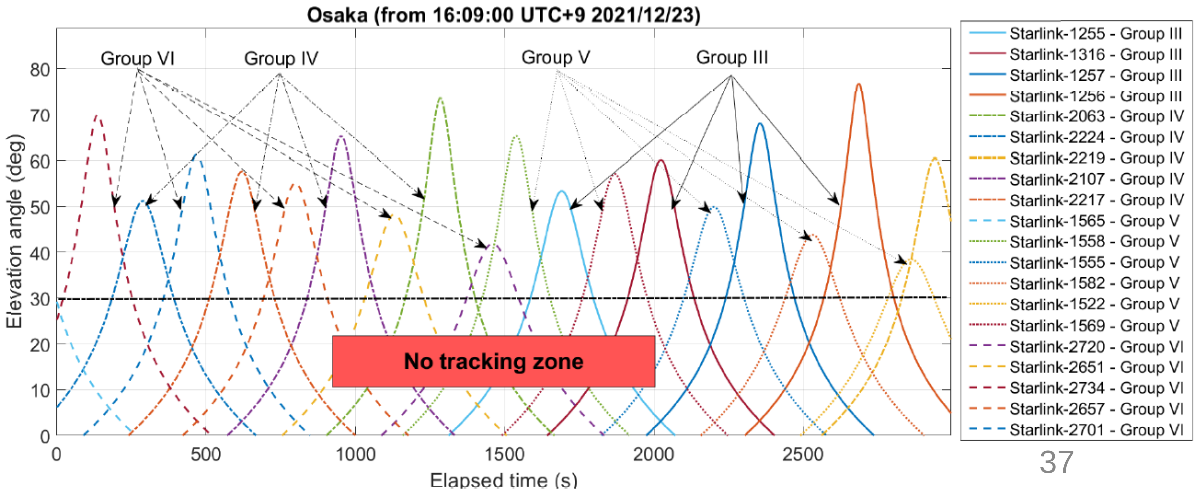
$$P_{AB_i}^{\text{excl}} = \sum_{j\neq i,1\leq j\leq N} P(AB_i \cap AB_j) + \sum_{j_1\neq j_2\neq i,1\leq j_1\leq j_2\leq N} P\left(AB_i \cap AB_{j_1} \cap AB_{j_2}\right) + \cdots + (-1)^{N+1} P\left(\bigcap_{i=1}^{N} AB_i\right)$$

ε: the exclusion ratio coefficient

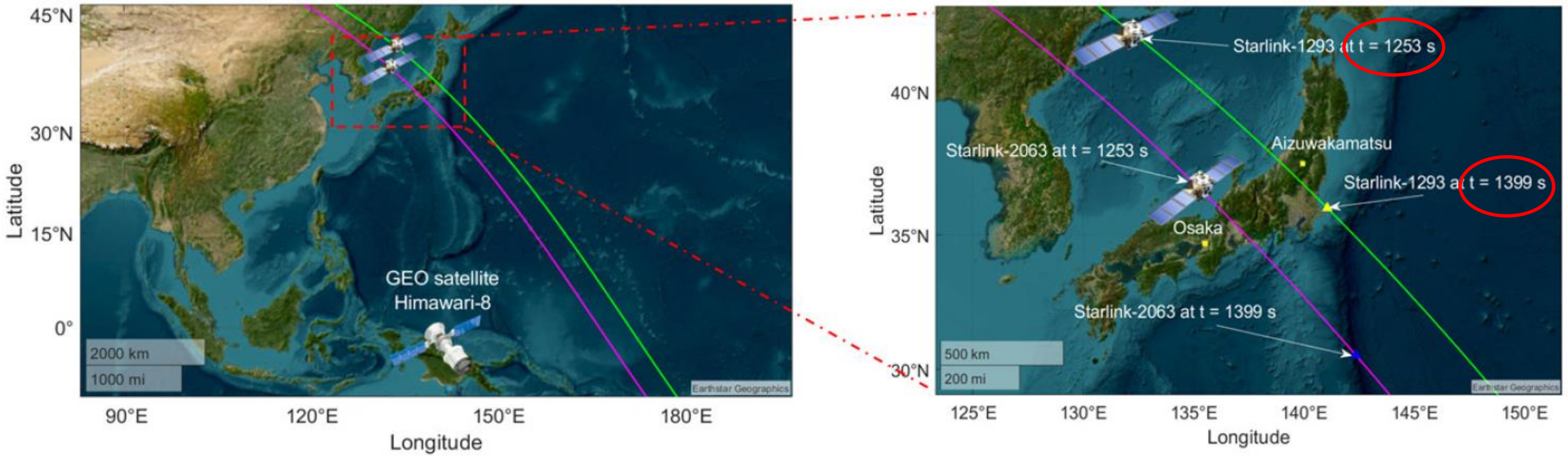
3.2.5. Practical Satellite Selections (1)

- We investigate the feasibility of our proposed satellite-QKD system in a case study for Japan QKD network using the existing Starlink LEO satellite constellation and a GEO satellite
  - A GEO satellite (Himawari-8) play a role as Charlie
  - LEO satellites in the Starlink constellation play a role as relay nodes
  - These satellites are supposed to equip with optical transmitters for FSO downlink transmission
  - Alice is assumed to locate in Aizuwakamatsu City, Fukushima, Japan
  - Multiple users Bob_i are assumed to locate in Osaka City, Japan





3.2.5. Practical Satellite Selections (2)



Position of GEO satellite on the Earth's surface and ground traces of LEO satellites over Japan observed from 16:09:00 UTC+9 2021/12/23

- To implement EB two-layer satellite FSO/QKD to distribute shared secret keys between Alice and multiple users Bob$_i$ in the considered scenario, there are **two requirements**
  - GEO satellite can always stay connected to LEO satellites of Starlink constellation over Japan
  - We can always choose two LEO satellites that can observe respective users located in Aizuwakamatsu City and Osaka City simultaneously
- Two LEO satellites, Starlink-1293 and Starlink-2063, are considered as the representative relay nodes to send signal to Alice and Bob$_i$, respectively (from t = 1253 s to t = 1399 s after 16:09:00 UTC+9, Dec. 23, 2021).

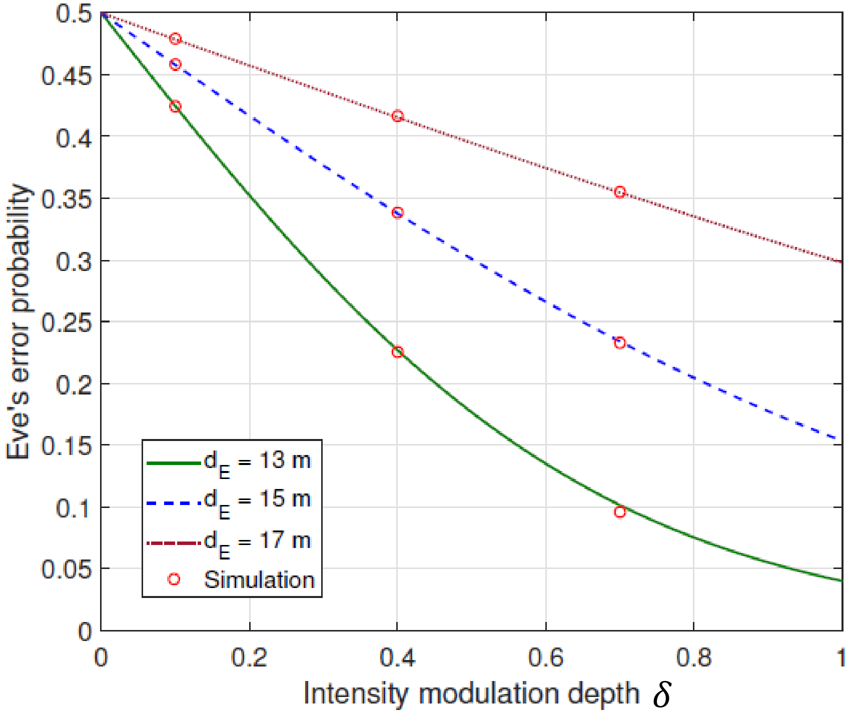
System Parameters

Name	Symbol	Value
GEO Satellite (Charlie)		
Wavelength	λ	1550 nm
Bit rate	R_b	1 Gbps
Altitude	H_C	35793 km
Divergence angle	θ_C	10 μrad
Transmitted power	P	32 dBm
LEO Satellites (Relay nodes)		
Wavelength	λ	1550 nm
Altitude	H_L	550 km
Divergence angle	θ_L	50 μrad
Receiving aperture radius	a_L	10 cm
EDFA Gain	G_a	40 dB
ASE Parameter	n_{sp}	5

Name	Symbol	Value
FSO Channel		
Sun's spectral irradiance from above the atmosphere at 1550 nm	Ω_l	0.1 $\mathrm{W/cm^2 \cdot \mu m}$
Sun's spectral irradiance from above the Earth at 1550 nm	Ω_r	0.005 $\mathrm{W/cm^2 \cdot \mu m}$
Wind speed	w	21 m/s
The refractive index structure parameter at the ground level	$C_n^2(0)$	$10^{-15}\mathrm{m}^{-2/3}$
Visibility (Clear weather condition)	V	30 km
Alice/Bob/Eve		
Altitude	H_U	2 m
Receiving aperture radius	a_U	5 cm
Optical bandwidth	B_0	250 GHz
Responsivity	R_e	0.9 A/W
Effective noise bandwidth	Δf	0.5 GHz
Temperature	T	298 K
Load resistor	R_L	1 kΩ
Amplifier noise figure	F_n	2

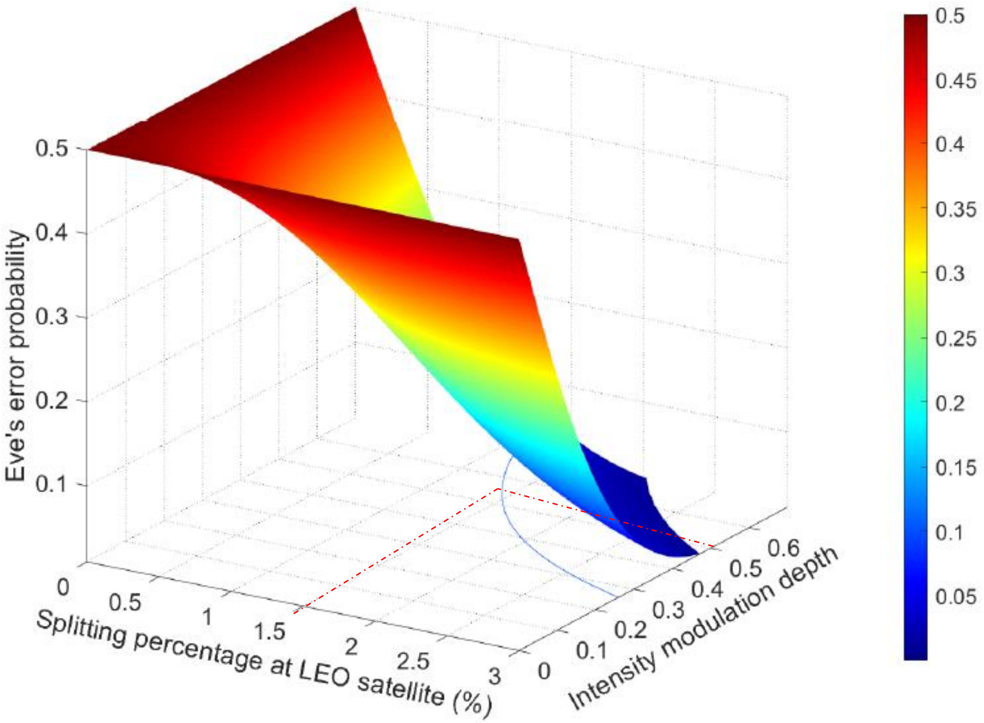
3.2.6. Charlie's Design

Unauthorized Receiver Attack (URA)



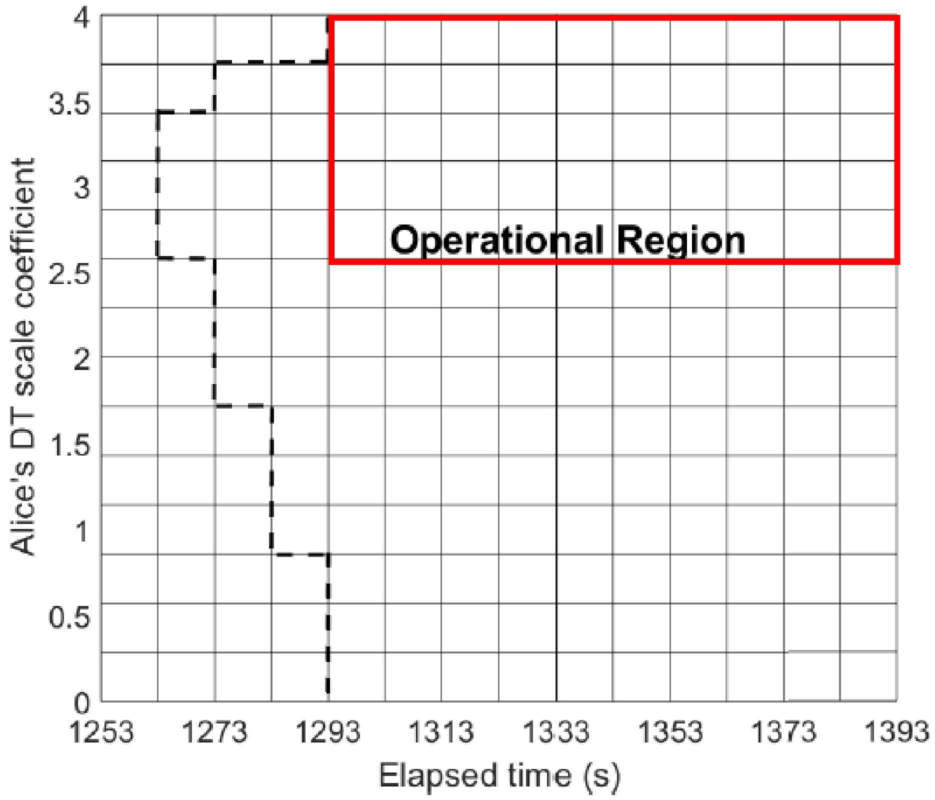
Eve's error probability versus intensity modulation depth

Beam Splitting Attack (BSA) at LEO satellite

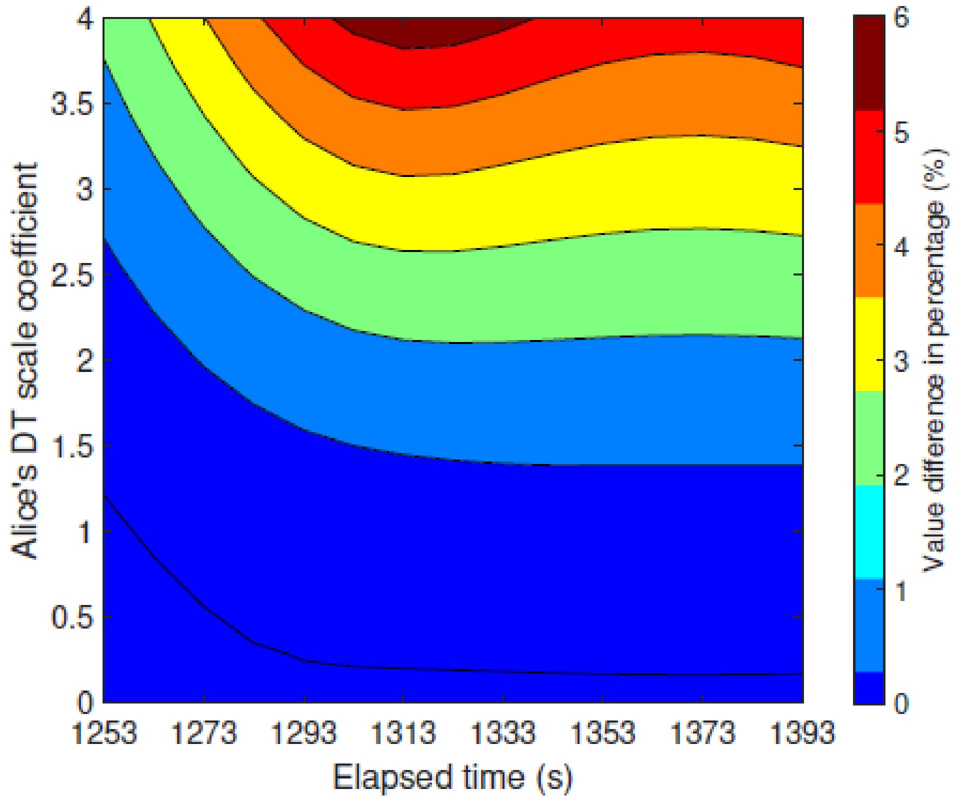


Eve's error probability versus splitting percentage (SP) at LEO satellites

3.2.7. Alice's Design

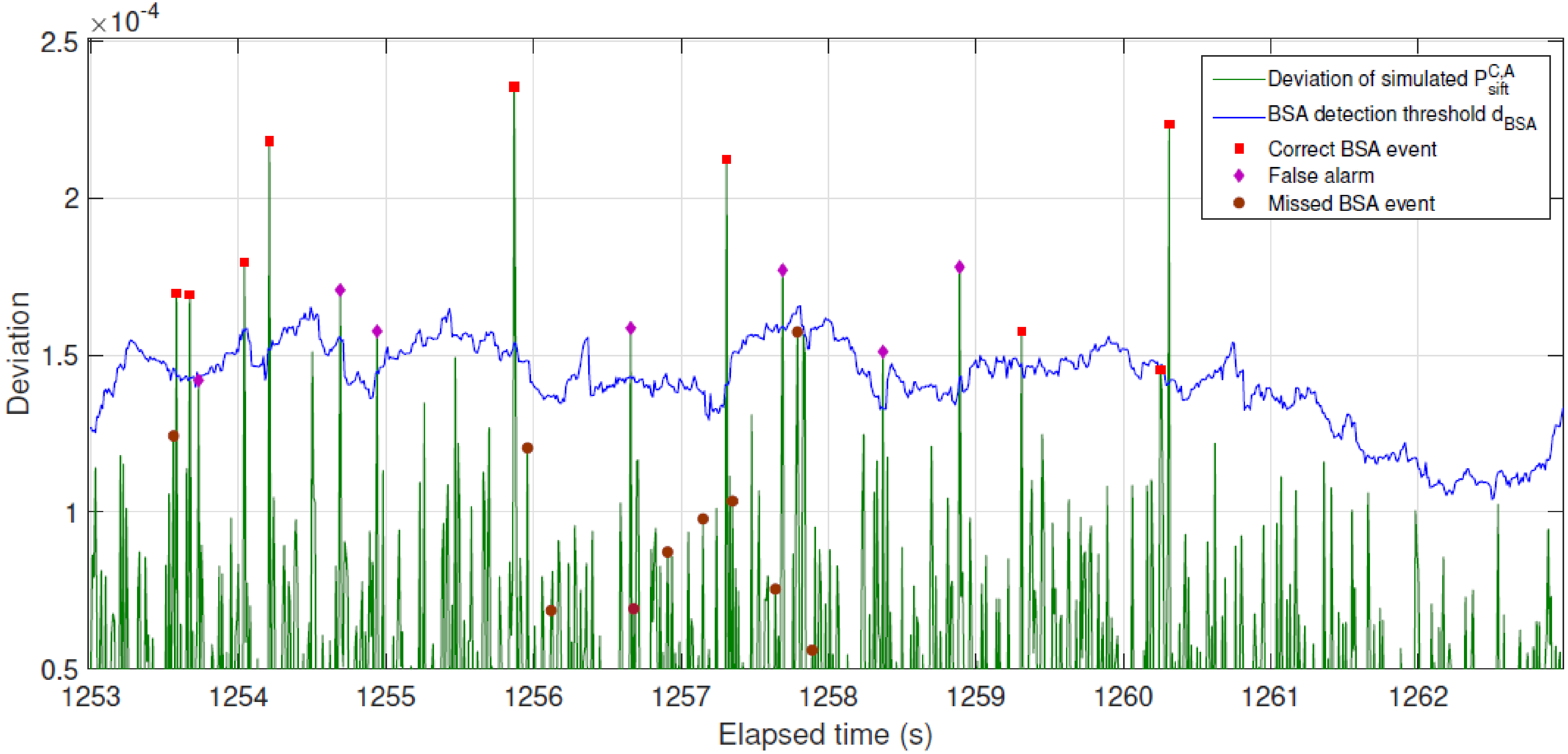


$P_{\text{sift}} \geq 10^{-3}$, QBER$\leq 10^{-3}$



The value difference in the sift probability between Alice and Charlie in the case that no BSA and BSA are performed by L_A , SP = 1.5 %

3.2.8. Beam Splitting Attack Detection (1)

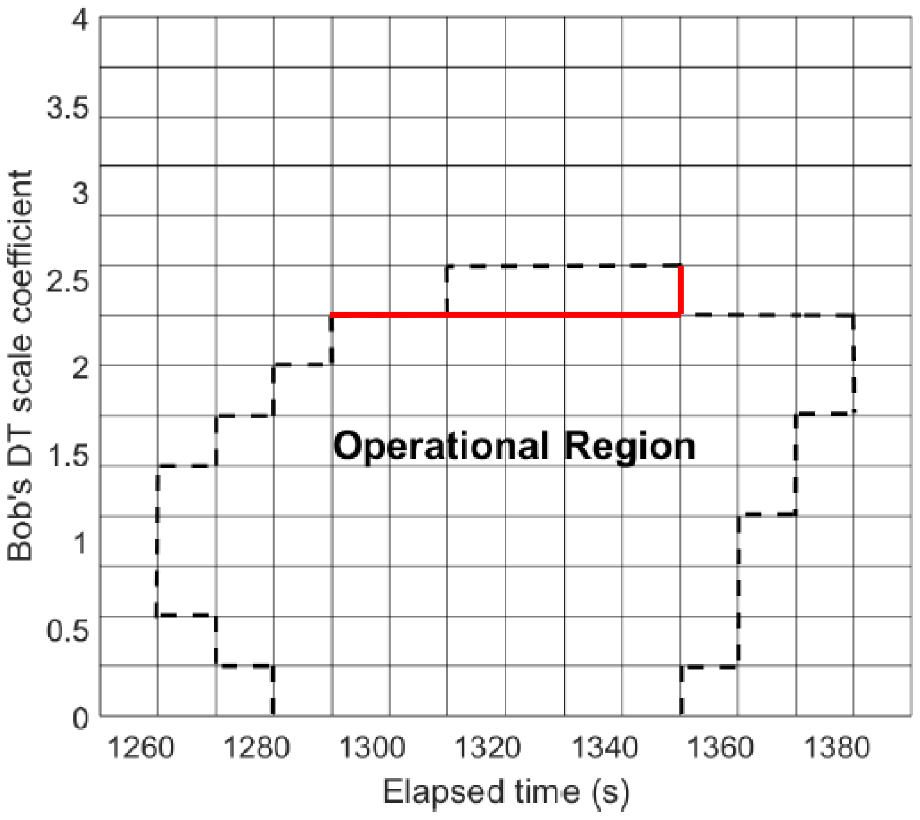


BSA detection by comparing the deviation of simulated sift probability between Alice and Charlie with the threshold d_{BSA}= 2.25σ_{sd}

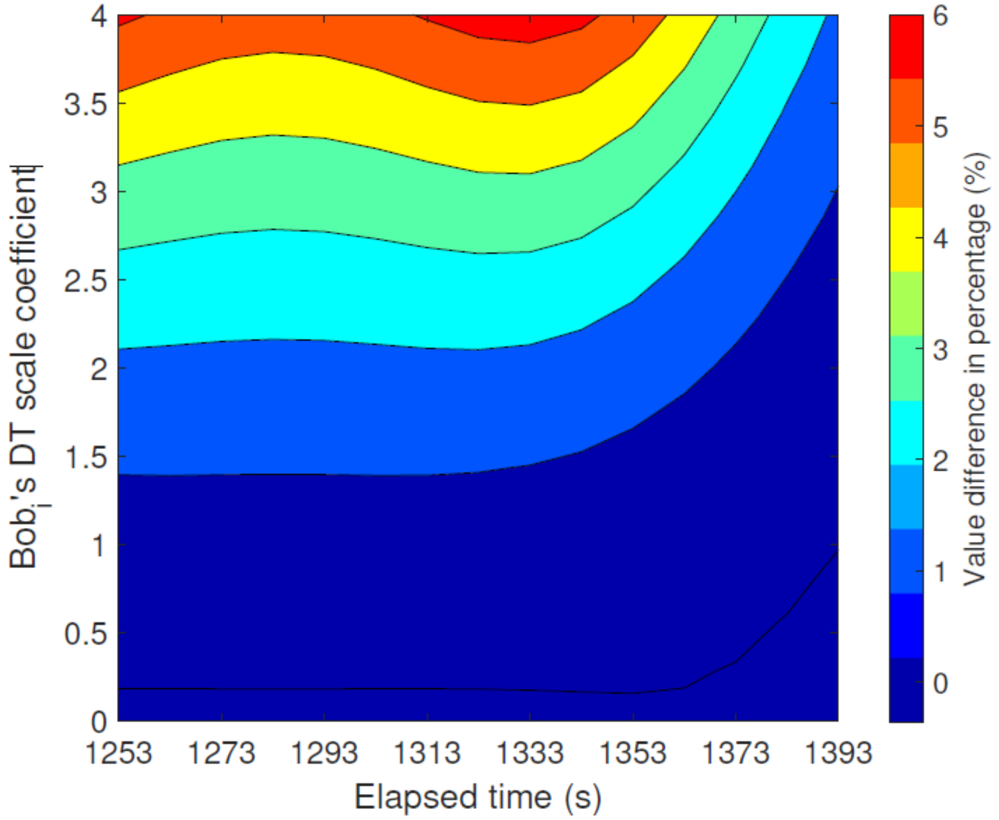
3.2.8. Beam Splitting Attack Detection (2)

Difference in $P_{\text{sift}}^{C,A}$ between no BSA and BSA	No. of actual BSA events	No. of probable BSA events	No. of correct BSA events	Percentage of correct detection (w.r.t No. of actual BSA events)	Percentage of correct detection (w.r.t No. of probable BSA events)	No. of false alarms	Percentage of false alarms (w.r.t No. of probable BSA events)
$d_{\text{BSA}} = 2\sigma_{\text{sd}}$							
1.1%-1.5%	19	21	13	68.42%	61.9%	8	31.9%
1.5%-1.8%	15	20	9	60%	45%	11	55%
1.8%-2%	12	24	12	100%	50%	12	50%
2%-2.4%	14	16	14	100%	87.5%	2	12.5%
$d_{\text{BSA}} = 2.25\sigma_{\text{sd}}$							
1.1%-1.5%	19	16	9	47.37%	56.25%	7	43.75%
1.5%-1.8%	15	12	8	53.33%	66.67%	4	33.33%
1.8%-2%	12	17	12	100%	70.59%	5	29.41%
2%-2.4%	14	15	14	100%	93.33%	1	0.67%
$d_{\text{BSA}} = 2.5\sigma_{\text{sd}}$							
1.1%-1.5%	19	11	8	42.1%	72.73%	3	27.27%
1.5%-1.8%	15	7	6	40%	85.71%	1	14.29%
1.8%-2%	12	11	10	83.33%	90.91%	1	9.09%
2%-2.4%	14	14	14	100%	100%	0	0%
$d_{\text{BSA}} = 2.75\sigma_{\text{sd}}$							
1.1%-1.5%	19	5	4	21.05%	80%	1	20%
1.5%-1.8%	15	6	6	40%	100%	0	0%
1.8%-2%	12	9	9	75%	100%	0	0%
2%-2.4%	14	14	14	100%	100%	0	0%
$d_{\text{BSA}} = 3\sigma_{\text{sd}}$							
1.1%-1.5%	19	4	4	21.05%	100%	0	0%
1.5%-1.8%	15	5	5	33.33%	100%	0	0%
1.8%-2%	12	7	7	58.33%	100%	0	0%
2%-2.4%	14	14	14	100%	100%	0	0%

3.2.9. Bob's Design



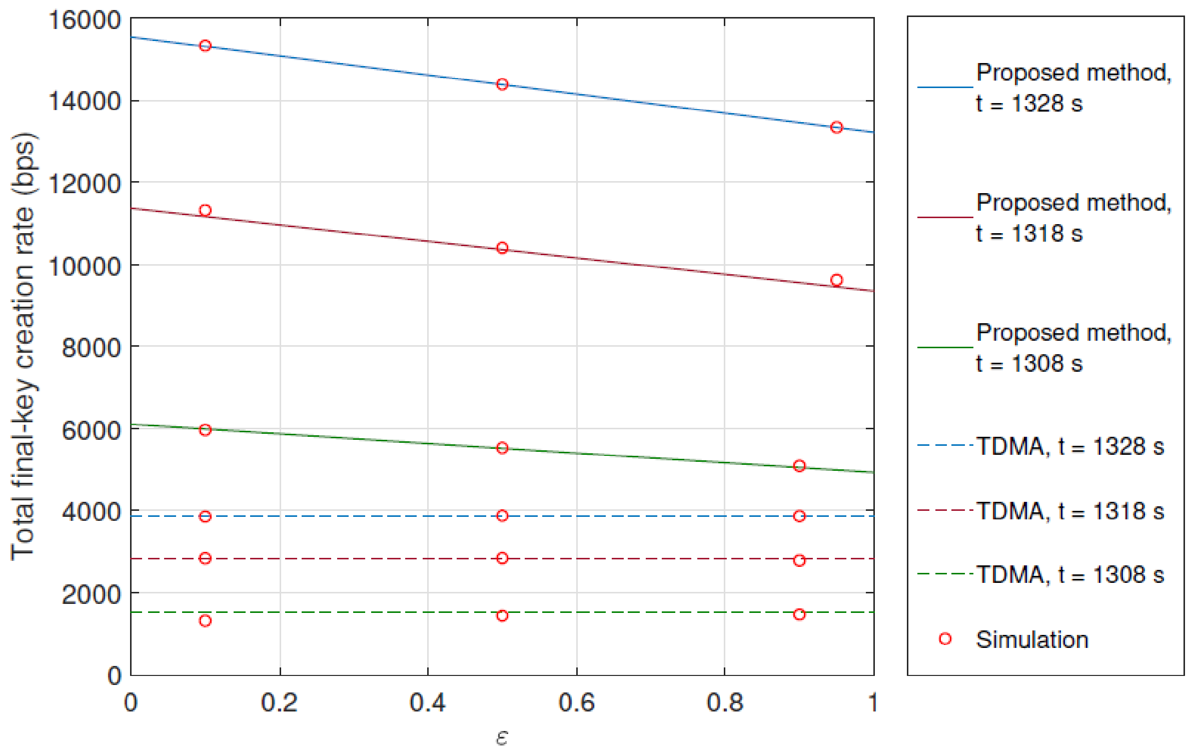
$P_{\text{sift}} \geq 10^{-3}$, QBER$\leq 10^{-3}$



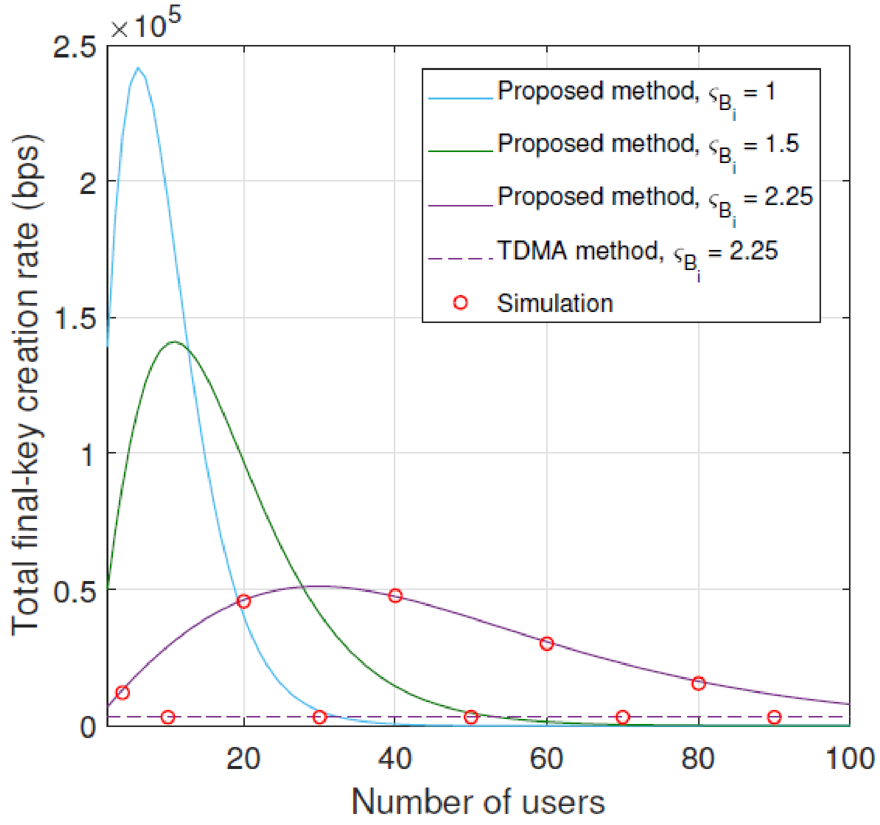
The value difference in the sift probability between Alice and Bob in the case that no BSA and BSA are performed by L_B , SP = 1.5 %

3.2.10. Secret Key Performance

- Total final-key creation rate



Total final-key creation rate versus the exclusion ratio coefficient with N = 4: Proposed method versus TDMA method. ς_{B_i}= 2.25.



Total final-key creation rate versus the number of users at Bob's cluster

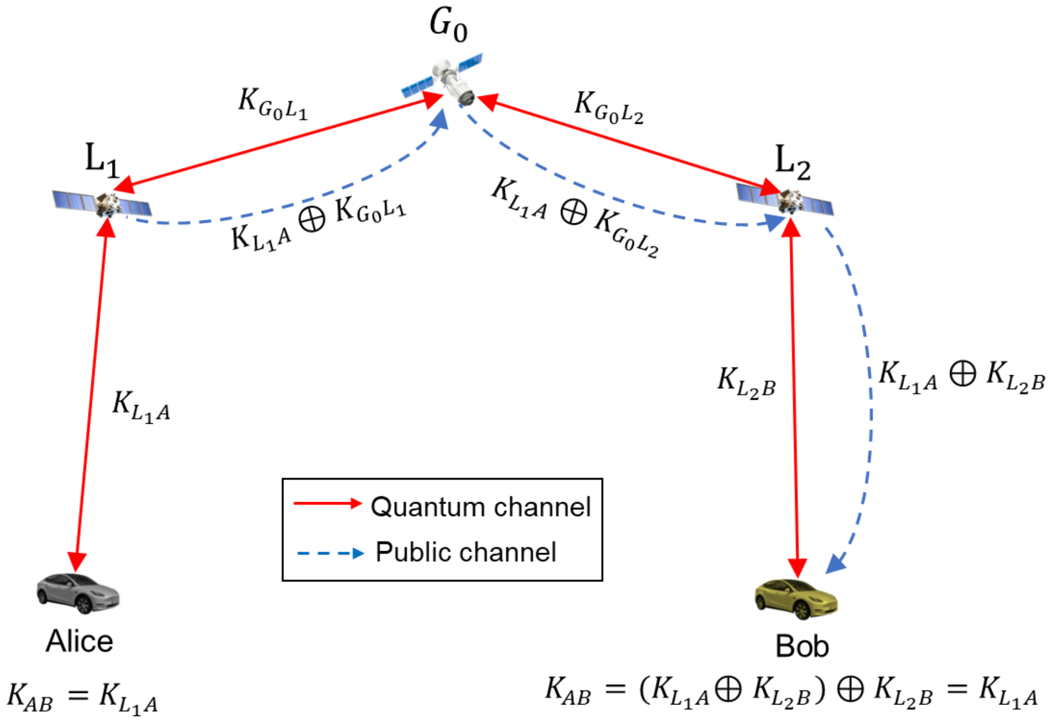
3.3. Network Coding aided Hybrid EB/PM Satellite FSO/QKD Systems using GEO/LEOs for Multiple Wireless Users

The content of this contribution was published in

[C3] Minh Q. Vu *et al.,* "Network coding aided hybrid EB/PM satellite-based FSO/QKD systems," International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), Jeju, Korea, Jun. 2023.

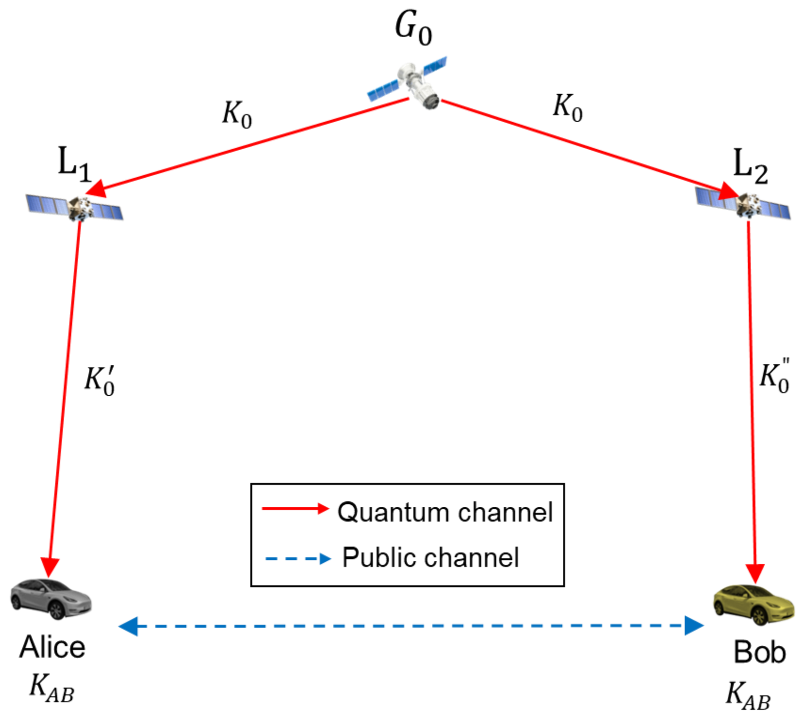
[J3] Minh Q. Vu *et al.,* "Satellite-based quantum key distribution: hybrid EB/PM scheme-assisted multiple users," Prepare for submit in a major journal

3.3.1. PM and EB in Two-layer GEO/LEO Satellite FSO/QKD



Prepare-and-measure (PM) scheme

Many phases are required to distribute the secret key K_{AB}→complexity, inefficient



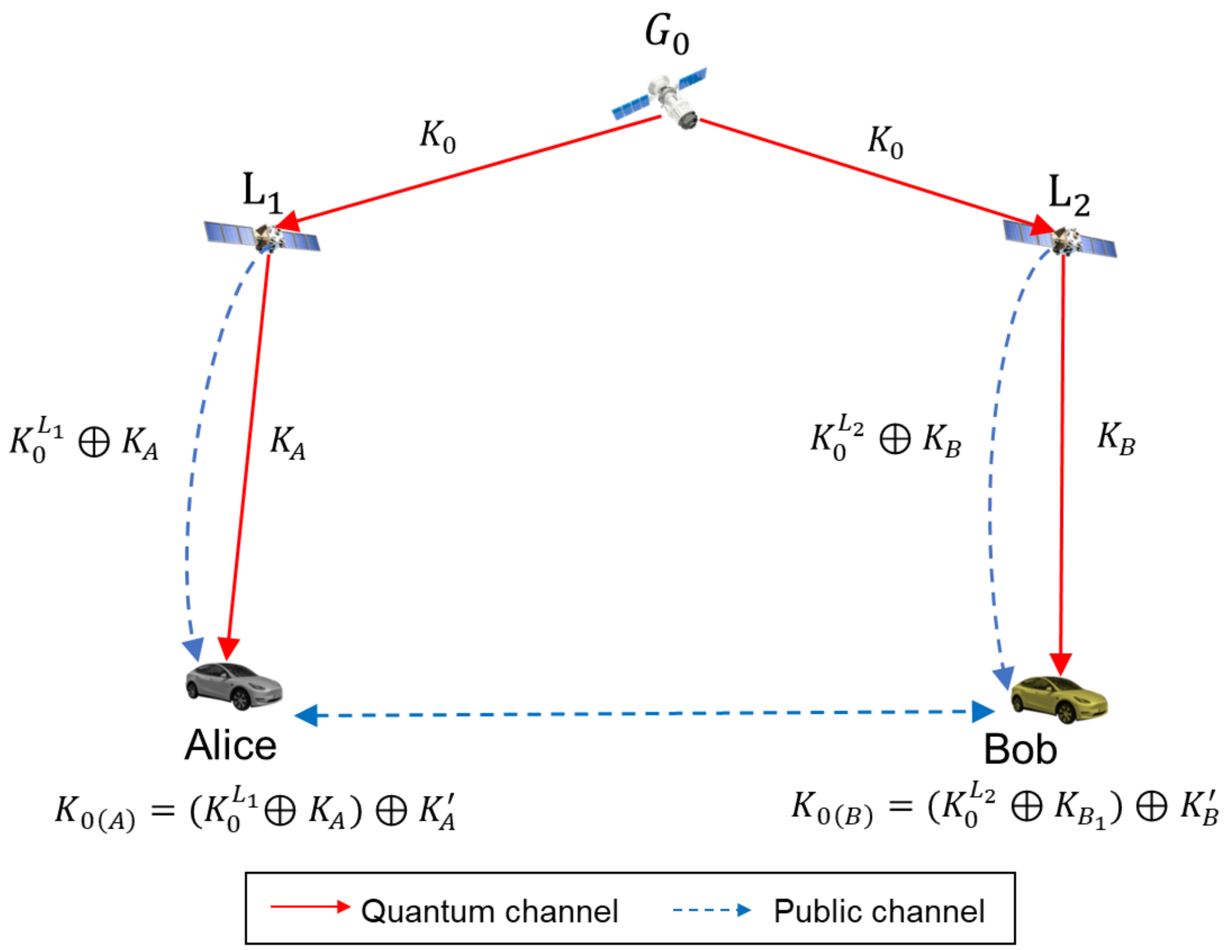
Entanglement-based (EB) scheme

Eavesdroppers may possess information about the keys while performing unauthorized received attack of the signal from LEO satellites

→ Our proposal: Network coding (NC)-aided hybrid EB/PM non-coherent CV satellite FSO/QKD system

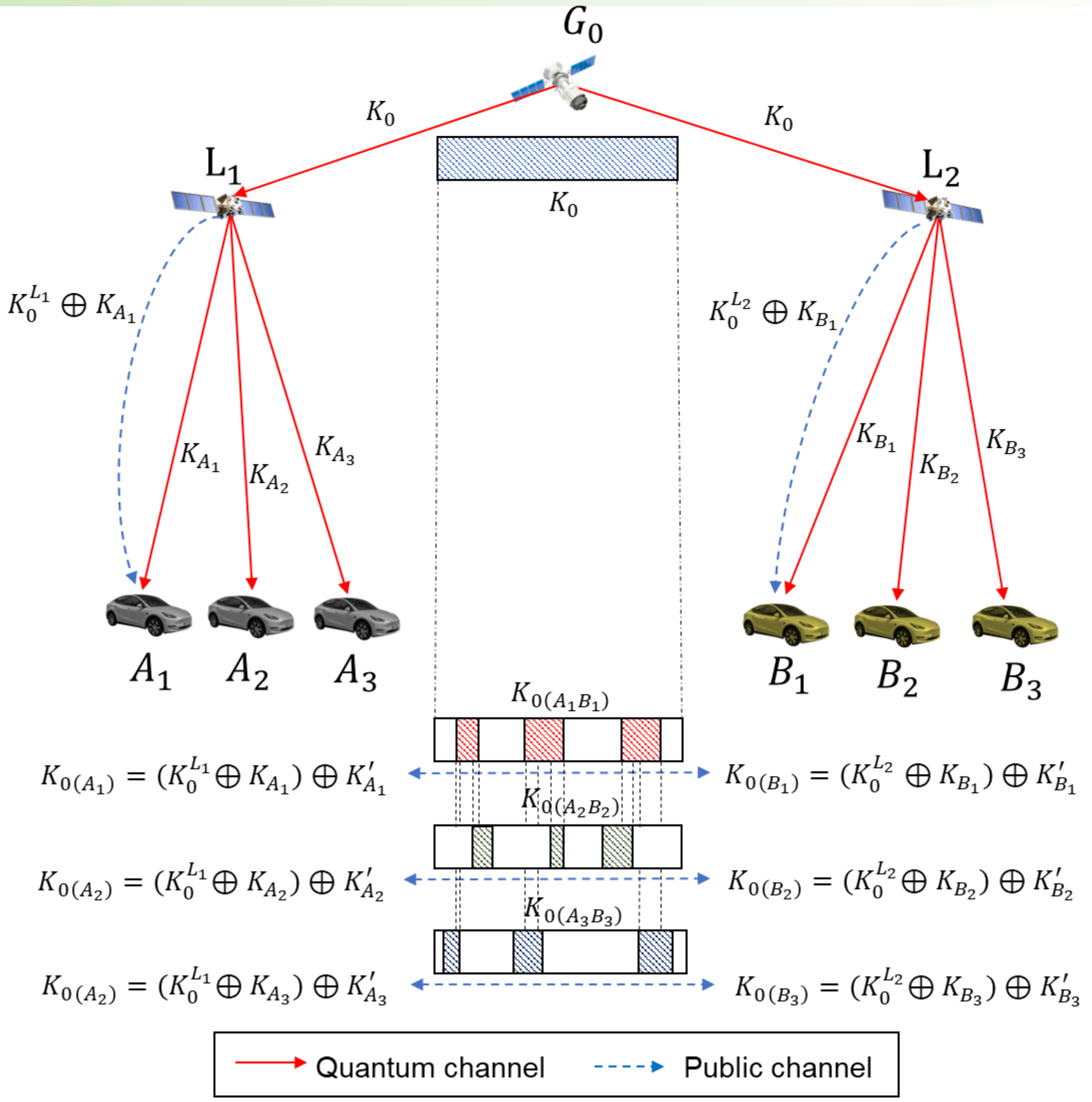
3.3.2. NC aided hybrid EB/PM satellite FSO/QKD systems

- **Stage 1:** EB scheme- GEO and LEO
  - GEO satellite (G_0) distributes K_0 to LEO satellites (L_1&L_2)
  - Using DT/DD receivers, L_1 detects $K_0^{L_1}$, L_2 detects $K_0^{L_2}$
- **Stage 2:** PM scheme- LEO and users
  - L_1 and L_2 distribute K_A and K_B to Alice and Bob
  - Using DT/DD receivers, Alice detects K_A', Bob detect K_B'
- **Stage 3:** Key forwarding & Post-processing
  - L_1 sends $(K_0^{L_1} \oplus K_A)$, L_2 sends $(K_0^{L_2} \oplus K_B)$ via public channel to Alice and Bob (error-free)
  - Alice and Bob decode $(K_0^{L_1} \oplus K_A)$, $(K_0^{L_2} \oplus K_B)$ by performing XOR operation with K_A' and K_B'
  - Sifting process
  - Error correction and privacy amplification



3.3.3. NC-aided hybrid EB/PM satellite FSO/QKD systems: Multiple Users (1)

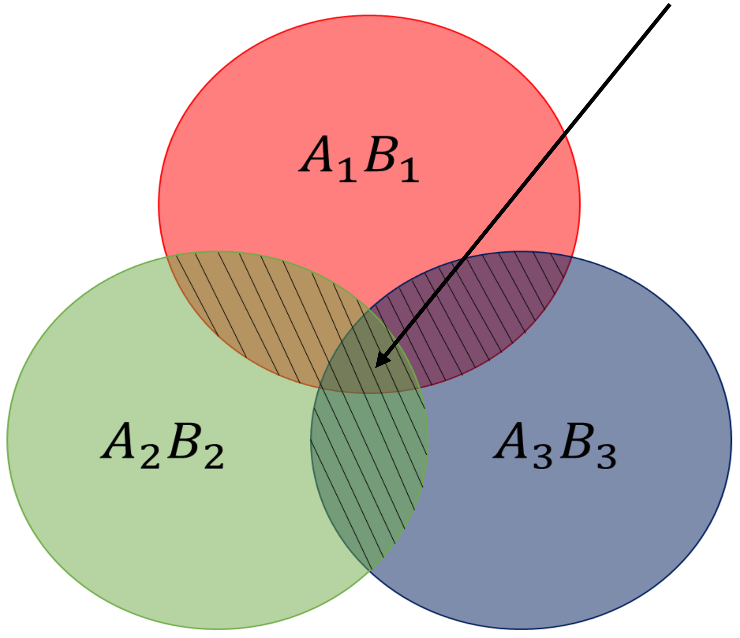
- Scenarios:
  - Multiple users at Alice's side ($A_1, A_2, \ldots$)
  - Multiple users at Bob's side ($B_1, B_2, \ldots$)
  - Each pair of user want to distribute secret keys for their communication session
- Challenging:
  - Distributing secret keys to multiple users at once
  - Each pair should not have the information of other pair's secret key



3.3.3. NC-aided hybrid EB/PM satellite FSO/QKD systems: Multiple Users (2)

- How to exclude the information of other pair's secret key?

The overlapping region: shows the probabilities that Alice_j, Bob_k decode bits at the same time instant



Visualization for the relationship of sift probabilities between Alice_j and Bob_k

$$P_{A_jB_k}^{\mathrm{sift-excl}} = P_{A_jB_k}^{\mathrm{sift}} - \varepsilon P_{A_jB_k}^{\mathrm{excl}}$$

$P_{A_jB_k}^{\mathrm{excl}}$: the mutual sift probability with other pair of users $\mathrm{A}_j\mathrm{B}_k$

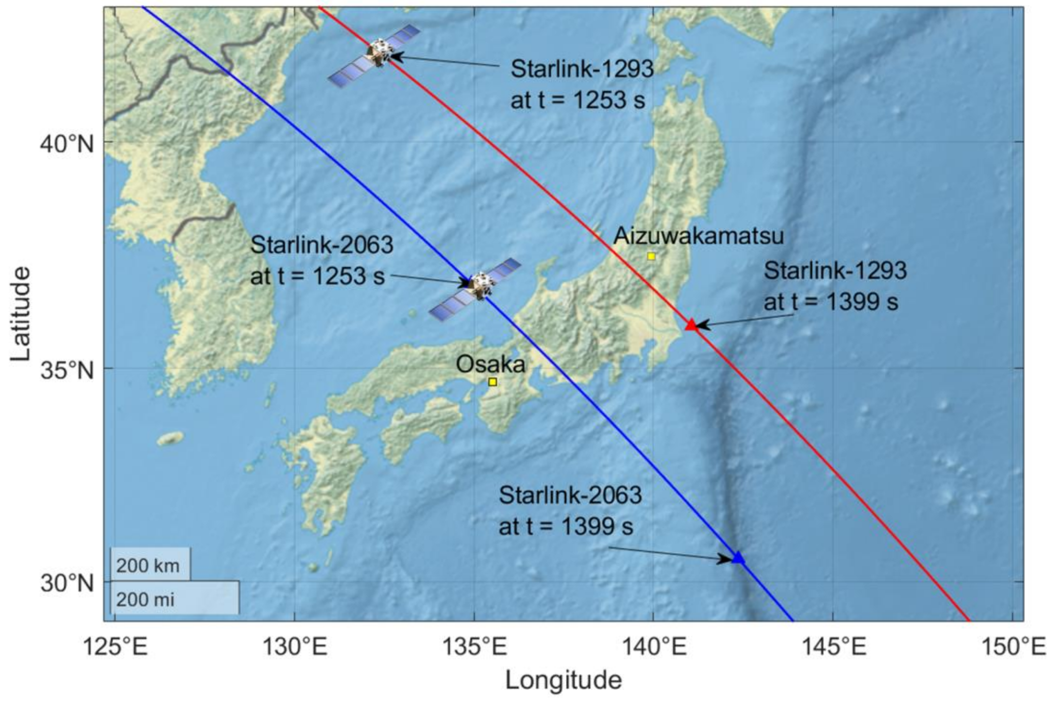
$$P_{AB_i}^{\mathrm{excl}} = \sum_{1\le j_2,k_2\le N} P(A_jB_k \cap A_{j_2}B_{k_2}) + \sum_{1\le j_2,k_2,j_3,k_3\le N} P\left(A_jB_k \cap A_{j_2}B_{k_2} \cap A_{j_3}B_{k_3}\right) + \cdots + (-1)^{N+1}P\left(\bigcap_{j,k=1}^{N} A_jB_k\right)$$

ε: the exclusion ratio coefficient

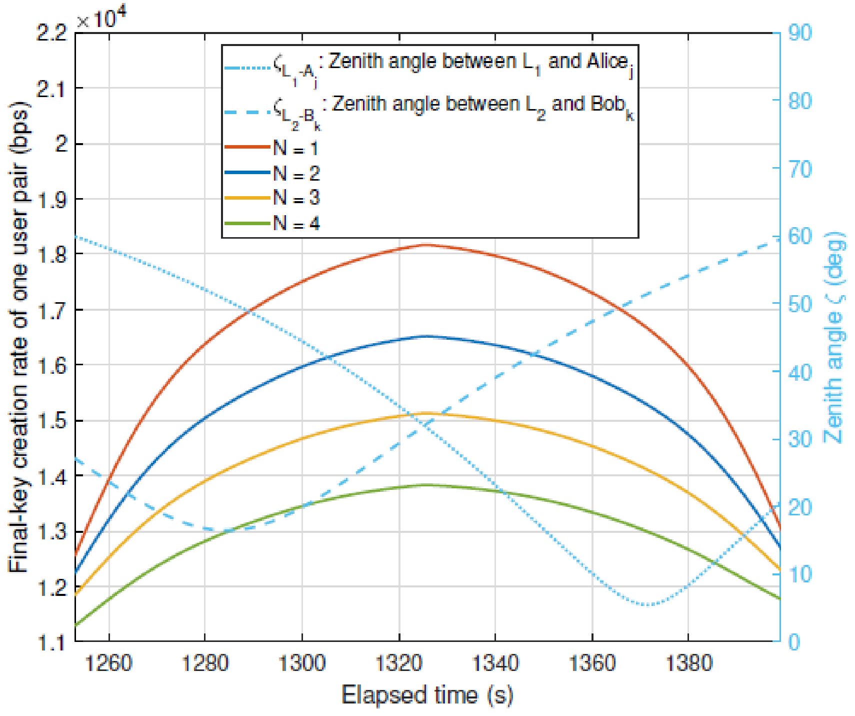
$\varepsilon = 1$: all detected bits at the same time instant are excluded

3.3.4. Secret-key Performance (1)

The parameters for GEO, LEO satellites and users are chosen to satisfy the requirement of sift probabilities and QBER: $\delta_{G_0} = 0.6$, $\delta_{L_i} = 0.6$, $\varsigma_{L_i} = 1$, $\varsigma_{A_j} = 0.25$, $\varsigma_{B_k} = 0.25$

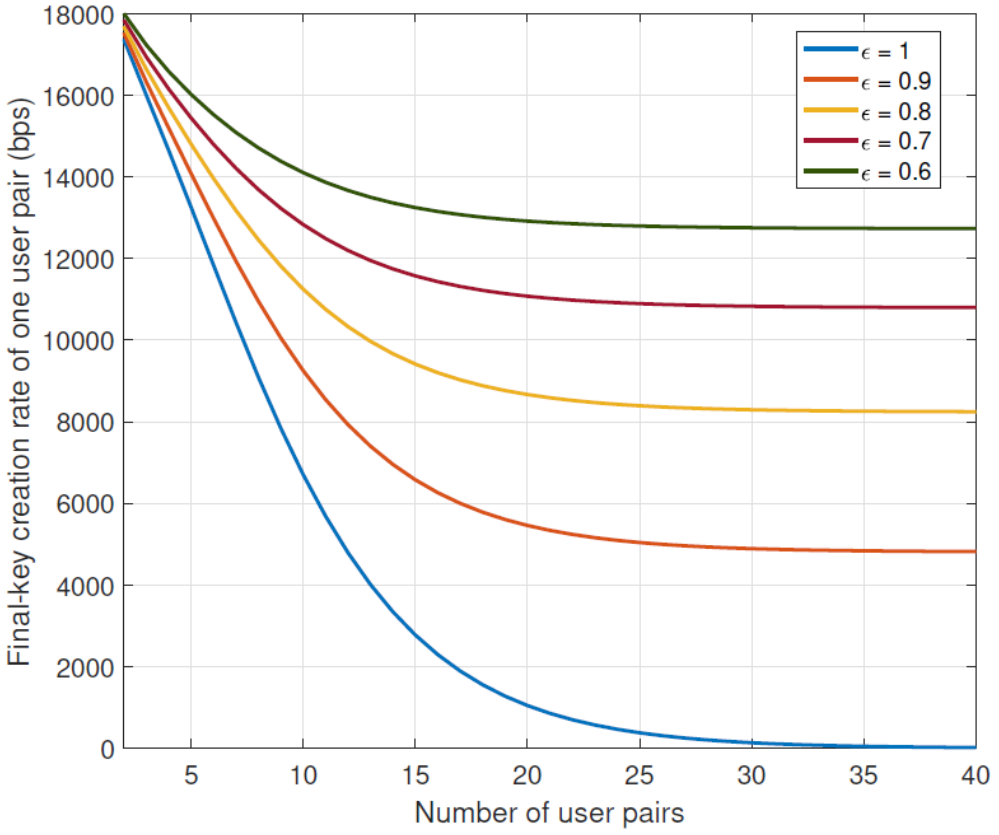


Ground traces of LEO satellites over Japan observed from 16:09:00 UTC+9 2021/12/23

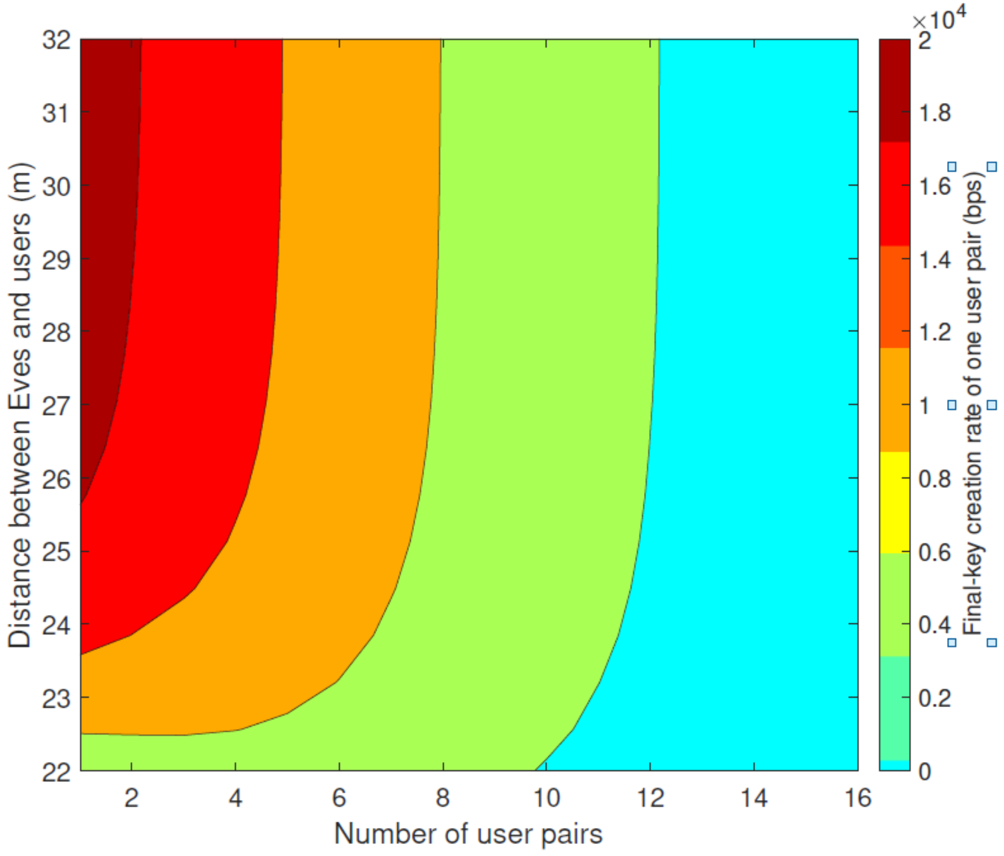


Final-key creation rate of one user pair with different numbers of user pairs (N) and zenith angle between L_i and users versus elapsed time from the epoch time, $d_{E_j} = d_{E_k}$ =25 m, $\varepsilon = 1$

3.3.4. Secret-key Performance (2)

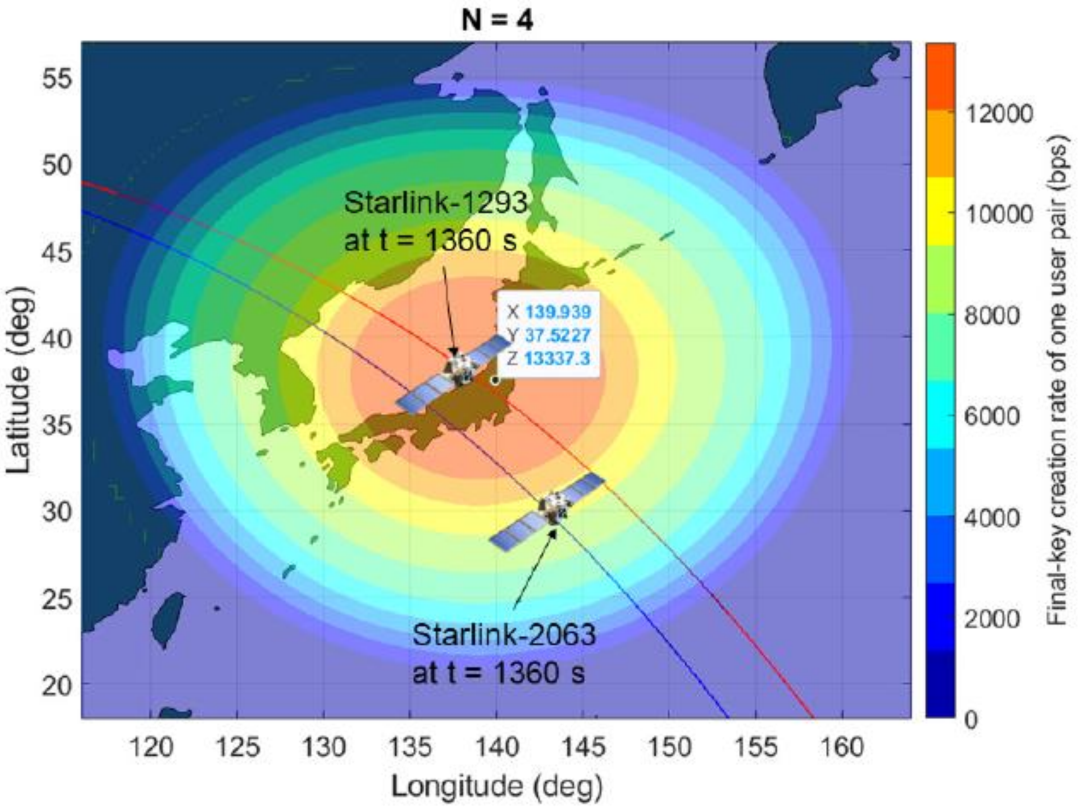


Final-key creation rate of one user pair versus the number of user pairs with different exclusion ratio coefficients (ε); t = 1360 s, $d_{E_j} = d_{E_k}$ = 25 m

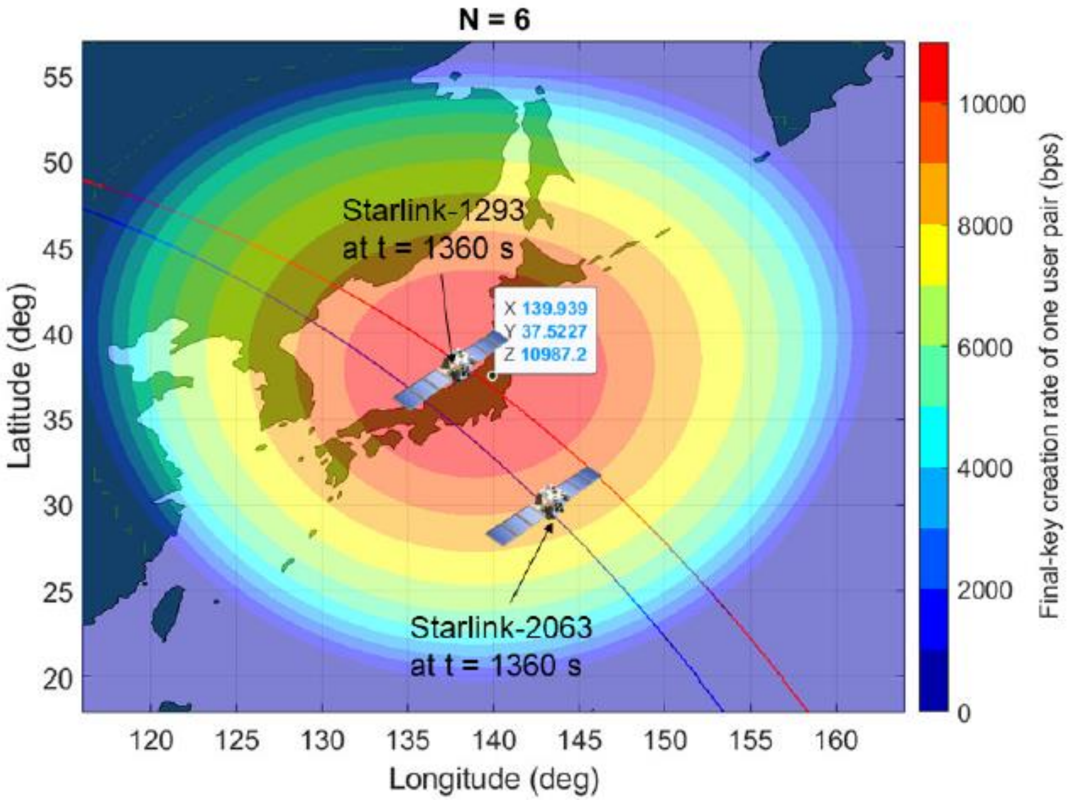


Final-key creation rate of one pair versus the distance between eavesdroppers and users (d_{E_j} ,d_{E_k}) and the number of user pairs; t = 1360 s, ε = 1

3.3.4. Secret-key Performance (3)



(a) N = 4



(b) N = 6

The spatial distribution of the final-key creation rate of one user pair with different numbers of user pairs, t = 1360 s (Bob$k$ are located in Osaka City)

Summary and Future Research

- This dissertation focuses on
  - Proposing a new design concept for satellite FSO/QKD systems by applying *non-coherent CV* for the *entanglement-based scheme*
  - Designing and investigating secret-key performance of satellite FSO/QKD systems using GEO/LEOs for multiple wireless users
  - Investigating the feasibility of a case study for Japan's QKD network using the existing GEO satellite and LEO satellite constellation to provide QKD service for legitimate users in Japan
- Future research
  - Post-processing algorithms for error estimation, error correction, and privacy amplification
  - Satellite-based FSO/QKD constellation design
  - Airborne quantum key distribution

Thank you!

References

[1] D. C. Nguyen et al., "6G Internet of Things: A Comprehensive Survey," in IEEE Internet of Things Journal, vol. 9, no. 1, pp. 359-383, 1 Jan.1, 2022

[2] https://www.frost.com/frost-perspectives/what-is-required-for-a-scalable-and-industry-wide-vehicle-to-everything-v2x-deployment/

[3] https://www.toshiba-clip.com/en/detail/p=863

[4] https://arxiv.org/ftp/arxiv/papers/2012/2012.14396.pdf

[5] https://physics.aps.org/articles/v15/172

[6] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, India, 1984, pp. 175–179.

[7] Grosshans, F., Grangier, P.: Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. **88**(5) (2002)

[8] P. V. Trinh, T. V. Pham, N. T. Dang, H. V. Nguyen, S. X. Ng, and A. T. Pham, “Design and security analysis of quantum key distribution protocol over free-space optics using dual threshold direct-detection receiver," IEEE Access, vol. 6, pp. 4159-4175, 2018.

[9] https://www.researching.cn/col/journalnewsdetails/8ff393fc-8952-407f-a9b8-db39547dda9c?type=recommendation

[10] T. Ikuta and K. Inoue, "Intensity modulation and direct detection quantum key distribution based on quantum noise", New J. Phys., vol. 18, no. 1, Jan. 2016.

[11] M. Q. Vu, T. V. Pham, N. T. Dang and A. T. Pham, "Design and Performance of Relay-Assisted Satellite Free-Space Optical Quantum Key Distribution Systems," in IEEE Access, vol. 8, pp. 122498-122510, 2020.

[11] https://www.researching.cn/col/journalnewsdetails/8ff393fc-8952-407f-a9b8-db39547dda9c?type=recommendation

[12] S. K. Liao et al., “Satellite-to-ground quantum key distribution,” Nature, vol. 549, pp. 44-47, Aug. 2017.

[10]
[7] G. Vallone et al., “Experimental satellite quantum communications,” Phys. Rev. Lett., vol. 115, no. 4, Art. no. 040502, Jul. 2015.
[8] S. K. Liao et al., “Satellite-to-ground quantum key distribution,” Nature, vol. 549, pp. 44-47, Aug. 2017.
[9] J. Yin et al., “Satellite-based entanglement distribution over 1200 kilometers,” Science, vol. 356, no. 6343, pp. 1140-1144, Jun. 2017.
[10] S. K. Liao et al., “Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 space lab,” Chin. Phys. Lett., vol. 34, no. 9, Art. no. 090302, 2017.
[11] K. Gunthner et al., “Quantum-limited measurements of optical signals from a geostationary satellite,” Optica, vol. 4, Art. no. 611, 2017.
[12] H. Takenaka et al., “Satellite-to-ground quantum-limited communication using a 50-kgclass microsatellite,” Nature Photon., vol. 11, pp. 502-508, Jul. 2017.
[13] S. K. Liao et al., “Satellite-relayed intercontinental quantum network,” Phys. Rev. Lett., vol. 120, no. 3, Art. no. 030501, Jan. 2018.
[14] J. Yin et al., “Entanglement-based secure quantum cryptography over 1,120 kilometres,” Nature, vol. 582, pp. 501-505, Jun. 2020.
[15]

[25] T. Ikuta and K. Inoue, "Intensity modulation and direct detection quantum key distribution based on quantum noise", New J. Phys., vol. 18, no. 1, Jan. 2016.
[26]

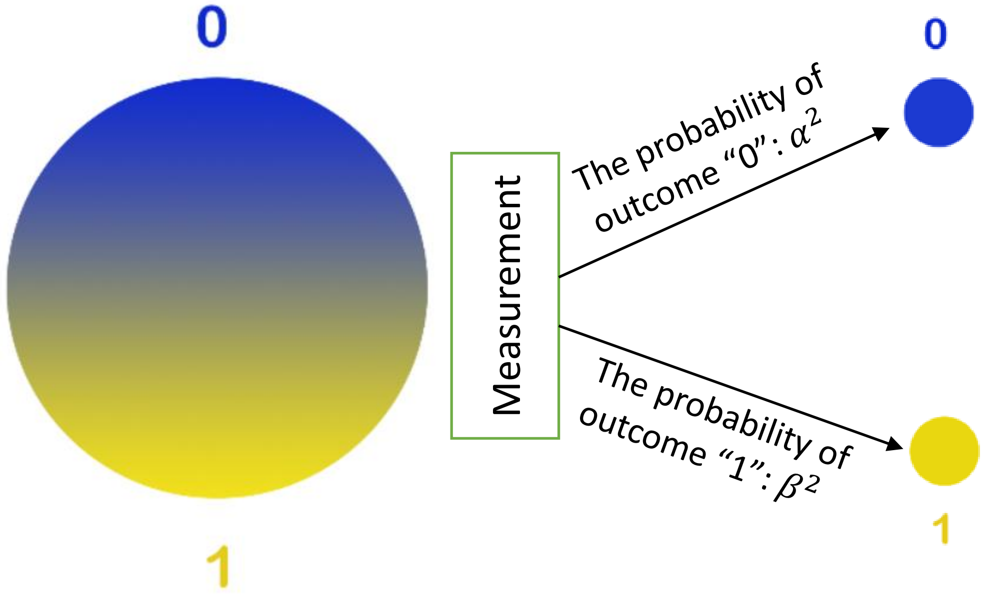
1. Motivation for QKD

- New Key Distribution Systems Needed
  - Quantum key distribution (QKD)
    - ❑ QKD is being considered a promising method to distribute secure keys secretly
    - ❑ Key distribution based on the laws of physics
      - ❖ In quantum mechanics, the **quantum no-cloning theorem** imposes that an unknown quantum state cannot be cloned reliably
      - ❖ If Alice distributes a key via quantum signals, there is no way for the eavesdropper (Eve) to clone the quantum state reliably to make two copies of the same quantum state
      - ❖ If Eve tries to eavesdrop, she will introduce disturbance unavoidably to the quantum signals → Alice and Bob can detect → Alice and Bob simply discard such a key and try the key distribution process again
    - ❑ First proposed by C. Bennett and G. Brassard in 1984: BB84 protocol

Classical Bits and Quantum Bits

A classical bit can be either “0” or “1”

A quantum bit (qubit) is a superposition of “0” and “1”

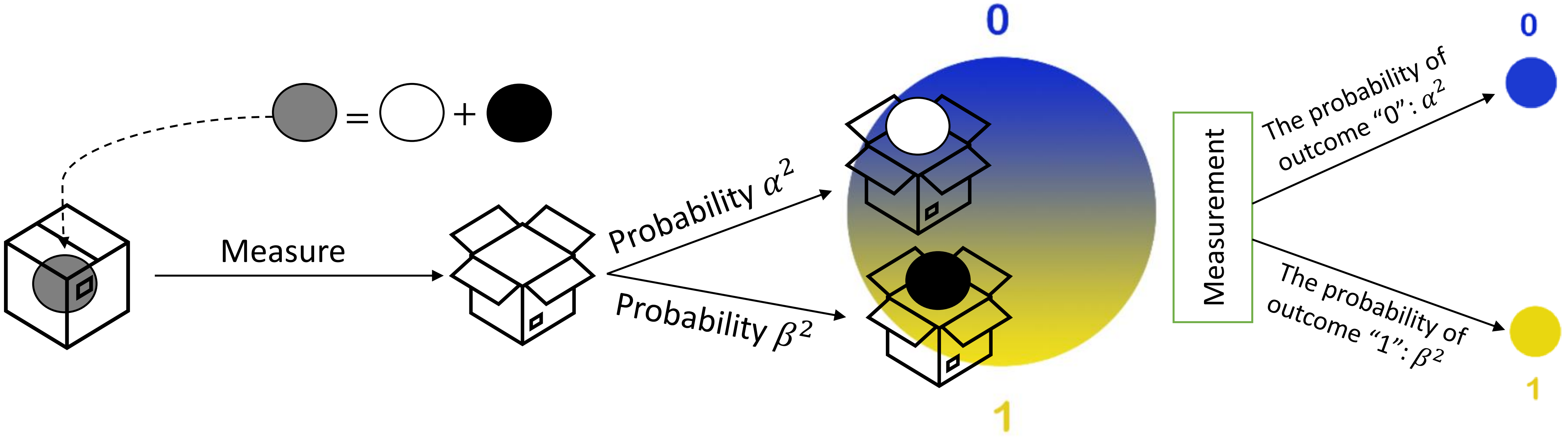


$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Classical Bits and Quantum Bits

A classical bit can be either “0” or “1”

A quantum bit (qubit) is a superposition of “0” and “1”



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Two Qubits and Entanglement

- Two classical bits: 4 definite states 00, 01, 10, 11
- The quantum state of two qubits:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

  The measurement result x (=00, 01, 10, 11) occur with probability $|\alpha_x|^2$

- We can also write the quantum state of two qubits as the "tensor product" of two quantum states of one qubit:
  - The state of the first qubit: $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$
  - The state of the second qubit: $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$

  → The state of two qubits:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\psi_2\rangle = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$$

- Two qubits are called *entangled* if the quantum state of two qubits can not analyze the state of each individual qubit → This quantum state is an *entangled* state

Entanglement Example

- Consider the quantum state of two qubits: $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$
- Try to write it as the product of two quantum state of one qubit:
  - The state of the first qubit: $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$
  - The state of the second qubit: $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$

→ The state of two qubits:

$$|\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\psi_2\rangle = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$$

We want $|\psi\rangle$ = $|\psi_1\rangle \otimes |\psi_2\rangle$, so $\alpha_1\alpha_2 = 0$, $\alpha_1\beta_2 = \frac{1}{\sqrt{2}}$, $\beta_1\alpha_2 = \frac{1}{\sqrt{2}}$, $\beta_1\beta_2 = 0$

→ It is not possible to find the value of $\alpha_1, \alpha_2, \beta_1, \beta_2$

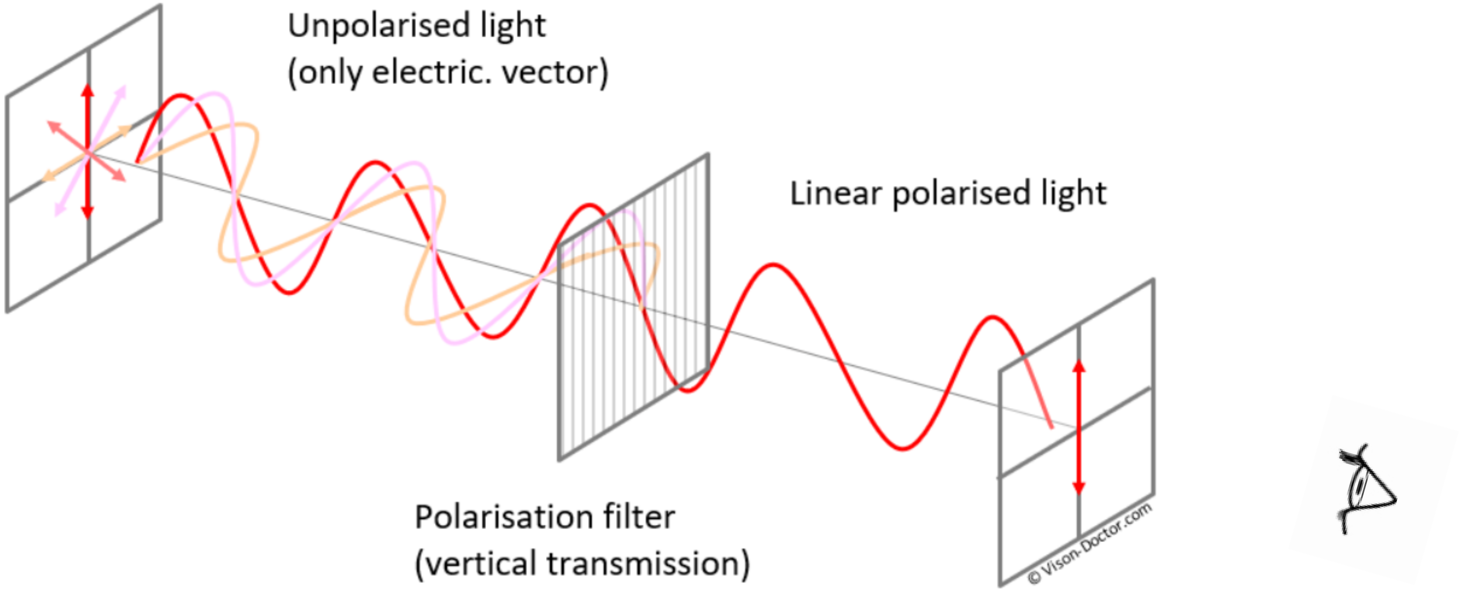
→ $|\psi\rangle$ can not analyze as the product of two quantum state of one qubit → an entangled state

Entanglement Example (2)

- Characteristic of the entangled state:
  - Each qubit can be separated by any distance
  - The measurement outcomes of two qubits have the correlation
    - For example, if *the first qubit* is measured:
      - The outcome is 0 → The measurement outcome of *the second qubit* is 1 with certainty
      - The outcome is 1 → The measurement outcome of *the second qubit* is 0 with certainty

Polarization of Photon

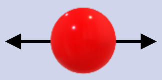
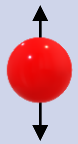
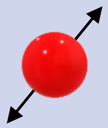
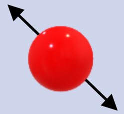
- Polarization of a single photon can represent a qubit
- The polarization of light (a photon is a particle of light) specifies the geometrical orientation of the oscillation of the electromagnetic field associated with its wave
- We focus here on *linear polarization* (the field only oscillates in one direction)



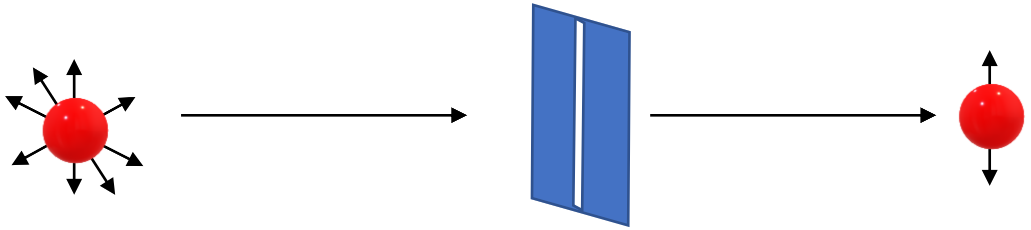
Observer

Send a Qubit

- Two kinds of bases of linear polarization
  - The rectilinear basis ⊕: horizontal $(0°)$ and vertical $(90°)$ orientations
  - The diagonal basis ⊗: orientations rotated by $+45°$ and $-45°$
- Photon polarization as a qubit

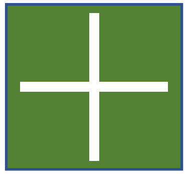
	The rectilinear basis (⊕)		The diagonal basis (⊗)	
Photon polarization				
State	$\vert 0\rangle$	$\vert 1\rangle$	$\frac{1}{\sqrt{2}}(\vert 0\rangle + \vert 1\rangle)$	$\frac{1}{\sqrt{2}}(\vert 0\rangle - \vert 1\rangle)$

- To send a qubit, we send a photon through a polarizer to get the desired polarization (e.g., if we use vertical polarizer, we will send a vertical polarized photon)



Measure a Qubit

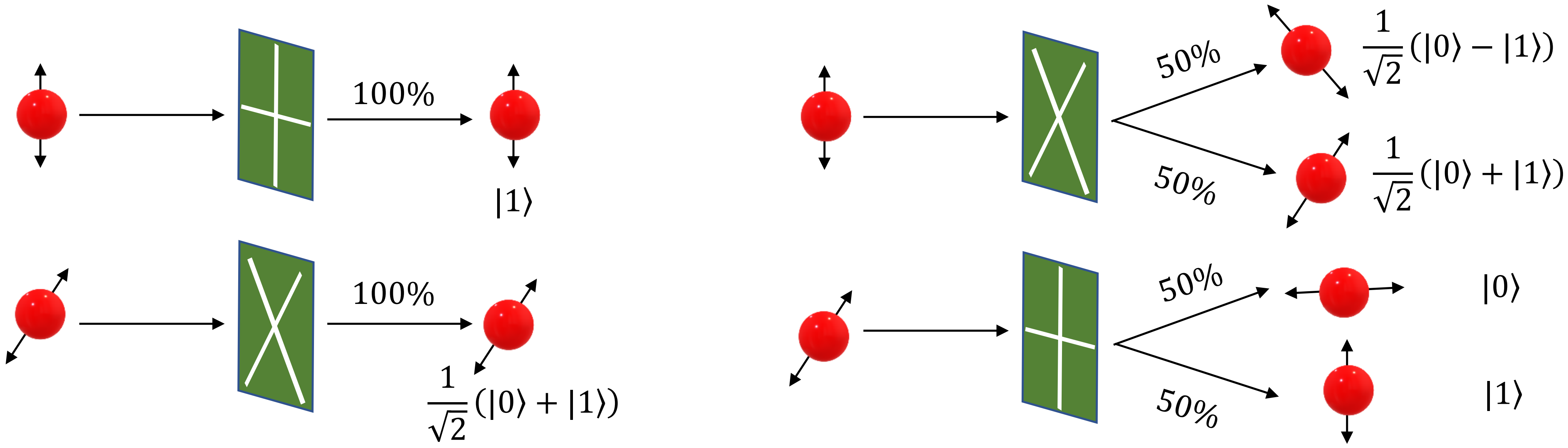
- Two polarization filters:



Rectilinear polarization filter

Diagonal polarization filter

- The receiver choose one of two polarization filters to measure a received qubit.



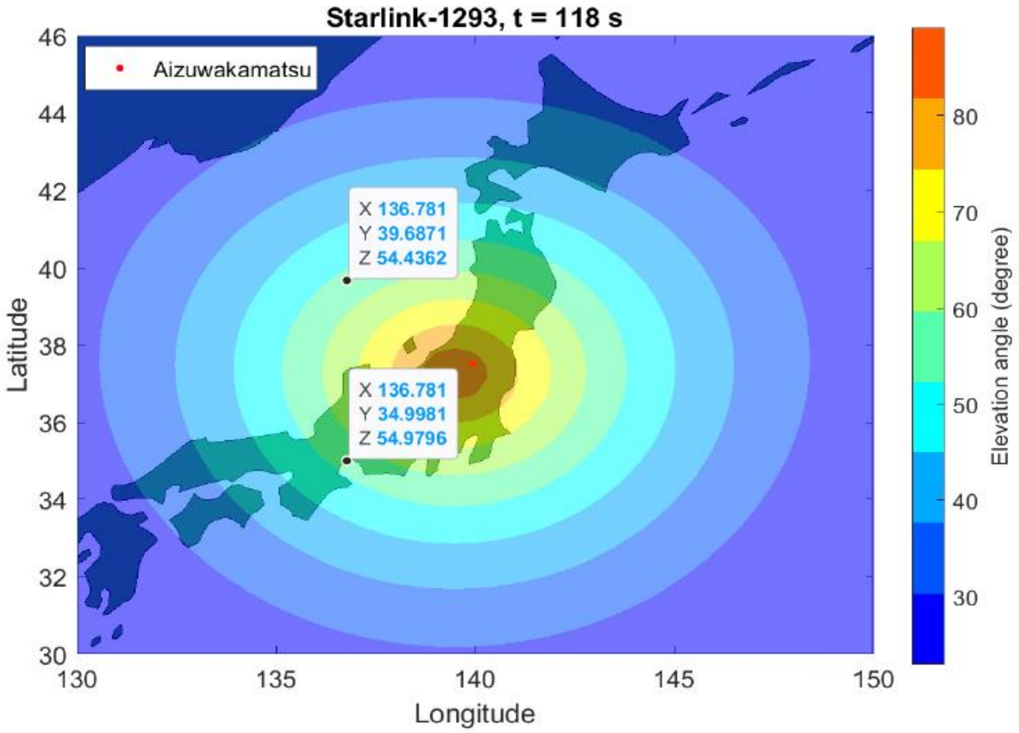
Cybersecurity: What?

- **Confidentiality:** assures that private or confidential information is not made available or disclosed to *unauthorized individuals*
- **Integrity:** assures that information and programs are changed only in a *specified and authorized manner*
- **Availability:** assures that system works promptly, and service is not denied to authorized users

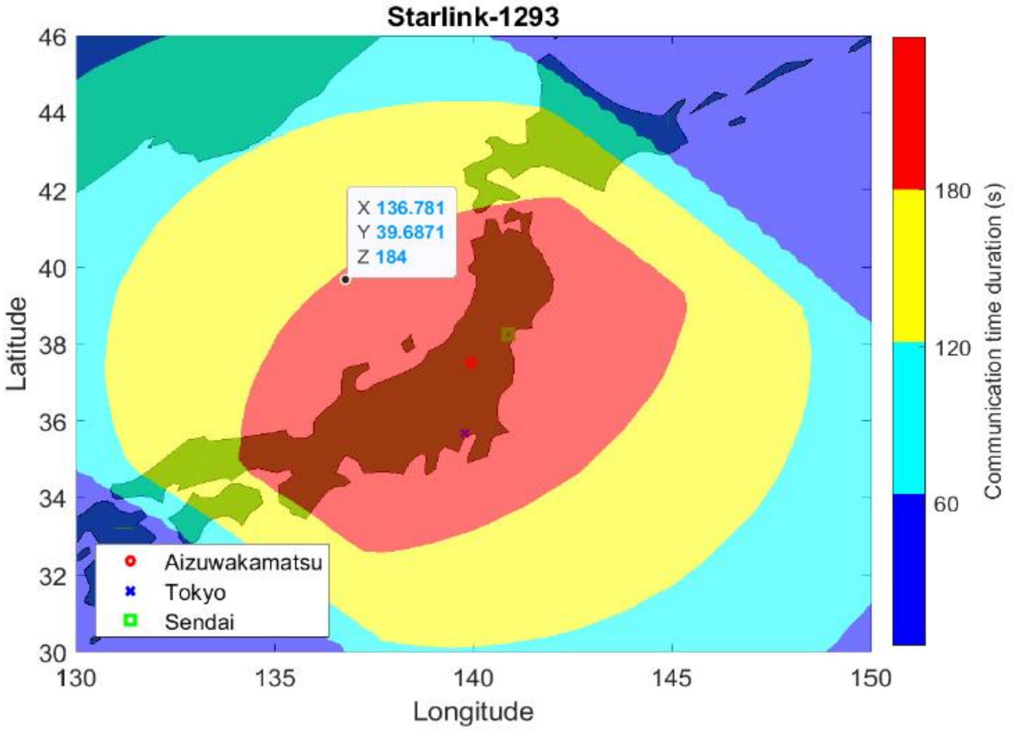
Confidentiality, Integrity, Availability (CIA) Triad

4A. Design of Practical EB Satellite FSO/QKD Systems

- Bob's design
  - The operational region of Bob



(a) The coverage area of Starlink-1293



(b) The distribution of communication time duration

The coverage area of Starlink-1293 at time instant that the elevation angle between the satellite and Alice is maximum and the distribution of communication time duration between Bob and Alice (Alice is located in Aizuwakamatsu City).

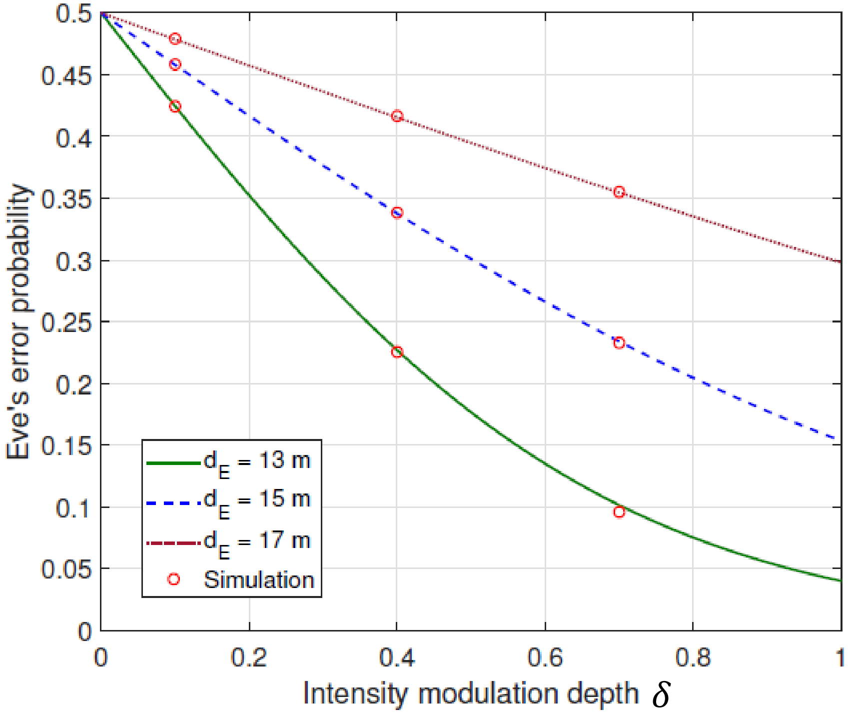
3B. Satellite-Based FSO/QKD Systems using GEO/LEOs for Multiple Wireless Users

TABLE III: Simulation results of BSA detection

The value difference of $P_{\text{sift}}^{C,A}$ with no BSA and BSA	No. of BSA events	No. of detectable BSA events	Correct BSA detection	Percentage of correct detection (in No. of BSA events)	Percentage of correct detection (in No. of detectable BSA events)	False alarms	Percentage of false alarms (in No. of detectable BSA events)
$d_{\text{BSA}} = 2\sigma_{\text{sd}}$							
1.1%-1.5%	19	21	13	68.42%	61.9%	8	31.9%
1.5%-1.8%	15	20	9	60%	45%	11	55%
1.8%-2%	12	24	12	100%	50%	12	50%
2%-2.4%	14	16	14	100%	87.5%	2	12.5%
$d_{\text{BSA}} = 2.25\sigma_{\text{sd}}$							
1.1%-1.5%	19	16	10	52.63%	62.5%	6	37.5%
1.5%-1.8%	15	12	8	53.33%	66.67%	4	33.33%
1.8%-2%	12	17	12	100%	70.59%	5	29.41%
2%-2.4%	14	15	14	100%	93.33%	1	0.67%
$d_{\text{BSA}} = 2.5\sigma_{\text{sd}}$							
1.1%-1.5%	19	11	8	42.1%	72.73%	3	27.27%
1.5%-1.8%	15	7	6	40%	85.71%	1	14.29%
1.8%-2%	12	11	10	83.33%	90.91%	1	9.09%
2%-2.4%	14	14	14	100%	100%	0	0%
$d_{\text{BSA}} = 2.75\sigma_{\text{sd}}$							
1.1%-1.5%	19	5	4	21.05%	80%	1	20%
1.5%-1.8%	15	6	6	40%	100%	0	0%
1.8%-2%	12	9	9	75%	100%	0	0%
2%-2.4%	14	14	14	100%	100%	0	0%
$d_{\text{BSA}} = 3\sigma_{\text{sd}}$							
1.1%-1.5%	19	4	4	21.05%	100%	0	0%
1.5%-1.8%	15	5	5	33.33%	100%	0	0%
1.8%-2%	12	7	7	58.33%	100%	0	0%
2%-2.4%	14	14	14	100%	100%	0	0%

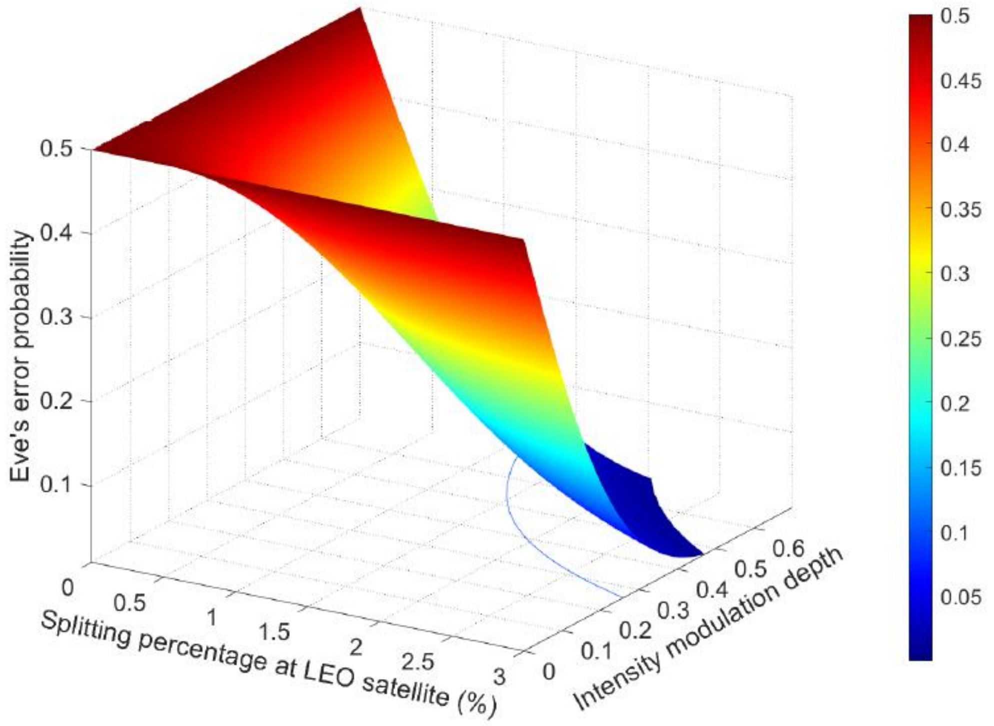
3.2.6. Charlie's Design

Unauthorized Receiver Attack (URA)



Eve's error probability versus intensity modulation depth

Beam Splitting Attack (BSA) at LEO satellite



Eve's error probability versus splitting percentage (SP) at LEO satellites

3.1.4. Key Features of Proposed Scheme

- Scalability:

- Simplicity:
- Security Robustness:
- Key Rate:
- Cost Effectiveness: