Information-theoretic secret key agreement in the presence of a wiretapper

Alireza Poostindouz

University of Calgary

May 29, 2020

Quantum Computers (QCs)
The $|\text{GOOD}\rangle + |\text{BAD}\rangle$ news:

- QCs efficiently solve integer factorization and discrete logarithms
- Security of Internet is based on factorization and discrete logarithms
- Rapid advancements in quantum technologies
- NSA announcement on transitioning to quantum resistant algorithms

Quantum safe keys $\Rightarrow$ Quantum safe communication

Quantum resistant SKAs

Existing approaches to quantum resistant secret key agreement (SKA)

- Post-quantum computational algorithm
- Quantum key distribution (QKD)
- Physical-layer information-theoretic SKA

We focus on "**Physical-layer information-theoretic SKA**".

Part I

Information Theory

Background - 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)

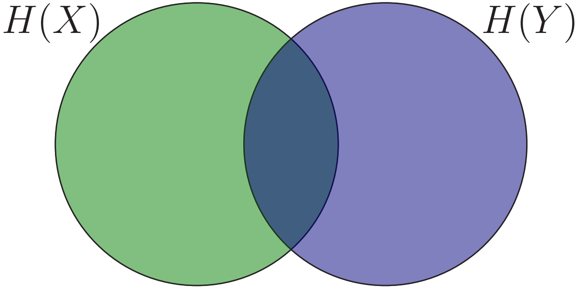
$$P_X(x) = \Pr\{X = x\}$$

- Information, Uncertainty, Entropy

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

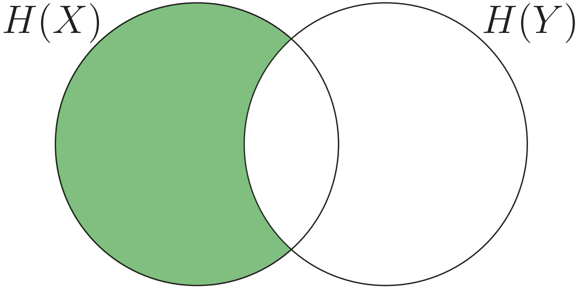
Background - Information theory

- Entropy, Joint Entropy, Conditional Entropy



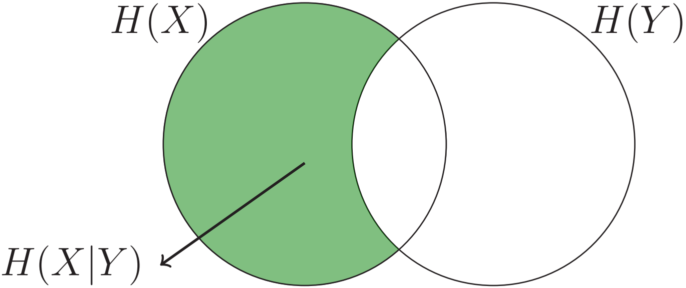
Background - Information theory

- Entropy, Joint Entropy, Conditional Entropy

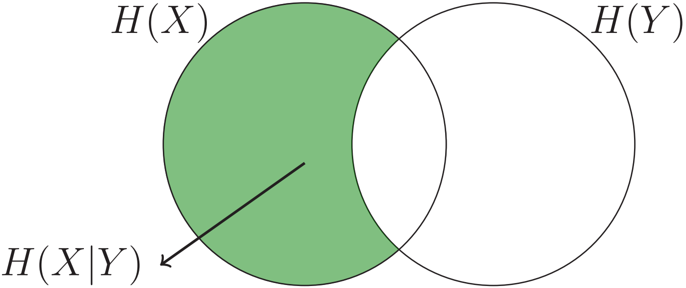


Background - Information theory

- Entropy, Joint Entropy, Conditional Entropy



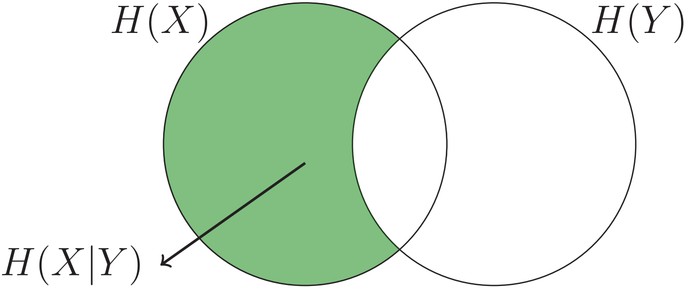
- Entropy, Joint Entropy, Conditional Entropy



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

Background - Information theory

- Entropy, Joint Entropy, Conditional Entropy

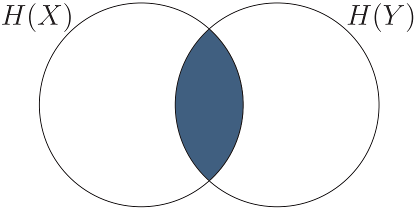


$$H(X,Y) = H(Y) + H(X|Y)$$

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

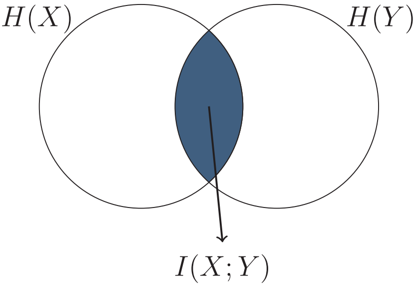
Background - Information theory

- Mutual Information



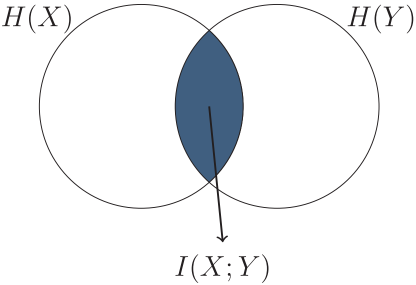
Background - Information theory

- Mutual Information



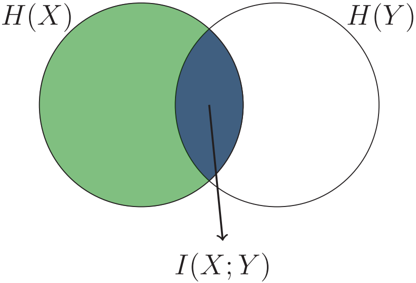
Background - Information theory

- Mutual Information



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

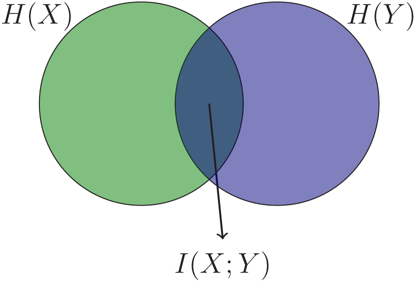
- Mutual Information



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

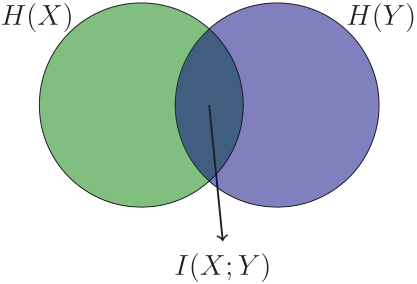
Background - Information theory

- Mutual Information



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

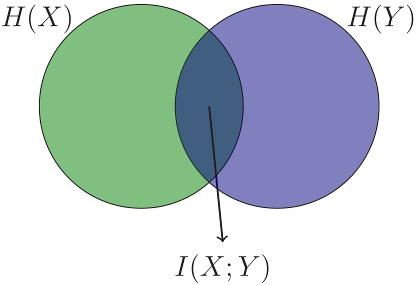
- Mutual Information



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

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

- Mutual Information



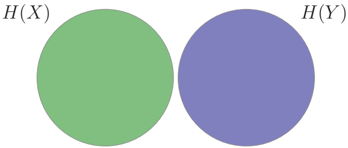
$$H(X,Y) = I(X;Y) + H(X|Y) + H(Y|X)$$

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

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

Background - Information theory

- Independence



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

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

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

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

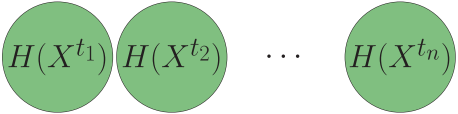
Background - Information theory

- $n-$IID Source (Independent and identically distributed)

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

$$\{X^{t_i}\}_{i \leq n} \text{ are mutually independent}$$

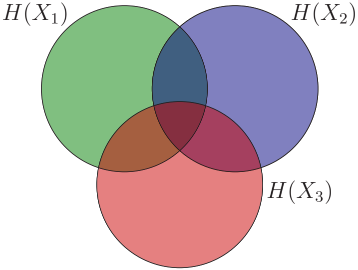
$$H(X^n) = H(X^{t_1}) + H(X^{t_2}) + \cdots + H(X^{t_n})$$
$$P_{X^{t_j}} = P_{X^{t_1}} \quad \forall j \leq n$$



Three Correlated Sources

In general, when three variables are correlated, we have

$$H(X_1|X_2X_3) \neq H(X_1|X_2)$$

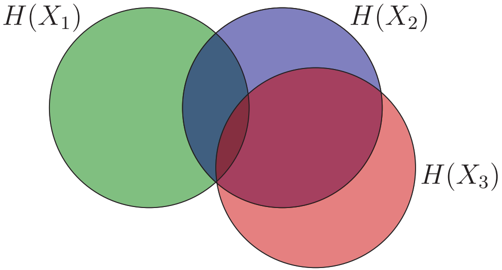


$$P_{X_1X_2X_3} = P_{X_1X_2}P_{X_3|X_1X_2}$$

Three Correlated Sources

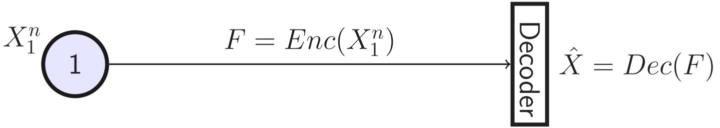
If Markov relation $X_1 - X_2 - X_3$ holds,

$$H(X_1|X_2X_3) = H(X_1|X_2)$$



$$P_{X_1X_2X_3} = P_{X_1X_2}P_{X_3|X_2}$$

- Source Coding (Compression)

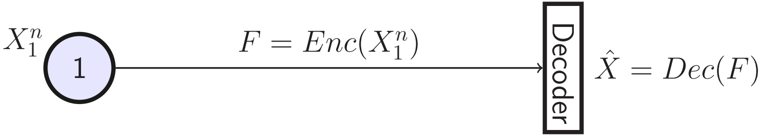


Objectives:
1) $\hat{X} = X$
2) length(F) be as small as possible.

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

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

Background - Information theory



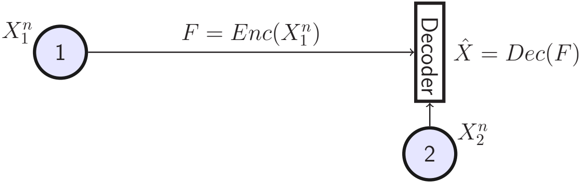
Source Coding Theorem: If P_{X_1} is known, for any rate

$$R_1 \geq H(X_1)$$

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

Shannon, 1948

Background - Information theory



Source Coding with Side Information at the Decoder: If $P_{X_1X_2}$ is known, for any rate

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

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

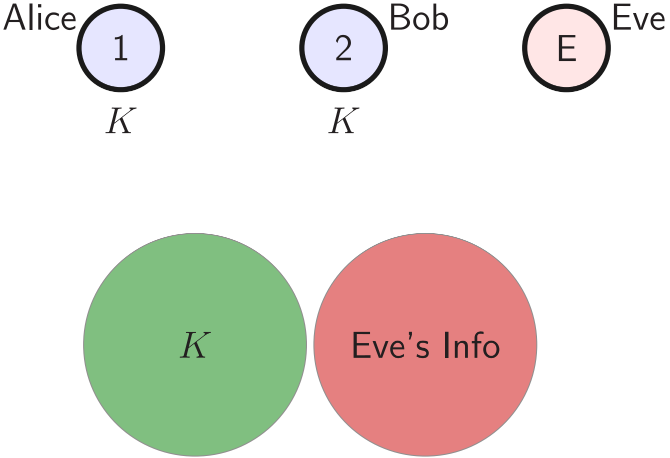
Slepian and Wolf, 1973

Part II

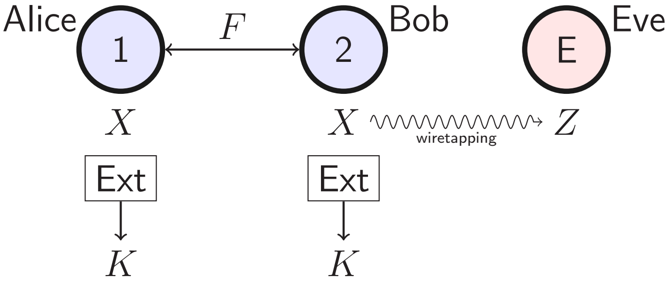
Two-party SKA

Information-theoretic key agreement

- **Key Agreement**

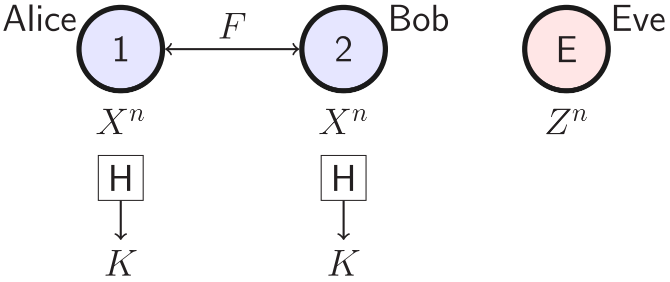


- **Key Extraction from Common Randomness (Privacy Amplification)**



Objectives: $\begin{cases} 1)\ I(K;(Z,F)) = 0 \\ 2)\ \text{length}(K) \text{ be as **large** as possible.} \end{cases}$

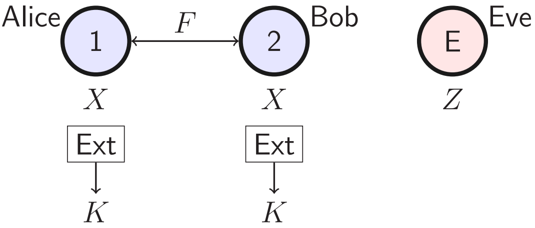
- **Key Extraction from Common Randomness**



An extraction code H has:

Extraction rate	$r_n^{ext}(\mathsf{H}) = \frac{\text{length}(K)}{n}$
Leakage	$I(K;(Z^n,F)) \leq \sigma_n$

Information-theoretic key agreement



Leftover Hash Lemma (LHL) (Asymptotic)
Let $R_{\min}$ be a lower bound on communication rate (length$(F)/n$). Then, for any rate

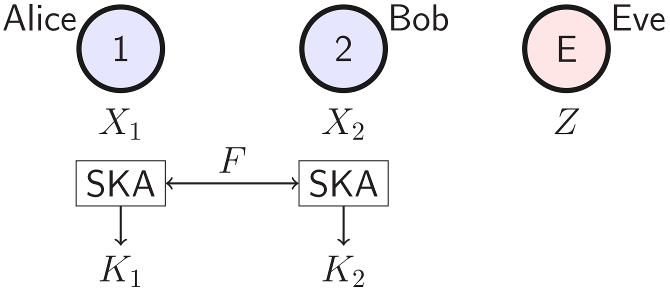
$$R^{ext} \leq H(X|Z) - R_{\min}$$

there is always exists an extraction code with asymptotic rate of R^{ext} ($r_n^{ext} \to R^{ext}$) with negligible information leakage ($\sigma_n \to 0$).

Dodis, et. al, 2008

Two-Party SKA against a wiretapper

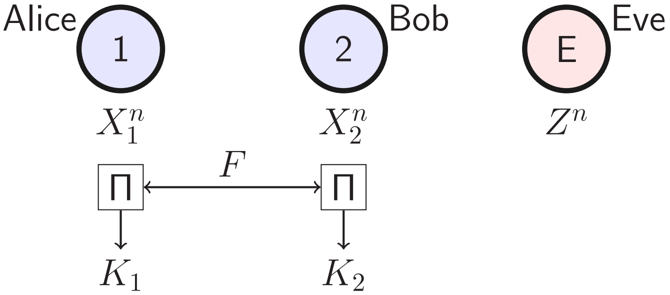
- **Secret Key Agreement (SKA)**



Objectives:
1) $K_1 = K_2 = K$
2) $I(K; (Z, F)) = 0$
3) length(K) be as **large** as possible.

Two-Party SKA against a wiretapper

- **Secret Key Agreement (SKA)**



A SKA protocol Π has:

Key rate	$r_n^{key}(\Pi) = \frac{\text{length}(K)}{n}$
Error probability	$\Pr\{K_1 \neq K_2\} \leq \epsilon_n$
Leakage	$I(K;(Z^n, F)) \leq \sigma_n$

Two-Party SKA against a wiretapper

- A SKA protocol **achieves** key rate R^{key} if as $n \to \infty$

$$r_n^{key} \to R^{key}$$
$$\epsilon_n \to 0$$
$$\sigma_n \to 0$$

- A key rate R^{key} is **achievable** if there exists a SKA protocol that achieves R^{key}.

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

Problem Statement: For a given source model (X_1, X_2, Z) with known distribution $P_{X_1X_2Z}$, what is the WSK capacity.

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

The PK Capacity

Definition: The private key (PK) capacity is the largest achievable key rate when parties know Eve's side information Z.

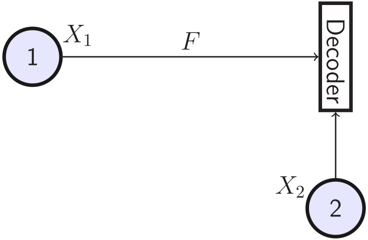
Lemma: By definition, PK capacity is an upper bound on WSK capacity.

$$C_{WSK}(X_1, X_2|Z) \leq C_{PK}(X_1, X_2|Z)$$

Let's find PK capacity $C_{PK}(X_1, X_2|Z) = ?$

Review

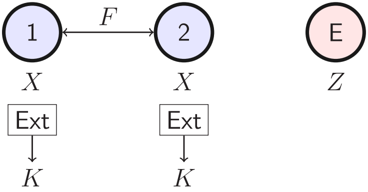
Source Coding with Side Info



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

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

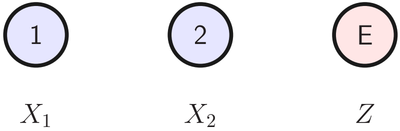
Leftover Hash Lemma (LHL)



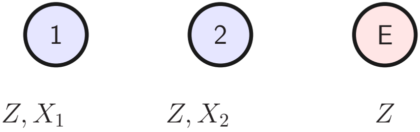
$$\frac{\text{length}(F)}{n} \geq R_{\min}$$

$$R^{ext} \leq H(X|Z) - R_{\min}$$

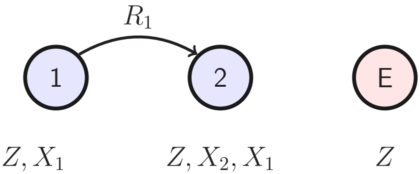
Achieving PK Capacity



Achieving PK Capacity

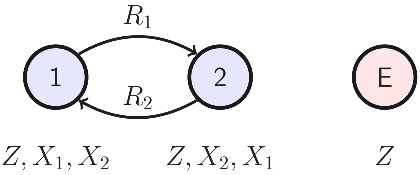


Achieving PK Capacity



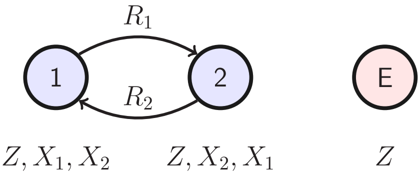
$$R_1 \geq H(X_1|X_2Z)$$

Achieving PK Capacity



$$R_1 \geq H(X_1|X_2 Z)$$
$$R_2 \geq H(X_2|X_1 Z)$$

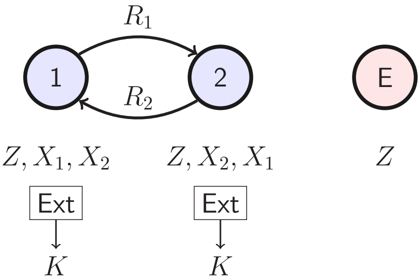
Achieving PK Capacity



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

$$\frac{\text{length}(F)}{n} \geq R_{\min} = \min\{R_1 + R_2\}$$
$$R_{\min} = H(X_1|X_2Z) + H(X_2|X_1Z)$$

Achieving PK Capacity

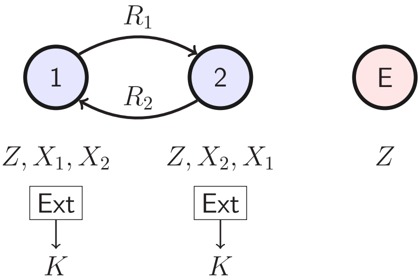


$$R_1 \geq H(X_1|X_2Z)$$
$$R_2 \geq H(X_2|X_1Z)$$

$$\frac{\text{length}(F)}{n} \geq R_{\min} = \min\{R_1 + R_2\}$$
$$R_{\min} = H(X_1|X_2Z) + H(X_2|X_1Z)$$

(X_1, X_2, Z) is a common randomness

Achieving PK Capacity



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

$$\frac{\text{length}(F)}{n} \geq R_{\min} = \min\{R_1 + R_2\}$$
$$R_{\min} = H(X_1|X_2Z) + H(X_2|X_1Z)$$

(X_1, X_2, Z) is a common randomness

By LHL, the following key rate is achievable

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

Thus

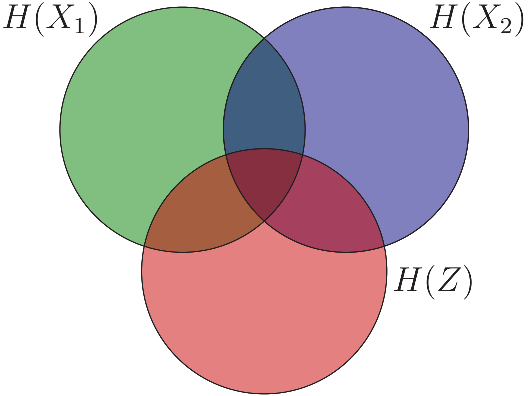
$$r^{key}_{\max} = H(X_1, X_2|Z) - H(X_1|X_2Z) - H(X_2|X_1Z)$$

Is $r^{key}_{\max}$ equal to C_{PK}?

PK Capacity

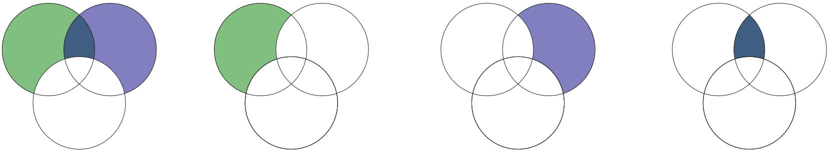
Yes! $C_{PK}(X_1, X_2|Z) = H(X_1, X_2|Z) - H(X_1|X_2 Z) - H(X_2|X_1 Z)$

Is there a simpler expression?



PK Capacity

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



$$H(X_1, X_2|Z) \quad - \quad H(X_1|X_2Z) \quad - \quad H(X_2|X_1Z) \quad = \quad I(X_1; X_2|Z)$$

Thus

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

WSK Capacity

A General Upper Bound on WSK Capacity

Theorem: $C_{WSK}(X_1, X_2|Z) \leq I(X_1; X_2|Z)$

Proof: $C_{PK}(X_1, X_2|Z) = I(X_1; X_2|Z)$
$C_{WSK}(X_1, X_2|Z) \leq C_{PK}(X_1, X_2|Z)$. □

General wiretapped model under restrictions

Theorem: If $X_1 - X_2 - Z$ (i.e., $P_{X_1 X_2 Z} = P_{X_1 X_2} P_{Z|X_2}$)
then $C_{WSK}(X_1, X_2|Z) = I(X_1; X_2|Z)$.

Ahlswede and Csiszár, 1993

Maurer, 1993

Question: Can we generalize the two-party source model to a multi-party model?

Answer: Yes!

But first, let us introduce **omniscience**.

Recall:

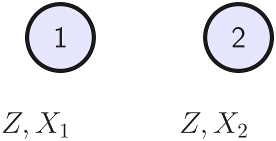
$$C_{PK}(X_1, X_2|Z) = H(X_1, X_2|Z) - R_{\min}$$

where

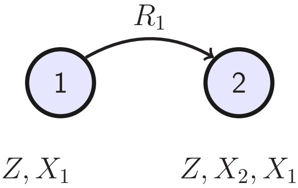
$$R_{\min} = H(X_1|X_2Z) + H(X_2|X_1Z)$$

What is a practical interpretation of $R_{\min}$?

Communication for Omniscience (CO)

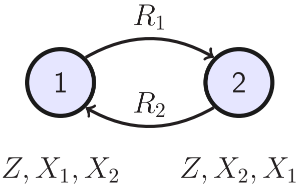


Communication for Omniscience (CO)



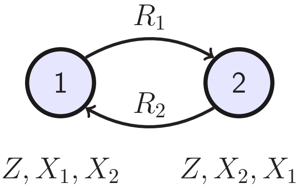
$$R_1 \geq H(X_1|X_2Z)$$

Communication for Omniscience (CO)



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

Communication for Omniscience (CO)



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

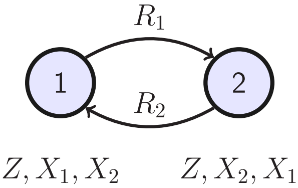
Definition: $R_{CO}(X_1, X_2|Z)$ is the min of total communication rate for achieving omniscience when party 1 knows X_1, party 2 knows X_2, given that both parties also know Z.

$$R_{\min} = R_{CO}(X_1, X_2|Z)$$

and

$$R_{CO} = H(X_1|X_2Z) + H(X_2|X_1Z)$$

Communication for Omniscience (CO)



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

Definition: $R_{CO}(X_1, X_2|Z)$ is the min of total communication rate for achieving omniscience when party 1 knows X_1, party 2 knows X_2, given that both parties also know Z.

$$R_{\min} = R_{CO}(X_1, X_2|Z)$$

and

$$R_{CO} = H(X_1|X_2Z) + H(X_2|X_1Z)$$

Thus,

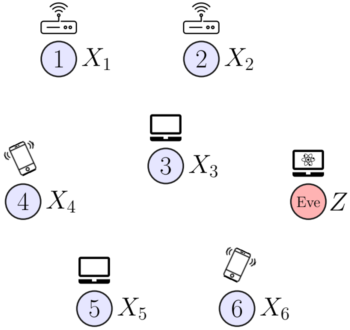
$$C_{PK}(X_1, X_2|Z) = H(X_1, X_2|Z) - R_{CO}(X_1, X_2|Z)$$

Part III

Multiterminal SKA

Multiterminal SKA

- Set of m terminals.
- E.g. $\mathcal{M} = \{1, 2, 3, 4, 5, 6\}$
- Each terminal j has RV X_j
- Eve has unlimited computation power
- and side information Z
- We know $P_{X_{\mathcal{M}} Z}$



$$X_{\mathcal{M}} = (X_1, X_2, \ldots, X_6)$$

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

Csiszár and Narayan, 2004

Multiterminal SKA

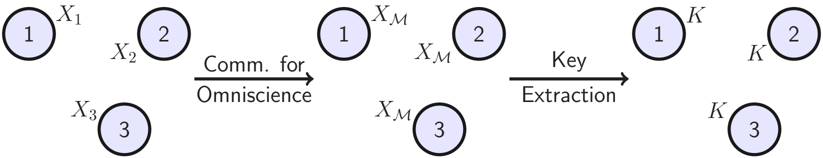
An immediate corollary: **Multiterminal SK Capacity**

When Eve is not wiretapping – there is no Z.

$$C_{SK}(X_{\mathcal{M}}) = H(X_{\mathcal{M}}) - R_{CO}(X_{\mathcal{M}})$$

Achieving Multiterminal SK Capacity:

Step 1) Communication for omniscience
Step 2) Key extraction from common randomness $X_{\mathcal{M}}$



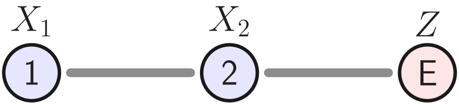
The WSK Capacity

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

WSK Capacity

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

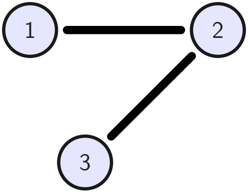
$$C_{WSK}(X_1, X_2|Z) = I(X_1, X_2|Z)$$



Can we extend this model to a multiterminal version?

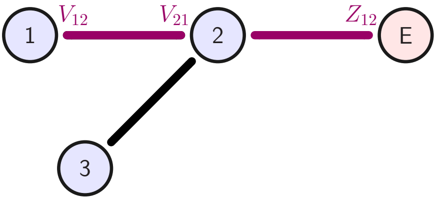
Example:

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



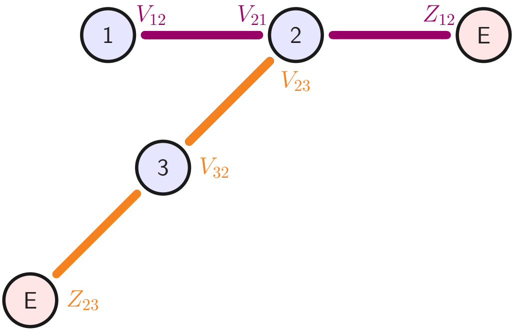
Example:

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



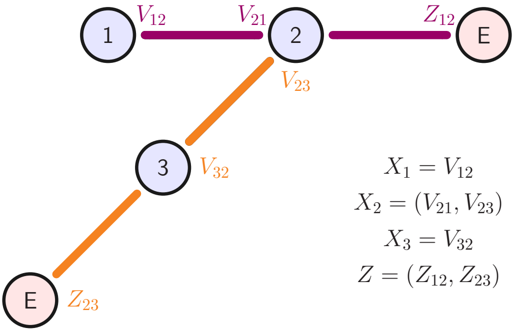
Example:

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



Example:

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



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

Wiretapped Tree-PIN

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

For any wiretapped Tree-PIN, the WSK capacity is

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

WSK Capacity of Tree-PIN

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

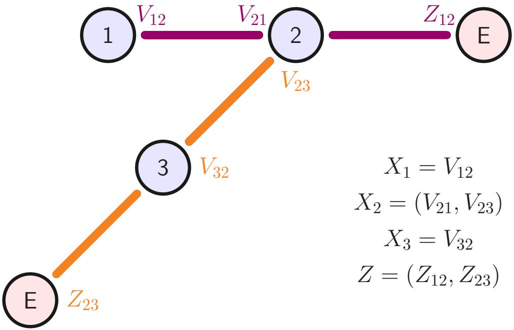
$$C_{WSK}(X_{\mathcal{M}}|Z) \leq \min_{i,j} I(V_{ij}; V_{ji}|Z_{ij}).$$

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

Achieving WSK capacity

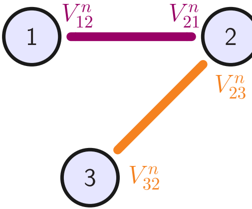
Example:

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

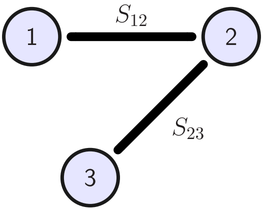


$$X_1 = V_{12}$$
$$X_2 = (V_{21}, V_{23})$$
$$X_3 = V_{32}$$
$$Z = (Z_{12}, Z_{23})$$

Achieving WSK capacity



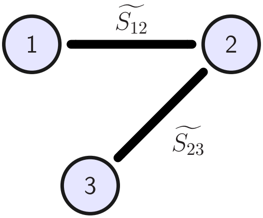
Achieving WSK capacity



Steps:

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

Achieving WSK capacity



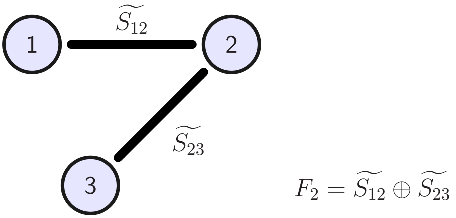
$\widetilde{S_{ij}} = S_{ij}|_\lambda$

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



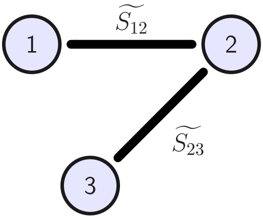
Steps:

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

Achieving WSK capacity



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

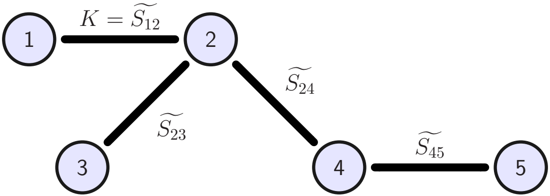
Steps:

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

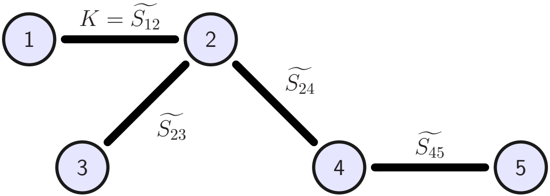
$$\lambda = \min\{\text{length}(S_{ij})\} \approx n \times \min I(V_{ij}; V_{ji}|Z_{ij})$$

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

Another Example



Another Example

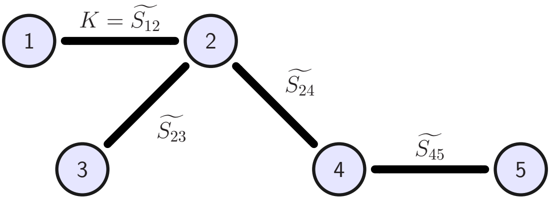


Public Broadcast Communication:

$$F_2 = (F_{23}, F_{24}) = (\widetilde{S_{12}} \oplus \widetilde{S_{24}}\ ,\ \widetilde{S_{12}} \oplus \widetilde{S_{23}})$$

$$F_4 = \widetilde{S_{24}} \oplus \widetilde{S_{45}}$$

Another Example



Public Broadcast Communication:

$$F_2 = (F_{23}, F_{24}) = (\widetilde{S_{12}} \oplus \widetilde{S_{24}}\ ,\ \widetilde{S_{12}} \oplus \widetilde{S_{23}})$$
$$F_4 = \widetilde{S_{24}} \oplus \widetilde{S_{45}}$$

Key Calculation:

$$K = \widetilde{S_{12}}$$
$$K_5 = \widetilde{S_{45}} \oplus F_4 \oplus F_{24} = \widetilde{S_{12}} = K$$

Wiretapped PIN

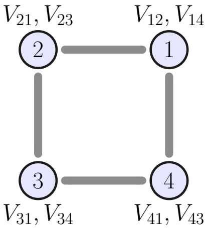
Wiretapped Pairwise Independent Network (PIN)

- 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

For any wiretapped PIN, the WSK capacity is

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

Example - Steiner tree packing



$V_{12} - V_{21} - Z_{12}$

$V_{23} - V_{32} - Z_{23}$

$V_{34} - V_{43} - Z_{34}$

$V_{41} - V_{14} - Z_{41}$

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

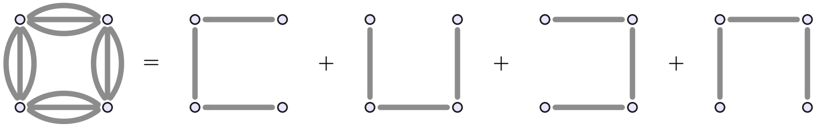
$$C_{WSK}(X_{\mathcal{M}}|Z) = \frac{2}{3}$$

Achieving WSK Capacity by Steiner tree packing

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

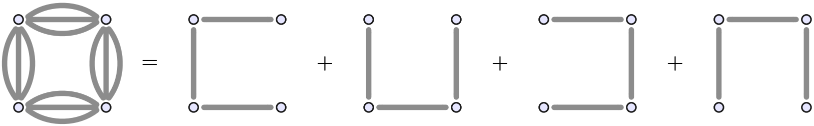
Achieving WSK Capacity by Steiner tree packing

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



Achieving WSK Capacity by Steiner tree packing

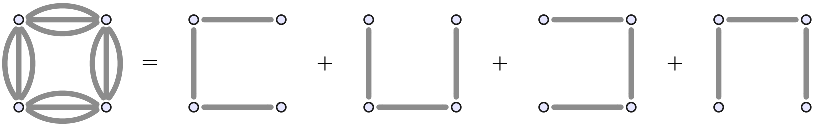
$$n = 6\nu \quad \text{and} \quad \lambda = \text{length}(S_{ij}) = 3\nu - \epsilon$$



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

Achieving WSK Capacity by Steiner tree packing

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



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

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

Other research directions:

- Key agreement for a subset $\mathcal{A} \subseteq \mathcal{M}$
  - WSK Capacity of Tree-PIN is proved
  - WSK Capacity of PIN remains open
- Channel models vs. Source models
- Finite blocklength analysis
- Communication complexity vs. Communication for Omniscience
- SKA under communication limitation
- Efficient SKA protocols with low implementation complexity $\mathcal{O}(n)$

Main References:

[1] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," IEEE Transactions on Information Theory, vol. 19, no. 4, pp. 471480, Jul. 1973.

[2] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," SIAM Journal on Computing, vol. 38, no. 1, pp. 97139, Jan. 2008.

[3] U. M. Maurer, "Secret key agreement by public discussion from common information," IEEE Transactions on Information Theory, vol. 39, no. 3, pp. 733742, May 1993.

[4] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. Secret sharing," IEEE Transactions on Information Theory, vol. 39, no. 4, pp. 11211132, Jul. 1993.

[5] I. Csiszár and P. Narayan, "Secrecy Capacities for Multiple Terminals," IEEE Transactions on Information Theory, vol. 50, no. 12, pp. 30473061, Dec. 2004.

[6] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik, "Secret Key Generation for a Pairwise Independent Network Model," IEEE Transactions on Information Theory, vol. 56, no. 12, pp. 64826489, Dec. 2010.

[7] A. Poostindouz and R. Safavi-Naini, "Wiretap Secret Key Capacity of Tree-PIN," in 2019 IEEE International Symposium on Information Theory (ISIT), 2019, pp. 315319.

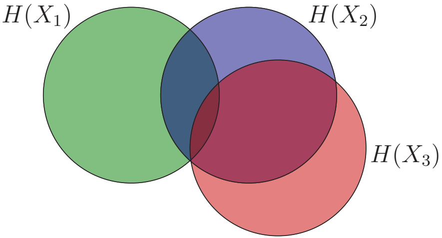
Thank You!

WSK Capacity

General wiretapped model under restrictions

Theorem: If $X_1 - X_2 - Z$ (i.e., $P_{X_1 X_2 Z} = P_{X_1 X_2} P_{Z|X_2}$) then $C_{WSK}(X_1, X_2|Z) = I(X_1; X_2|Z)$.

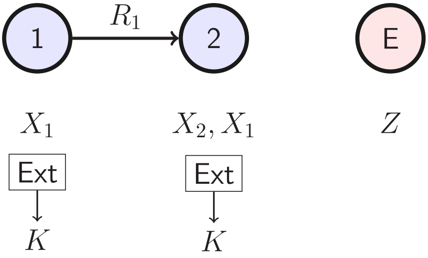
Three Correlated Sources



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

$$P_{X_1 X_2 Z} = P_{X_1 X_2} P_{Z|X_2}$$
$$H(X_1|X_2 Z) = H(X_1|X_2)$$
$$I(X_1; X_2|Z) = H(X_1|Z) - H(X_1|X_2)$$

Achieving PK Capacity



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

$$\frac{\text{length}(F)}{n} \geq R_{\min} = \min\{R_1\}$$

$$R_{\min} = H(X_1|X_2)$$

(X_1) is a common randomness

By LHL, the following key rate is achievable

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

Thus

$$r^{key}_{\max} = H(X_1|Z) - H(X_1|X_2)$$

$r^{key}_{\max}$ is equal to

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