A Proposal of Satellite-based FSO/QKD System for Multiple Wireless Users

Minh Q. Vu, Hoang D. Le, and Anh T. Pham

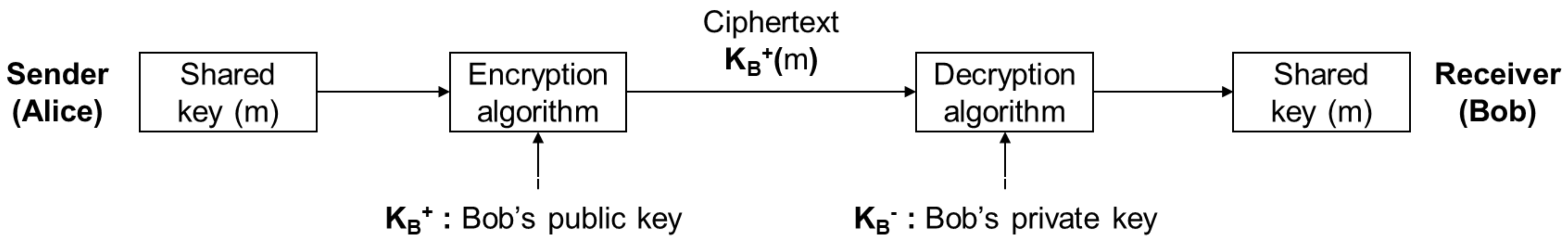
The University of Aizu

Contents

Quantum Key Distribution (QKD)

In network security, how can two users share secret keys in a secure manner?

- Conventional approach is *Public-Key Cryptography (PKC)*



  - The security of PKC relies on mathematical complexity

→ Becomes vulnerable to advances in computational technologies (e.g., quantum computing, DNA computing)

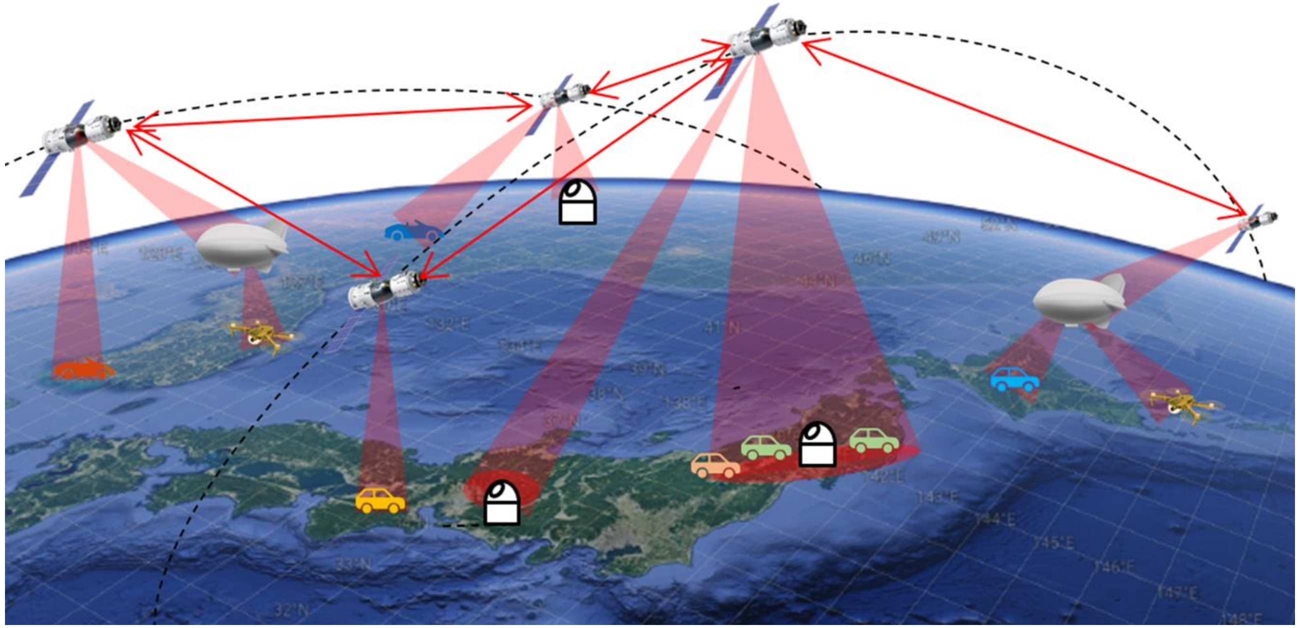
- To solve this issue, a promising solution is *Quantum Key Distribution (QKD)*
  - It is based on the laws of physics to distribute secret keys between two legitimate users
  - Possible unconditional security can be achieved

Satellite-based QKD Systems: Overview

- QKD can be implemented over *optical fiber* and *free-space optics (FSO)* (terrestrial or satellite)
- Conventional QKD systems mainly focus on
  - Optical fiber: for fixed users, inflexibility
  - Terrestrial FSO: limited distance (several kilometers)

→ Difficult to support global QKD services, large-scale networks, especially for mobile users (e.g., autonomous cars, UAVs)

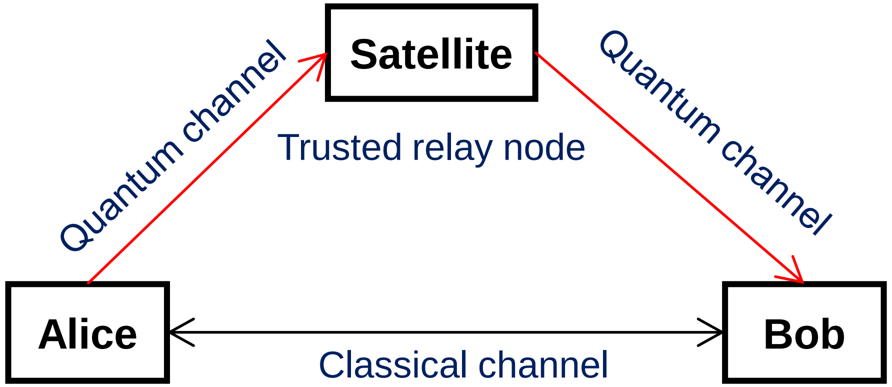
- To tackle those issues, *FSO-based satellite* has been recently considered for QKD systems thanks to flexible deployment and wide coverage area



Satellite-based QKD Systems: Implementation

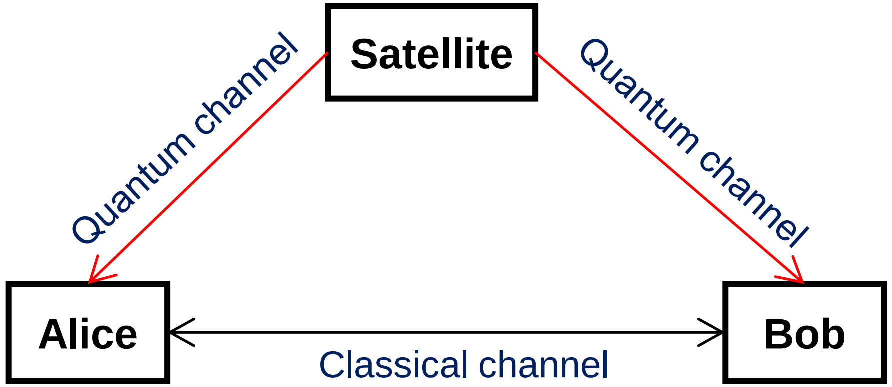
Implementation Schemes

(1) Prepare-and measure



More than one phase is needed to transmit key from Alice to Bob → complexity and inefficiency

(2) Entanglement-based



Satellite does not need to be a trusted node

➡ **Entanglement-based scheme is more efficient and more secure as Alice and Bob can settle secret keys without the involvement of the satellite**

Entanglement-based Satellite QKD: Literature Survey

- There are two main approaches to implement entanglement-based QKD
  - *Discrete-variable (DV)*: Entangled photon-pairs are sent and then detected by single-photon detectors
  - *Continuous-variable (CV)*: Two-mode entangled states created from laser are sent and then detected by coherent detectors
- Both DV and CV-QKD have recently studied for satellite-based QKD
  - [1], [2] considered DV-QKD for entanglement-based satellite QKD

  → Low key rate and incompatibility with standard optical communication technologies
  - [3], [4] addressed CV-QKD for entanglement-based satellite QKD

  → Complexity (require a sophisticated phase stabilized local light for coherent detection)

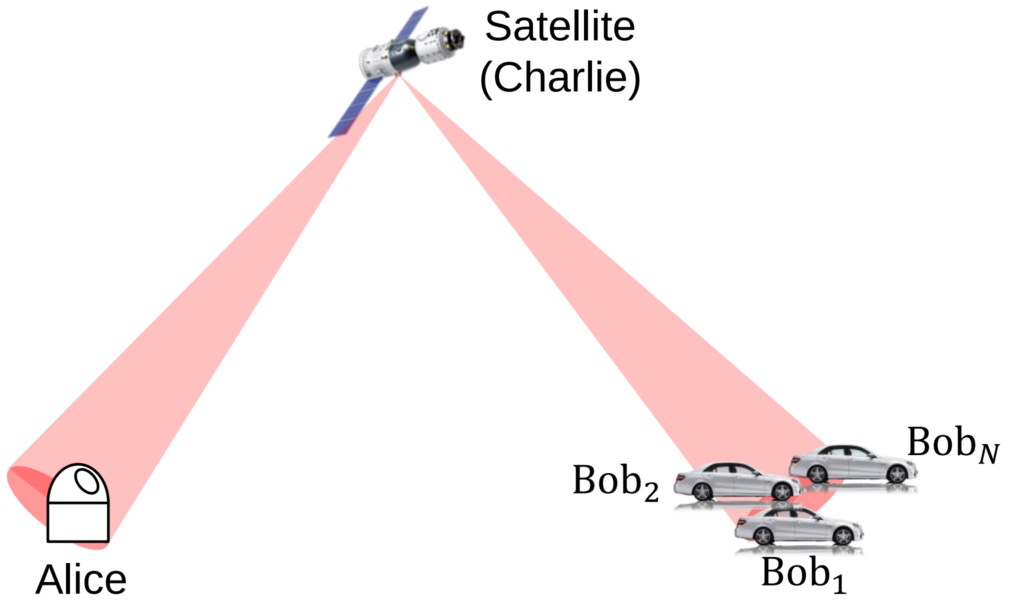
  And all of them just considered a pair of users (between Alice and Bob)

➡ **A simpler approach that is compatible with standard communication technologies and can support multiple users is needed**

[1] J. Yin, Y.-H. Li, L. Shengkai et al., "Entanglement-based secure quantum cryptography over 1,120 kilometres," Nature, vol. 582, pp. 1–5, Jun. 2020.
[2] S.-K. Liao, W.-Q. Cai, J. Handsteiner et al., "Satellite-relayed intercontinental quantum network," Phys. Rev. Lett., vol. 120, Jan. 2018, Art. no. 030501.
[3] N. Hosseinidehaj, Z. Babar, R. Malaney et al., "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," IEEE Commun. Surv. & Tut., vol. 21, no. 1, pp. 881–919, 2019.
[4] D. Dequal, L. Trigo Vidarte, V. Roman Rodriguez et al., "Feasibility of satellite-to-ground continuous-variable quantum key distribution," npj Quantum Inf., vol. 7, no. 1, Jan. 2021, Art. no. 3.

Goals

1. **Design an entanglement-based satellite QKD system with simple, low-cost implementation, and compatibility with standard communication technologies for multiple users**
   - Applying SIM/BPSK FSO system with dual-threshold (DT)/direct detection (DD) receivers based on BBM92 QKD protocol [5]
2. **Investigate performance results**
   - Total key-creation rate, the number of users

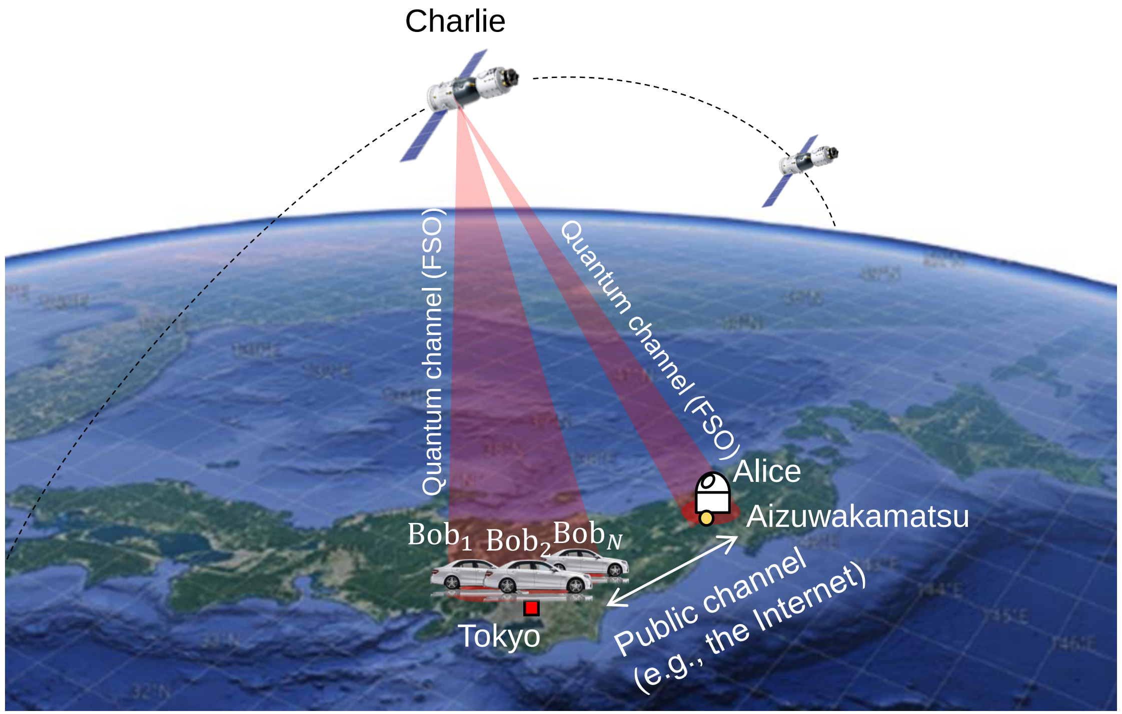


[5] M. Q. Vu, H. D. Le and A. T. Pham, "Entanglement-based Satellite FSO/QKD System using Dual-Threshold/Direct Detection," ICC 2022 - IEEE International Conference on Communications, 2022, pp. 3245-3250

Our System Implementation

- **Considered system scenario**
  - Charlie transmits signal simultaneously to both Alice and Bob *via FSO channel*
  - Alice and Bob detect received signal and then confirm via public channel to *create the secret key*
  - Eavesdropers (Eve) are *within the satellite's beam footprint* trying to *collect secret keys*

- **Protocol implementation**
  - Satellite CV-QKD using non-coherent detection (realized by *dual-threshold/direct detection* (DT/DD) receivers) for the entanglement-based scheme based on *BBM92 protocol* [5]



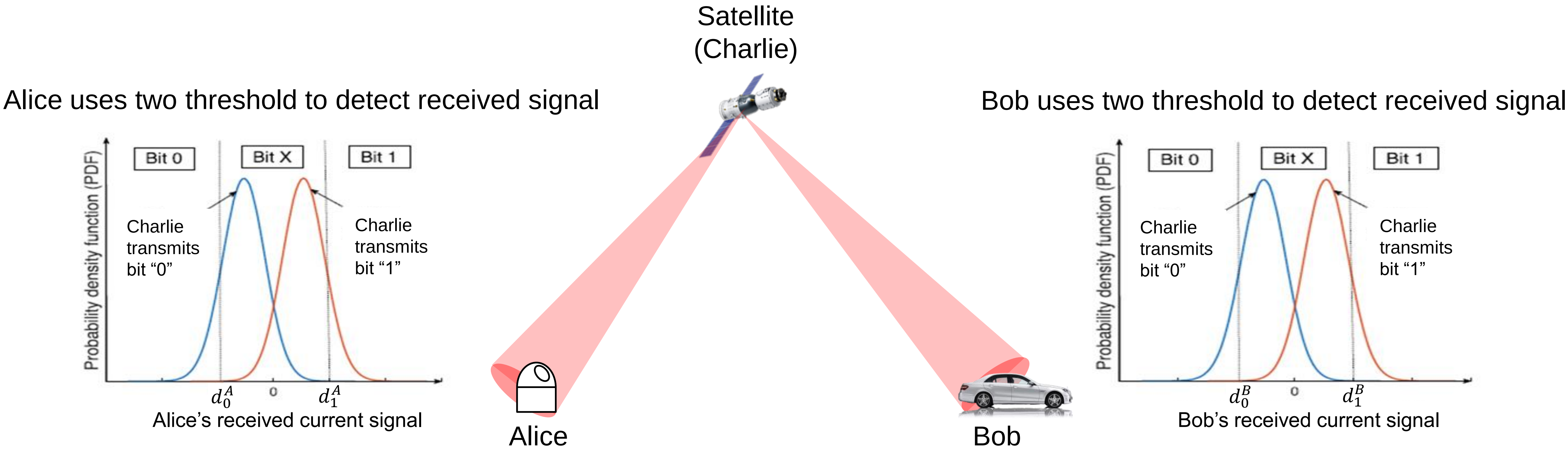
Satellite-based QKD system for multiple users

[5] M. Q. Vu, H. D. Le and A. T. Pham, "Entanglement-based Satellite FSO/QKD System using Dual-Threshold/Direct Detection," ICC 2022 - IEEE International Conference on Communications, 2022, pp. 3245-3250

Protocol Implementation: BBM92 with DT/DD

- The idea of the protocol proposal: mimic the key transmitting/decoding of BBM92 protocol [6]
- Implement on standard FSO system with non-coherent detection

Charlie transmits SIM/BPSK modulated signal to Alice and Bob with small intensity modulation depth (0<δ<1)

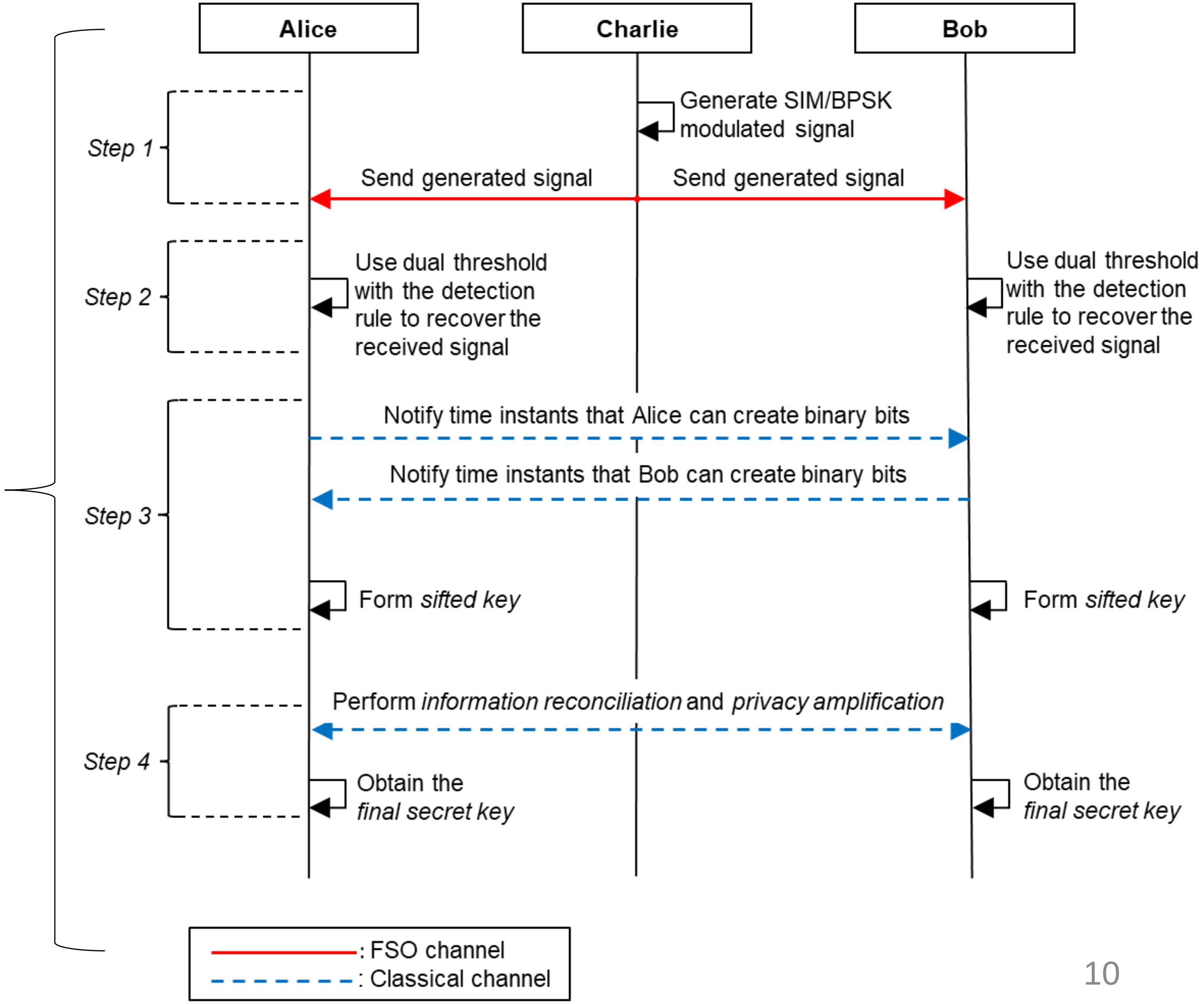


[6] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without Bell’s theorem,” Phys. Rev. Lett., vol. 68, pp. 557–559, Feb. 1992.

Protocol Implementation: Flowchart

Our protocol includes 4 steps

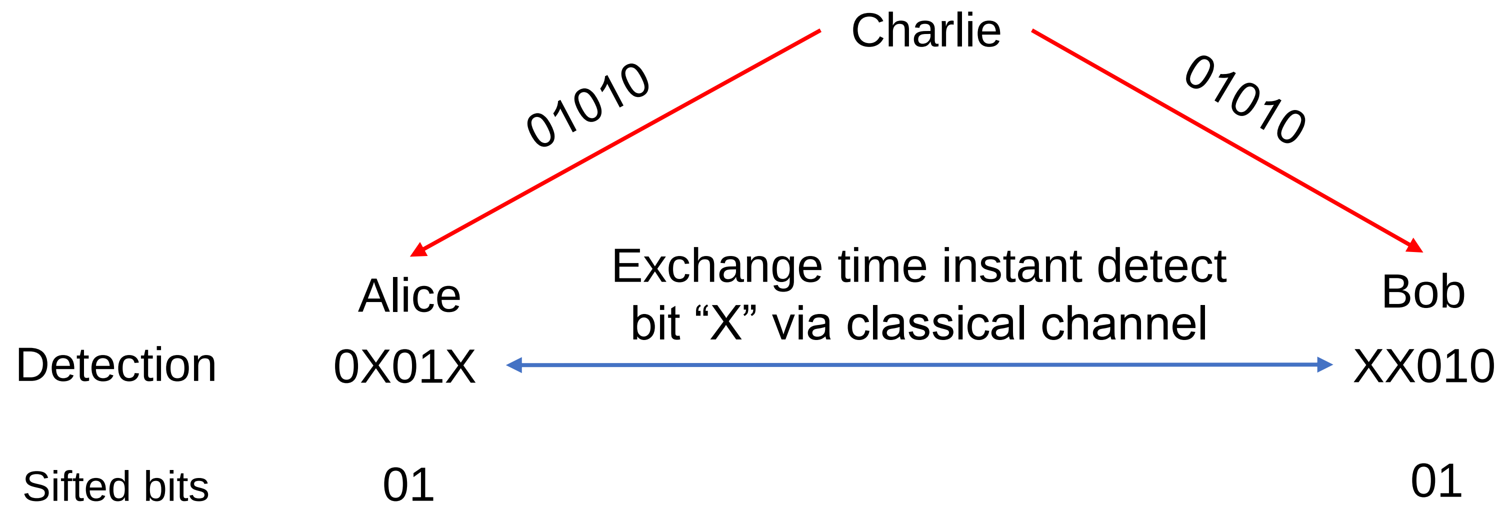
The key issue for simple and low-cost implementation comes from *the non-coherent detection (realized by dual-threshold/direct detection)*



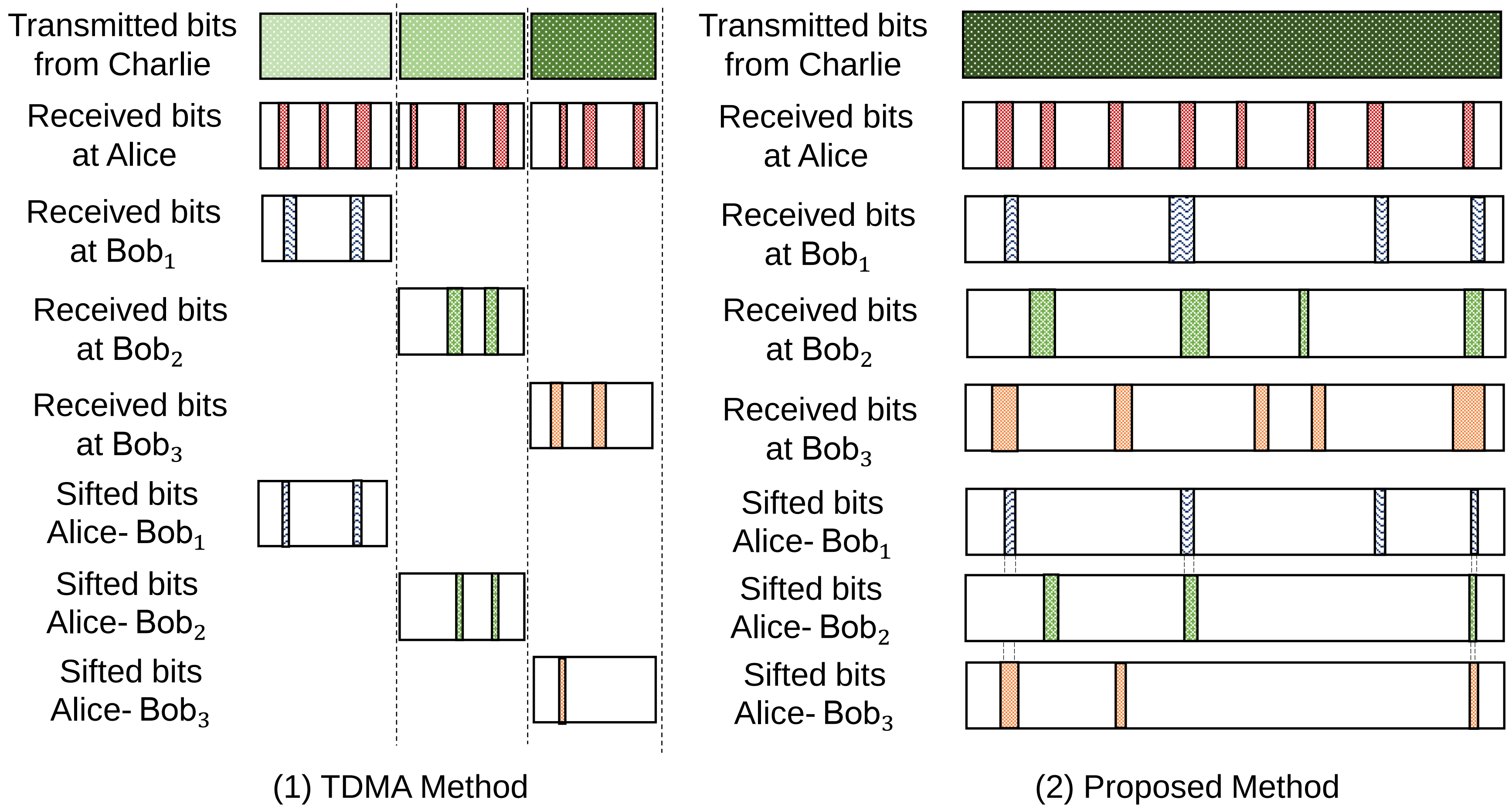
Protocol Implementation: An Example

- An example of the proposed protocol

Satellite (Charlie)			**Alice**			**Bob**			Sifted bits
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*



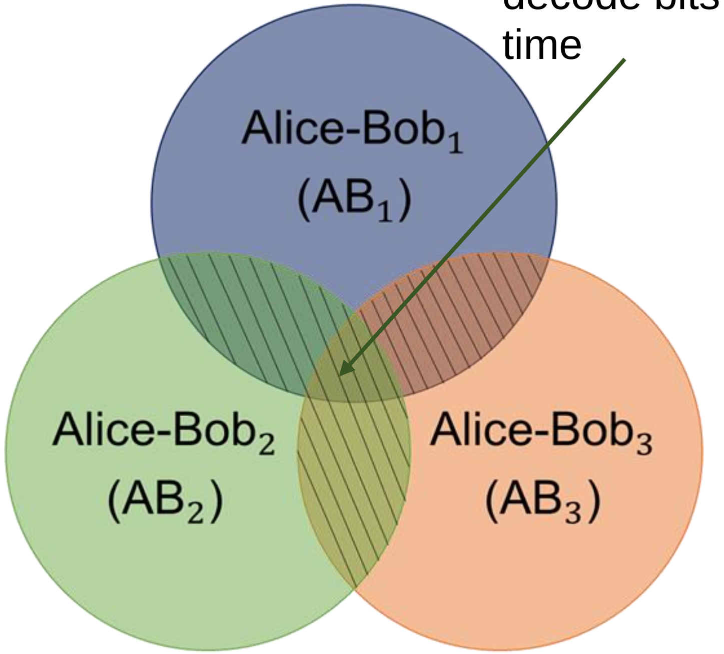
Satellite-based FSO/QKD for Multiple Wireless Users



Time Division Multiplexing Access (TDMA) vs. the proposed method for key distribution with the number of users at Bob's site = 3

Performance Analysis (1)

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



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

Sift Probability:

- 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

Performance Analysis (2)

Final-key creation rate:

- We assume that there are two eavesdroppers (Eve_1 and Eve_2) who perform unauthorized receiver attacks near Alice's and Bob's sites, respectively
- After sharing the sifted key between Alice and Bob and performing error correction, Alice and Bob:
  - Estimate the information leaked to eavesdroppers
  - Exclude it through privacy amplification to obtain the final key
- Final-key creation rate can be derived as

$$R_i^f = R_i^s\{\alpha I(A;B_i) - \max[I(A;E_1), I(B_i;E_2), I(E_1;E_2)]\}$$

R_i^s: the sifted-key rate → In TDMA system: $R_i^s = P_{AB_i}^{\mathrm{sift}} \frac{R_b}{N}$

→ In the proposed system: $R_i^s = P_{AB_i}^{\mathrm{sift-excl}} R_b$

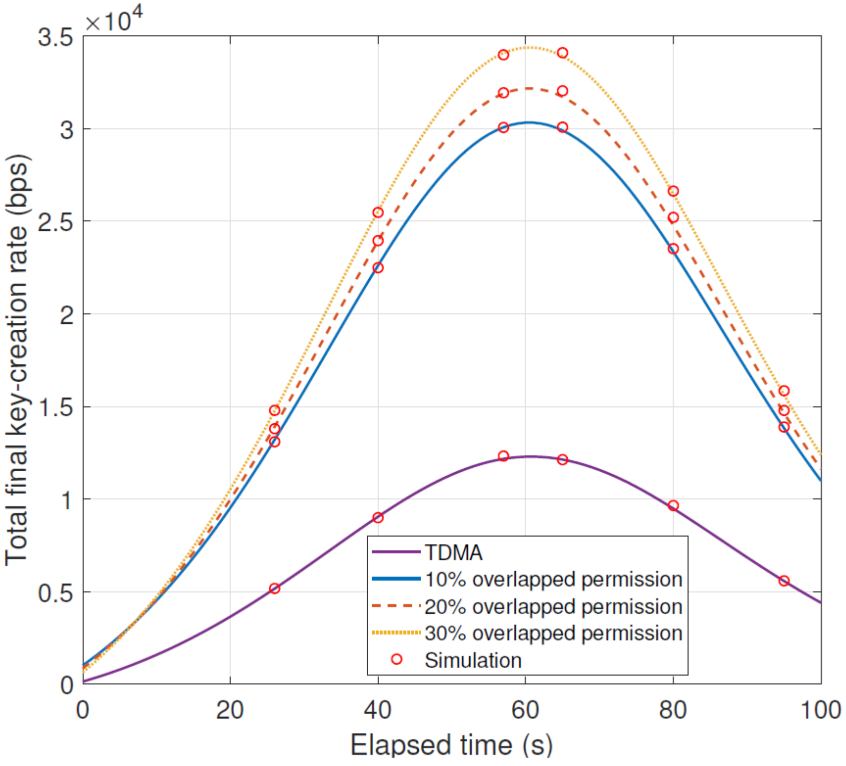
R_b: the system's bit rate

α: error correction efficiency in post-processing procedures

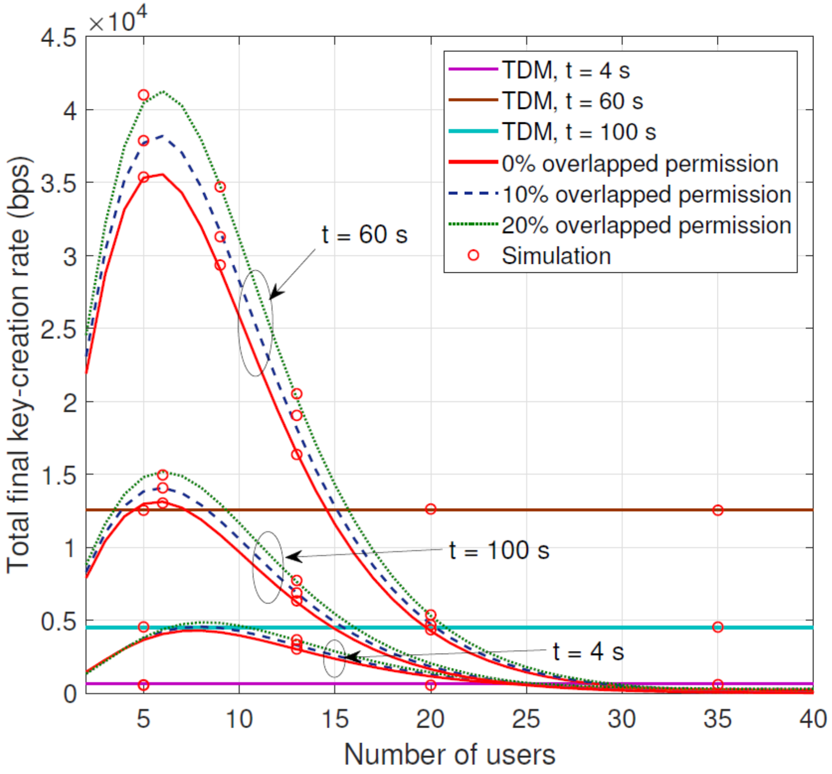
$I(X;Y), X \in \{A, B_i, E_1\}, Y \in \{B_i, E_1, E_2\}$: the amount of information shared between X and Y

Results

Results are analyzed under the impact of ***the effects of channel loss, atmospheric turbulence-induced fading, and receiver noises***



Total final key-creation rate vs. the elapsed time with the number of users =3: Proposed method vs. TDMA method



Total final key-creation rate vs. the number of users (N): Proposed method vs. TDMA method

Conclusions

- This paper proposes satellite-based CV-QKD using DT/DD to distribute secret keys to multiple users
- We analyzed the system performance regarding sift probability and total final-key creation rates for legitimate users
- The numerical results are given under the effects of channel loss, atmospheric turbulence-induced fading, and receiver noises
- The correctness of derived formulas was verified by Monte-Carlo simulations

International Conference on Emerging Technologies for Communications

Thank you!

TABLE 3: 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