SmartQuantum

Can you keep a secret?

SmartQuantum

High speed networks security experts

CryptArchi 2008

Agenda

High Speed Networks Security

QKG : Quantum Key Generation

Protocols (BB84, B92...)

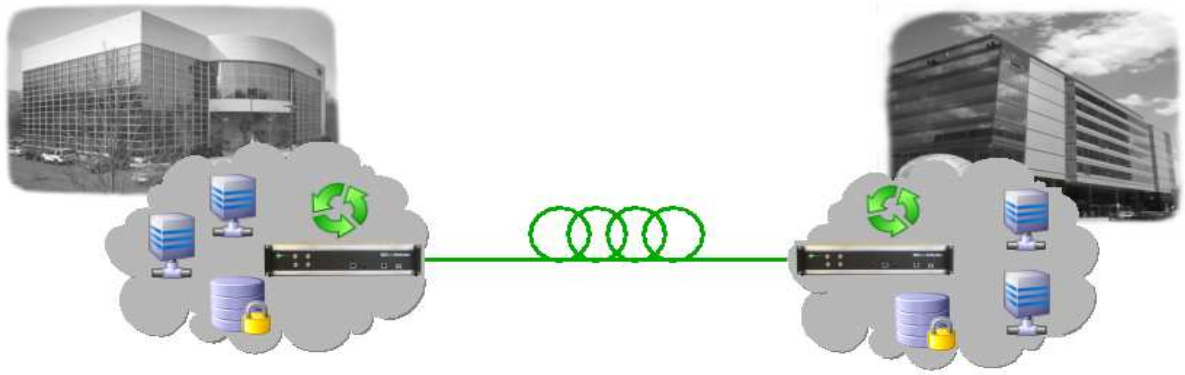
Practical implementation

SmartQuantum Products

High Speed Networks Security

How to Secure High Speed Data transmission links?

- **Use Symmetrical Encryption Algorithms**
- **Secure Key Management**



Quantum Key Generation : Principles

Quantum Key Generation

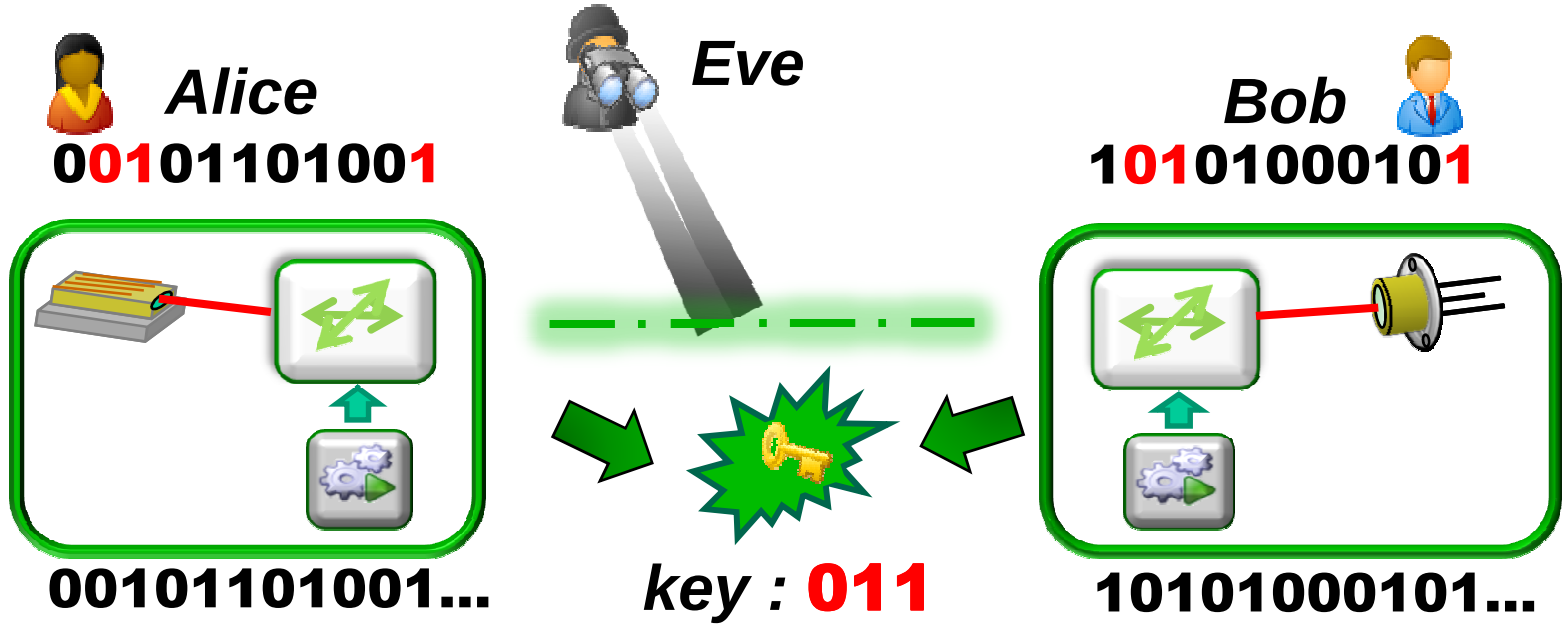
Principles :

- **Each bit is encoded with one photon pulse (polarized light)**
- **Two protagonists : Alice and Bob**
- **A spy : Eve**
- **“Quantum physic laws” are used to bring security**

Quantum Key Generation : Principles

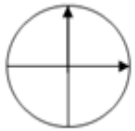
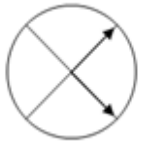
Key Generation : To create a secret shared only by Alice and Bob

- **The Key : A common bit stream between Alice and Bob**
- **A random Generator is used in each site to generate a raw bit stream**
- **Objective : Find some common bits, without giving enough info to Eve.**



Protocol BB84

- First protocol from Bennett and Brassard in 1984 (BB84)
- Use polarisation principles
- A Public Channel for basis reconciliation
- Two basis are used to transmit 0 or 1 :

- Standard  Base A
- Diagonal  Base B

4 states to transmit 0 or 1 : (0,0) (0,1) (1,0) (1,1)

Protocol BB84

Key Generation Matrix

(ALICE)				(BOB)			
Bit sent	Base used	Polarisation State		Base used		Bit Detected	Error
0	Std	↔		Std		0	NO
0	Std	↔		Diag	Undetermined	0	NO
						1	YES
0	Diag	⤢		Std	Undetermined	0	NO
						1	YES
0	Diag	⤢		Diag		0	NO
1	Std	↕		Std		1	NO
1	Std	↕		Diag	Undetermined	0	YES
						1	NO
1	Diag	⤡		Std	Undetermined	0	YES
						1	NO
1	Diag	⤡		Diag		1	NO

Protocol BB84

Error Correction process : Basis reconciliation

(ALICE)			(BOB)			
Bit sent	Base used	Polarisation State	Base used		Bit Detected	Error
0	Std	↔	Std		0	NO
0	Std	↔	Diag	Undetermined	0	NO
					1	YES
0	Diag	⤢	Std	Undetermined	0	NO
					1	YES
0	Diag	⤢	Diag		0	NO
1	Std	↕	Std		1	NO
1	Std	↕	Diag	Undetermined	0	YES
					1	NO
1	Diag	⤡	Std	Undetermined	0	YES
					1	NO
1	Diag	⤡	Diag		1	NO

Protocol BB84

Error Correction process

(ALICE)			(BOB)		
Bit sent	*Base used*	*Polarisation State*	*Base used*	*Bit Detected*	*Error*
0	*Std*	↔	*Std*	**0**	**NO**
0	*Diag*	⤢	*Diag*	**0**	**NO**
1	*Std*	↕	*Std*	**1**	**NO**
1	*Diag*	⤡	*Diag*	**1**	**NO**

Protocol BB84

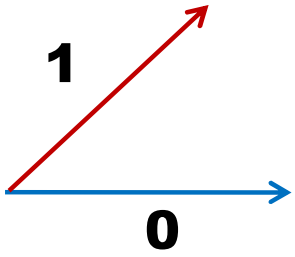
Process securisation against Eve attack

(ALICE)			(EVE)				(BOB)		
Bit sent	*Base used*	*Polarisation State*	*Base used*	*Bit Detected*	*Bit Sent*	*Polarisation State*	*Base used*	*Bit Detected*	*Post Reconciliation Error*
0	*Std*	↔	*Std*	**0**	**0**	↔	*Std*	**0**	**NO**
			Diag	undetermined	**0**	⤢	*Std*	**0**	**NO**
								1	**YES**
			Diag	undetermined	**1**	⤡	*Std*	**0**	**NO**
								1	**YES**

Monitor Error Rate to detect Eve potential attack

Protocol B92

- Similar to BB84
- Bennett in 1992 : B92
- Only one non orthogonal basis :



Only 2 states to transmit 0 or 1

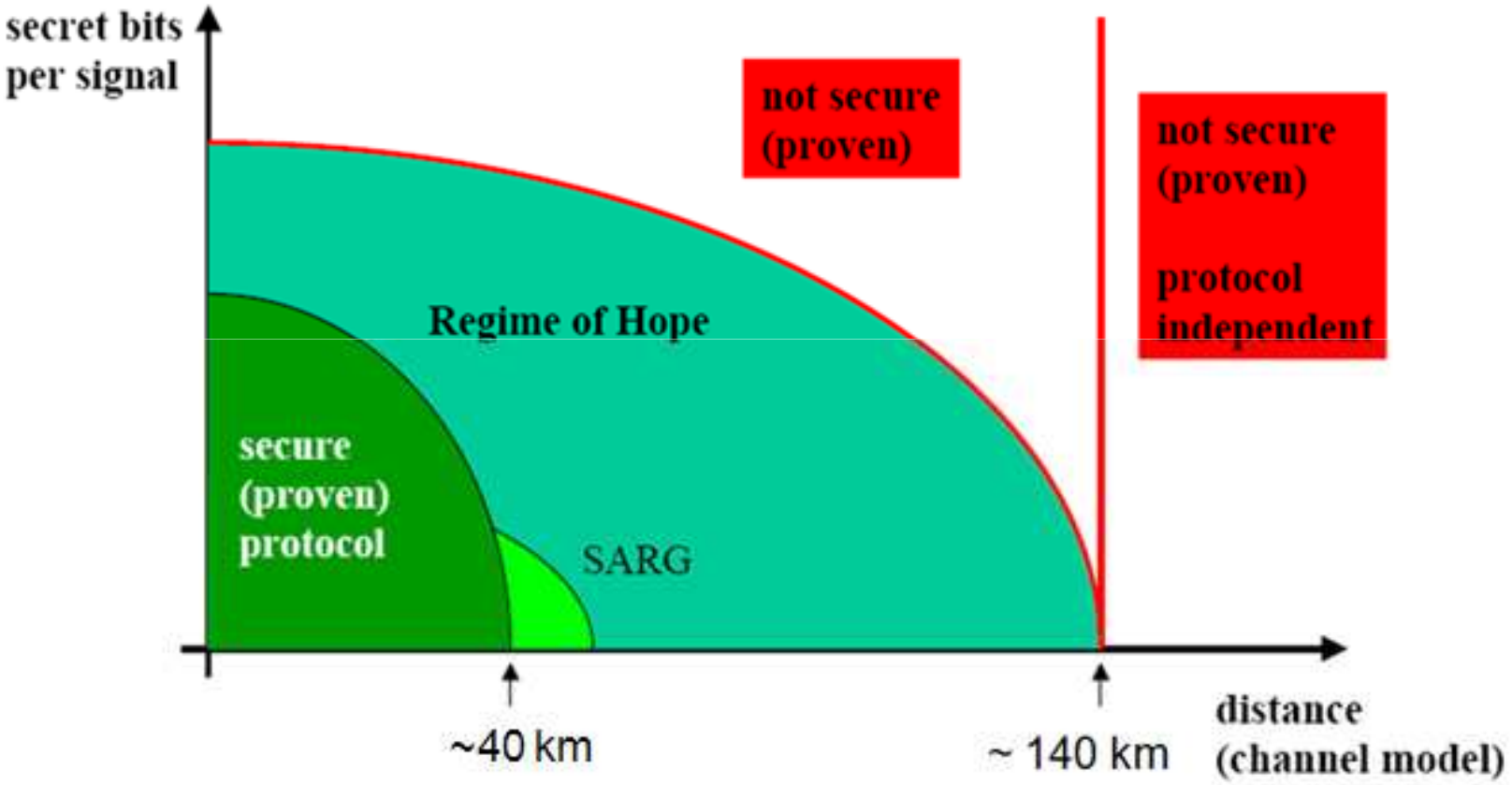
BB84 Practical implementation

- Theorical approach : Need “Single photon Source” or photon gun
- Practical implementation : “coherent weak laser pulse”

Eve attack : PNS
(Photon Number Splitting)

Define New protocols

New protocols : SARG, Decoy State



Technical Implementation

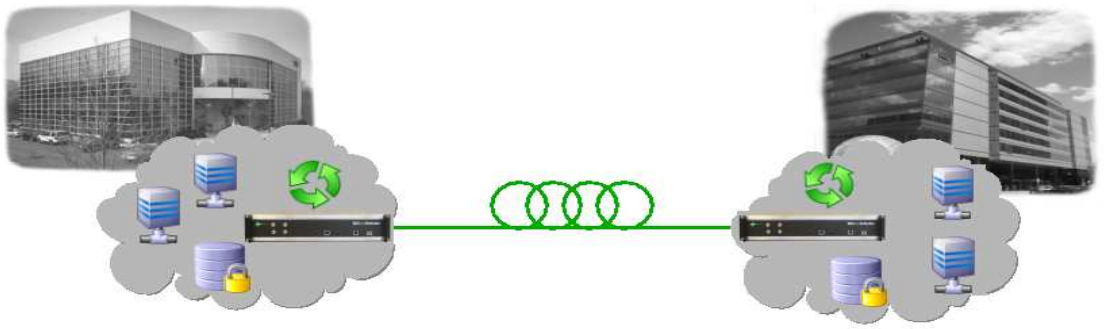
Phase modulation inTime Domain

- **Based on Long Arm Interferometer**
- **Long term stability? Sensitive to polarisation diversity**

Phase modulation in Frequency domain

- **SmartQuantum and CNRS leadership**
- **Easy to implement**
- **Patented technology**

SQBox Defender

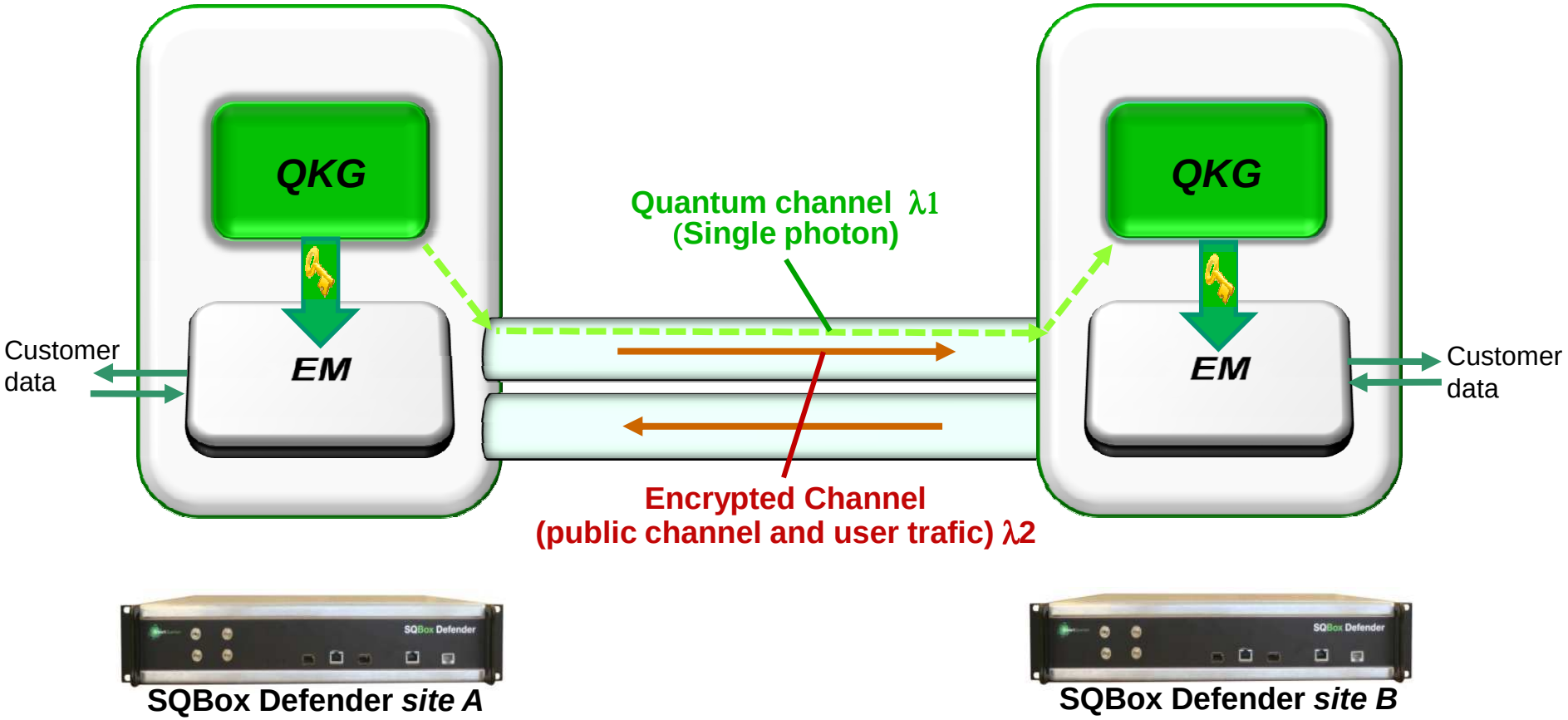


2U

QKG
+
High Speed Encryption
(AES)

- **Highly Integrated solution**
- **2 U 19'' telecom subrack**
- **High speed real-time encryption (1 Gb/s)**
- **AES 192 bits**
- **Dynamic Quantum Key Generation (QKG)**
- **1 Fibre technology (WDM)**
- **Point to point solution**

SQBox Defender



EM Encryption Module

QKG Quantum Key Generation Module

Conclusion

Quantum Key Generation :

- **High speed key updating**
- **Intrusion detection attempt**
- **Physical key security**
- **Easy of use security solution**

INDUSTRIAL

FINANCE

BACKUP

DEFENSE

TELECOM

SmartQuantum

4 rue de Broglie
22300 Lannion, France
Tel : 00.33.(0)2.96.48.59.35
Fax : 00.33.(0)2.96.48.50.24
@ : info@smartquantum.com
Url : www.smartquantum.com