

# *Game Theoretic Security Framework for Quantum Key Distribution*

Walter O. Krawec  
Department of Computer Science  
University of Connecticut  
Storrs, CT USA

walter.krawec@uconn.edu

Fei Miao  
Department of Computer Science  
University of Connecticut  
Storrs, CT USA

fei.miao@uconn.edu

Presented by: **Omar Amer**, University of Connecticut

# *Quantum Key Distribution (QKD)*

- Allows two users – Alice (A) and Bob (B) – to establish a shared secret key
- Secure against an all powerful adversary
  - Does not require any computational assumptions
  - Attacker bounded only by the laws of physics
  - Something that is not possible using classical means only
- Accomplished using a *quantum communication channel*

# *QKD in Practice*

- Quantum Key Distribution is here already
- Several companies produce commercial QKD equipment
  - MagiQ Technologies
  - id Quantique
  - SeQureNet
  - Quintessence Labs
- Have also been used in various applications:
  - QKD was used to transmit ballot results for national elections in Switzerland
  - Has also been used to carry out bank transactions <sup>3</sup>

# *QKD in Practice*

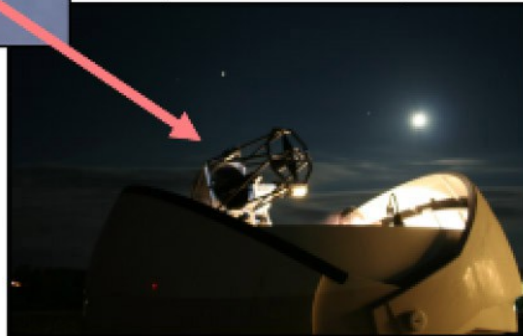
- Quantum Networks being developed or in use now
  - Boston area (DARPA)
  - Tokyo
  - Vienna
  - Wuhu, China
  - Geneva
- Freespace QKD being developed...

# *QKD in Practice: Freespace*

Alice



Bob



<http://spie.org/newsroom/5189-free-space-laser-5-system-for-secure-air-to-ground-quantum-communications>

# *QKD Protocols*

- QKD Protocols are designed and analyzed in a *standard adversarial model (SAM)*
  - Alice and Bob run the protocol with the goal of establishing a shared secret key
  - An all-powerful adversary (Eve) sits in the middle of the channel intercepting each qubit sent
  - This adversary is *malicious* and has no motivation to attack nor does she care about the cost of attacking

# *Game Theoretic Model*

- In this work, we investigate the use of *game theory* to study the security of QKD protocols
- Motivational idea is that, while QKD technology is available now, it is very expensive to purchase and operate.
  - e.g., good measurement devices must be super-cooled
- Thus, participants, including attackers, may take this expense into account
- If attacking a quantum channel requires a great expense and, at the end of it, all you can hope to do is **slow the communication rate**, perhaps it is not worth the cost

## *Game Theoretic Model - Related*

- Game Theory has been used to analyze some **classical** cryptographic primitives (e.g., rational secret sharing)
- Some recent preliminary work has been done by other authors in attempting to combine game theory with QKD, however past approaches have been restrictive



# *Our Contributions*

- We propose a new, general, game-theoretic framework for QKD protocols
- Our approach allows for important security computations vital to understanding the security of QKD protocols
- We apply our approach to two different QKD protocols and in two different adversarial models
- We show that, in the game theoretic model, noise tolerance upper-bounds in the SAM are comparable, however *greater communication efficiency may be attained*

# *General QKD Operation*

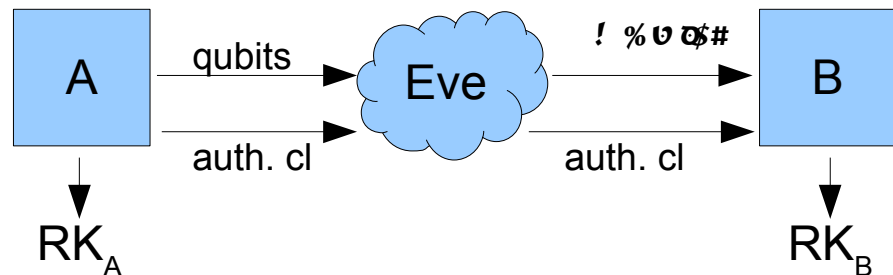
# *QKD Operation*

- QKD Protocols utilize:
  - Quantum Communication Channel
  - Authenticated Classical Channel

# QKD Operation

## Quantum Communication Stage: Numerous Iterations

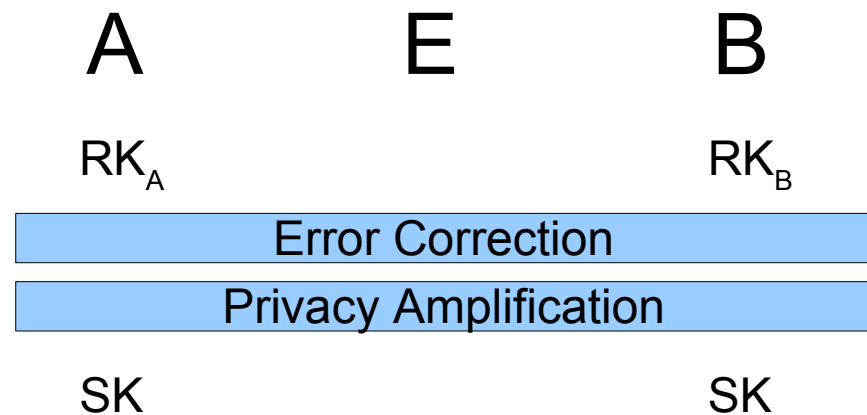
A + B communicate using qubits and the auth. channel through numerous **iterations**; Eve's attack disturbs the qubits; result is a **raw-key**



## Information Reconciliation (Classical Post Processing)

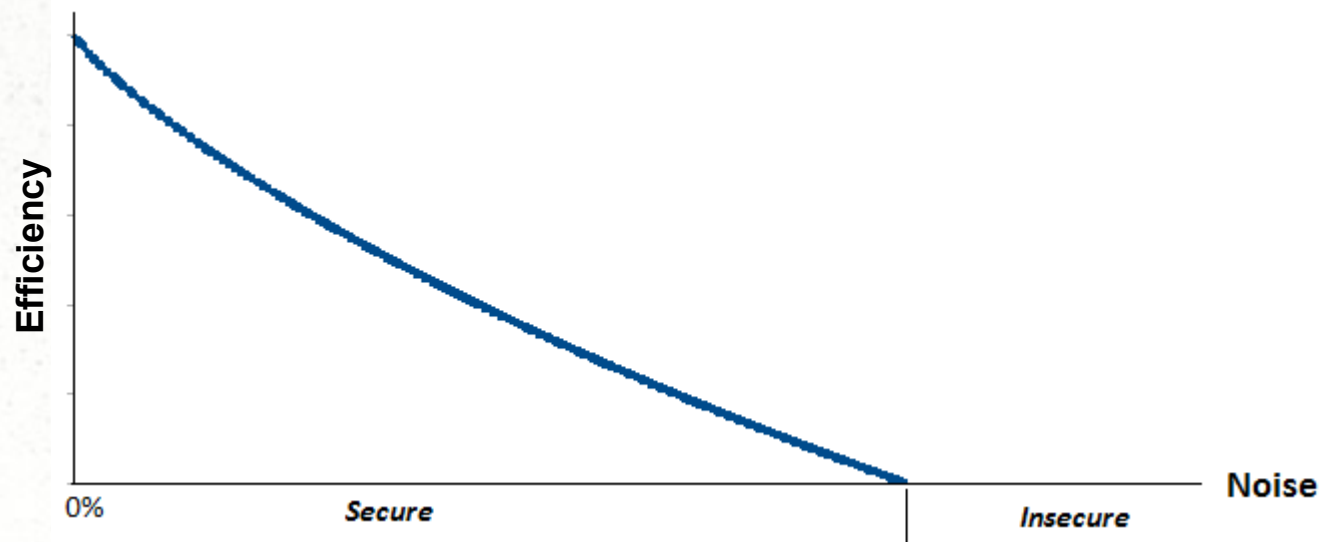
A + B use the auth. channel to run “error correction” (**leaking extra information to Eve**) and “privacy amplification” to produce the actual secret key.

Note:  $|SK| \leq |RK|$



# *QKD – General Operation*

- Eve cannot copy qubits – has to attack **actively**
- Direct correlation between **noise** and adversary's potential **information**
- The more information E has, the more PA must “shrink” the key by – thus as the noise increases, the efficiency drops:



# *Our Model*

# *Game Theoretic Model*

- We model QKD as a two-party game:
- Player 1: “AB”
  - Technically two separate entities, however we model them as one player
  - Their goal is to establish a long shared secret key between one another
- Player 2: “E”
  - The adversary whose goal is to limit the length of the final secret key

## *Game Theoretic Model*

- Using the quantum channel, however, is costly
- Thus, AB may wish to simply “abort” and do nothing depending on the **noise** in the channel
- Furthermore, if attacking the channel is too expensive for too little reward (simply decreasing users' efficiency), E may wish not to attack



## *Eve's Strategy*

- Denial-of-Service attacks are outside of our model
  - Thus all attacks must induce noise less than some value “Q”
- This noise level can represent natural noise in a quantum channel plus some “leeway” for example.
- We are interested in finding the **maximal allowed Q** for which a key may be established in our rational model
  - This is also an important question in the SAM allowing us to compare!

## *Model*

- Let  $S_{AB}$  be the set of strategies (i.e., *protocols*) which AB may choose to run and let  $S_E$  be the set of strategies (i.e., *attacks*) which party E may choose to use.
- We always assume the “do nothing” strategy is available to both players (denoted  $I_{AB}$  and  $I_E$ )
- Let  $Q$  be the maximal noise in the channel (which we wish to upper-bound).

# Utility

- AB: the outcome is a function of the resulting *secret key length*, denoted “M” (after error correction and privacy amplification) along with the cost of running the chosen protocol:

$$u_{AB}(M, C_{AB}(\Pi)) = w_g^{AB} M - w_c^{AB} C_{AB}(\Pi)$$

- E: the utility is a function of information gained on the *error-corrected* raw key, denoted “K” (before privacy amplification) and cost:

$$u_E(K, C_E(A)) = w_g^E K - w_c^E C_E(A)$$

## *Goal of the Model*

- The goal of the model is to construct a protocol “P” for AB such that  $(P, I_E)$  is a strict Nash Equilibrium (NE).
- That is, assuming *rational entities*, AB are motivated to run the protocol while E is motivated to not perform any attack on the quantum communication
- Model guarantees that the resulting key is information theoretic secure.
- While this is the same guarantee as in SAM, we will show greater efficiency is possible for certain noise scenarios!

# *Protocol Construction*

## *Protocols as Strategies*

- To create protocols so that  $(P, I_E)$  is a strict NE, in this work we take standard QKD protocols (such as BB84) and introduce “decoy iterations”
  - Decoy iterations are indistinguishable (to an adversary) from standard iterations
  - They are introduced randomly each iteration with probability “ $1-a$ ”

## *Protocols as Strategies*

- Decoy iterations cost AB resources and do not contribute to the raw key
- However, Eve is also forced to attack these iterations (as she does not know which are real or decoy iterations)
- We find scenarios when an optimal “a” exists depending on the noise level  $Q$ .

# *Application 1 – BB84 + All Powerful Attacks*



## *All-powerful Attacks Against BB84*

- We first consider the BB84 protocol, appended with decoy iterations
- Eve is allowed to perform an optimal all-powerful attack
  - This include a perfect quantum memory

# *All-powerful Attacks Against BB84*

- The expected utility for AB if Eve uses  $I_E$  is:

$$U_{AB}(BB84[a], I_E) = a \frac{N}{2} (1 - h(Q)) - C_{AB}$$

$$U_{AB}(I_{AB}, I_E) = 0$$

- Thus for a strict NE to exist, we require:

$$a > \frac{2C_{AB}}{N(1 - h(Q))}$$

Note: This already places a limit on how high “Q” can be before AB are unmotivated!

## *Eve's Utility*

- For Eve, if she does not attack but only listens passively to the error-correction information:

$$U_E(BB84[a], I_E) = a \frac{N}{2} h(Q)$$

- If she does attack, using an optimal quantum attack “V” (assuming such an attack is in  $S_E$ ), it can be shown that:

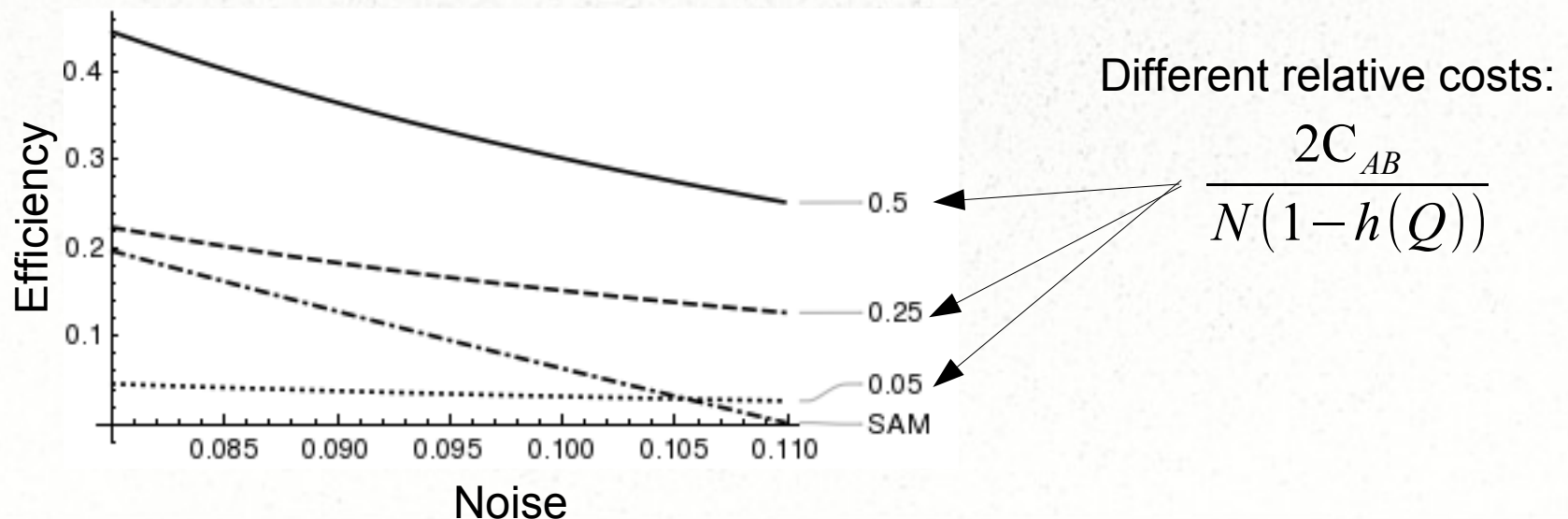
$$U_E(BB84[a], V) = a \left( \frac{N}{2} h(Q) + \frac{N}{2} h(Q) \right) - C_E = \boxed{aNh(Q) - C_E}$$

# Improvement in Efficiency

- If  $C_{AB} = C_E$ , then “a” exists only if

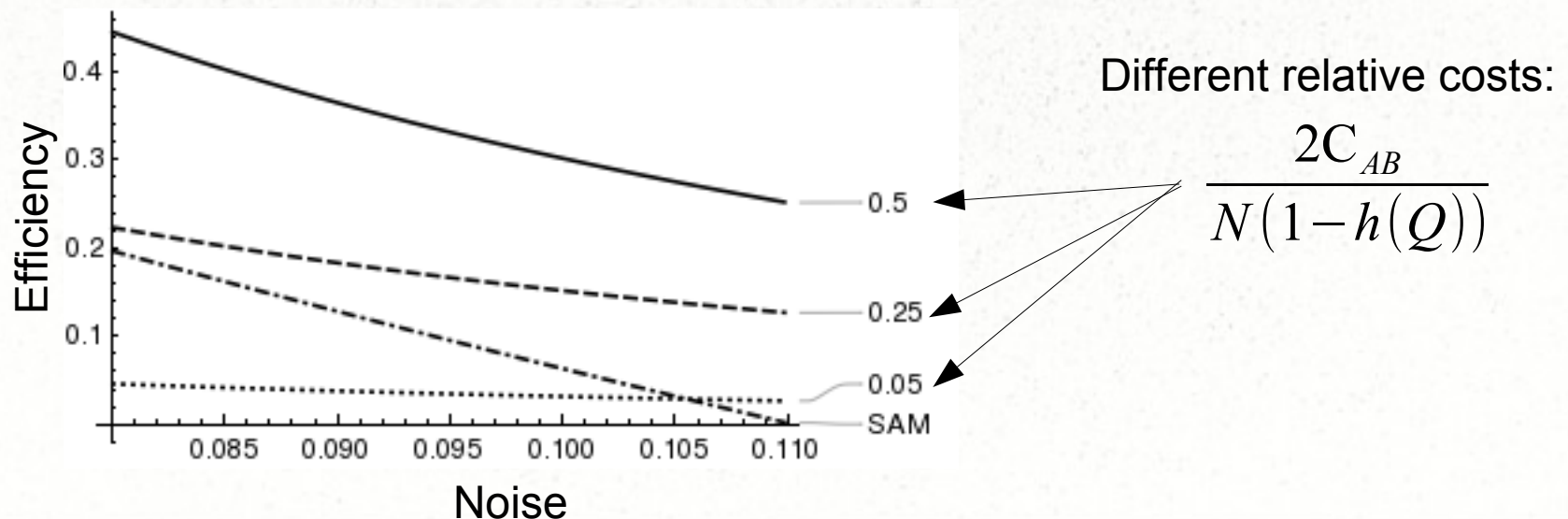
$$1 - 2h(Q) > 0 \quad \longrightarrow \quad Q < 11\%$$

- But, greater efficiency is possible:



# Improvement in Efficiency

- Note that, as the cost goes down (for both parties equally), the protocol becomes less efficient.
- This is because Eve is more motivated to attack and so more decoy iterations must be used
  - Decoy iterations decrease efficiency



## *Application 2: Practical Intercept/Resend Attacks*

## *Intercept/Resend Attack*

- We also consider more “practical” Intercept/Resend (I/R) attacks
- These use the same technology as AB (i.e., they do not require a perfect **quantum memory**)
- This allows us to more precisely compute  $C_E$  based on  $C_{AB}$

# *Intercept/Resend Attack*

- Eve attacks by **measuring** every qubit (something Bob must do) and **sending** a new one (something Alice must do)
- How she measures and sends is dependent on the attack
  - We consider three different strategies



# *Strategies*

- AB (3 strategies):
  - BB84[a]: Run the BB84 protocol using decoy iteration parameter “a”
  - B92[a]: Run the B92 protocol using decoy iteration parameter “a”
  - $I_{AB}$ : Do nothing
- E (4 strategies):
  - Three different “bases” for Intercept/Resend Attacks
    - Note, in the paper, we work out the algebra to allow future work analyzing arbitrary I/R attacks
  - $I_E$ : Do nothing

# *Strategies*

- BB84 and B92 are two commonly used protocols in practice.
- B92 is “cheaper” to implement but BB84 is more “robust” to noise in SAM
- We will show BB84 is the preferred choice in our game-theoretic model (despite its higher cost) for realistic noise levels

# *Cost Function*

**This allows us more control in computing cost of protocols and attacks:**

$C_S$ : Initial cost for E to setup attack equipment

$\gamma_x C_M$ : Cost to perform a measurement with “x” possible outcomes

$\gamma_x C_P$ : Cost to prepare (i.e., “send”) a qubit from “x” possible states

$C_R(d)$ : Cost to produce a d-biased bit

- We assume  $C_R(d) = h(d)C_R$ , for some  $C_R$

$C_{\text{auth}}$ : Cost for AB to use the authenticated channel

**Main Result:** If classical resources are free for both parties ( $C_R = C_{\text{auth}} = C_S = 0$ ) and if  $C_P \leq C_M$ , then there exists an  $0 < a < 1$  such that:

(BB84[a],  $I_E$ )

is a strict NE if the noise in the channel  $Q$  satisfies:

$$\left\{ \begin{array}{l} 10.025 \left( \frac{1}{4} + \frac{1}{4} h\left(\frac{2Q}{1-2Q}\right) - \frac{1}{2} h(Q) \right) - \left( \frac{\gamma_4}{\gamma_2} - 1 \right) > 0 \quad \text{If } A_1 > A_2 \\ 2.506 (1 - h(Q)) - \frac{\gamma_4}{\gamma_2} > 0 \quad \text{Otherwise} \end{array} \right.$$

Where:

$$A_1 = \frac{(\gamma_4 - \gamma_2) C_P}{\frac{1}{4} + \frac{1}{4} h\left(\frac{2Q}{1-2Q}\right) - \frac{1}{2} h(Q)} \quad A_2 = \frac{2 \gamma_4 (C_M + C_P)}{1 - h(Q)}$$

# *Theorem 1 – Noise Tolerance*

	$A_2 \geq A_1$	$A_1 > A_2$
$\gamma_4 = \gamma_2$	$Q \leq .146$	$n/a$
$\gamma_4 = 2\gamma_2$	$Q \leq .031$	$Q \leq .207$

# *Theorem 1 – Noise Tolerance*

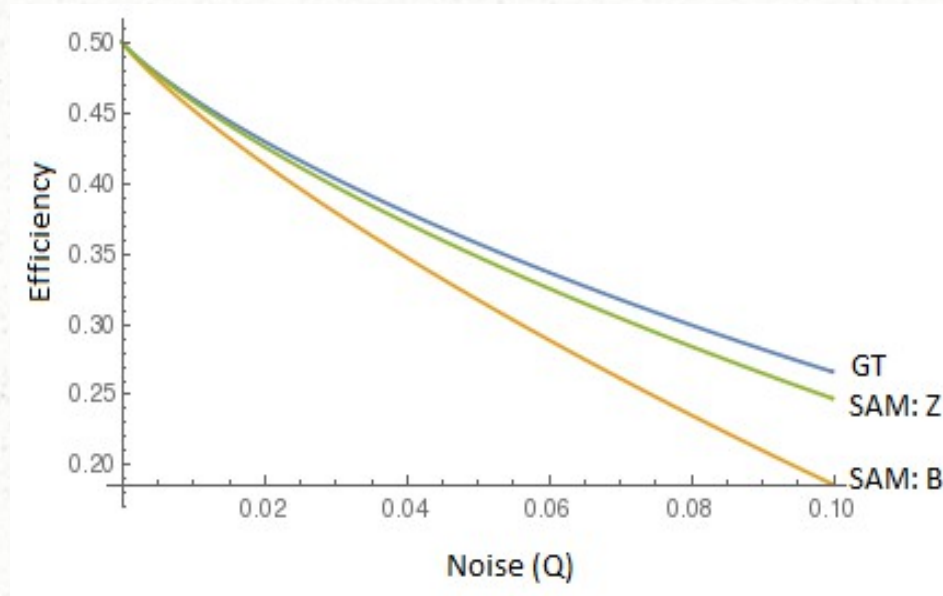
	$A_2 \geq A_1$	$A_1 > A_2$
$\gamma_4 = \gamma_2$	$Q \leq .146$	$n/a$
$\gamma_4 = 2\gamma_2$	$Q \leq .031$	$Q \leq .207$

This is the same noise tolerance against optimal **individual attacks** in SAM.

Individual attacks are **stronger** than I/R attacks.

Thus, our noise tolerance is lower than SAM; but, as before, efficiency may improve.

# *Theorem 1 – Noise Tolerance*



This is the same noise tolerance against optimal **individual attacks** in SAM.

Individual attacks are **stronger** than I/R attacks.

Thus, our noise tolerance is lower than SAM; but, as before, efficiency may improve.

# *Theorem 1 – Noise Tolerance*

	$A_2 \geq A_1$	$A_1 > A_2$
$\gamma_4 = \gamma_2$	$Q \leq .146$	$n/a$
$\gamma_4 = 2\gamma_2$	$Q \leq .031$	$Q \leq .207$

If it is more costly to prepare 4 states vs. 2, then Eve has a greater incentive and so there are more strict requirements on the channel noise.



# *Closing Remarks*

## *Closing Remarks*

- We proposed a general game-theoretic model of security for QKD
- Unlike prior work, our method can be applied to arbitrary QKD protocols + attacks; furthermore, it allows for important noise tolerance and key-rate computations
- The noise tolerance of QKD protocols in the GT model is similar or lower than the SAM
- **However, greater efficiency is possible!**

# *Future Work*

## **Many interesting problems remain!**

- Additional strategies for AB and E
  - We only looked at two protocols but our methods work for others
  - Also, while we worked out the equations for arbitrary I/R attacks, we only considered three in our theorems
- Different, non-linear, utility functions
- Multi-user protocols
- Different game models
  - Including games where players are allowed to change their strategy after N iterations

*Thank you! Questions?*

# References

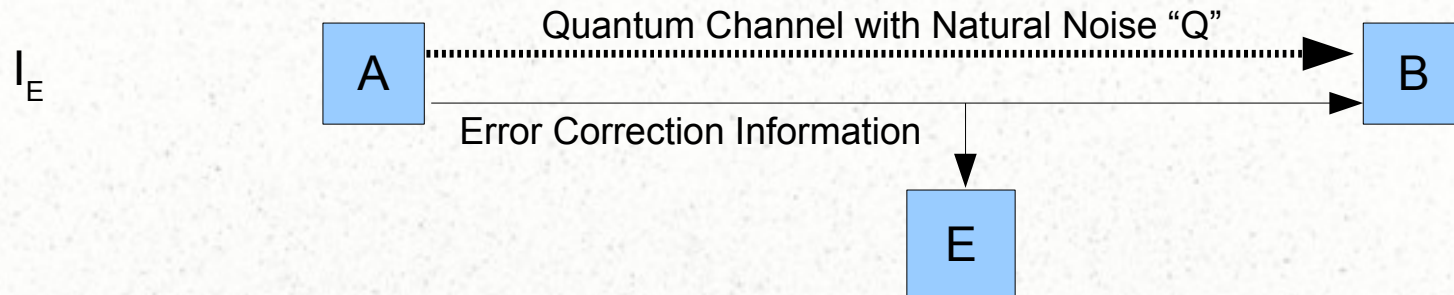
- C.H. Bennett and G. Brassard, 1984, Quantum cryptography: Public key distribution and coin tossing. in Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing. Vol 175, NY.
- C.H. Bennett, 1992, Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett., 68:3121-3124.
- M. Boyer, D. Kenigsberg, and T. Mor, 2007, Quantum Key Distribution with classical bob, in ICQNM.
- C.H.F. Fung and H.K. Lo, 2006, Security proof of a three-state quantum key distribution protocol without rotational symmetry. Phys. Rev. A, 74:042342.
- Katz, J.: Bridging game theory and cryptography: Recent results and future directions. In: Theory of Cryptography Conference, Springer (2008) 251–272
- Houshmand, M., Houshmand, M., Mashhadi, H.R.: Game theory based view to the quantum key distribution bb84 protocol. In: Intelligent Information Technology and Security Informatics (IITSI), 2010 Third International Symposium on, IEEE (2010) 332–336
- Kaur, H., Kumar, A.: Game-theoretic perspective of ping-pong protocol. Physica A: Statistical Mechanics and its Applications 490 (2018) 1415–1422

## *References (cont.)*

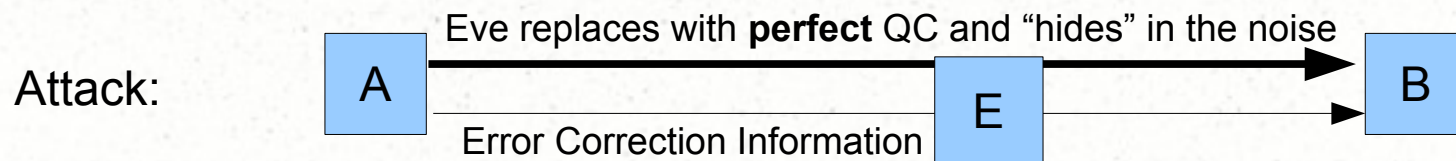
- H. Lu and Q.-Y. Cai, 2008, Quantum key distribution with classical Alice, *Int. J. Quantum Information* 6, 1195.
- R. Renner, N. Gisin, and B. Kraus, 2005, Information-theoretic security proof for QKD protocols. *Phys. Rev. A*, 72:012332.
- R. Renner, 2007, Symmetry of large physical systems implies independence of subsystems, *Nat. Phys.* 3, 645.
- V. Scarani, A. Acin, G. Ribordy, and N. Gisin, 2004, *Phys. Rev. Lett.* 92, 057901.
- Z. Xian-Zhou, G. Wei-Gui, T. Yong-Gang, R. Zhen-Zhong, and G. Xiao-Tian, 2009, Quantum key distribution series network protocol with m-classical bobs, *Chin. Phys. B* 18, 2143.
- Xiangfu Zou, Daowen Qiu, Lvzhou Li, Lihua Wu, and Lvjun Li, 2009, Semiquantum key distribution using less than four quantum states. *Phys. Rev. A*, 79:052312.

# Model

- Note that, even if Eve choose  $I_E$ , she still learns information on the raw key *without incurring any cost*



- However, if she wants to learn *more*, (causing AB's efficiency to drop further), she must choose to commit resources to attack the channel



## *E's Motivation*

$$u_E(K, C_E(A)) = w_g^E K - w_c^E C_E(A)$$

- Eve wants to maximize information on the “raw key” before privacy amplification (PA) even though this is not the “secret key” used for further cryptography.
- Would it make more sense to define utility in terms of learning the secret key?
- PA, however, guarantees that Eve's knowledge on the secret key will be negligible! Thus, this can never motivate a rational entity
- Instead, we chose motivation based on raw key as this will have the effect of **decreasing A and B's communication efficiency**
- Thus, decreasing the key-rate of A and B is Eve's main goal



## *All-powerful Attacks Against BB84*

- We first consider BB84 augmented with decoy iterations, denoted “BB84[a]”
- After “N” iterations, assuming only “natural noise” AB are left with a secret-key of expected size:

$$a \frac{N}{2} (1 - h(Q))$$

# *All-powerful Attacks Against BB84*

- We first consider BB84 augmented with decoy iterations, denoted “BB84[a]”
- After “N” iterations, assuming only “natural noise” AB are left with a secret-key of expected size:

$$a \frac{N}{2} (1 - h(Q))$$

Non-decoy  
iteration



# *All-powerful Attacks Against BB84*

- We first consider BB84 augmented with decoy iterations, denoted “BB84[a]”
- After “N” iterations, assuming only “natural noise” AB are left with a secret-key of expected size:

$$a \frac{N}{2} (1 - h(Q))$$

Non-decoy iteration      Efficiency of BB84

# *All-powerful Attacks Against BB84*

- We first consider BB84 augmented with decoy iterations, denoted “BB84[a]”
- After “N” iterations, assuming only “natural noise” AB are left with a secret-key of expected size:

$$a \frac{N}{2} (1 - h(Q))$$

Non-decoy iteration

Efficiency of BB84

Loss due to error correction leakage

## *Cost for BB84*

$$C_{AB}(BB84[a]) = N[(3 + h(a))C_R + \gamma_4 C_M + \gamma_4 C_P] + C_{auth}$$

## *Cost for BB84*

$$C_{AB}(BB84[a]) = N[(3 + h(a))C_R + \gamma_4 C_M + \gamma_4 C_P] + C_{auth}$$

Decoy Parameter




# *Cost for BB84*

$$C_{AB}(BB84[a]) = N[(3 + h(a))C_R + \gamma_4 C_M + \gamma_4 C_P] + C_{auth}$$

Decoy Parameter



Number of  
Iterations



# *Cost for BB84*

$$C_{AB}(BB84[a]) = N[(3+h(a))C_R + \gamma_4 C_M + \gamma_4 C_P] + C_{auth}$$

Decoy Parameter

Number of  
Iterations

AB must produce 3  
uniform bits each iteration  
and one a-biased bit  
(for decoy choice)



# Cost for BB84

$$C_{AB}(BB84[a]) = N[(3+h(a))C_R + \gamma_4 C_M + \gamma_4 C_P] + C_{auth}$$

Decoy Parameter

Number of  
Iterations

AB must produce 3  
uniform bits each iteration  
and one a-biased bit  
(for decoy choice)

AB Must  
prepare and  
measure  
qubits (four  
states each)

# Cost for BB84

$$C_{AB}(BB84[a]) = N[(3+h(a))C_R + \gamma_4 C_M + \gamma_4 C_P] + C_{auth}$$

Decoy Parameter

Number of Iterations

AB must produce 3 uniform bits each iteration and one a-biased bit (for decoy choice)

AB Must prepare and measure qubits (four states each)

Authentication Channel used once at end typically

# Cost for B92

$$C_{AB}(B92[a]) = N[(2+h(a))C_R + \gamma_4 C_M + \gamma_2 C_P] + C_{auth}$$

Fewer  
Random  
Choices  
Needed

Only  
need to  
prepare  
two  
states

$$C_{AB}(BB84[a]) = N[(3+h(a))C_R + \gamma_4 C_M + \gamma_4 C_P] + C_{auth}$$

**B92 is less tolerant to noise in the SAM**

**Also, Eve can gain more information through the I/R attacks we consider than with BB84**

# *Cost for Eve*

$$C_E(V) = N[h(p)C_R + p\gamma_2(C_M + C_P)] + C_S$$

Number of  
Iterations

If she attacks, she  
must measure and  
send a qubit

Eve decides to attack each  
iteration with probability "p"; thus  
she must produce a p-biased bit

One-time cost to  
setup attack