HAP-Aided Relaying Satellite FSO/QKD Systems for Secure Vehicular Networks

Minh Q. Vu[1], Ngoc T. Dang[1,2], and Anh T. Pham[1]

[1]Computer Communications Laboratory
The University of Aizu, Japan

[2]Department of Wireless Communications
Posts and Telecoms. Institute of Technology, Vietnam

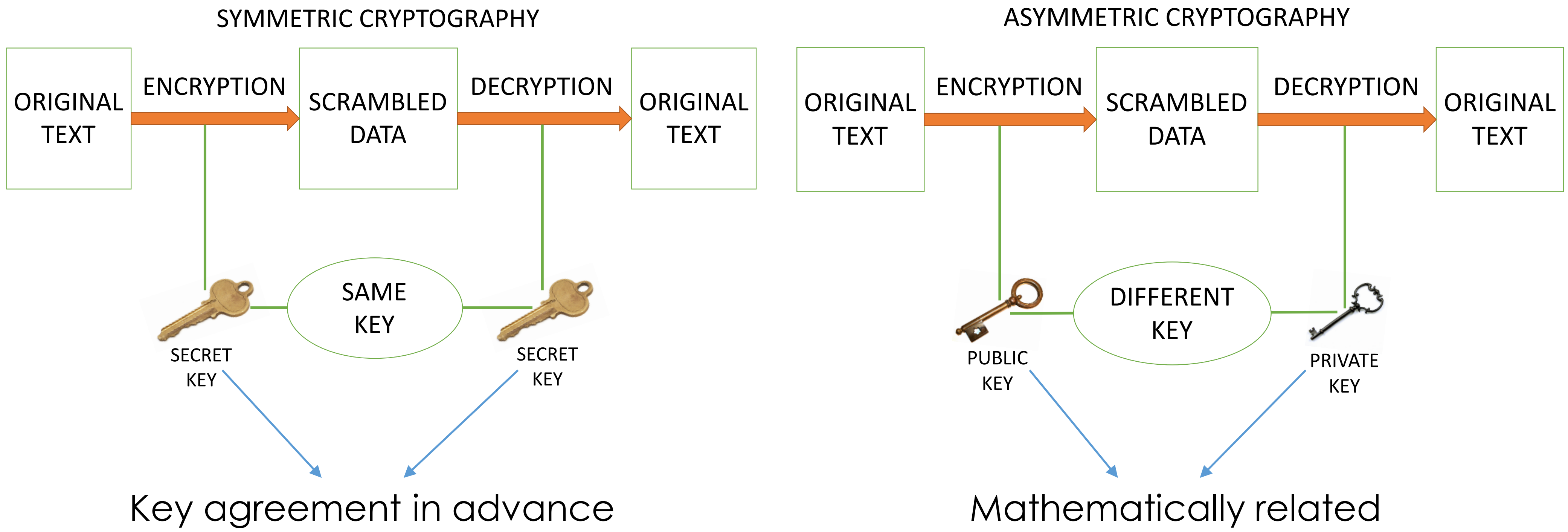
Contents

Network Security

- Network and the Internet play important role in everyday activities
  - Email, online shopping etc.
- Network security is one of the most critical issues
  - Confidentiality: keep data/communication secret
  - Authentication: verify user/provider
  - Integrity: keep data/communication intact
  - Availability: the information is available when it is needed

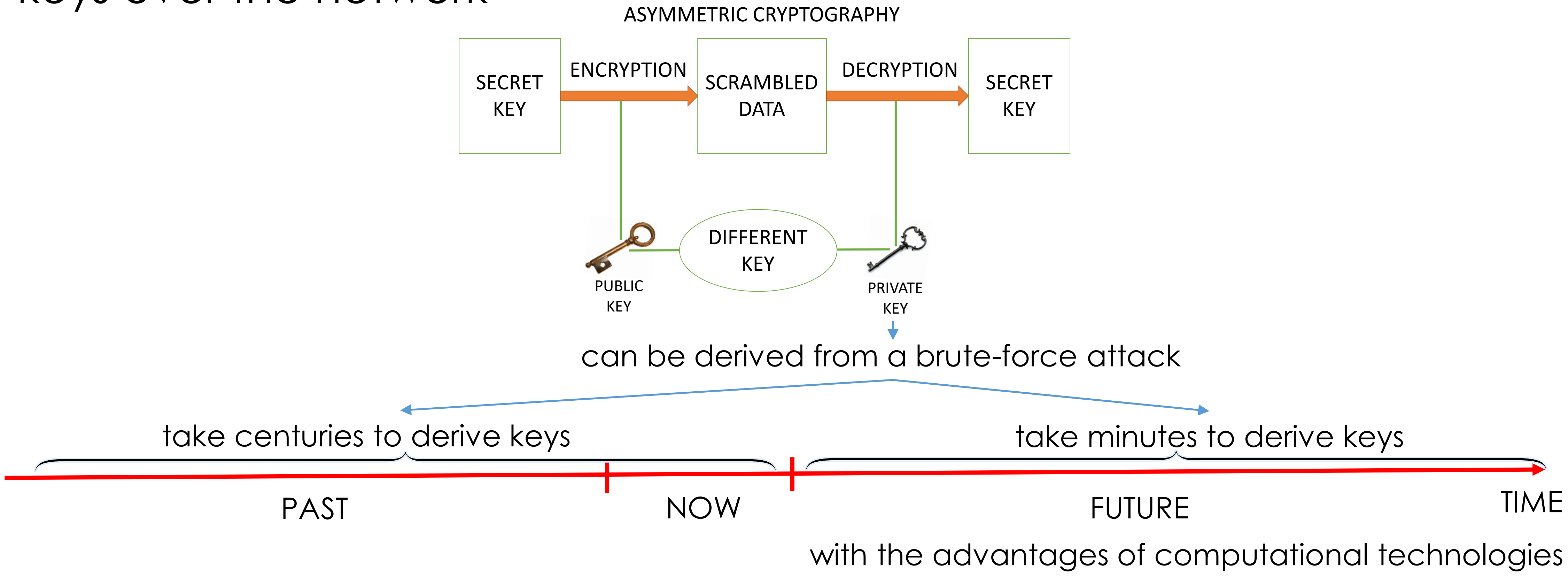
Cryptography & Future Challenge

- The current Internet security is based on Cryptography – the science of secret writing



Cryptography & Future Challenge (Cont.)

- Usually, asymmetric cryptography is used to distribute symmetric keys over the network



Quantum Key Distribution (QKD)

- QKD is a secure method to distribute keys over the network
- Based on the law of quantum mechanics
- The first QKD protocol (BB84) was published by Charles Bennett and Gilles Brassard in 1984
  - BB84 uses photon polarization states to encode the bits of the key

BB84 Example

(Key) bits are transmitted over quantum channel, e.g. photo transmission

Alice	Alice's random bit	0	1	1	0	1	0	0	1
	Alice’s random sending basis	×	+	+	×	+	+	+	×
	Photon polarization Alice sends	↘	↑	↑	↘	↑	→	→	↗
Bob	Bob’s random measuring basis	+	+	×	×	+	×	+	+
	Photon polarization Bob measures	↑	↑	↘	↘	↑	↗	→	→
	PUBLIC DISCUSSION OF BASIS								
Alice and Bob	Shared secret key		1		0	1		0	

QKD: State of the Arts

- Mainly implemented over optical fiber → optical fiber connectivity is the MUST
- **1999:** The quantum key distribution system **over 48 km of optical fiber** was described [1]
- **2013:** The quantum key distribution system **over 80 km of optical fibe**r was experimentally demonstrated [2]
- **In 2016:** The first quantum key distribution system **over 370 km of optical fiber** was presented [3]

Motivation of FSO/QKD System

1. Security for Vehicular Networks → wireless solution needed

Self-driving car/truck

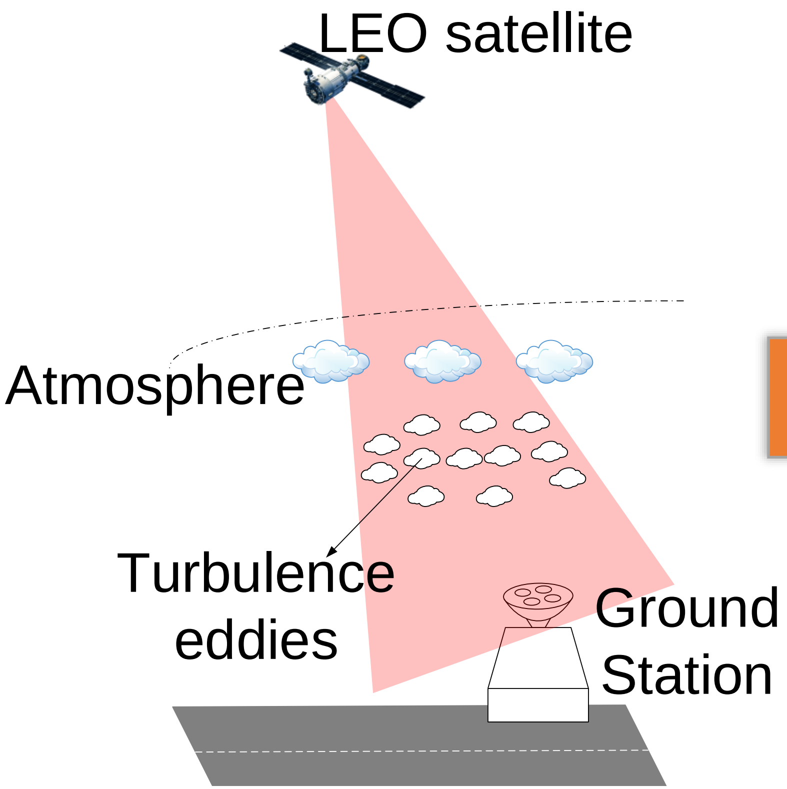
Unmanned aerial vehicle

Express train

Ship

2. Simper, cheaper implementation → Dual-Threshold Direct-Detection (DT-DD) was proposed [4]

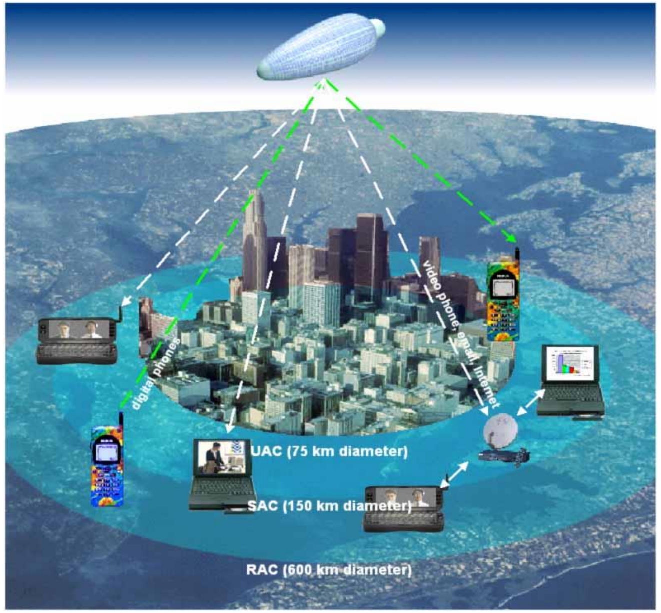
Satellite FSO/QKD



Conventional satellite-based FSO System

Coverage: high power required
Cost: more satellites required

High Altitude Platform (HAP)



- The altitude of HAP: 17-25 km
- HAP communications has many advantages such as large coverage area, high speed connection, easy maintenance, and rapid deployment

DT-DD: How it Works?

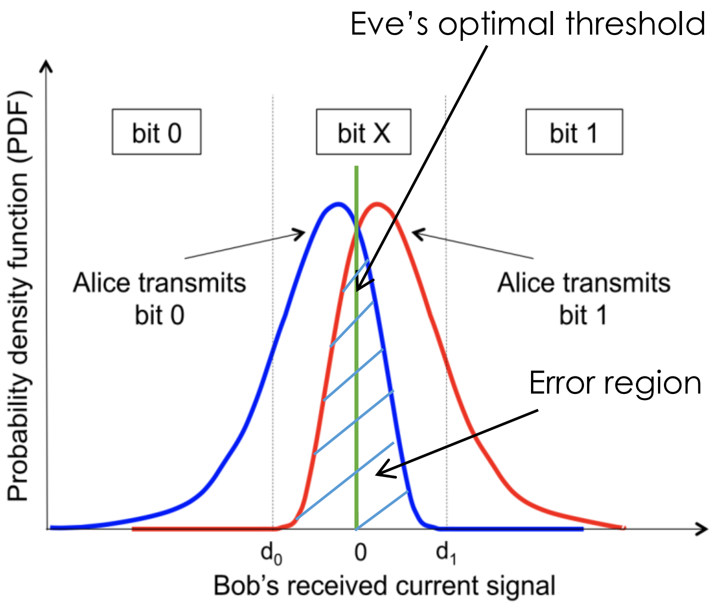
- Dual Threshold-Direct Detection (DT-DD) mimics the BB84 protocol
- This protocol could implement feasibly on standard FSO systems with simple configurations
- Operational steps:
  - Step 1: Alice transmit Subcarrier Intensity Modulation/Binary Phase Shift Keying (SIM/BPSK) signal corresponding to random bits "0" or "1" which have very close intensity level
    - In BB84, Alice choose two bases randomly

DT-DD (Cont.)

- Step 2: Bob received signal → use a DT detector with detection rule

$$\text{Decision} = \begin{cases} 0\ if\ (i \le d_0) \\ 1\ if (i \ge d_1) \\ X\ (no\ bit) otherwise\ \ \rightarrow Bob\ does\ not\ recover\ the\ transmitted\ bit \end{cases}$$

  - In DT-DD, Bob can adjust 2 threshold
  - In BB84 , Bob choose two bases randomly to detect the received photon
  - X is is similar to the case of inaccurate basis selection in BB84
- Step 3: Bob notifies time instants he recovered binary bits → Alice discard time instants Bob recovered no bit → form **sifted key**
  - In BB84, Alice and Bob discard the photon measurements where Bob used a different basis → form **sifted key**
- Step 4: **Information reconciliation** & **privacy amplification**
- Eve try to use DT → Eve's signal fluctuation is uncorrelated to Bob's one → key bits created by Bob and Eve do not match
- Eve does not know 2 threshold → use optimal threshold → high error rate

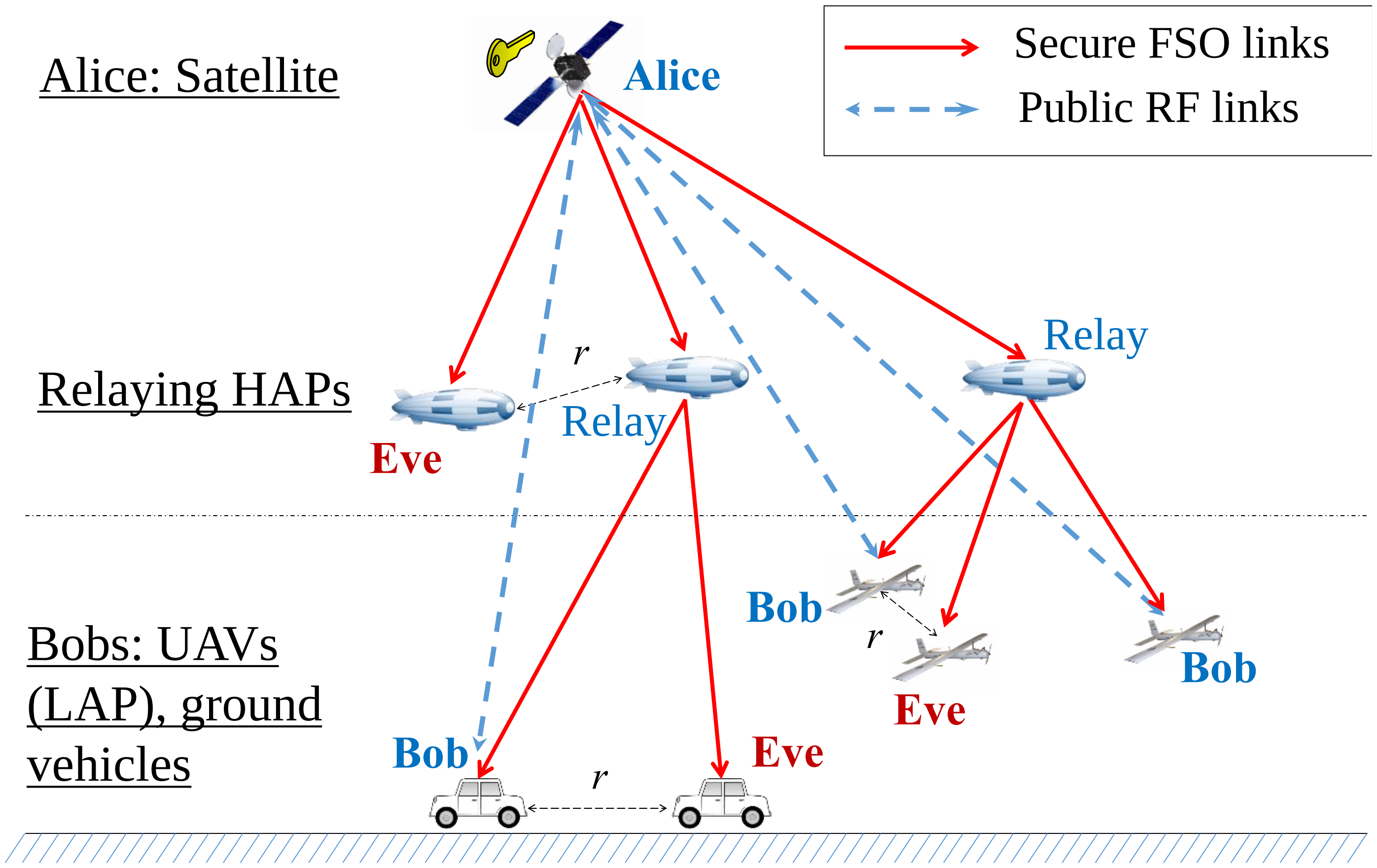


The probability density function of Bob's received signal over atmospheric turbulence induced-fading channel [4]

Our Design

1. QKD over free space optics (FSO) system to offer optical wireless solution
2. Instead of using single-photo based QKD, we use standard intensity-modulation (IM) FSO system with dual-threshold detection
3. Satellite-based system with **High-altitude platform (HAP) as a relaying station** → extend the coverage and system performance

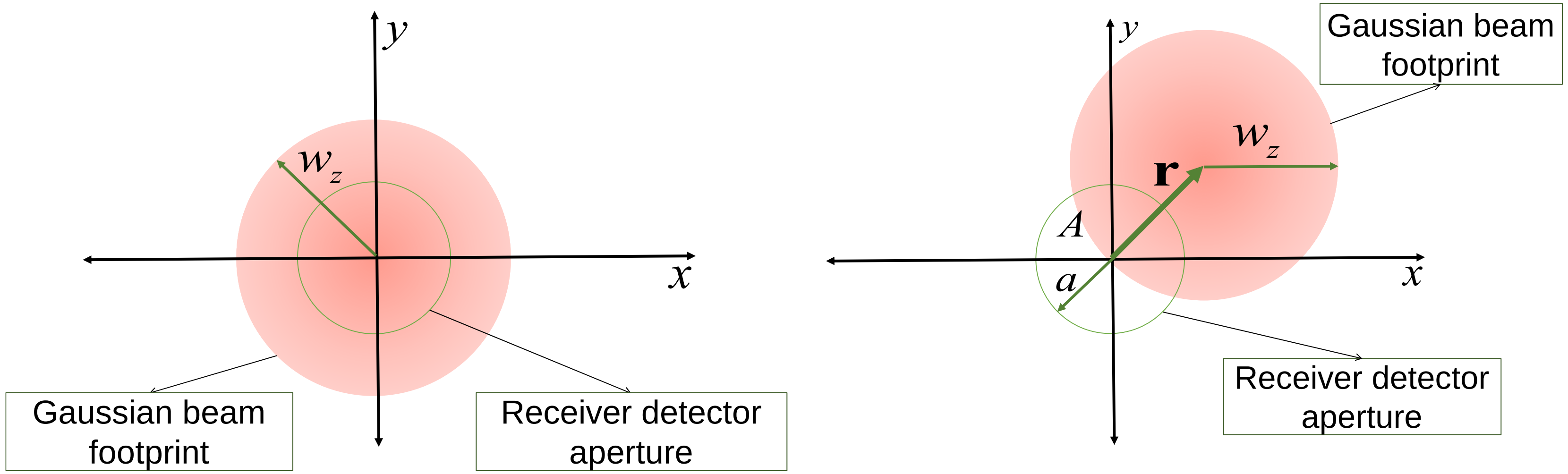
System Model



- Satellite (Alice): low to high orbits, key generation and distribution hub
- HAP: as relaying station, amplify signal
- Bob: UAV, regular vehicles
- Eve: eavesdropper
- FSO link: Intensity Modulation (IM) and Dual-Threshold/Direct-Detection (DT/DD)

Channel Model

- Path loss
- Beam spreading and misalignment: Gaussian beam



- Atmospheric turbulence
  - Gamma-Gamma turbulence model

Performance Analysis

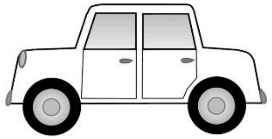
- We focus on deriving the ergodic secret key rate – the most critical performance metric of QKD system

$$\boxed{S = I(A,B) - I(A,E)}$$

  - $S > 0$: The proposed system is secured
  - $S < 0$: The security of the proposed system is threatened by Eve

- Eve could be

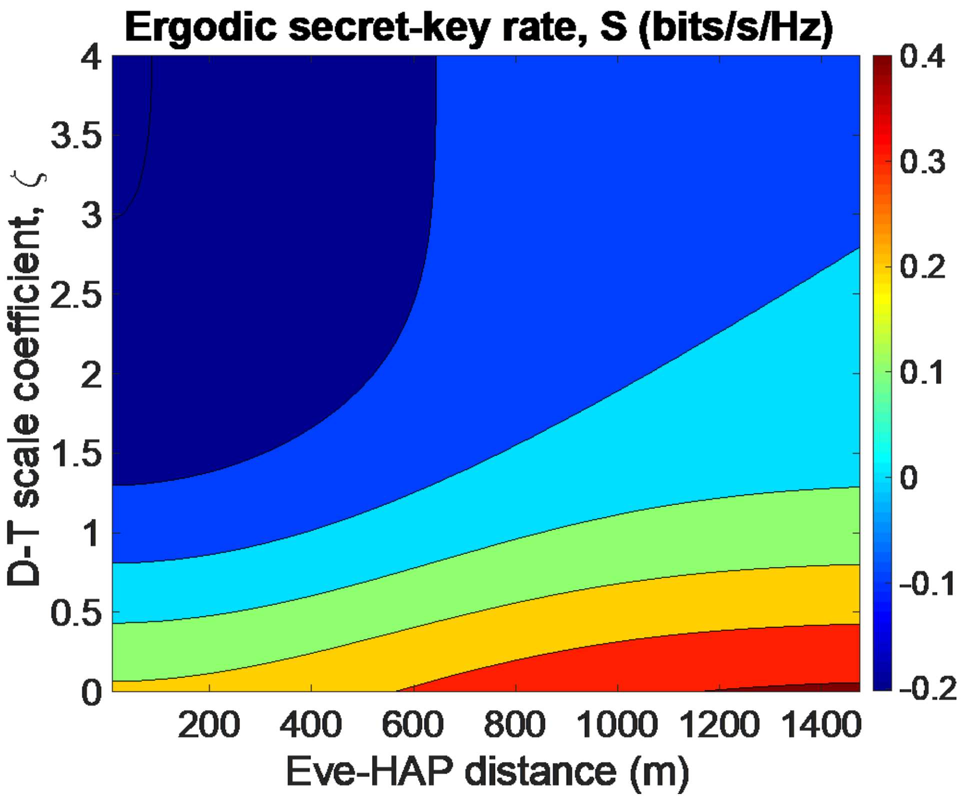
Scenario 1



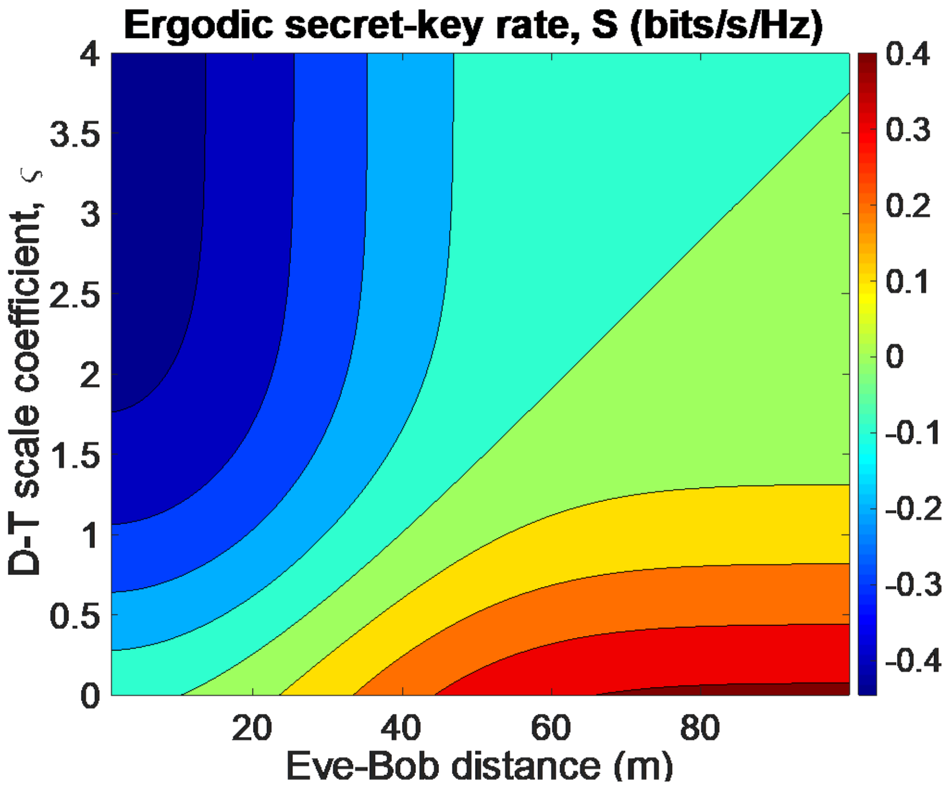
Scenario 2

Results and Discussion

Scenario 1



Scenario 2



- With adjustment of D-T scale coefficient, the secrecy with Alice can be improved
- The minimum distance between HAP & Eve, Bob & Eve to guarantee the proposed system is secure can be determined

Conclusion

- We proposed HAP-aided relaying satellite FSO/QKD systems for vehicular networks
- Some initial results confirm the feasibility of the proposed system and help find out suitable parameters for preventing eavesdroppers

References

[1] Richard J. Hughes, George L. Morgan, C. Glen Peterson; “Practical quantum key distribution over a 48-km optical fiber network”; Journal of Modern Optics,LA-UR-99-1593, 1999.

[2] Jouguet P., Kunz-Jacques S., Leverrier A., Grangier P. & Diamanti E. Experimental demonstration of long-distance continuous-variable quantum key distribution. Nature Photon. 7, 378–381 (2013).

[3] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre, Nat. Photonics 9, 163 (2015)

[4] 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," in IEEE Access, vol. 6, pp. 4159-4175, 2018.

Thank you!

HAP: Examples

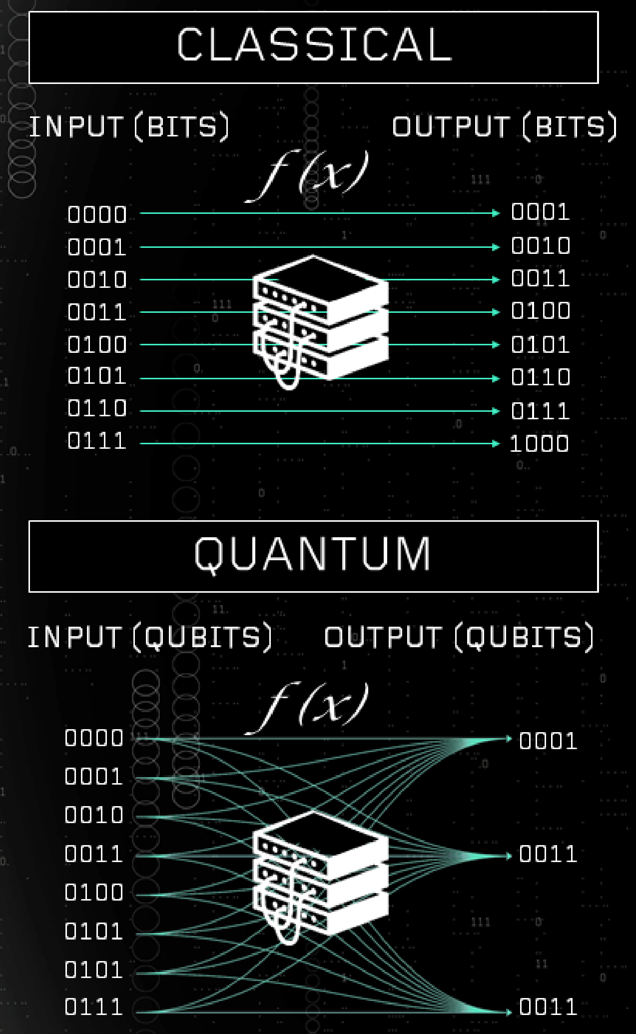
Manned Planes
–e.g. Grob G520T Egrett

Unmanned Hydrogen Powered Planes
– e.g. Global Observer

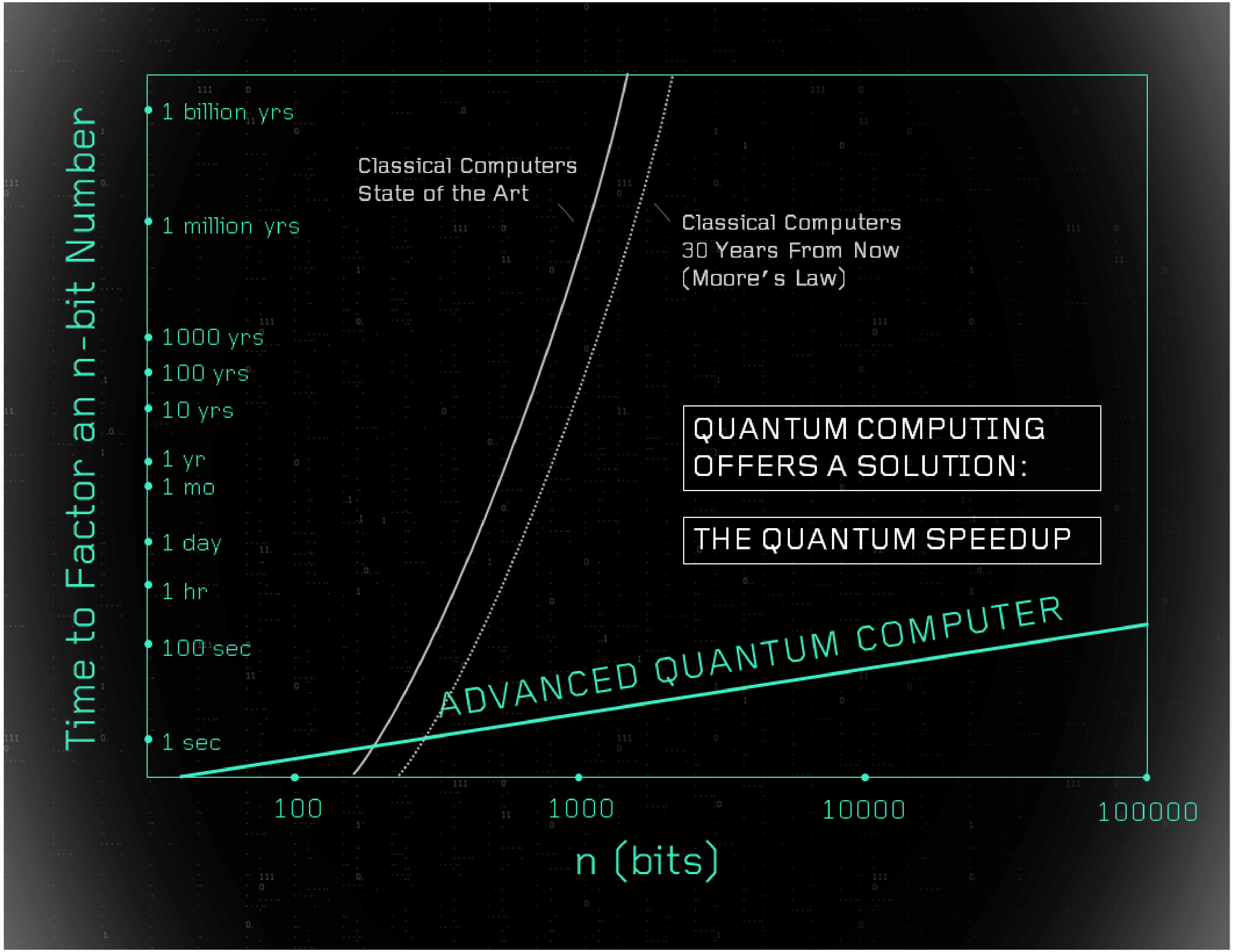
Unmanned Solar Powered Planes
–e.g. NASA/AV Pathfinder Plus

Unmanned Solar Powered Airships
–e.g. Lockheed Martin HAA

ex



- A quantum system replaces classical bits with quantum bits (qubits)
- Qubits follow the superposition principle, and can exist as a logical 0 and 1 *at the same time*
- Using qubits instead of bits, with a single input, one can process all combinations of 0s and 1s in a string *at the same time*
- Quantum algorithms using this ability could solve certain types of problems much faster than any classical computer


Time to Factor an n-bit Number
1 billion yrs
1 million yrs
1000 yrs
100 yrs
10 yrs
1 yr
1 mo
1 day
1 hr
100 sec
1 sec
Classical Computers
State of the Art
Classical Computers
30 Years From Now
(Moore's Law)
QUANTUM COMPUTING
OFFERS A SOLUTION:
THE QUANTUM SPEEDUP
ADVANCED QUANTUM COMPUTER
100
1000
10000
100000
n (bits)

ex

BB84 Protocol

- (Key) bits are transmitted over quantum channel, e.g. photo transmission
- **Step 1**: Alice encode bits (0 or 1) by randomly using either one of two encoding bases

Bit	Encoding Basis	
	Rectilinear	Diagonal
1	$\rightarrow$	$\nearrow$
0	$\uparrow$	$\searrow$

- **Step 2**: Bob also randomly select a basis to decode
  - Alice's encoding basis = Bob's decoding basis → the corresponding bit is read correctly with **high probability**
  - Alice's encoding basis ≠ Bob's decoding basis → the received photon is measured as one of two polarization states of the used basis at Bob

BB84 Protocol (cont.)

- **Step 3**: Alice broadcasts her bases choice → Bob reveals on which detected photon the same bases was used to measure→ Alice and Bob discard bits where the different bases was used → form **sifted key**
- **Step 4**:
  - Alice and Bob perform **information reconciliation** → identify, remove erroneous bits
  - Alice and Bob apply **privacy amplification** → produce a new, shorter key