Quantum Key Distribution (QKD)

Prashanta Kharel

Applied Physics Seminar

November 2012

Welcome to Facebook – Log In, Sign Up or Learn More

https www.facebook.com/index.php?stype=lo&lh=Ac-zkc_D4XgaKfMK

Reader

Application Apple Yahoo! Google Maps YouTube Wikipedia News GRE Popular

facebook

Email or Phone

Password

Log In

Keep me logged in

Forgot your password?

Facebook helps you connect and share with the people in your life.

Sign Up

It's free and always will be.

Your First Name

Your Last Name

Your Email

Re-enter Email

New Password

Birthday:

Month: Day: Year: Why do I need to provide my birthday?

Female Male

By clicking Sign Up, you agree to our Terms and that you have read our Data Use Policy, including our Cookie Use.

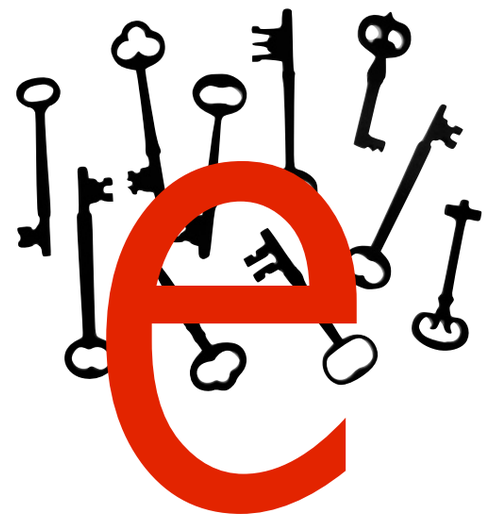
Sign Up

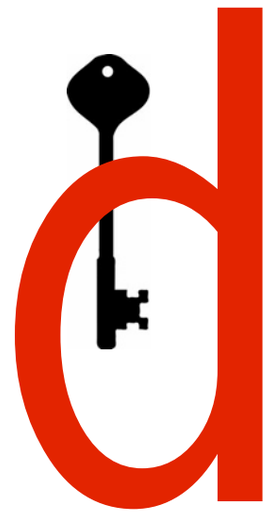
Classical Key Distribution

RSA Encryption

- Relies on two distinct large prime numbers
- factorization of prime
- exponential problem
- limited only by computational power

Message: “SEAS” “01000101”





Public Key

$c = m^e \pmod{n}$

Encode

“01000101”

Private Key

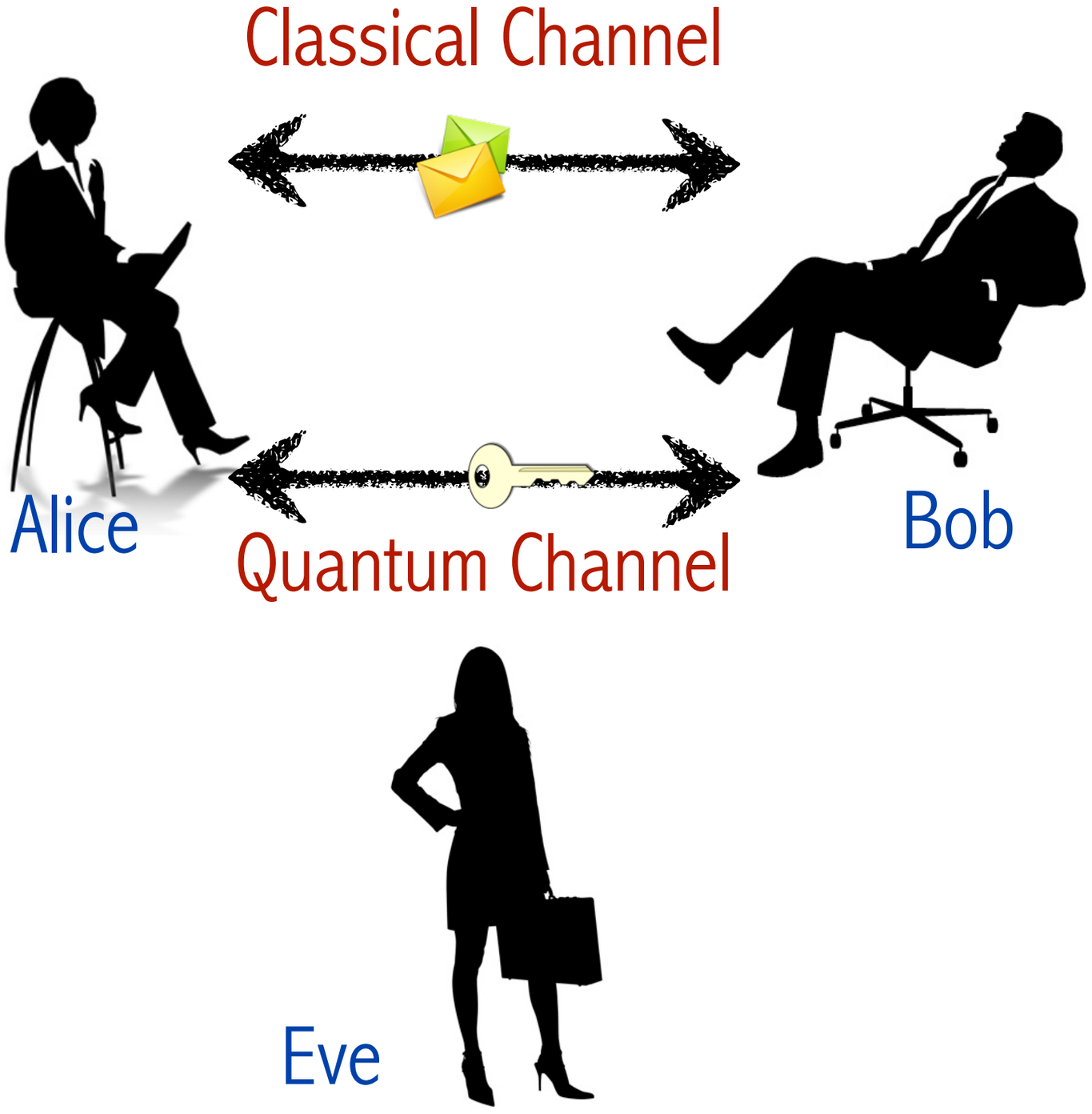
$m = c^d \pmod{n}$

Decode

“SEAS”

Quantum Key Distribution(QKD)

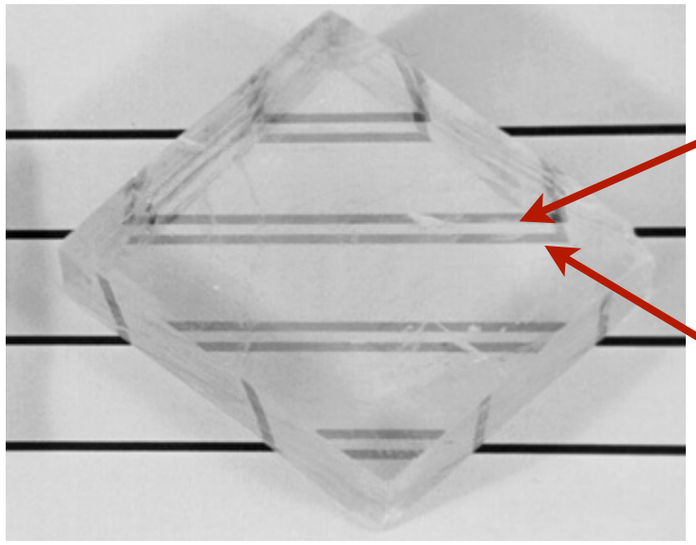
- relies on fundamental quantum mechanics
- unconditionally secure
- eavesdropper can be detected



BB84-Protocol

RSA Encryption

- Uses polarized light
- Uncertainty principle for single photons



V- Polarized

H-Polarized

Calcite Crystal

Measure

D

d

Diagonal Basis

P = 1/2

P=1/2

Measure

V

H

Rectilinear Basis

BB84-Protocol

How to share a secret key?

H/V Basis
H=0 →
V=1 ↑

D/d Basis
D=0 ↖
d=1 ↗

Quantum Channel

Bits	0	1	1	0	1	1	0	0	1	0	1
Alice's Random Basis	D	R	D	R	R	R	R	D	R	D	D
Photon Alice Sends	↖	↑	↗	→	↑	↑	→	↖	↑	↖	↗
Bob's Random Basis	D	D	R	R	R	R	D	D	R	R	D
Bits received by Bob	0	0	1	0		1	1	0	1		1

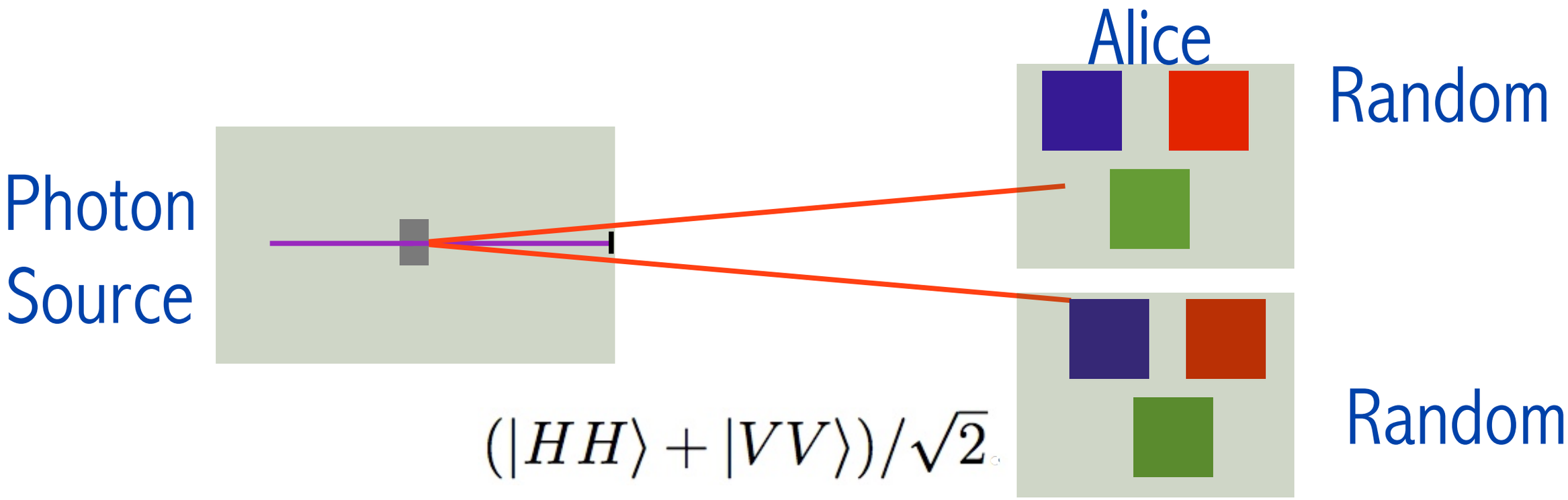
Public Channel

Bob Report Basis	D	D	R	R		R	D	D	R		D
Alice confirms correct ones	OK			OK		OK		OK	OK		OK
Shifted Key	0			0		1		0	1		1

Correlated measurements

Ekert's Protocol

Three Conjugate Basis: H/V, D/d, L/R

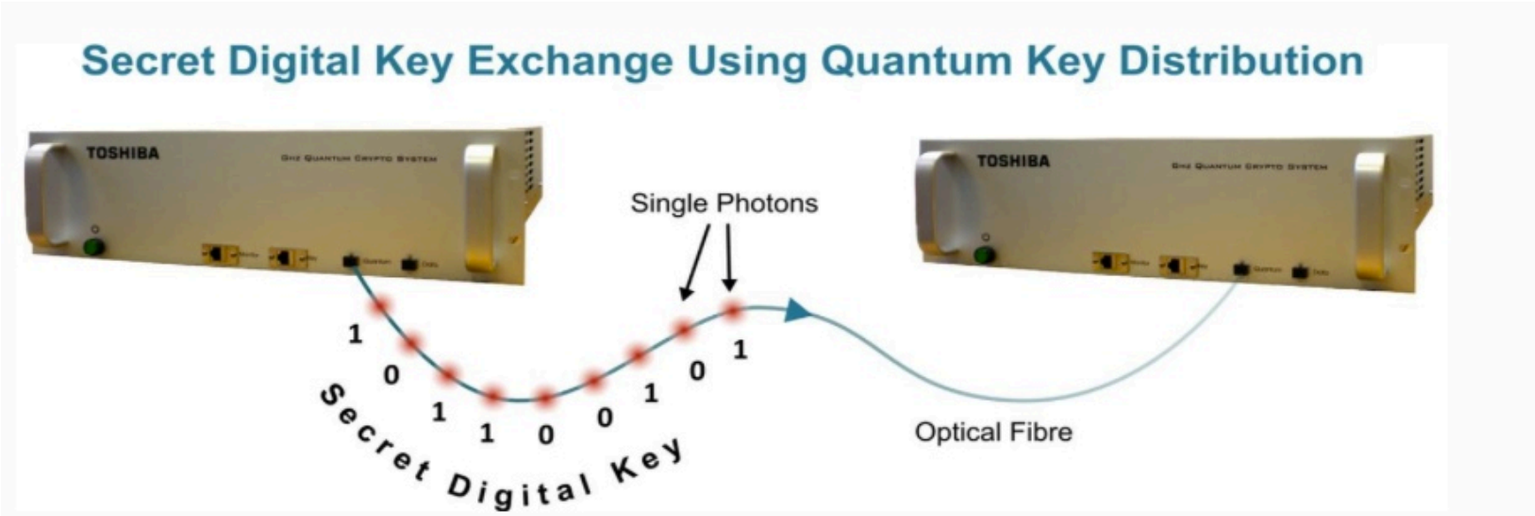


$$(|HH\rangle + |VV\rangle)/\sqrt{2}$$

- Shifted key is smaller
- More sensitive to eavesdropping

Conclusion

- 2009 Yamamoto, up to 105 km, 17 kbits/sec
- 2012 Shields, up to 90 km, ~1Gbits/sec



Future:

- High Key Generation Rate
- Noisy channel
- QKD over longer distances

Questions

Sources

- 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, Bangalore, India, 1984, (IEEE Press, 1984), pp. 175–179; C.H. Bennett and G. Brassard, “Quantum public key distribution,” IBM Technical Disclosure Bulletin 28, 3153–3163 (1985).

- N. Ilic, “The Ekert Protocol”, University of Waterloo

- Y. Yamamoto et al., “Quantum key distribution over 40 dB channel loss using superconducting single photon detectors,” arXiv, 2009

- Zeeya Merali, “Quantum cryptography conquers noise problem,” Nature, 2012