Key Relay Protocol for Quantum Key Distribution

Mitsubishi-B Team, G-RIPS Sendai 2025

August 6, 2025

Authors:
Ed Chen[1]
Maho Maruyama[2]
Derek Zhang[3]
Donald Zvada[4]

Mentors:
Yuji Ando[*]
Natsuo Miyatake[*]
Toyohiro Tsurumaru[†]
Go Kato[‡]

[1] New York University [2] Ochanomizu University
[3] University of Maryland [4] AIMS South Africa
[*] Academic Mentor, Tohoku University
[†] Industry Mentor, Mitsubishi Electric
[‡] External Mentor, NICT

Outline

What is a key?

- Goal: Alice sends a secret message to Bob.
- Solution:

  Step 1: Alice and Bob share a private key.

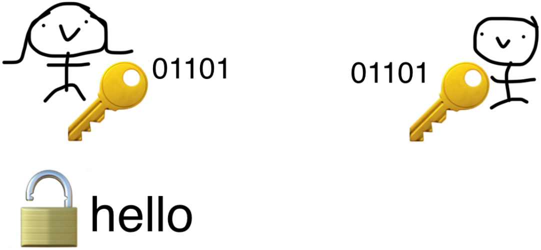
  Step 2: Encrypt/decrypt a message with the key.

What is a key?

- Goal: Alice sends a secret message to Bob.
- Solution:

  Step 1: Alice and Bob share a private key.

  Step 2: Encrypt/decrypt a message with the key.

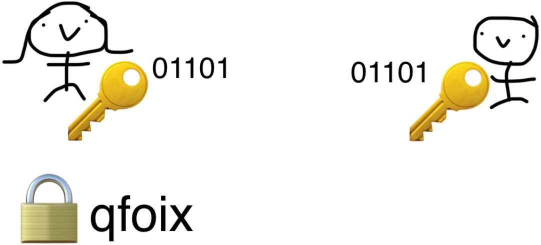


What is a key?

- Goal: Alice sends a secret message to Bob.
- Solution:

  Step 1: Alice and Bob share a private key.

  Step 2: Encrypt/decrypt a message with the key.

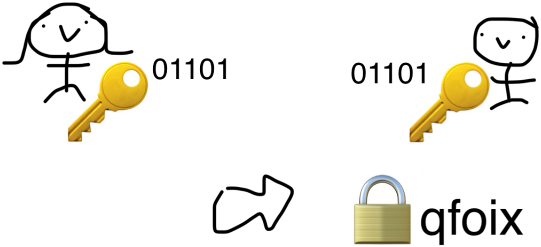


What is a key?

- Goal: Alice sends a secret message to Bob.
- Solution:

  Step 1: Alice and Bob share a private key.

  Step 2: Encrypt/decrypt a message with the key.

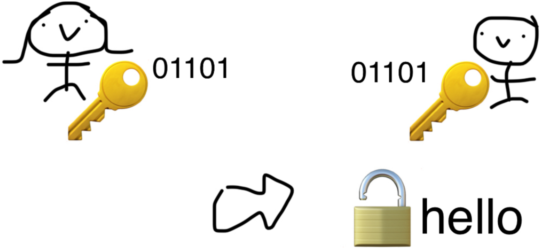


What is a key?

- Goal: Alice sends a secret message to Bob.
- Solution:

  Step 1: Alice and Bob share a private key.

  Step 2: Encrypt/decrypt a message with the key.



Overview

The Problem

- Classical key distribution can be broken by quantum computers.
- Quantum key distribution (QKD) is always secure.

The Big Picture

- KRP (Key Relay Protocol) is a mathematical model for QKD
- KRP is recent and unexplored
- KRP $\simeq$ SNC (Secure Network Coding), which is well-known
- **How secure is KRP?**

Overview

The Problem

- Classical key distribution can be broken by quantum computers.
- Quantum key distribution (QKD) is always secure.

The Big Picture

- KRP (Key Relay Protocol) is a mathematical model for QKD
- KRP is recent and unexplored
- KRP $\simeq$ SNC (Secure Network Coding), which is well-known
- **How secure is KRP?**

Outline

Quantum Communication

Theoretical vs. Practical

Quantum communication (QKD) is theoretically unbreakable. However, it faces physical and practical challenges.

Key Issues

- QKD suffers from high error rates beyond 50–100 km
- Optical amplifiers collapse quantum states — unlike classical signals.
- Long-distance transmission is only feasible with quantum networks.

Quantum Communication

Theoretical vs. Practical

Quantum communication (QKD) is theoretically unbreakable. However, it faces physical and practical challenges.

Key Issues

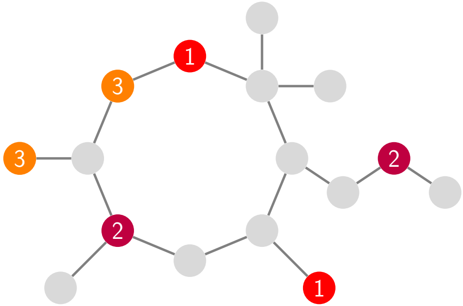
- QKD suffers from high error rates beyond 50–100 km
- Optical amplifiers collapse quantum states — unlike classical signals.
- Long-distance transmission is only feasible with quantum networks.

Networking

Network

A graph $G = (V, E)$ where:

- Nodes $=$ users
- Edges $=$ communication links
- $U = \{(a_i, b_i)\}$ is the set of user pairs wishing to communicate



Adversary Model

Types of Adversaries

- **Eavesdroppers**
  Can intercept transmissions, but does not alter them.
  We call this a **passive adversary**

Wiretap Model

- A **wiretap set** is a subset of communication links (edges) that an eavesdropper can observe.
- Let $\mathcal{E} = \{E_1, E_2, \ldots, E_k\}$ denote the **wiretap collection**, where each E_i is a wiretap set.
- The network is secure if the eavesdropper gains no information by wiretapping any $E_i \in \mathcal{E}$.

Adversary Model

Types of Adversaries

- **Eavesdroppers**
  Can intercept transmissions, but does not alter them.
  We call this a **passive adversary**

Wiretap Model

- A **wiretap set** is a subset of communication links (edges) that an eavesdropper can observe.
- Let $\mathcal{E} = \{E_1, E_2, \ldots, E_k\}$ denote the **wiretap collection**, where each E_i is a wiretap set.
- The network is secure if the eavesdropper gains no information by wiretapping any $E_i \in \mathcal{E}$.

Information Theory

Information Theory: is a branch of statistics used to quantify the amount of randomness in a certain event given some some information has been gained.

Entropy

$$H(X) = -\sum_{x} P_X(x) \log P_X(x)$$

- Measures the **uncertainty** or **randomness** in a variable X, in bits.
- Entropy quantifies how many bits of information are needed to describe a secret key.

Information Theory

Mutual Information

$$I(X;Y) = H(X) - H(X|Y)$$

- Quantifies how much knowing Y reduces **uncertainty** about X; zero mutual information implies **information-theoretic secrecy**.
- **Security Criterion:** We require $I(\text{Key};\mathcal{E}) = 0$, hence, reveal nothing about the **Key**.

Outline

Edge Primitive Definitions

Public Channels

Broadcast unencrypted information to all nodes. **Unlimited use**. Eavesdroppers can fully read the content.

Secret Channels

Encrypted, **one-time use** private links between two nodes. If wiretapped, the eavesdropper also receives the message.

Local Key Sources

Distributes randomly generated bit(s) to both ends. LKS are implemented via QKD links

Secure Network Coding

Goal

Given a communication network $G = (V, E)$, user pairs (a_i, b_i) wish to share **secure messages** over a directed and untrusted network.

Methodology

- Any node can generate **random bits**. These bits can be forwarded through the network using **secret channels**.
- Any node can compute **linear combinations** of known information to improve throughput

Secure Network Coding

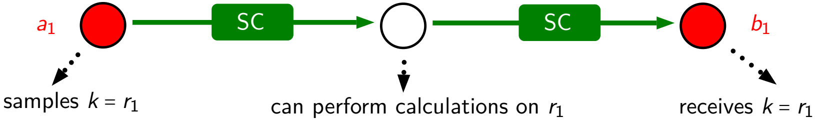
Goal

Given a communication network $G = (V, E)$, user pairs (a_i, b_i) wish to share **secure messages** over a directed and untrusted network.

Methodology

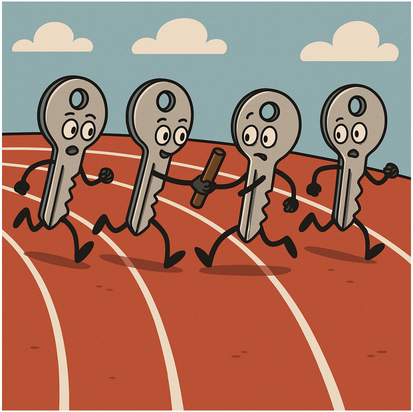
- Any node can generate **random bits**. These bits can be forwarded through the network using **secret channels**.
- Any node can compute **linear combinations** of known information to improve throughput

Secure Network Coding



Key Relay Protocol

Not this type of *"Key Relay"* ☺



Key Relay Protocol

Goal

Given a **communication network** $G = (V, E)$, user pairs (a_i, b_i) wish to share **secure keys** over an **undirected** and **untrusted** network.

Methodology

- **Local Key Sources (LKS)** generate identical, **random bits** to both endpoints using **QKD**.
- Use **public channels** to publish the **linear combination** of random bits generated by **LKS**.

Key Relay Protocol

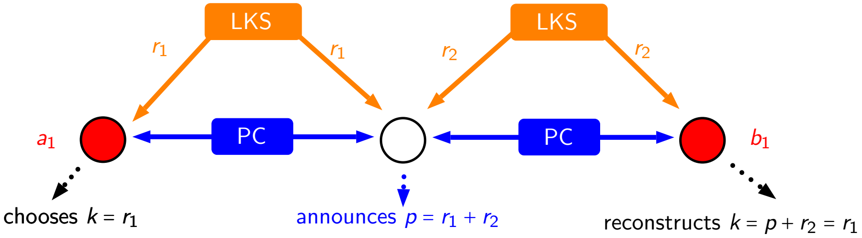
Goal

Given a **communication network** $G = (V, E)$, user pairs (a_i, b_i) wish to share **secure keys** over an **undirected** and **untrusted** network.

Methodology

- **Local Key Sources (LKS)** generate identical, **random bits** to both endpoints using **QKD**.
- Use **public channels** to publish the **linear combination** of random bits generated by **LKS**.

Key Relay Protocol



Equivalence of Protocols

Security Notions

- User Pairs share identical keys or detect a failure.
- Protocol **A** is said to be more secure than Protocol **B** , if **A** is secure against more **wiretap** sets $\mathcal{E}$ for any (G, U): $\mathbf{B} \subseteq \mathbf{A}$

Protocols Equivalence

- $\mathbf{B} \subseteq \mathbf{A}$: any level of security attained by **B** can also be attained by **A**. If $\mathbf{A} \subseteq \mathbf{B}$ and $\mathbf{B} \subseteq \mathbf{A}$, then $\mathbf{A} \cong \mathbf{B}$ and the two protocols are said to be equivalent, achieving the same level of security.

Equivalence of Protocols

Security Notions

- User Pairs share identical keys or detect a failure.
- Protocol **A** is said to be more secure than Protocol **B** , if **A** is secure against more **wiretap** sets $\mathcal{E}$ for any (G, U): $\mathbf{B} \subseteq \mathbf{A}$

Protocols Equivalence

- $\mathbf{B} \subseteq \mathbf{A}$: any level of security attained by **B** can also be attained by **A**. If $\mathbf{A} \subseteq \mathbf{B}$ and $\mathbf{B} \subseteq \mathbf{A}$, then $\mathbf{A} \cong \mathbf{B}$ and the two protocols are said to be equivalent, achieving the same level of security.

SNC vs KRP

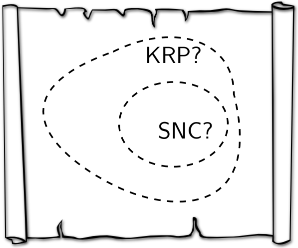
Prior Results by G. Kato and T. Tsurumaru

Proved results:

- SNC $\subseteq$ KRP, but **not vice versa**.
- **Counterexample Network**: KRP supports multiple pairs; SNC fails even in absence of eavesdroppers.
- 9-user pairs: KRP is able to share keys and SNC fails

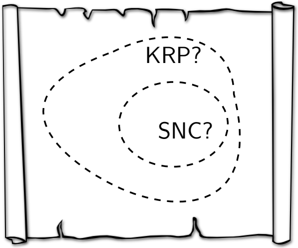
Outline

Where do we start?



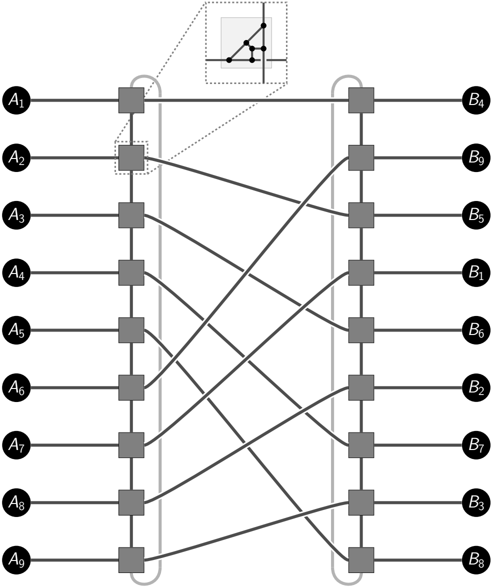
- Approaches
  1. Nonequivalence
  2. Equivalence
  3. Study KRP on its own
- Many possible graphs and parameters

Where do we start?



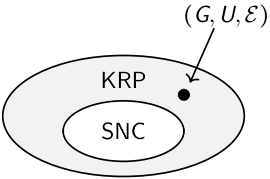
- Approaches
  1. Nonequivalence
  2. Equivalence
  3. Study KRP on its own
- Many possible graphs and parameters

Existing Counterexample



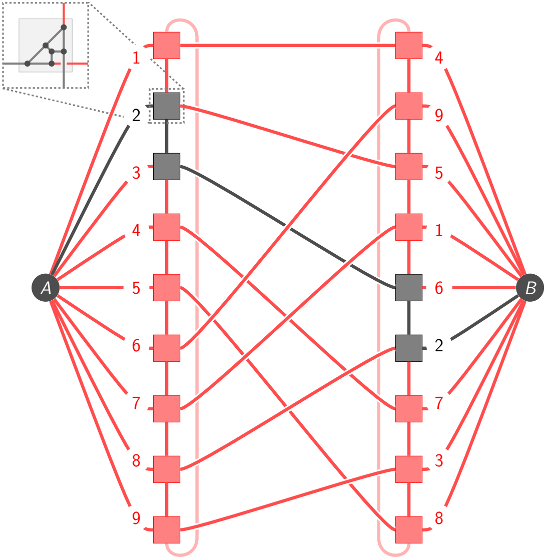
Tsurumaru, *et al.*

- $(G, U, \mathcal{E}) \in$ KRP
- $(G, U, \mathcal{E}) \notin$ SNC
- $\mathcal{E} = \emptyset$



(For 9+ user pairs)

Conjecture for One User Pair



We couldn't prove or disprove this ☹

Linear Algebra Formulation

Can we use mathematical terms to describe the KRP design problem?

*Yes, we only need to track **which** pieces of randomness are applied (in $\mathbb{Z}_2$)*

Incidence Vector

Vector of length $|E|$ that has a 1 in index i if e_i is applied

Linear Algebra Formulation

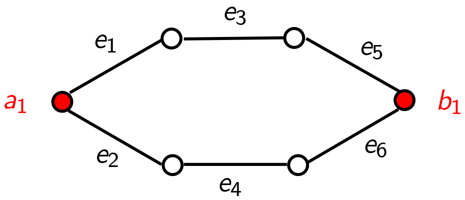
Can we use mathematical terms to describe the KRP design problem?

Yes, we only need to track ***which*** *pieces of randomness are applied (in $\mathbb{Z}_2$)*

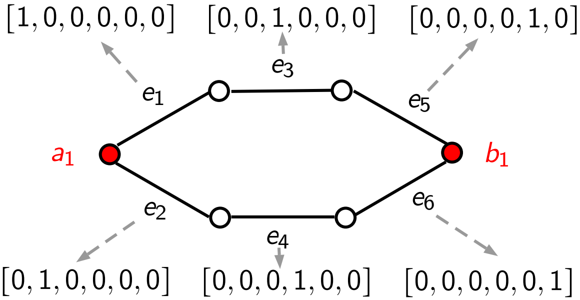
Incidence Vector

Vector of length $|E|$ that has a 1 in index i if e_i is applied

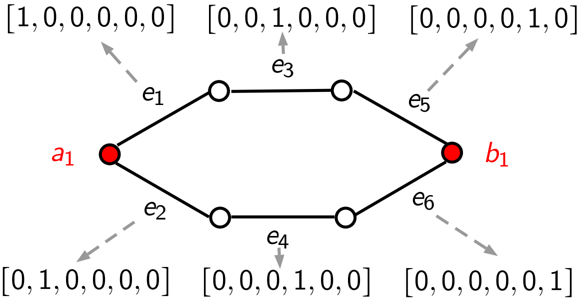
Linear Algebra Formulation (Incidence)



Linear Algebra Formulation (Incidence)

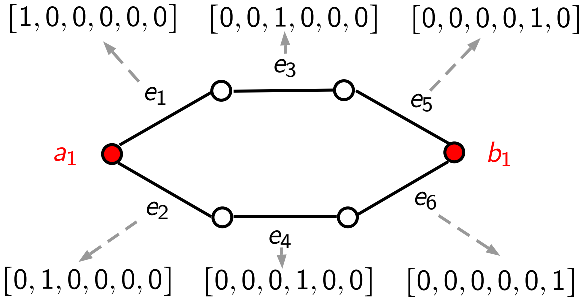


Linear Algebra Formulation (Incidence)



$$\mathbb{Z}_2^6 = \mathrm{span}\{e_1, e_2, e_3, e_4, e_5, e_6\}$$

Linear Algebra Formulation (Incidence)

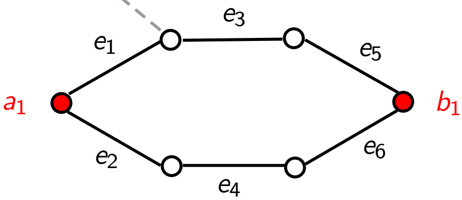


$$\mathbb{Z}_2^6 = \text{span}\{e_1, e_2, e_3, e_4, e_5, e_6\}$$

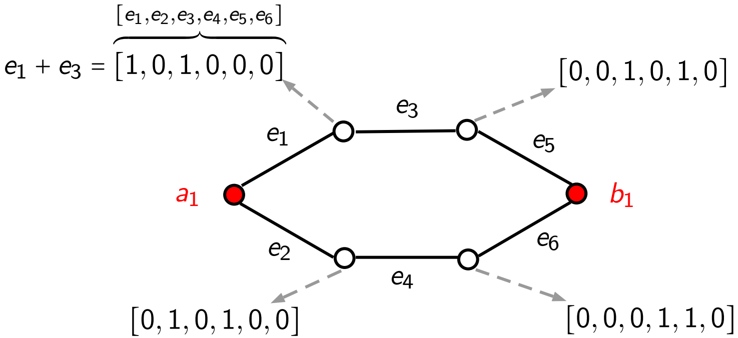
$$k = e_1 + e_2 := [1, 1, 0, 0, 0, 0]$$

Linear Algebra Formulation (Public Channels)

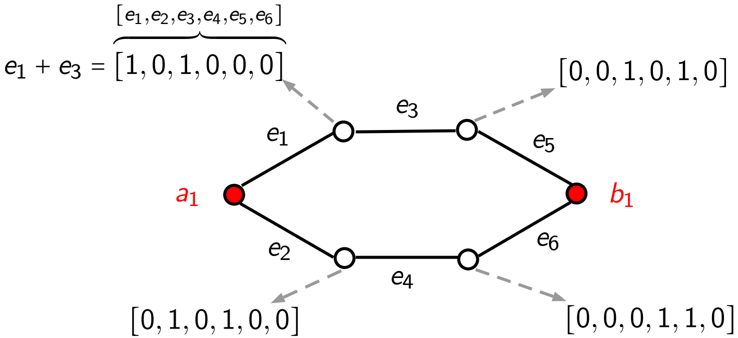
$$e_1 + e_3 = \overbrace{[1, 0, 1, 0, 0, 0]}^{[e_1, e_2, e_3, e_4, e_5, e_6]}$$



Linear Algebra Formulation (Public Channels)

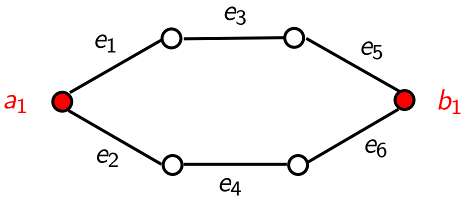


Linear Algebra Formulation (Public Channels)



$$\mathbf{P} = \begin{bmatrix} [1,0,1,0,0,0]^T, [0,1,0,1,0,0]^T \\ [0,0,1,0,1,0]^T, [0,0,0,1,1,0]^T \end{bmatrix}$$

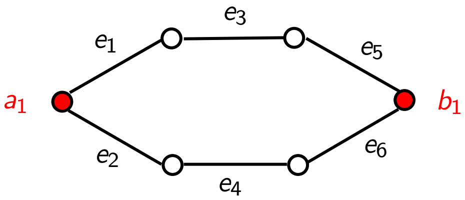
Linear Algebra Formulation (Node Reconstruction)



$k = \sum \mathbf{P} + e_5 + e_6 \in \mathbf{N}_{b_1}$ ✓

Linear Algebra Formulation (Node Reconstruction)

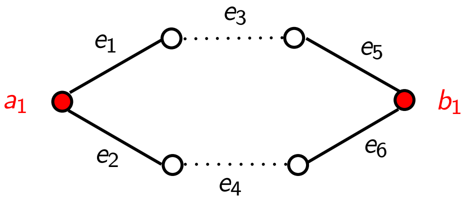
$$\mathbf{N}_{n_i} = \mathrm{span}\Big\{ \big[e \big| n_i \in e \big] \cup \mathbf{P} \Big\}$$



$$k = \sum \mathbf{P} + e_5 + e_6 \in \mathbf{N}_{b_1} \quad ✓$$

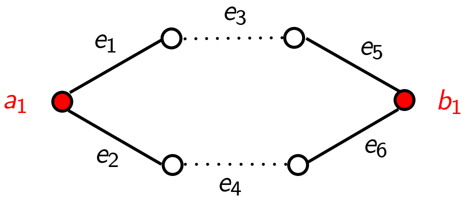
Linear Algebra Formulation (Eavesdropper Secrecy)

$$\mathbf{A}_{E_w} = \mathrm{span}\left\{e_3, e_4 \cup \mathbf{P}\right\}$$



Linear Algebra Formulation (Eavesdropper Secrecy)

$$\mathbf{A}_{E_w} = \mathrm{span}\left\{e_3, e_4 \cup \mathbf{P}\right\}$$



$$k = [1,1,0,0,0] = \left(\begin{array}{c} \underbrace{[1,0,1,0,0,0] + [0,1,0,1,0,0]}_{\text{from } \mathbf{P}} \\ + \underbrace{[0,0,1,0,0,0]}_{e_3} + \underbrace{[0,0,0,1,0,0]}_{e_4} \end{array} \right) \in \mathbf{A}_{E_w} \quad ✗$$

Linear Algebra Formulation

Soundness requires key k satisfies

$$v_k \in N_{n_i} = \mathrm{span}\{[v_e | n_i \in e] \cup \mathbf{P}\} \text{ for } n_i \in (a_i, b_i)$$

Security requires key k satisfies

$$v_k \notin A_{E_w} = \mathrm{span}\{[v_{e_i} | e_i \in E_w] \cup \mathbf{P}\}$$

Takeaway

Choice and timing of **P defines** a KRP instance

Linear Algebra Formulation

Soundness requires key k satisfies

$$v_k \in N_{n_i} = \text{span}\{[v_e | n_i \in e] \cup \mathbf{P}\} \text{ for } n_i \in (a_i, b_i)$$

Security requires key k satisfies

$$v_k \notin A_{E_w} = \text{span}\{[v_{e_i} | e_i \in E_w] \cup \mathbf{P}\}$$

Takeaway

Choice and timing of **P defines** a KRP instance

Linear Algebra Applications

Why is this useful?

Security

Analysis of adversary knowledge

$$A_{KRP} = \text{span}\{[v_{e_i} | e_i \in E_w] \cup \mathbf{P}\} \qquad A_{SNC} = \text{span}\{[s_{e_i} | e_i \in E_w]\}$$

Which choices of $\mathbf{P}$ are useful?

Linear Algebra Applications

Why is this useful?

Security

Analysis of adversary knowledge

$$A_{KRP} = \text{span}\{[v_{e_i} | e_i \in E_w] \cup \mathbf{P}\} \qquad A_{SNC} = \text{span}\{[s_{e_i} | e_i \in E_w]\}$$

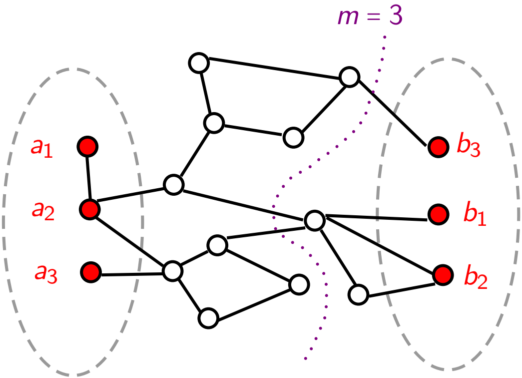
Which choices of **P** are useful?

Minimum Cut Result

Theorem Min-Cut Feasibility

A **necessary but not sufficient condition** for KRP with n user pairs and a min cut separating the user pairs of size m is that $\mathbf{n \leq m}$

.



Minimum Cut Result

KRP requires that

1. **Privacy** of the keys: $I(K;P) = 0$
2. **Independence** of the keys: $H(K) = n$
3. **Constructibility** of the keys: $H(K|L,P) = 0$

Constructibility Remark

The **"defining" information** about the keys is entirely dependent on the **random bits on the cut**.

Minimum Cut Result

KRP requires that

1. **Privacy** of the keys: $I(K;P) = 0$
2. **Independence** of the keys: $H(K) = n$
3. **Constructibility** of the keys: $H(K|L,P) = 0$

Constructibility Remark

The **"defining" information** about the keys is entirely dependent on the **random bits on the cut**.

Minimum Cut Result

$$\begin{aligned}
\underbrace{H(K)}_{n \text{ via independence}} &= \underbrace{\cancel{H(K|L,P)}}_{\text{via constructibility}} + \underbrace{\cancel{I(K;P)}}_{\text{via privacy}} + I(K;L|P) \\
&= I(K;L|P) \\
&\leq H(L|P) \\
&= H(L) \\
&= m
\end{aligned}$$

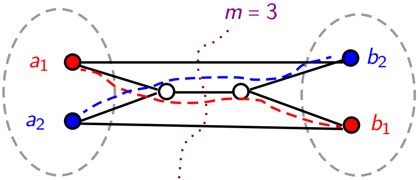
Takeaway

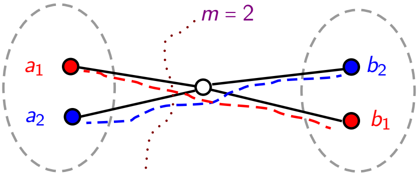
The minimum unwiretapped cut, equivalently, number of edge-disjoint paths, needs to **at least match** the number of secret keys shared.

Minimum Cut Conjecture

Theorem KRP Soundness

If there is an edge disjoint path between each **unique user pair**, successful communication is possible.

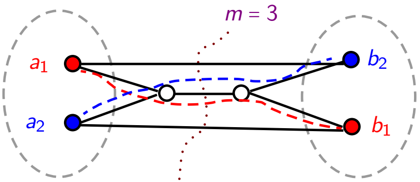


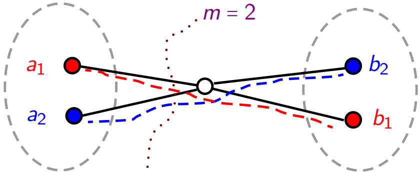


Minimum Cut Conjecture

Conjecture

If there are no edge disjoint paths between **unique user pair**, there is possibly a tighter minimum cut bound that restricts the number of edge disjoint paths between the **vertex sets**.





Outline

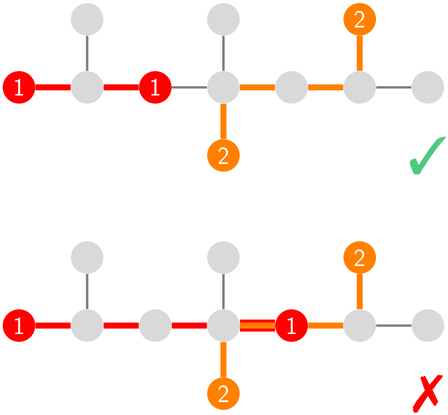
Tree Graphs

Theorem

KRP is sound on tree graphs iff there are edge disjoint paths connecting each pair.

Corollary

KRP $\cong$ SNC on tree graphs.



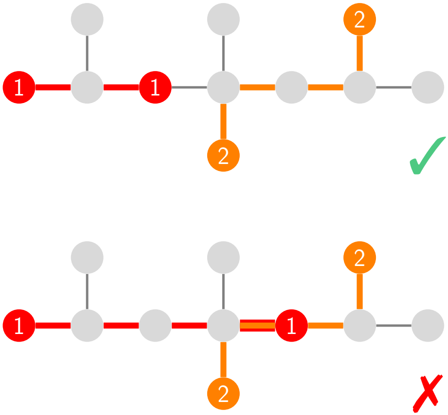
Tree Graphs

Theorem

KRP is sound on tree graphs iff there are edge disjoint paths connecting each pair.

Corollary

KRP $\cong$ SNC on tree graphs.



Tree Graphs Proof

Every node pair in a tree has a **unique** path

- If two user pairs' path overlaps, $m < n$
- If they do not, each pair only has one possible communication pattern. KRP and SNC both admit the same capabilities

Tree Graphs Proof

Every node pair in a tree has a **unique** path

- If two user pairs' path overlaps, $m < n$
- If they do not, each pair only has one possible communication pattern. KRP and SNC both admit the same capabilities

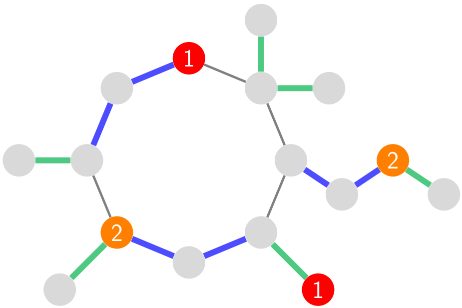
Graph Simplification

Theorem

Contracting a leaf edge does not change the security of SNC or KRP.

Theorem

Contracting a node with two neighbors does not change the security of SNC or KRP.



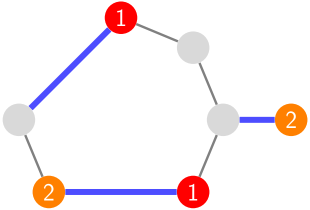
Graph Simplification

Theorem

Contracting a leaf edge does not change the security of SNC or KRP.

Theorem

Contracting a node with two neighbors does not change the security of SNC or KRP.



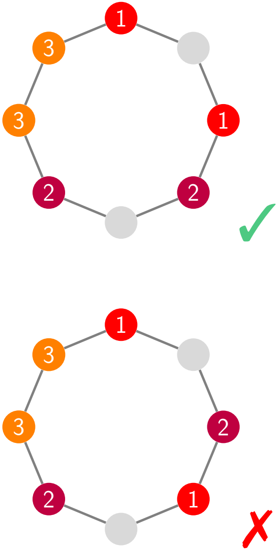
Cycle Graphs

Theorem

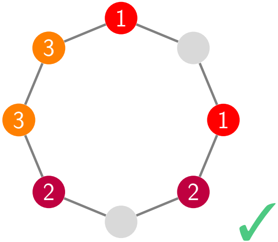
KRP is sound on cycle graphs iff user pairs are adjacent.

Corollary

KRP $\cong$ SNC on cycle graphs.



Cycle Graphs

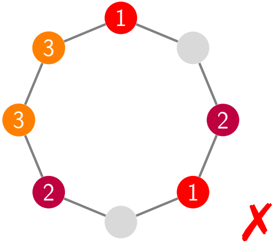


Theorem

KRP is sound on cycle graphs iff user pairs are adjacent.

Corollary

KRP $\cong$ SNC on cycle graphs.



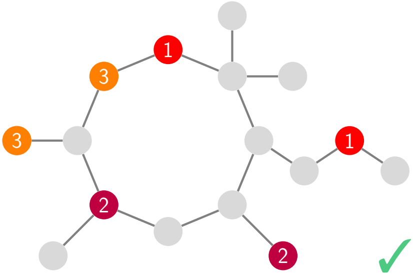
Pseudotree Graphs

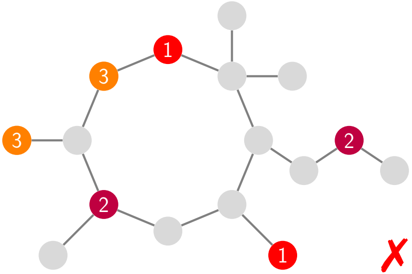
Theorem

KRP is sound on pseudotree graphs iff there are edge disjoint paths connecting each pair.

Corollary

KRP $\cong$ SNC on pseudotree graphs.





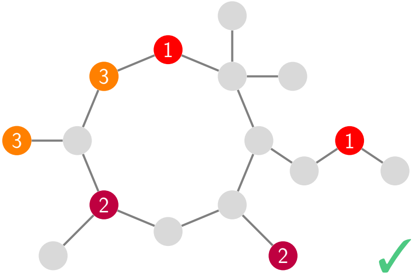
Pseudotree Graphs

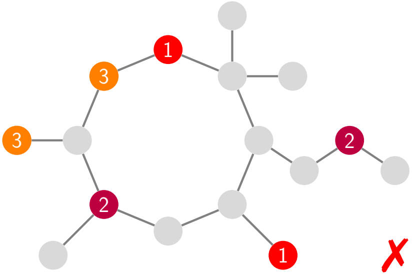
Theorem

KRP is sound on pseudotree graphs iff there are edge disjoint paths connecting each pair.

Corollary

KRP $\cong$ SNC on pseudotree graphs.

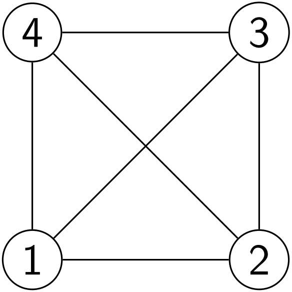




Complete Graphs

Definition

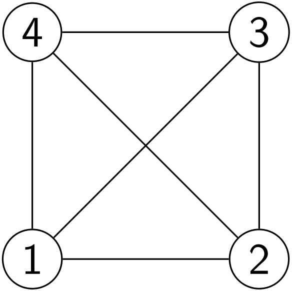
A graph in which there is an edge between any two vertices is called a complete graph. A complete graph with n vertices is denoted by K_n



Complete Graphs

Theorem

On a complete graph with a single user pair, KRP and KRP-by-SNC are equivalent.



Note: Since any tree can be embedded in a complete graph, and depending on the wiretap sets, this result implies a general equivalence for KRP and SNC in the 1-user-pair setting

KRP: Algorithm Overview

Input Parameters

- Graph $G = (V, E)$
- User pairs $\{(a_i, b_i)\}$
- Wiretap sets $\mathcal{E}$

Step 1: Graph Validation

- Check if G is connected
- Verify min-cut bound

Step 2: Local Key Distribution

- Each edge generates a random key r_e
- Keys are distributed to incident nodes
- Nodes announce Public values

KRP: Algorithm Overview

Input Parameters

- Graph $G = (V, E)$
- User pairs $\{(a_i, b_i)\}$
- Wiretap sets $\mathcal{E}$

Step 1: Graph Validation

- Check if G is connected
- Verify min-cut bound

Step 2: Local Key Distribution

- Each edge generates a random key r_e
- Keys are distributed to incident nodes
- Nodes announce Public values

KRP: Algorithm Overview

Input Parameters

- Graph $G = (V, E)$
- User pairs $\{(a_i, b_i)\}$
- Wiretap sets $\mathcal{E}$

Step 1: Graph Validation

- Check if G is connected
- Verify min-cut bound

Step 2: Local Key Distribution

- Each edge generates a random key r_e
- Keys are distributed to incident nodes
- Nodes announce Public values

KRP: Graph Verification Overview

Step 3: Security Checks

- Ensure key + public announcements are linearly independent
- Failure implies potential leakage $\Rightarrow$ Insecure protocol

Step 4: Key Delivery Verification

- Verify that each (a_i, b_i) can compute their shared key K_i

Step 5: Visualization

- Plot the graph with:
  - User pairs highlighted
  - Wiretap sets shown

KRP: Graph Verification Overview

Step 3: Security Checks

- Ensure key + public announcements are linearly independent
- Failure implies potential leakage $\Rightarrow$ Insecure protocol

Step 4: Key Delivery Verification

- Verify that each (a_i, b_i) can compute their shared key K_i

Step 5: Visualization

- Plot the graph with:
  - User pairs highlighted
  - Wiretap sets shown

KRP: Graph Verification Overview

Step 3: Security Checks

- Ensure key + public announcements are linearly independent
- Failure implies potential leakage ⇒ Insecure protocol

Step 4: Key Delivery Verification

- Verify that each (a_i, b_i) can compute their shared key K_i

Step 5: Visualization

- Plot the graph with:
  - User pairs highlighted
  - Wiretap sets shown

Incomplete and Future Work

- Feasibility Algorithm (NP or P)?
- Multi-Cycle graphs?
- Planarity Effect?

Thanks for listening!

MITSUBISHI

AIMR

ipam

東北大学 数理科学共創社会センター
Mathematical Science Center for Co-creative Society, Tohoku University
MathCCS

TOHOKU FORUM for CREATIVITY

References

- Go Kato, Mikio Fujiwara, and Toyohiro Tsurumaru.
  Advantage of the Key Relay Protocol Over Secure Network Coding.
  IEEE Transactions on Quantum Engineering, 4:1–17, 2023.
- Michael A. Nielsen and Isaac L. Chuang.
  Quantum Computation and Quantum Information: 10th Anniversary Edition.
- Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan.
  Secure quantum key distribution with realistic devices.
- Tao Cui, Tracey Ho, and Jörg Kliewer.
  On secure network coding with unequal link capacities and restricted wiretapping sets.
  In *2010 IEEE Information Theory Workshop*, pages 1–5, 2010.
- Ning Cai and Raymond W. Yeung.
  Secure network coding on a wiretap network.
  IEEE Transactions on Information Theory, 57(1):424–435, 2010.