Multiterminal Secret Key Agreement

Alireza Poostindouz

University of Calgary
AB, Canada

December 17, 2021

UNIVERSITY OF CALGARY

UNIVERSITY OF CALGARY

Why key agreement?

- Symmetric-Key Crypto is secure *if* a key is shared among parties, so it requires a secure **S**ecret **K**ey **A**greement **(SKA)**
- Asymmetric-Key Crypto does not require the same shared key *but* current symmetric-Key protocols, that are widely used over the Internet, are **not secure** when the adversary has **a Quantum Computer!**

Goal: Quantum-safe SKA + Symmetric-Key Encryption

Why information theoretic key agreement?

- Gives **provable security** guarantee against adversaries with **unlimited computational power**
- Raises many **new insights** and gives a **powerful framework** to study the **fundamental limits of information networks**
- Has **many applications** based on practical physical-layer assumptions
- It is **quantum-safe**

Outline

- Part I: Information Theory
- Part II: Secret Key Agreement in Source Model
- Part III: Secret Key Agreement in Channel Model (if time permits)

Part I

Information Theory

- Random variables (RVs)

$$P_X(x) = \Pr\{X = x\}$$

Background - Information theory

- Random variables (RVs)

$$P_X(x) = \Pr\{X = x\}$$

- Information, Uncertainty, Entropy

Background - Information theory

- Random variables (RVs)

$$P_X(x) = \Pr\{X = x\}$$

- Information, Uncertainty, Entropy

$$\log_2 \frac{1}{P_X(x)}$$

Background - Information theory

- Random variables (RVs)

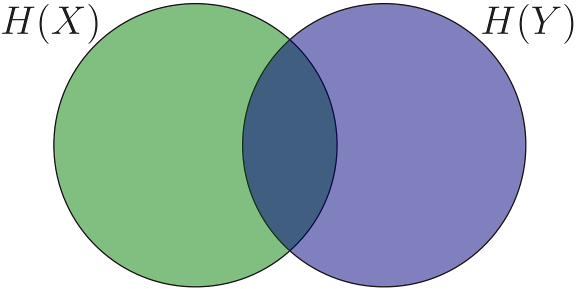
$$P_X(x) = \Pr\{X = x\}$$

- Information, Uncertainty, Entropy

$$H(X) = \sum_{x \in \mathcal{X}} P_X(x) \log_2 \frac{1}{P_X(x)}$$

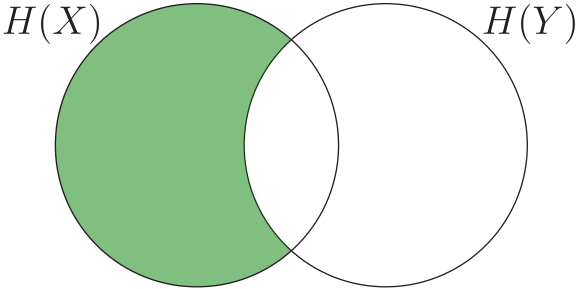
Background - Information theory

- Entropy, Joint Entropy, Conditional Entropy

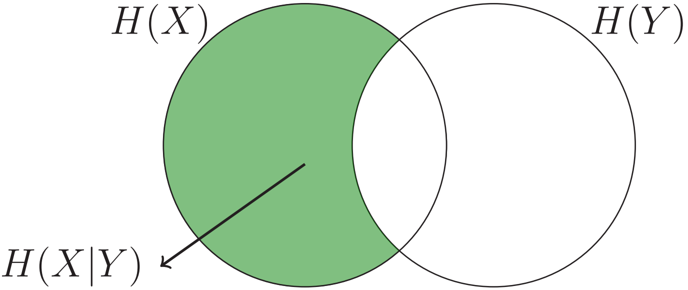


Background - Information theory

- Entropy, Joint Entropy, Conditional Entropy

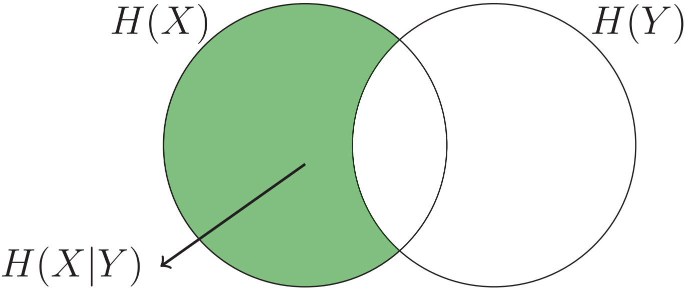


- Entropy, Joint Entropy, Conditional Entropy



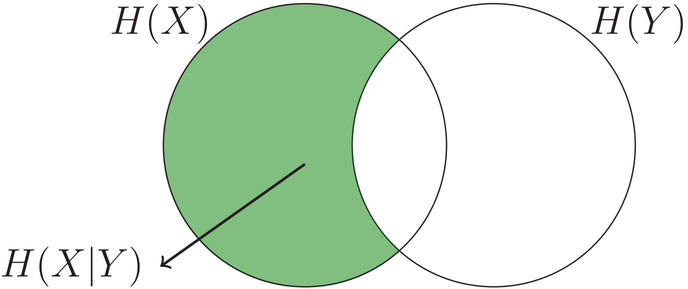
Background - Information theory

- Entropy, Joint Entropy, Conditional Entropy



$$H(X,Y) = H(Y) + H(X|Y)$$

- Entropy, Joint Entropy, Conditional Entropy

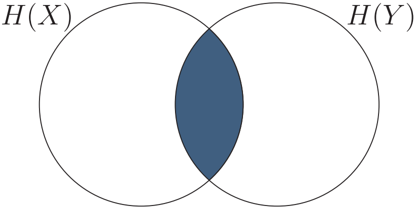


$$H(X,Y) = H(Y) + H(X|Y)$$

$$H(X,Y) = H(X) + H(Y|X)$$

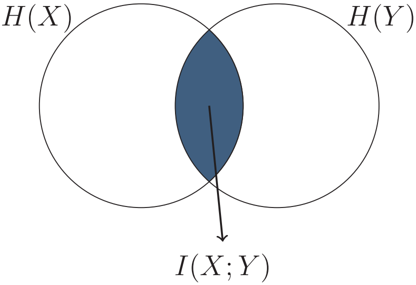
Background - Information theory

- Mutual Information

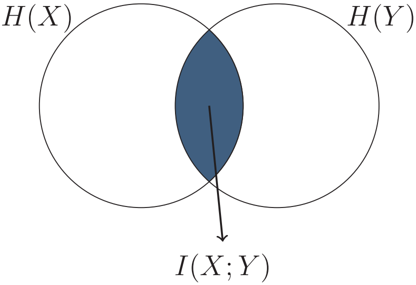


UNIVERSITY OF CALGARY

- Mutual Information



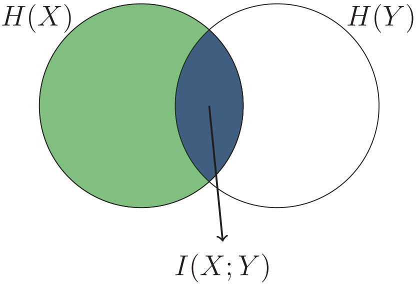
- Mutual Information



$$H(X,Y) = I(X;Y) +$$

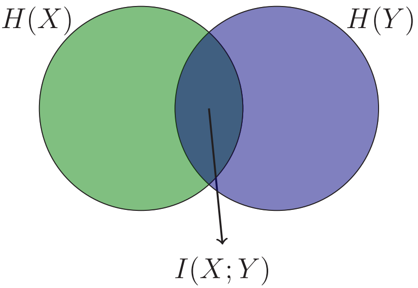
UNIVERSITY OF CALGARY

- Mutual Information



$$H(X,Y) = I(X;Y) + H(X|Y)$$

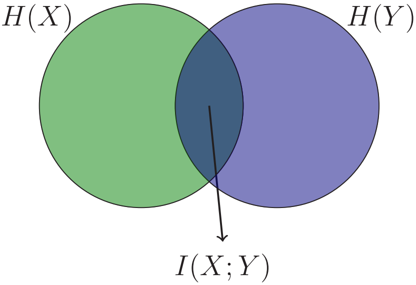
- Mutual Information



$$H(X,Y) = I(X;Y) + H(X|Y) + H(Y|X)$$

UNIVERSITY OF CALGARY

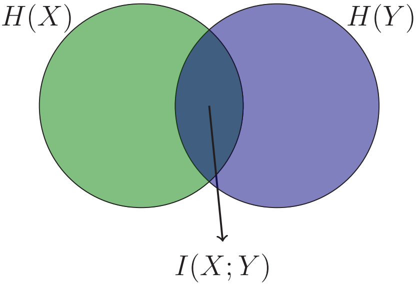
- Mutual Information



$$H(X,Y) = I(X;Y) + H(X|Y) + H(Y|X)$$

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

- Mutual Information



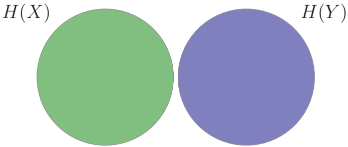
$$H(X,Y) = I(X;Y) + H(X|Y) + H(Y|X)$$

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

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

UNIVERSITY OF CALGARY

- Independence



$$\Pr\{X|Y\} = \Pr\{X\}$$

$$H(X|Y) = H(X)$$

$$I(X;Y) = 0$$

$$H(X,Y) = H(X) + H(Y)$$

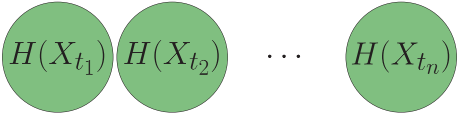
Background - Source Model

- IID Source (Independent and identically distributed)

$$X^n = (X_{t_1}, X_{t_2}, X_{t_3}, X_{t_4}, \ldots, X_{t_n})$$

$$\begin{aligned} H(X^n) &= H(X_{t_1}) + H(X_{t_2}) + \cdots + H(X_{t_n}) \\ &= nH(X_{t_1}) \end{aligned}$$

$$P_{X^n} = (P_{X_{t_1}})^n$$



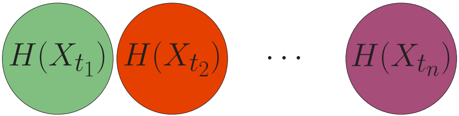
Background - Source Model

- INID Source (Independent but not identically distributed)

$$X^n = (X_{t_1}, X_{t_2}, X_{t_3}, X_{t_4}, \ldots, X_{t_n})$$

$$H(X^n) = H(X_{t_1}) + H(X_{t_2}) + \cdots + H(X_{t_n})$$

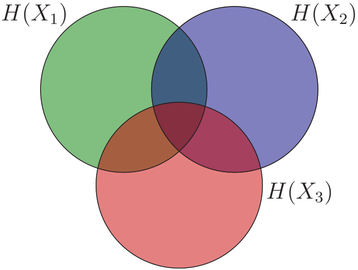
$$P_{X^n} = \prod_{j=1}^{n} P_{X_{t_j}}$$



Background - Three Correlated Sources

In general, when three variables are correlated, we have

$$I(X_1; X_3 | X_2) \neq 0$$

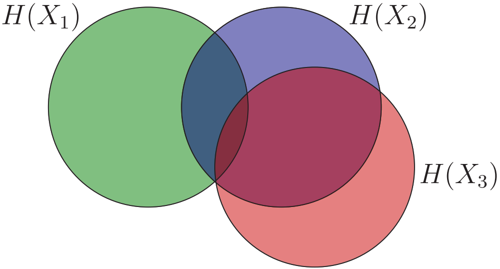


$$P_{X_1X_2X_3} = P_{X_1X_2}P_{X_3|X_1X_2}$$

Background - Conditional Independence

If Markov relation $X_1 - X_2 - X_3$ holds,

$$I(X_1; X_3 | X_2) = 0$$



$$P_{X_1 X_2 X_3} = P_{X_1 X_2} P_{X_3 | X_2}$$

- Measuring Length

Consider a random binary string X

$$x = (0,1,0,1,0,0,0,1,0,1,1,0,1,1,1,0)$$

We have

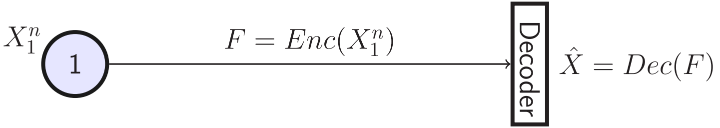
- $\text{length}(X) = 16$ and
- $\mathcal{X} = \{0,1\}^{16}$.

Observe that

$$\text{length}(X) = \log|\mathcal{X}|$$

UNIVERSITY OF CALGARY

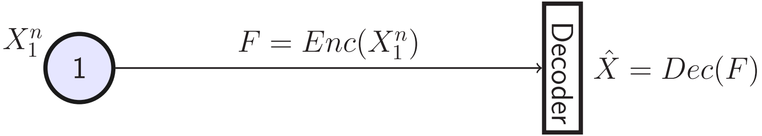
- Source Coding (Compression)



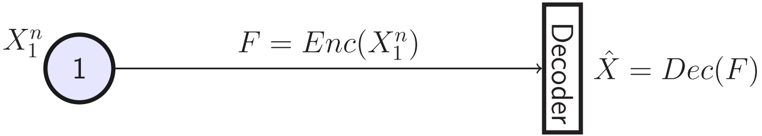
Objectives: $\begin{cases} 1)\ \hat{X} = X \\ 2)\ \text{length}(F) \text{ be as small as possible.} \end{cases}$

Consider a compression code $\Phi = (Enc, Dec)$, and a fixed n:

Comprssion rate	$r_n^{comp}(\Phi) = \frac{\text{length}(F)}{n}$
Error probability	$\Pr\left\{X \neq \hat{X}\right\} \leq \epsilon_n$



Problem:
Find the minimum real value R^* such that $r_n^{comp} \to R^*$ and $\epsilon_n \to 0$?

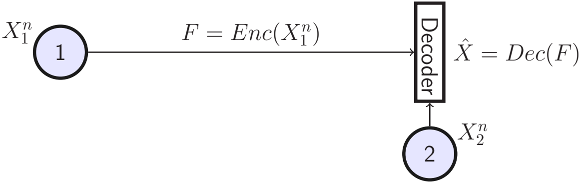


Source Coding Theorem: If P_{X_1} is known, then

$$R^* = H(X_1).$$

That is for any rate $R_1 \geq H(X_1)$ $\exists$ a compression code with asymptotic rate $r_n^{comp} \to R_1$, and negligible error probability ($\epsilon_n \to 0$); and for any coding rate $R_1 < H(X_1)$ there does not exist any compression code with negligible error probability.

Shannon, 1948



Source Coding with Side Information at the Decoder: If $P_{X_1 X_2}$ is known, then

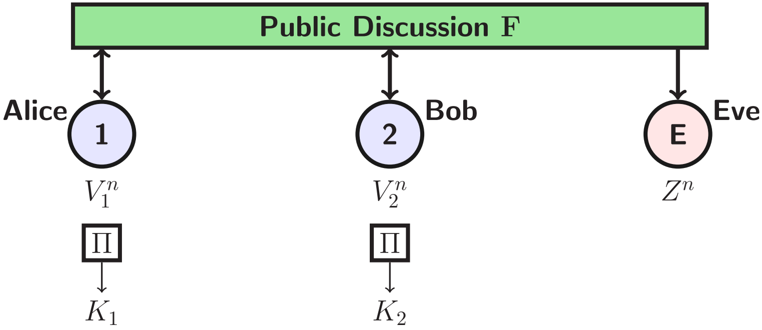
$$R^* = H(X_1|X_2).$$

That is for any rate $R_1 \geq H(X_1|X_2)$ $\exists$ a compression code with asymptotic rate $r^{comp} \to R_1$, and negligible error probability ($\epsilon_n \to 0$); and for any coding rate $R_1 < H(X_1|X_2)$ there does not exist any compression code with negligible error probability.

Slepian and Wolf, 1973

Part II

SKA in Source Model



An $(\epsilon, \sigma)-$Secret Key (SK):

- Reliability: $\Pr\{K_1 \neq K_2\} \leq \epsilon$
- Secrecy: $\mathbf{SD}(K_1 \mathbf{F} Z, U \mathbf{F} Z) \leq \sigma$

Wiretap Secret Key Capacity

Let Π be an SKA protocol family that $\forall n \in \mathbb{N}$ generates an $(\epsilon_n, \sigma_n)-$SK.

Key rate of Π is:

$$r_n^{key}(\Pi) = \frac{\text{length}(K)}{n}$$

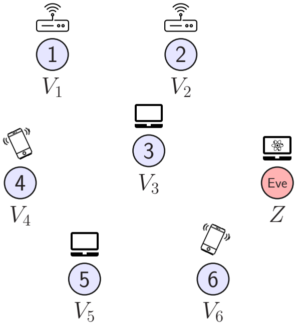
A key rate R is **achievable** if $\exists$ an SKA Π s.t.

- $r_n^{key}(\Pi) \to R$
- $\epsilon_n \to 0$
- $\sigma_n \to 0$

Wiretap secret key **(WSK) capacity** is the largest achievable key rate.

UNIVERSITY OF CALGARY

- Set of m terminals
- E.g. $\mathcal{M} = \{1, 2, 3, 4, 5, 6\}$
- Each terminal j has RV V_j
- Eve has **unlimited computation power**
- Establish a shared **Secret Key** for $\mathcal{A} \subseteq \mathcal{M}$
- E.g. $\mathcal{A} = \{3, 4, 5, 6\}$ or $\mathcal{A} = \mathcal{M}$
- Terminals 1 and 2 are helpers
- Free access to a noiseless **public channel**



Csiszár and Narayan, "Secrecy Capacities for Multiple Terminals," IEEE Trans. Inf. Theory, Dec. 2004.

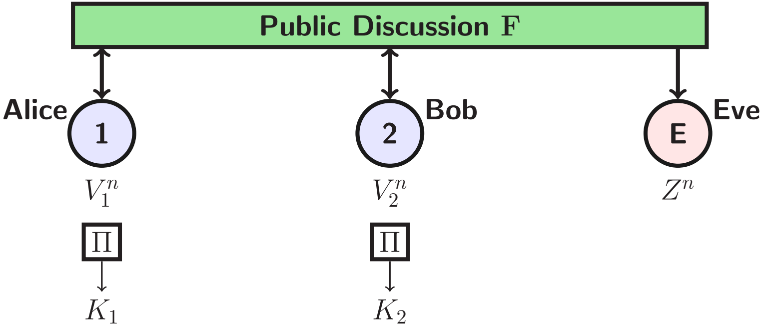
Finding a general expression for **WSK capacity**, $C_{WSK}(P_{V_{\mathcal{M}}})$, even for the case of two terminals ($|\mathcal{M}| = 2$) is an **open problem**.

Our Objective:

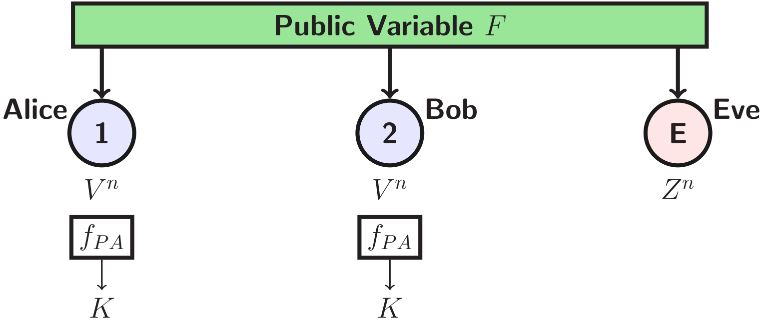
Find the WSK capacity of special-case models that are of practical importance.

Two-party SKA

Two-party Secret Key Agreement (SKA)



Key Extraction (Privacy Amplification)



A PA function f_{PA} is $(\sigma)-$**Secure** if $\mathbf{SD}(K\mathbf{F}Z, U\mathbf{F}Z) \leq \sigma$.

Universal Hash Functions are good key extractors.
Alice and Bob need to arrive at a common randomness.

Privacy Amplification Lemma (PAL)

Key rate of f_{PA} is:

$$r_n^{key}(f_{PA}) = \frac{\text{length}(K)}{n}$$

A key rate R is **achievable** if $\exists$ a PA function f_{PA} s.t.

- $r_n^{key}(f_{PA}) \to R$
- $\sigma_n \to 0$

PA Lemma [HTW16]: For every $R \in \mathbb{R}$ satisfying

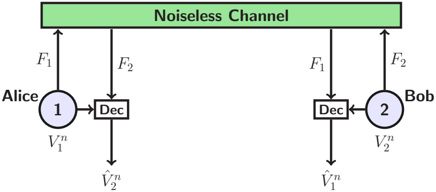
$$R \leq H(V|Z) - \lim_{n\to\infty} \frac{1}{n} \log|\mathcal{F}|,$$

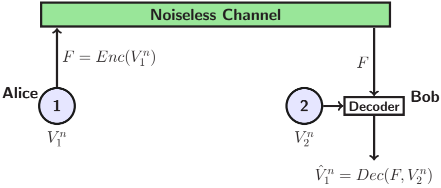
there always exists a σ_n-secure privacy amplification function $f_{PA} : \mathcal{V}^n \to \mathcal{K}$, with $r_n^{key}(f_{PA}) \to R$ and $\sigma_n \to 0$.

Hayashi, Tyagi, and Watanabe, IEEE Trans. on Inf. Theory, vol. 62, no. 7, July 2016.

Information Reconciliation (IR) a.k.a. Common Randomness Generation

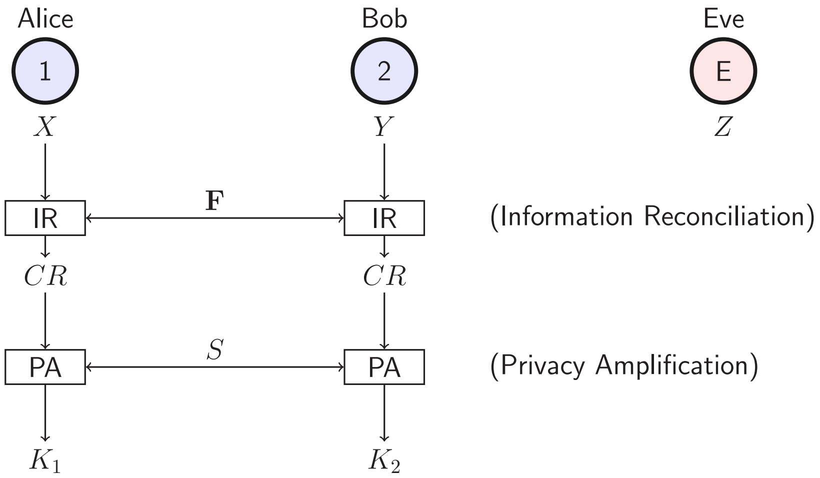
Objective: arrive at a common variable $CR = CR(V_1, V_2)$

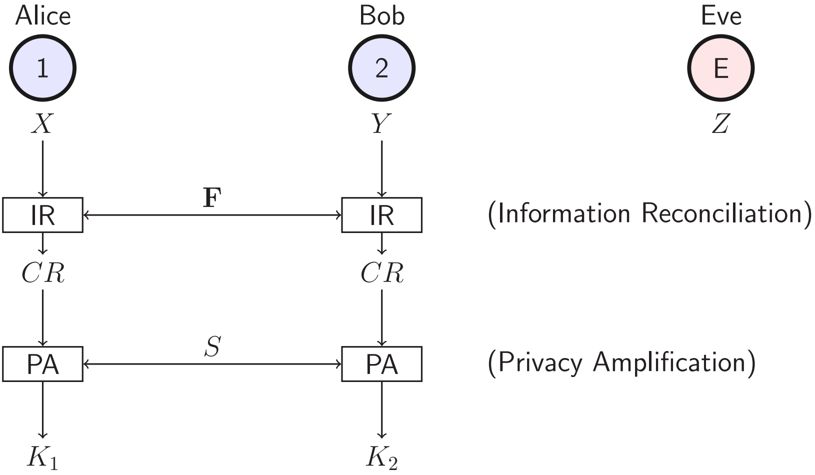




$$CR = (V_1, V_2)$$
$$R_1 \geq H(V_1|V_2)$$
$$R_2 \geq H(V_2|V_1)$$

$$CR = V_1$$
$$R_1 \geq H(V_1|V_2)$$


Alice
Bob
Eve
1
2
E
X
Y
Z
IR
$\mathbf{F}$
IR
(Information Reconciliation)
CR
CR
PA
S
PA
(Privacy Amplification)
K_1
K_2



$$r_n^{key} = \frac{\log|\mathcal{K}|}{n} \to H(CR|Z) - \lim_{n\to\infty} \frac{\log|F|}{n}$$

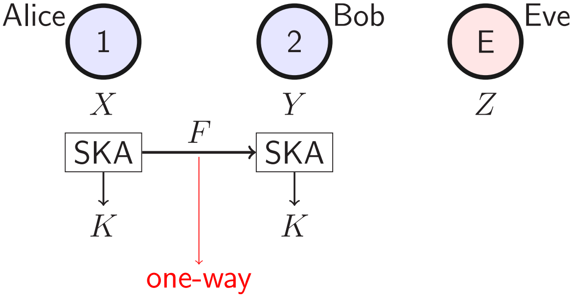
UNIVERSITY OF CALGARY

Problem: For a given source model (X, Y, Z) with known distribution P_{XYZ}, what is the key capacity, if

Problem: For a given source model (X, Y, Z) with known distribution P_{XYZ}, what is the key capacity, if **the public communication F is <u>one-way</u> (from Alice to Bob)**

$$C^{\rightarrow}_{WSK}(P_{XYZ}) = ?$$

One-way SKA against a wiretapper



Theorem [AC93]: For a given source model (X, Y, Z) with known distribution P_{XYZ}, the one-way secret key capacity is

$$C_{WSK}^{\rightarrow} = \max_{P_{VU}} H(U|ZV) - H(U|YV),$$

where $V - U - X - (Y, Z)$.

Theorem [AC93]: If $X - Y - Z$

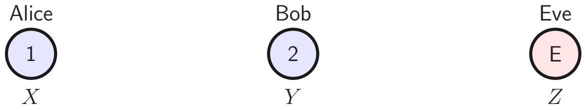
$$C_{WSK} = H(X|Z) - H(X|Y).$$

Moreover, this capacity can be achieved by one-way communication.

[AC93] Ahlswede and Csiszár, IEEE Trans. Inf. Theory, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

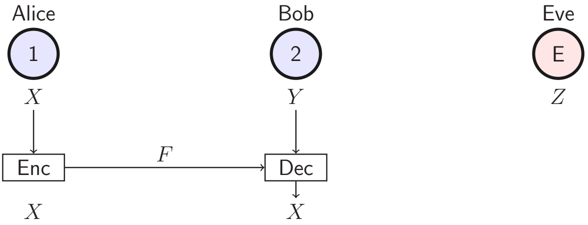
How to Achieve WSK capacity?

OW-SKA when $X - Y - Z$ holds.



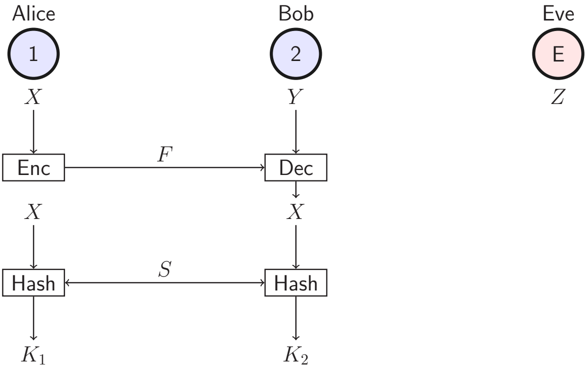
How to Achieve WSK capacity?

OW-SKA when $X - Y - Z$ holds.



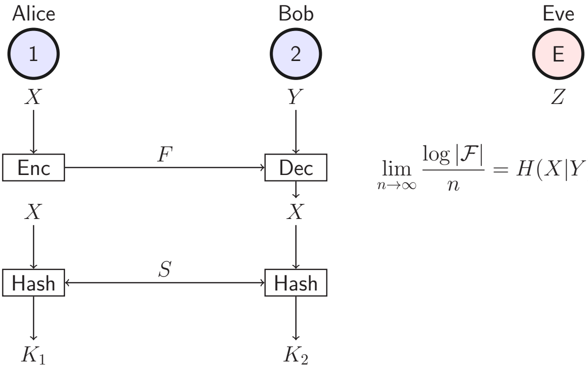
How to Achieve WSK capacity?

OW-SKA when $X - Y - Z$ holds.



How to Achieve WSK capacity?

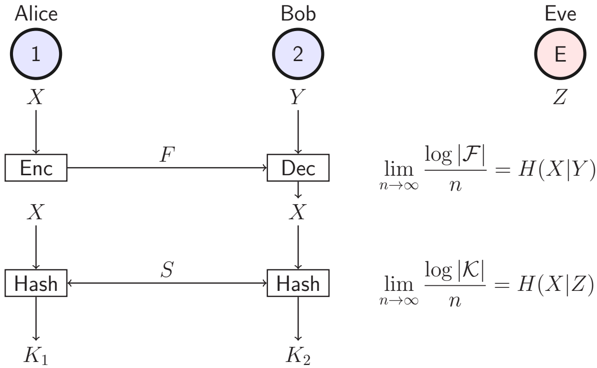
OW-SKA when $X - Y - Z$ holds.



$$\lim_{n\to\infty} \frac{\log|\mathcal{F}|}{n} = H(X|Y) + \mu$$

How to Achieve WSK capacity?

OW-SKA when $X - Y - Z$ holds.

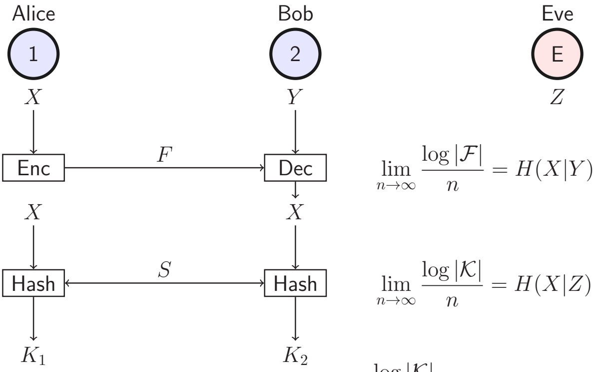


$$\lim_{n\to\infty} \frac{\log|\mathcal{F}|}{n} = H(X|Y) + \mu$$

$$\lim_{n\to\infty} \frac{\log|\mathcal{K}|}{n} = H(X|Z) - \lim_{n\to\infty} \frac{\log|\mathcal{F}|}{n} - \xi$$

How to Achieve WSK capacity?

OW-SKA when $X - Y - Z$ holds.



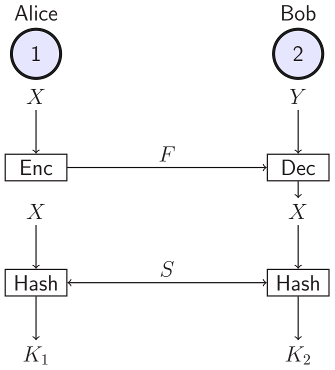
$$\lim_{n\to\infty} \frac{\log|\mathcal{F}|}{n} = H(X|Y) + \mu$$

$$\lim_{n\to\infty} \frac{\log|\mathcal{K}|}{n} = H(X|Z) - \lim_{n\to\infty} \frac{\log|\mathcal{F}|}{n} - \xi$$

$$\lim_{n\to\infty} \frac{\log|\mathcal{K}|}{n} = H(X|Z) - H(X|Y) = C_{WSK}^{\rightarrow} - \mu - \xi$$

How to Achieve WSK capacity?

OW-SKA when $X - Y - Z$ holds.



$$\lim_{n\to\infty} \frac{\log|\mathcal{F}|}{n} = H(X|Y) + \mu$$

$$\lim_{n\to\infty} \frac{\log|\mathcal{K}|}{n} = H(X|Z) - \lim_{n\to\infty} \frac{\log|\mathcal{F}|}{n} - \xi$$

$$\lim_{n\to\infty} \frac{\log|\mathcal{K}|}{n} = H(X|Z) - H(X|Y) = C_{WSK}^{\rightarrow} - \mu - \xi$$

$$\mu, \xi \to 0$$

Our Results

Problem: Consider a source model (X, Y, Z) that is INID where $X_j - Y_j - Z_j$ holds for every j.

What is the WSK capacity of this model?

Problem: Consider a source model (X, Y, Z) that is INID where $X_j - Y_j - Z_j$ holds for every j.

What is the WSK capacity of this model?

Theorem [SPS'20]: For the INID source model above

$$C_{WSK} = \liminf_{n\to\infty} H(X^n|Z^n) - H(X^n|Y^n).$$

Moreover, this capacity can be achieved by one-way communication.

[SPS'20] Sharifian, Poostindouz and Safavi-Naini, "A Capacity-achieving One-way Key Agreement with Improved Finite Blocklength Analysis," ISITA 2020

Our Results

Let n be a fixed finite integer. Define $S^{\rightarrow}_{\epsilon,\sigma}$ as the largest key length of all $(\epsilon,\sigma)-$SK's generated by OW-SKA.

Previous capacity results imply that

$$S^{\rightarrow}_{\epsilon,\sigma} = nC^{\rightarrow}_{WSK} - o(n).$$

Problem: Consider a source model (X,Y,Z) for OW-SKA.

Find more accurate finite-length approximations of $S^{\rightarrow}_{\epsilon,\sigma}$?

UNIVERSITY OF CALGARY

We proposed a OW-SKA protocol $\mathbf{\Pi_{HH}}$ and proved the following.

Theorem [SPS'20]: For the INID source model

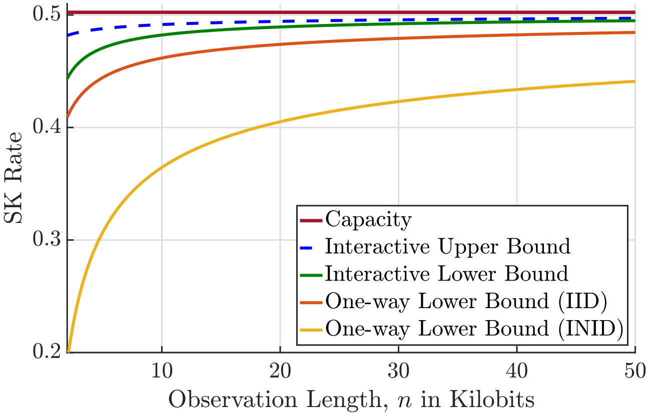
$$S^{\rightarrow}_{\epsilon,\sigma} \geq H(X^n|Z^n) - H(X^n|Y^n) - \sqrt{n}G_1 - \log n + \mathcal{O}(1),$$

where G_1 is a function of $(|\mathcal{X}|, \epsilon, \sigma)$.

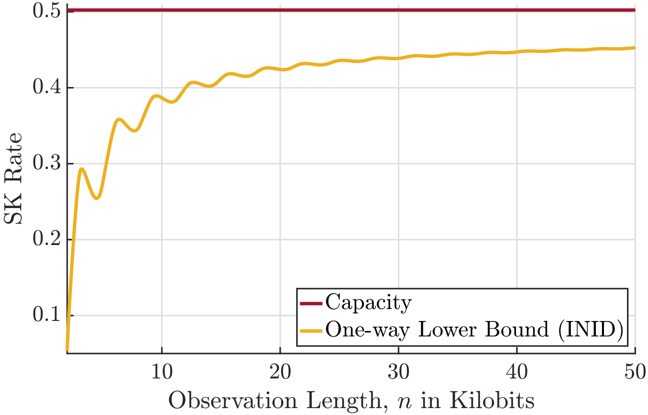
Theorem [SPS'20]: For the IID source model

$$S^{\rightarrow}_{\epsilon,\sigma} \geq n\big(H(X|Z) - H(X|Y)\big) - \sqrt{n}G_2 - \log n + \mathcal{O}(1),$$

where G_2 is a function of $(P_{XYZ}, \epsilon, \sigma)$.



Optimum finite-length bounds of interactive SKA, and the finite-length lower bounds of OW-SKA protocol $\mathbf{\Pi_{HH}}$. Here $\epsilon = \sigma = 0.05$, P_X is uniform, $Y = BSC_a(X)$, and $Z = BSC_b(Y)$, where $a = 0.02$, and $b = 0.15$. Note that in this example, as $X - Y - Z$ holds, both interactive and one-way bounds achieve the WSK capacity.



Finite-length performance of $\mathbf{\Pi_{HH}}$ for an INID source. Here $\epsilon = \sigma = 0.05$, P_X is uniform IID, $Y_n = BSC_{a_n}(X_n)$, and $Z_n = BSC_{b_n}(Y_n)$, where $a_n = 0.02 + \frac{500}{n}\sin\left(\frac{n}{500}\right)$, and $b_n = 0.15$. Here $X_n - Y_n - Z_n$ holds for all n, and both interactive and one-way SKA approaches achieve the WSK capacity.

We observed that the computational cost of $\mathbf{\Pi_{HH}}$ is exponential so we proposed a second OW-SKA protocol, $\mathbf{\Pi_{PH}}$, that has computational complexity $\mathcal{O}(n \log n)$ and proved its finite-length analysis.

Theorem [PS'21]: For every $\delta \in (0, 1]$

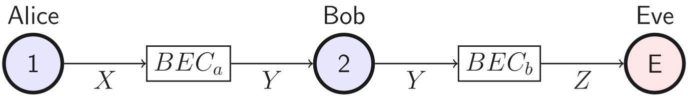
$$\ell_{\mathbf{\Pi_{PH}}}(n) = nC_{WSK} - \sqrt[\tau]{n^{\tau-1}}G_{IR}(\epsilon) - \sqrt{n}G_{PA}(\sigma) \pm o(\sqrt{n}),$$

where $\tau = 2 + \delta$.

[PS'21] Poostindouz and Safavi-Naini, "Second-Order Asymptotics for One-way Secret Key Agreement," ISIT 2021.

Efficient OW-SKA Protocol Π_{PH}

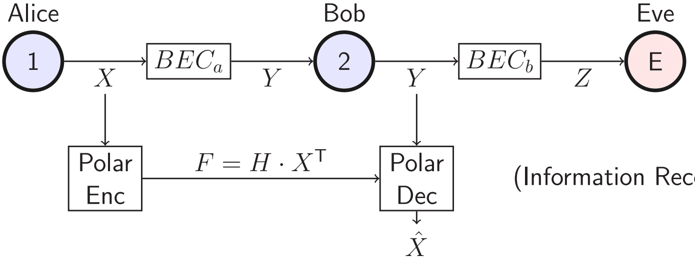
One-way SKA using Polar coding



- The computational complexity is $\mathcal{O}(n \log n)$

Efficient OW-SKA Protocol Π_{PH}

One-way SKA using Polar coding

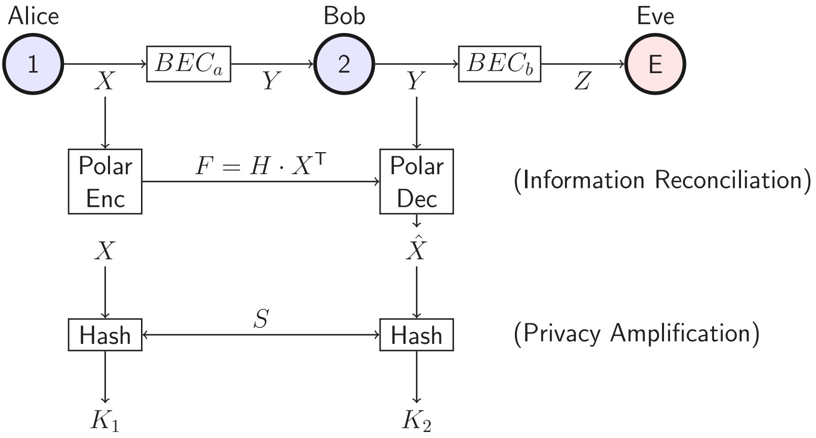


(Information Reconciliation)

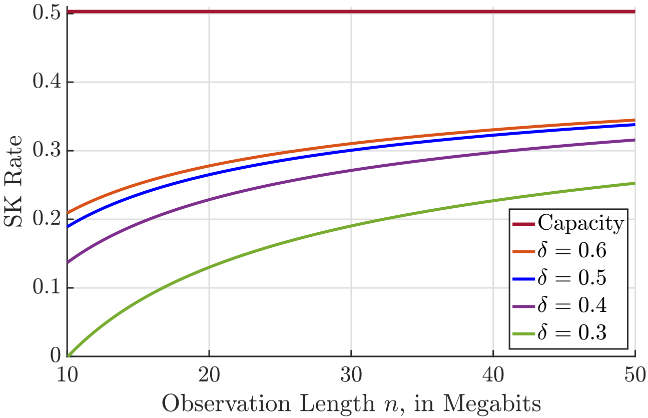
- The computational complexity is $\mathcal{O}(n \log n)$

UNIVERSITY OF CALGARY

One-way SKA using Polar coding



- The computational complexity is $\mathcal{O}(n \log n)$



Finite-length performance of OW-SKA Protocol $\mathbf{\Pi_{PH}}$ for different δ's in, $(0.3, 0.4, 0.5, 0.6)$. These values correspond to polarization kernel sizes of $(30, 13, 8, 6)$ (in the same order). Here $\epsilon = \sigma = 0.05$, P_X is uniform, $Y = BEC_a(X)$, and $Z = BEC_b(Y)$, where $a = 0.1$, and $b = 0.67$.

UNIVERSITY OF CALGARY

Finite-length Analysis of One-Way Two-party SKA

- Proposed two new concrete protocol constructions for one-way SKA
- Proved multiple finite-length lower bound on maximum key length

$$S^{\rightarrow} \geq nC_{WSK} - \mathcal{O}(\sqrt{n})$$

- Proved a finite-length upper bound through new spectral entropies
- Proved WSK capacity for the general case when variables are INID

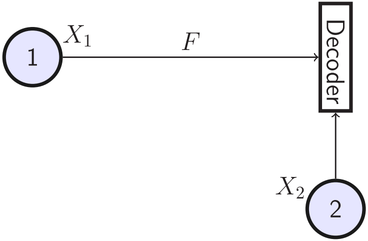
Poostindouz and Safavi-Naini, "Second-Order Asymptotics for One-way Secret Key Agreement," ISIT 2021.

Sharifian, Poostindouz and Safavi-Naini, "A Capacity-achieving One-way Key Agreement with Improved Finite Blocklength Analysis," ISITA 2020

Multiterminal Results SKA

Review

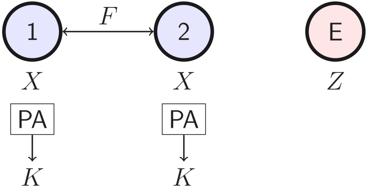
Source Coding with Side Info



$$\lim_{n\to\infty} \frac{\text{length}(F)}{n} = R_1$$

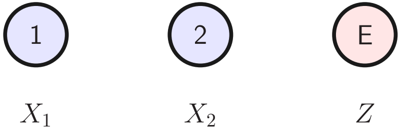
$$R_1 \geq H(X_1|X_2)$$

Privacy Amplification Lemma

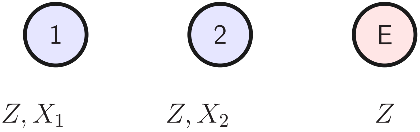


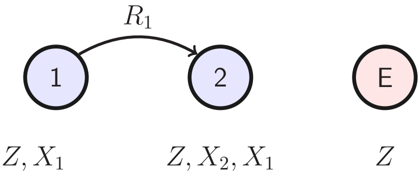
$$\lim_{n\to\infty} \frac{\text{length}(F)}{n} \geq R_{\min}$$

$$r^{key} \leq H(X|Z) - R_{\min}$$


1
2
E
X_1
X_2
Z

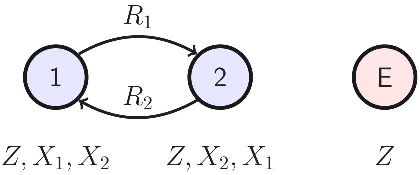
SKA by Omniscience (When Z is known)





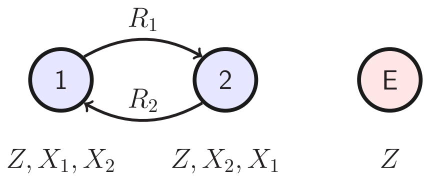
$$R_1 \geq H(X_1|X_2Z)$$

SKA by Omniscience (When Z is known)



$$R_1 \geq H(X_1|X_2Z)$$
$$R_2 \geq H(X_2|X_1Z)$$

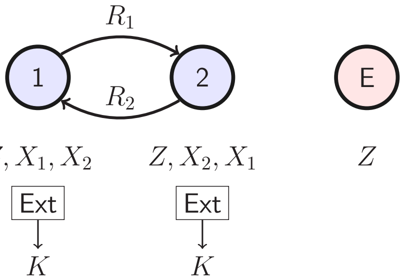
SKA by Omniscience (When Z is known)



$$R_1 \geq H(X_1|X_2Z)$$
$$R_2 \geq H(X_2|X_1Z)$$

$$\lim_{n\to\infty} \frac{\text{length}(F)}{n} \geq R_{\min}$$
$$R_{\min} = H(X_1|X_2Z) + H(X_2|X_1Z)$$

SKA by Omniscience (When Z is known)



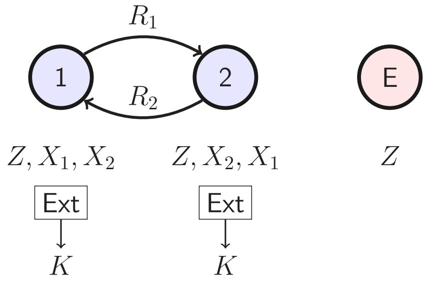
$$R_1 \geq H(X_1|X_2Z)$$
$$R_2 \geq H(X_2|X_1Z)$$

$$\lim_{n\to\infty} \frac{\text{length}(F)}{n} \geq R_{\min}$$
$$R_{\min} = H(X_1|X_2Z) + H(X_2|X_1Z)$$

Common randomness

$$CR = (X_1, X_2, Z)$$

SKA by Omniscience (When Z is known)



$$R_1 \geq H(X_1|X_2Z)$$
$$R_2 \geq H(X_2|X_1Z)$$

$$\lim_{n\to\infty} \frac{\text{length}(F)}{n} \geq R_{\min}$$
$$R_{\min} = H(X_1|X_2Z) + H(X_2|X_1Z)$$

Common randomness

$$CR = (X_1, X_2, Z)$$

By PAL, we have

$$r^{key} \leq H(X_1, X_2|Z) - R_{\min}$$

Thus

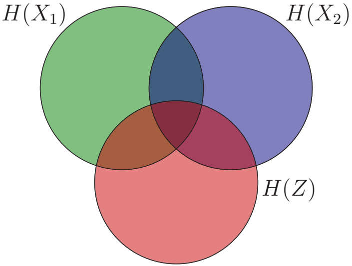
$$r^{key} = H(X_1, X_2|Z) - H(X_1|X_2Z) - H(X_2|X_1Z)$$

is an achievable key rate.

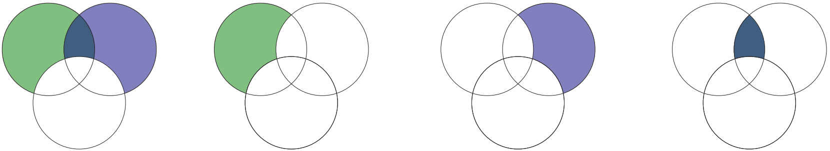
When Z is known WSK capacity is called the PK capacity.

$$C_{PK} = H(X_1, X_2|Z) - H(X_1|X_2Z) - H(X_2|X_1Z)$$

Is there a simpler expression?



$C_{PK} = ?$



$$H(X_1, X_2|Z) \quad - \quad H(X_1|X_2 Z) \quad - \quad H(X_2|X_1 Z) \quad = \quad I(X_1; X_2|Z)$$

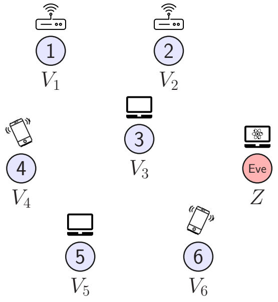
Thus

$$C_{PK} = I(X_1; X_2|Z)$$

Theorem [CN04]: For a given multiterminal source model $P_{X_{\mathcal{M}}Z}$, the PK capacity is

$$C_{PK} = H(X_{\mathcal{M}}|Z) - R_{CO}(X_{\mathcal{M}}|Z)$$

where $R_{CO}(X_{\mathcal{M}}|Z)$ is the minimum asymptotic public communication sum rate that is required for terminals in subset $\mathcal{A}$ to achieve omniscience (learn $X_{\mathcal{M}}$ in addition to the common variable Z).

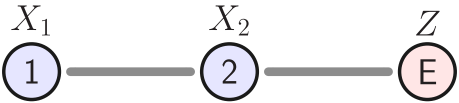


Lemma [CN04]: $C_{WSK} \leq C_{PK}$

[CN04] Csiszár and Narayan, IEEE Trans. Inf. Theory, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

Recall: If $X_1 - X_2 - Z$, then

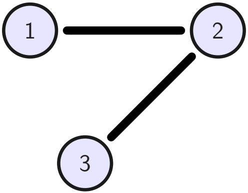
$$C_{WSK} = C_{PK} = I(X_1, X_2|Z)$$



Can we extend this model to a multiterminal version?

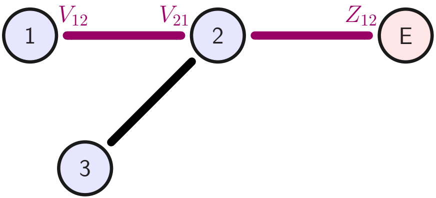
Example:

$$\mathcal{M} = \{1, 2, 3\} \qquad \mathcal{E} = \{e_{12}, e_{23}\} \qquad G = (\mathcal{M}, \mathcal{E})$$



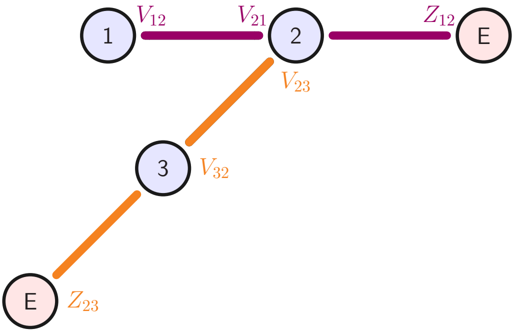
Example:

$$\mathcal{M} = \{1, 2, 3\} \qquad \mathcal{E} = \{e_{12}, e_{23}\} \qquad G = (\mathcal{M}, \mathcal{E})$$



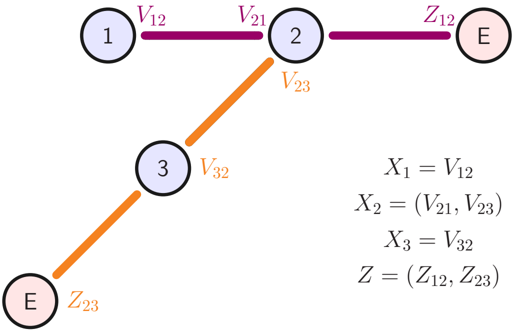
Example:

$$\mathcal{M} = \{1,2,3\} \qquad \mathcal{E} = \{e_{12}, e_{23}\} \qquad G = (\mathcal{M}, \mathcal{E})$$



Example:

$$\mathcal{M} = \{1, 2, 3\} \qquad \mathcal{E} = \{e_{12}, e_{23}\} \qquad G = (\mathcal{M}, \mathcal{E})$$



$$X_1 = V_{12}$$
$$X_2 = (V_{21}, V_{23})$$
$$X_3 = V_{32}$$
$$Z = (Z_{12}, Z_{23})$$

UNIVERSITY OF CALGARY

Wiretapped Tree over a Pairwise Independent Network (PIN)

- Terminal set $\mathcal{M} = \{1, 2, \ldots, m\}$
- Tree $G = (\mathcal{M}, \mathcal{E})$
- $\{(V_{ij}, V_{ji}, Z_{ij})\}_{i<j}$ are mutually independent
- For all $i < j$, Markov relation $V_{ij} - V_{ji} - Z_{ij}$ holds

Theorem [PS21]: For any wiretapped Tree-PIN,

$$C_{WSK} = \min_{i,j} I(V_{ij}; V_{ji} | Z_{ij}).$$

[PS21] Poostindouz and Safavi-Naini, "Secret key agreement in wiretapped Tree-PIN," arXiv:1903.06134.

Proof (Sketch):

We show that

$$R_{CO}(X_{\mathcal{M}}|Z) = H(X_{\mathcal{M}}|Z) - \min_{i,j} I(V_{ij};V_{ji}|Z_{ij}).$$

Then, by

$$C_{WSK}(X_{\mathcal{M}}|Z) \leq C_{PK}(X_{\mathcal{M}}|Z) = H(X_{\mathcal{M}}|Z) - R_{CO}(X_{\mathcal{M}}|Z),$$

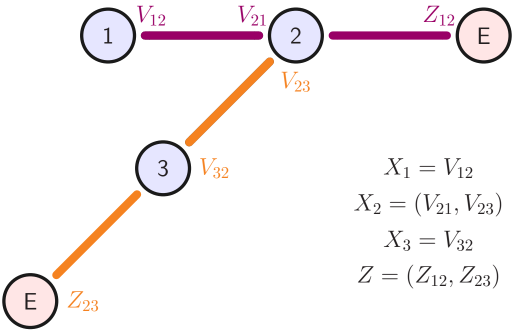
we have

$$C_{WSK}(X_{\mathcal{M}}|Z) \leq \min_{i,j} I(V_{ij};V_{ji}|Z_{ij}).$$

Finally, we show that the above rate is an achievable key rate.

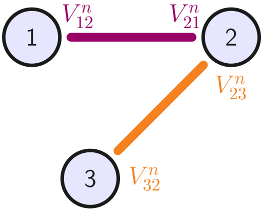
Example:

$$\mathcal{M} = \{1, 2, 3\} \qquad \mathcal{E} = \{e_{12}, e_{23}\} \qquad G = (\mathcal{M}, \mathcal{E})$$

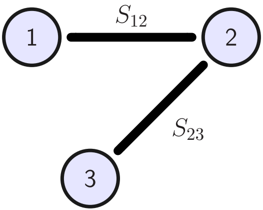


$$X_1 = V_{12}$$
$$X_2 = (V_{21}, V_{23})$$
$$X_3 = V_{32}$$
$$Z = (Z_{12}, Z_{23})$$

Achieving WSK capacity



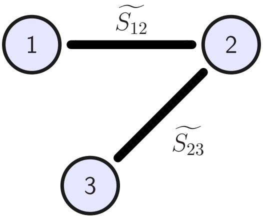
Achieving WSK capacity



Steps:

1. Pairwise key agreement S_{12}, S_{12}

Achieving WSK capacity



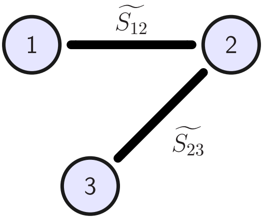
$$\widetilde{S_{ij}} = S_{ij}|_{\lambda}$$

Steps:

1. Pairwise key agreement S_{12}, S_{12}
2. Cutting pairwise keys to the minimum length

$$\lambda = \min\{\text{length}(S_{ij})\} \approx n \times \min I(V_{ij}; V_{ji}|Z_{ij})$$

Achieving WSK capacity



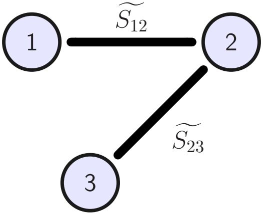
$F_2 = \widetilde{S_{12}} \oplus \widetilde{S_{23}}$

Steps:

1. Pairwise key agreement S_{12}, S_{12}
2. Cutting pairwise keys to the minimum length

$$\lambda = \min\{\text{length}(S_{ij})\} \approx n \times \min I(V_{ij}; V_{ji} | Z_{ij})$$

3. XOR propagation $F_2 = \widetilde{S_{12}} \oplus \widetilde{S_{23}}$



$F_2 = \widetilde{S_{12}} \oplus \widetilde{S_{23}}$

Steps:

1. Pairwise key agreement S_{12}, S_{12}
2. Cutting pairwise keys to the minimum length

$$\lambda = \min\{\text{length}(S_{ij})\} \approx n \times \min I(V_{ij}; V_{ji}|Z_{ij})$$

3. XOR propagation $F_2 = \widetilde{S_{12}} \oplus \widetilde{S_{23}}$
4. Key calculation $K = \widetilde{S_{12}} = \widetilde{S_{23}} \oplus F_2$

Wiretapped Pairwise Independent Network (PIN)

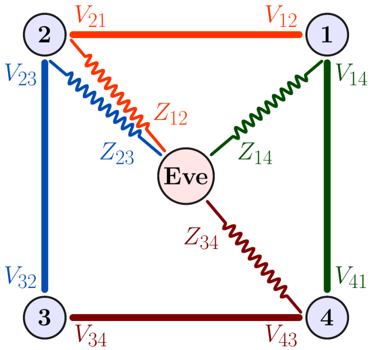
- Graphs (with loops) $G = (\mathcal{M}, \mathcal{E})$
- $\{(V_{ij}, V_{ji}, Z_{ij})\}_{i<j}$ are mutually independent
- For all $i < j$, Markov relation $V_{ij} - V_{ji} - Z_{ij}$ holds

Theorem [PS21]: For any wiretapped PIN, the WSK capacity is

$$C_{WSK} = \min_{\mathcal{P}} \left(\frac{1}{|\mathcal{P}| - 1} \right) \left[\sum_{\substack{i<j \text{ s.t.} \\ (i,j) \text{ crosses } \mathcal{P}}} I(V_{ij}; V_{ji} | Z_{ij}) \right]$$

[PS21] Poostindouz and Safavi-Naini, "Secret key agreement in wiretapped Tree-PIN," arXiv:1903.06134.

Example - Steiner tree packing

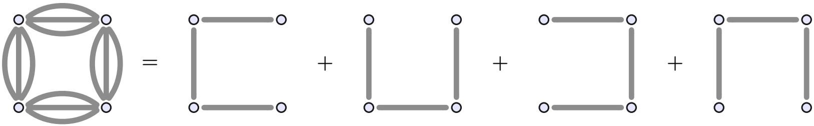


If $I(V_{ij}; V_{ji} | Z_{ij}) = \frac{1}{2}$ for all i, j then, for $\mathcal{P} = \{\{1\}, \{2\}, \{3\}, \{4\}\}$

$$C_{WSK} \leq \frac{\frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2}}{4 - 1} = \frac{2}{3}$$

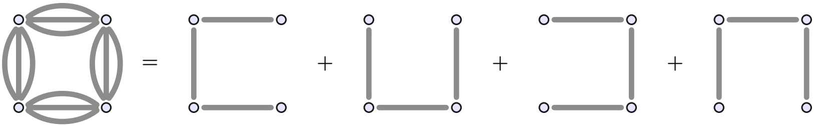
$$n = 6\nu \quad \text{and} \quad \lambda = \text{length}(S_{ij}) = 3\nu - \epsilon$$

$$n = 6\nu \quad \text{and} \quad \lambda = \text{length}(S_{ij}) = 3\nu - \epsilon$$



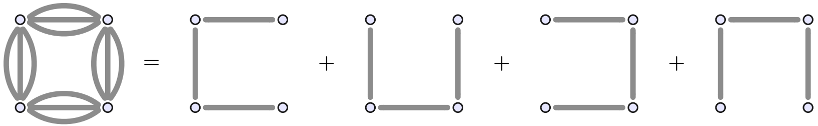
Achieving WSK Capacity by Steiner tree packing

$$n = 6\nu \quad \text{and} \quad \lambda = \text{length}(S_{ij}) = 3\nu - \epsilon$$



$$\text{length}(K) = 4\nu - \mathcal{O}(\epsilon)$$

$$n = 6\nu \quad \text{and} \quad \lambda = \text{length}(S_{ij}) = 3\nu - \epsilon$$



$$\text{length}(K) = 4\nu - \mathcal{O}(\epsilon)$$

$$r^{key} = \lim_{n\to\infty} \frac{\text{length}(K)}{n} = \lim_{\nu\to\infty} \frac{4\nu - \mathcal{O}(\epsilon)}{6\nu} = \frac{2}{3} = C_{WSK}$$

UNIVERSITY OF CALGARY

SKA in Wiretapped Pairwise Independent Networks

- Proved WSK capacity of wiretapped Tree-PIN
- Proposed an optimum capacity achieving SKA protocol
- Proved WSK capacity of wiretapped PIN when $\mathcal{A} = \mathcal{M}$
- Proposed an SKA protocol using Steiner Tree Packing
- Proved WSK capacity of multiple generalizations (e.g., $\exists$ a non-cooperating compromised terminal)

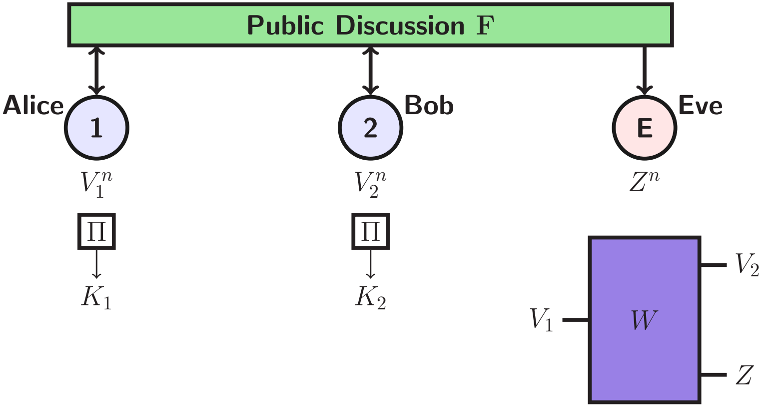
Poostindouz and Safavi-Naini, "Wiretap Secret Key Capacity of Tree-PIN," ISIT 2019.

Poostindouz and Safavi-Naini, "Secret Key Agreement in Wiretapped Tree-PIN," arXiv:1903.06134.

Part III

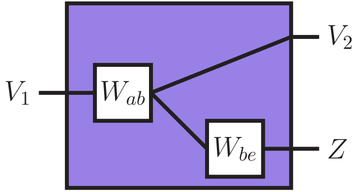
SKA in Channel Model

Two-party SKA in Channel Model



Alice can send adaptive channel input symbols.

UNIVERSITY OF CALGARY



W

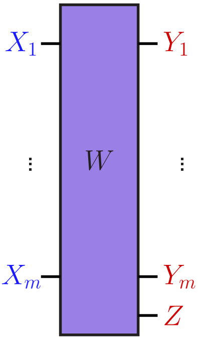
Theorem [AC93]: When the channel W is degraded

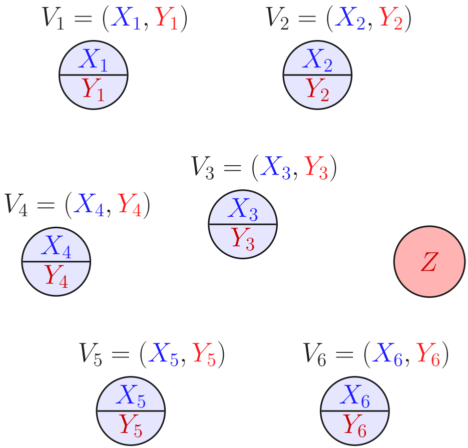
$$C_{WSK}(W) = \max_{P_{V_1}} H(V_1|Z) - H(V_1|V_2).$$

Moreover, this capacity can be achieved without adaptive inputs.

[AC93] Ahlswede and Csiszár, IEEE Trans. Inf. Theory, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

The Transceivers Channel Model

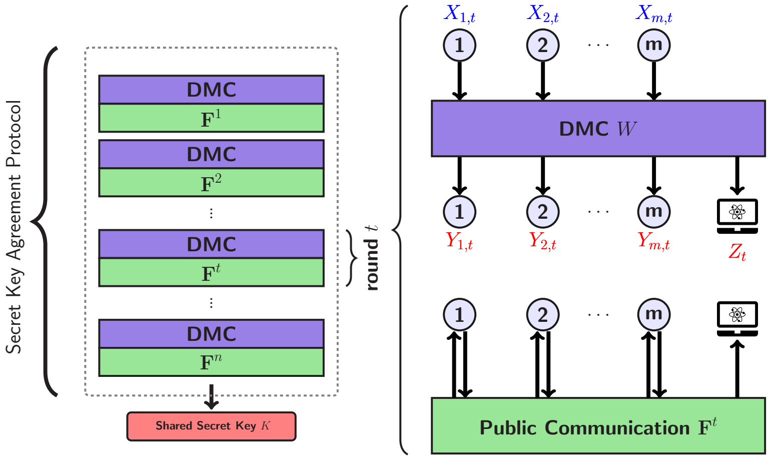




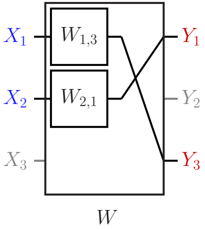
$$W = P_{ZY_{\mathcal{M}}|X_{\mathcal{M}}}$$

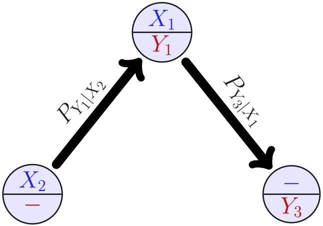
Poostindouz and Safavi-Naini, "A channel model of transceivers for multiterminal secret key agreement," ISITA 2020.

UNIVERSITY OF CALGARY



A simple example (non-wiretapped)





$$W = P_{Y_{\mathcal{M}}|X_{\mathcal{M}}} = P_{Y_1|X_2} \cdot P_{Y_3|X_1}$$

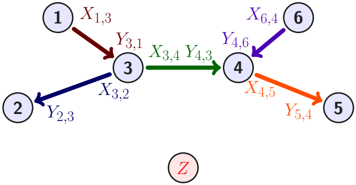
The model can be represented by a directed graph $G = (\mathcal{M}, \mathcal{E})$, where $\mathcal{M} = \{1, 2, 3\}$ and $\mathcal{E} = \{e_{2,1}, e_{1,3}\}$.

Polytree-PIN

Let $W = P_{ZY_{\mathcal{M}}|X_{\mathcal{M}}} = P_{Y_{\mathcal{M}}|X_{\mathcal{M}}} P_{Z|X_{\mathcal{M}}Y_{\mathcal{M}}}$

There exists a polytree $G = (\mathcal{M}, \mathcal{E})$ that defines $P_{Y_{\mathcal{M}}|X_{\mathcal{M}}}$ as a pairwise independent network (PIN) of point-to-point channels:

$$W = P_{Y_{\mathcal{M}}|X_{\mathcal{M}}} P_{Z|X_{\mathcal{M}}Y_{\mathcal{M}}} = \left(\prod_{e_{ij} \in \mathcal{E}} P_{Y_{ij}|X_{ji}}\right) P_{Z|X_{\mathcal{M}}Y_{\mathcal{M}}}$$



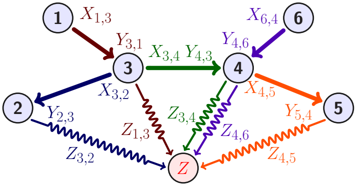
UNIVERSITY OF CALGARY

Polytree-PIN
with independent leakage

$$W = P_{ZY_{\mathcal{M}}|X_{\mathcal{M}}} = P_{Y_{\mathcal{M}}|X_{\mathcal{M}}} P_{Z|Y_{\mathcal{M}}}$$

$$Z = (Z_{ij}|\ e_{ij} \in \mathcal{E})$$

$X_{ij} - Y_{ji} - Z_{ij}$ holds for all $e_{ij} \in \mathcal{E}$



$$W = P_{Y_{\mathcal{M}}|X_{\mathcal{M}}} P_{Z|Y_{\mathcal{M}}}$$
$$= \prod_{e_{ij} \in \mathcal{E}} P_{Y_{ij}|X_{ji}} P_{Z_{ij}|Y_{ji}}$$

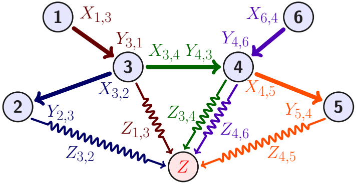
UNIVERSITY OF CALGARY

Polytree-PIN
with independent leakage

Theorem: WSK Capacity of Polytree-PIN with independent leakage is given by

$$C_{WSK}^{\mathcal{A}}(W) = \max_{P_{X_{\mathcal{M}}}} \min_{\substack{i,j\in\mathcal{M} \\ e_{ij}\in\mathcal{E}_{\mathcal{A}}}} I(X_{ij};Y_{ji}|Z_{ij}).$$

Moreover, this capacity can be achieved without adaptive inputs.



Poostindouz and Safavi-Naini, "Secret Key Capacity of Wiretapped Polytree-PIN," ITW 2021.

Multiterminal SKA in Wiretapped Network of Transceivers

- Introduced the general multiterminal channel model of Transceivers
- Proved Upper and Lower bounds on the SK, PK, and WSK capacities
- Proved the nonadaptive SK capacity of general Transceivers
- Proved the WSK capacity of Polytree-PIN Model

Poostindouz and Safavi-Naini, "Secret Key Capacity of Wiretapped Polytree-PIN," ITW 2021.
Poostindouz and Safavi-Naini, "Multiterminal Secret Key Agreement in Wiretapped Transceiver Channel Model," to be submitted to Entropy.

Poostindouz and Safavi-Naini, "A channel model of transceivers for multiterminal secret key agreement," ISITA 2020.

Thanks for your attention!