Multi-Key Generation over a Cellular Model with a Helper

By:

Chaganti Revanth Chowdary (Q929B649)

Pakalapati Sri Lakshmi Prasanna Kumar (W845T858)

Mengani Ajay Kumar(Y955T859)

ABSTRACT

The project throws some light on the issue generating multiple keys for a cellular source model with a helper simultaneously. The model proposed consists of four terminals, X0, X1, X2, and X3, each of them observes one component of a vector source. Terminal X0 tries to generate two secret keys K1 and K2 respectively with terminals X1 and X2 with the help of terminal X3. All terminals are allowed to communicate over a public channel. An eavesdropper is assumed to have access to the public discussion. Both symmetric and asymmetric key generations are considered in implementing the proposed model.

INTRODUCTION

- Security is a prominent issue in means of remote communications. These days secure remote data exchange depends basically on encryption.
- The most common way of encoding data is by generating secret key.
- Since all terminals are allowed to communicate over a public channel, an eavesdropper is assumed to have access to the public discussion.
- As generating secret key is considered it can be done in both symmetric and asymmetric way.

There are number of different criteria that should be considered in estimating the value of a proposed secrecy system. Some of them are:

1. **Amount of Secrecy.**
2. **Size of Key.**
3. **Expansion of Message.**

Security attacks from unknown:

1. **Ciphertext-just Attacks**
2. **Known-plaintext Attacks**
3. **Picked/Chosen plaintext Attacks**

Referred from: Communication Theory of Secrecy Systems By C. E. SHANNON

HELPER

The introduction of the helper is motivated by the role played by a “third party” which facilitates the generation of secret key by user terminals by furnishing them additional correlated information

Also, the idea of a helper has potential significance for practical schemes for the generation of secret key by three or more user terminals, wherein the different users can take turns serving as helper in successive rounds of generation of secret key.

Referred from:

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 46, NO. 2, MARCH 2000 Common Randomness and Secret Key Generation with a Helper Imre Csiszár, Fellow, IEEE, and Prakash Narayan, Senior Member, IEEE

- In symmetric key generation, model 1a with a trusted helper requires that the two keys are hidden from the eavesdropper.
- In symmetric key generation, model 1b with an untrusted helper further requires that the two keys are hidden from the helper in addition to the eavesdropper.
- The asymmetric key generation models 2a and 2b are same as symmetric key generation models 1a and 1b, respectively, except that the key K2 is further required to be hidden from terminal X1.
- For all models studied, the key capacity region is established by designing a unified achievable strategy to achieve the cut-set outer bounds.

WEAK POINTS (LIMITS OF PREVIOUS RESEARCH)

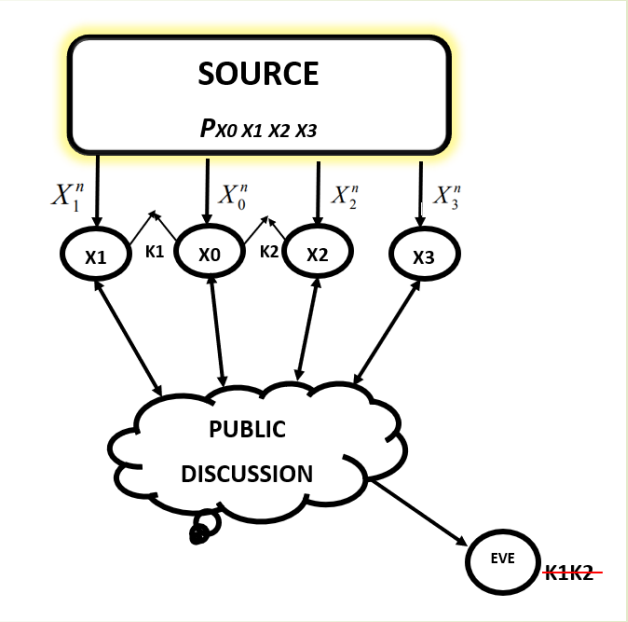
- Although the key capacity region for the three-terminal model was shown to be equal to the cut-set bound, it is not clear at the outset whether the cut-set bound can still be achieved for models with different secrecy requirements and for four-terminal models with an additional helper.
- For the three-terminal model, there are three cuts for generating two keys, and schemes can be designed to achieve corner points of the cut-set bound for each case of the source distribution.
- However, for four-terminal models with a helper, there are six cuts for generating two keys, and these six cuts yield eight possible cases of the cut-set bound due to different source distributions. It is not clear whether there exists a unified design of schemes to achieve the cut-set bound for all cases.

STRONG POINTS(NEW ABOUT THE RESULTS)

- Something new is implemented to overcome the issues in establishing key capacity regions for four source models of generating a pair of secret keys which was never done by anyone before.
- The results provide 2 affirmative answers to both of the limits that are observed.
- For all the four models, the cut-set bound is established to be the key capacity region by showing that the cut-set bound is indeed achievable.
- Derivation of the Slepian-Wolf conditions is done in this project that guarantee correct key agreement which derive sufficient conditions that guarantee the secrecy requirements

Model 1A:Symmetric key generation with a trusted helper

- The project consists of four different models, and in all models the base station terminal X0 wishes to agree on keys K1 and K2 with mobile terminals X1 and X2, respectively, under the help of terminal X3. The models differentiate from each other due to secrecy requirements.
- Models 1a address symmetric key generation, in which secrecy requirements for two keys are the same.
- Model 1a (with a trusted helper) requires that the two keys are hidden from the eavesdropper.



For symmetric key generation with a trusted helper, K1 and K2 are required to respectively satisfy the secrecy condition:

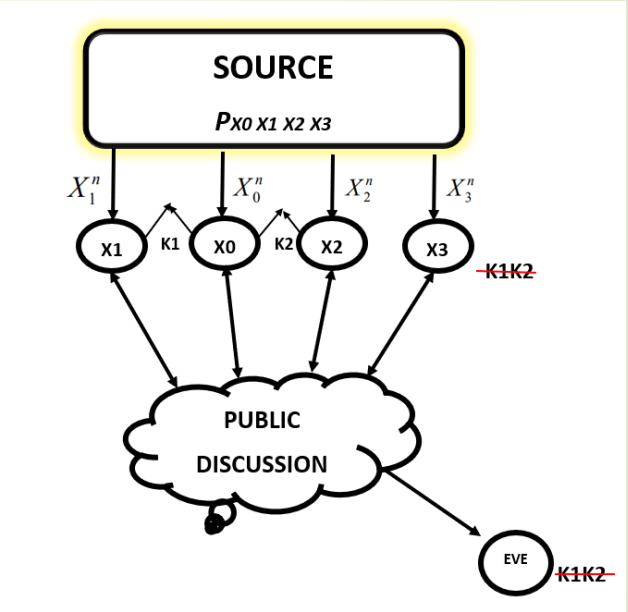
$$1/n\ I(K1K2; F) < \varepsilon$$

Model 1B: Symmetric key generation with an untrusted helper

- Models 1B address symmetric key generation, in which secrecy requirements for two keys are the same.
- Model 1B with an untrusted helper requires that the two keys are hidden from the eavesdropper
- Further it requires that the two keys are hidden from terminal X3 in addition to the eavesdropper.
- In the case of untrusted helper, we assume that the helper is curious but honest. The helper attempts to infer the information about the generated keys but still follows the protocol.

For asymmetric key generation with a untrusted helper, K1 and K2 are required to respectively satisfy the secrecy condition:

1/n I(K1K2; X3^nF) < ε



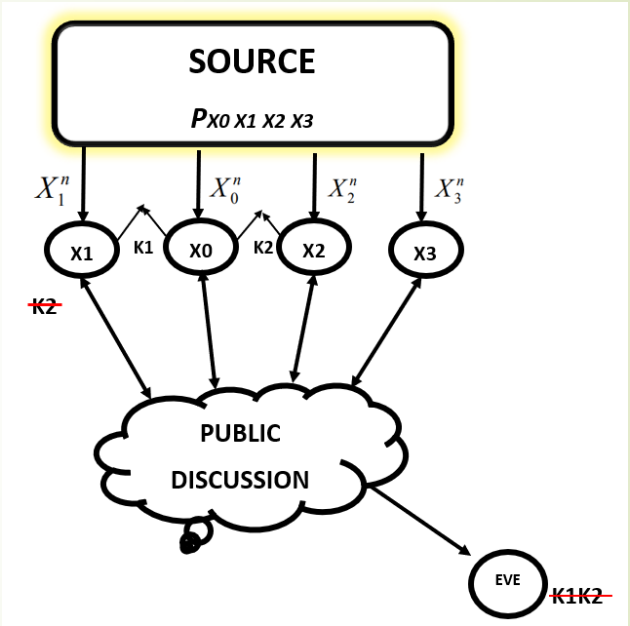
Model 2A: Asymmetric key generation with a trusted helper

- Models 2a with a trusted helper have the same secrecy requirements for the two keys as models 1a and 1b, respectively, in addition to that the key K2 is further required to be hidden from terminal X1.
- Thus, models 2a address asymmetric key generation.

❖ For asymmetric key generation with a trusted helper, K1 and K2 are required to respectively satisfy the secrecy conditions:

$$1/n\ I(K1; F) < \varepsilon\ ,$$

$$1/n\ I(K2;F,X1^n) < \varepsilon$$



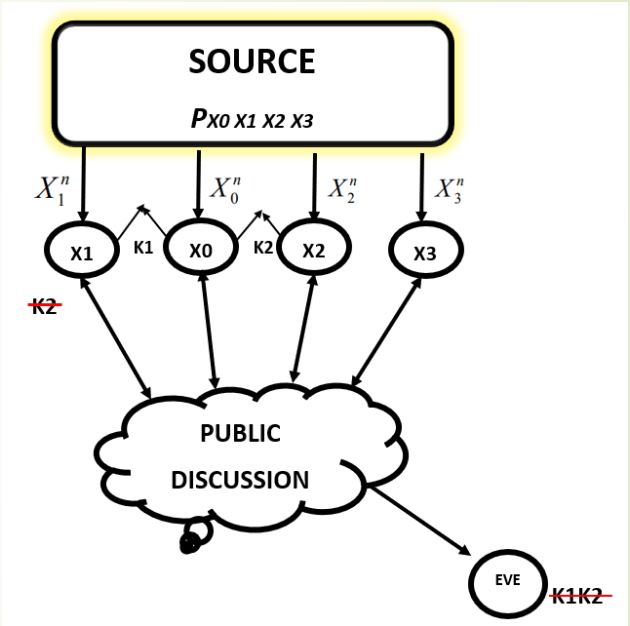
Model 2B: Asymmetric key generation with an untrusted helper

- Models 2B with an untrusted helper have the requirement that the two keys are hidden from terminal X3 in addition to the eavesdropper.
- In addition to that the key K2 is further required to be hidden from terminal X1.

❖ For asymmetric key generation with an untrusted helper, K1 and K2 are required to respectively satisfy the secrecy conditions:

$$1/n\ I(K1;\ F,X3^n) < \varepsilon\ ,$$

$$1/n\ I(K2;F,X1^n,X3^n) < \varepsilon$$



SYMETRIC GENERATION WITH UNTRUSTED HELPER

- How to share keys among 4 terminals is a challenging problem in Shannon's secrecy system.
- Towards this end, the paper showed that public discussion can promote key sharing between two remote terminals with correlated observations.
- Here we explain the problem of symmetric key generation with an untrusted helper, in which the two generated keys are required to be secure from both the eavesdropper and the helper terminal X3.

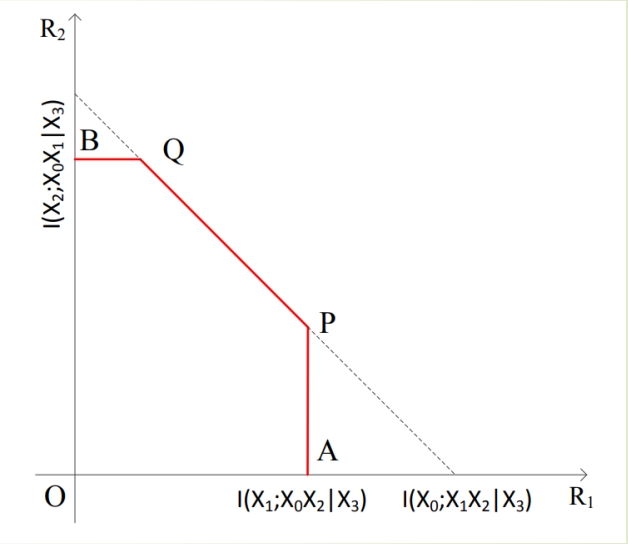
- The key capacity region for symmetric key generation with an untrusted helper contains rate pairs (R1, R2) which satisfies the following inequalities:

  $R1 < I(X1; X0X2|X3)$, (1)

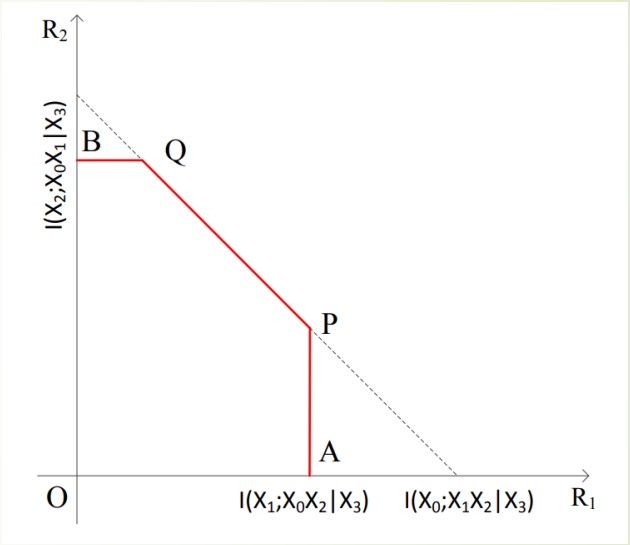
  $R2 < I(X2; X0X1|X3)$, (2)

  $R1 + R2 < I(X0; X1X2|X3)$. (3)

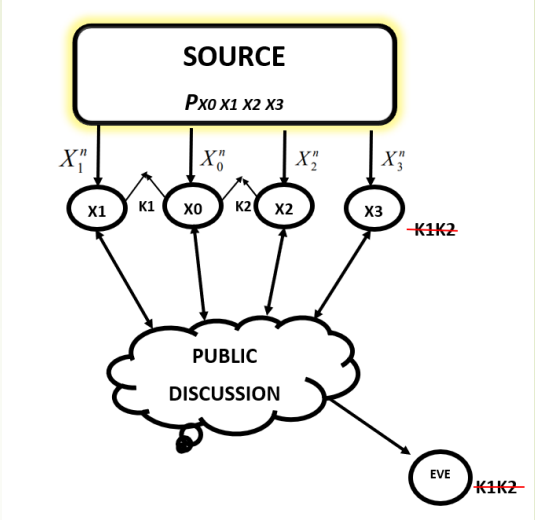
- As we can see, the upper bound on R1 in (1) is due to the cut separating X0 and X1 terminals for generating secret key K1 (one more bound due to the other cut separating X0 and X1 is redundant due to the sum rate bound (3)).

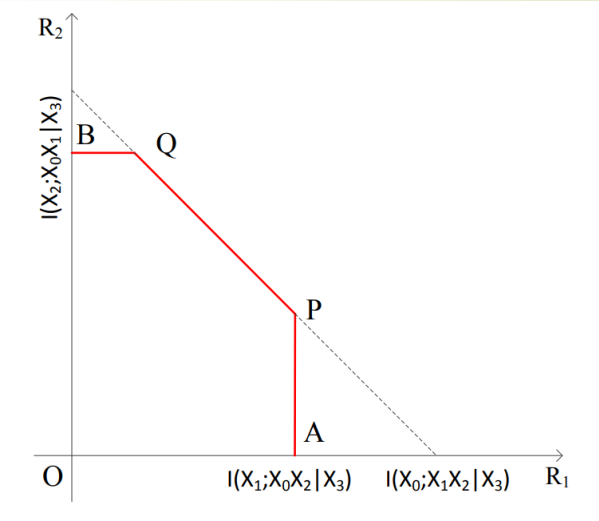


- The upper bound on R2 in (2) is due to the cut separating X0 and X2 terminals for generating secret key K2 (one more bound due to the other cut separating X0 and X1 is redundant due to the sum rate bound (3)).
- The sum rate bound (3) is due to the cut separating X0 and (X1, X2) for generating two keys K1 and K2 simultaneously.
- All the bounds (1) to (3) are conditioned on X3 because both K1 and K2 are required to be secure from terminal X3.
- This is reasonable because additional requirement for the keys needs to be hidden from the helper as the helper is untrusted.



- The structure of the key capacity region is shown in the figure as the pentagon O-A-P-Q-B-O.
- In order to make sure the achievability of the region, by symmetry, it is sufficient to show the achievability of the point P in the figure.
- The idea to achieve the point P follows the unified strategy in which public discussion first guarantees that terminal X0 recovers Xn1, Xn2 and Xn3 correctly.
- Then K1 is generated by terminals X0 and X1 based on Xn1and K2 is generated by terminals X0 and X2 based on Xn2.
- Since the generated keys should be hidden from the helper terminal X3, Xn 3 cannot be used as random resource for generating the keys.
- The helper can still participate in the public discussion to assist the recovery of source sequences.





- Since the rate of K1 needs to be maximized, terminal X1 should reveal as little information as possible.
- In addition to it, terminals X2 and X3 first reveal information at the rate

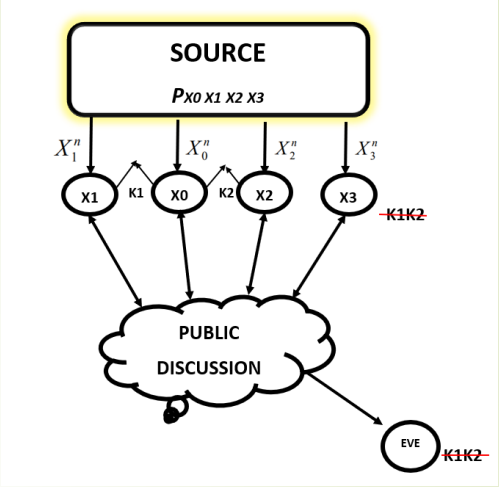
$$\tilde{R}_2 + \tilde{R}_3 = H(X_2X_3|X_0)$$

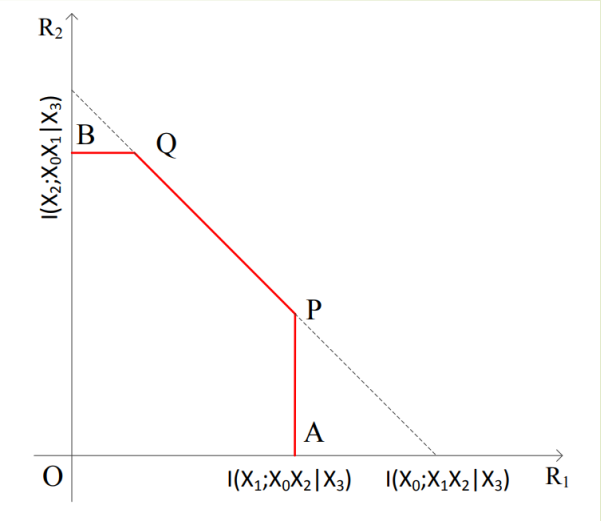
so that terminal X1 needs to release only at

the rate $\tilde{R}_1 = H(X_1|X_0X_2X_3)$

in order to X0 to recover Xn1.

- Since X3 is an untrusted helper, it can reveal information at any rate.
- So,R2 can be set to be H(X2|X0X3).
- Since the generation of K1 already uses up information contained in Xn1, K2 can be generated only based on information contained in Xn2 given Xn1 and Xn3 .





PROOF OF THE THEOREM

There are different factors to be considered in order to prove that the findings are done. They are as follows:

Proof of Converse.

- Let's say if we want to generate secret key K1, the model proposed reduces to the private key generation problem.
- The key capacity is shown as

$$R1 = \min\{I(X1; X0X2|X3), I(X0; X1X2|X3)\},$$

which provides an outer bound on R1 which can be shown as

$$R1 < I(X1; X0X2|X3).$$

- Let's say if we want to generate secret key K2, the key capacity is shown to be $R2 = \min\{I(X2; X0X1|X3), I(X0; X1X2|X3)\}$, which provides an outer bound on R2 which can be shown as

$$R2 < I(X2; X0X1|X3).$$

- For the sum rate bound, if we consider an enhanced model by replacing terminals X1 and X2 with a super terminal Xs which observes both Xn1 and Xn2.
- The rate of the private key between X0 and Xs concealed from terminal X3 is upper bounded by I(X0; X1, X2|X3), which yields the sum rate bound that can be shown as

$$R1 + R2 < I(X0; X1X2|X3).$$

Proof of Achievability:

- The key capacity region is the pentagon O-A-P-Q-B-O where the coordinates of the points A and B are given by $\min\{I(X1; X0X2|X3), I(X0; X1X2|X3)\}$ and $\min\{I(X2; X0X1|X3), I(X0; X1X2|X3)\}$, respectively.
- The corner point A can be achieved by letting X2 be a dedicated helper in order to generate secret key K1.
- The corner point B can be achieved by letting X1 be a dedicated helper to generate K2 .
- We note that the point P would collapse to the point A

  if $I(X0; X1X2|X3) \leq I(X1; X0X2|X3)$.
- The point Q would collapse to the point B

  if $I(X0; X1X2|X3) \leq I(X2; X0X1|X3)$.
- Thus, it is sufficient to show that the corner points P and Q are achievable whenever they are different from the points A and B, respectively.

- We note that since the secrecy requirements on K1 and K2 are symmetric, it is sufficient to show that the corner point P is achievable, and then the achievability of the point Q follows by symmetry.
- Furthermore, we assume that

$$I(X1; X0X2|X3) < I(X0; X1X2|X3),$$

which implies

$$H(X2|X0X3) < H(X2|X1X3),$$

because otherwise the point P would collapse to the point A

and has been justified to be achievable.

- To mention particularly, Slepian-Wolf conditions also guarantee the correct key establishment.

PROOF OF SECRECY

The key leakage rates averaged over the random codebook ensemble is evaluated. Let $f := f(X^n_1)$, $g := g(X^n_2)$ and $l := l(X^n_3)$. Then it is clear that $F = \{f, g, l\}$. We further let $\varphi := \varphi(X^n_1)$ and $\psi := \psi(X^n_2)$. Hence, $K1 = \varphi$ and $K2 = \psi$. Firstly

$$I(K1, K2; X^n_3, F|C)$$

$$= I(\varphi, \psi; f, g, l, X^n_3 |C)$$

$$= I(\varphi; f, g, X^n_3 |C) + I(\psi; f, g, X^n_3 |\varphi, C)$$

$$\leq I(\varphi; f|C) + I(\varphi, f; g, X^n_3 |C) + I(\psi; \varphi, f, g, X^n_3|C)$$

$$\leq I(\varphi; f|C) + I(\varphi, f; g, X^n_3 |C) + I(\psi; g|C) + I(\psi, g; \varphi, f, X^n_3 |C)$$

$$\leq I(\varphi; f|C) + I(\varphi, f; X^n_3|C) + I(\varphi, f; g| X^n_3, C) + I(\psi; g|C)$$

$$+ I(\psi, g; X^n_3|C) + I(\psi, g; \varphi, f| X^n_3, C) \quad \text{-----(1)}$$

We consider each of the six terms in (1). it can be shown that if

$$\tilde{R} 1 + R1 < H(X1) - 2\delta(\mathcal{E}), \text{ ----------(2)}$$

then $1/n\, I(\varphi; f|C) < \delta(\mathcal{E})$; ----------(3) and

if $\tilde{R} 2 + R2 < H(X2) - 2\delta(\mathcal{E})$, ----------(4)

then $1/n\, I(\psi; g|C) < \delta(\mathcal{E})$. ----------(5)

In order to bound the second term in (1), we have the following derivation:

$$
\begin{aligned}
&I(\varphi, f; X^n_3|C) \\
&\quad = I(X^n_1; X^n_3|C) - I(X^n_3; X^n_3|\varphi, f, C) \\
&\quad = H(X^n_1|C) - H(X^n_1| X^n_3, C) - H(X^n_1|\varphi, f, C) \\
&\qquad + H(X^n_1|\varphi, f, X^n_3, C) \\
&\quad \leq n[R\tilde{}\ 1 + R1 - H(X1|X3)] + H(X\ n\ 1\ |\varphi, f, X^n_3, C)
\end{aligned}
$$

if

$$R\tilde{}\ 1 + R1 \leq H(X1|X3) - 2\delta(\mathcal{E}), \text{ ----------(6)}$$

Then

$$\limsup n\to\infty\ 1/n\ H(X^n_1\ |\varphi, f, X^n_3, C) < H(X1|X3) - R\tilde{}\ 1 - R1 + \delta(\mathcal{E})\text{----(7)}$$

Consequently,

$$1/n\ I(\varphi, f; X^n_3\ |C) < \delta(\mathcal{E})\text{---------- (8)}$$

Similarly, it can be shown that if

$$R\tilde{}\ 2 + R2 \leq H(X2|X3) - 2\delta(\mathcal{E}), \text{ ----------(9)}$$

then

$$1/n\ I(\psi, g; X^n_3|C) < \delta(\mathcal{E})\text{---------- (10)}$$

By noting that $I(\varphi, f; g|\, X^n_3\,, C) \le I(\psi, g; \varphi, f|\, X^n_3\,, C)$, it is sufficient to bound the latter term:

$$
\begin{aligned}
& I(\psi, g; \varphi, f|\, X^n_3, C) \\
& \quad \le I(\psi, g; X^n_1|\, X^n_3, C) \\
& \quad = I(X^n_2\, X^n_1 \,|\, X^n_3, C) - I(X^n_2; X^n_1|g, \psi, X^n_3\,, C) \\
& \quad = H(X^n_2|\, X^n_3, C) - H(X^n_2|\, X^n_1\,, X^n_3, C) \\
& \qquad - H(X^n_2|g, \psi, X^n_3, C) + H(X^n_2|g, \psi, X^n_1, X^n_3, C) \\
& \le n[R\tilde{}\, 2 + R2 - H(X2|X1X3)] + H(X^n_2|g, \psi, X^n_1, X^n_3, C)
\end{aligned}
$$

if

$$R\tilde{}\, 2 + R2 < H(X2|X1X3) - 2\delta(\mathcal{E}),\text{-------- (11)}$$

then

$$
\begin{aligned}
& \limsup n\to\infty\ 1/\,n\, H(X^n_1\,|g, \psi, X^n_1\,, X^n_3, C) \\
& \qquad < H(X2|X1X3) - R\tilde{}\, 2 - R2 + \delta(\mathcal{E})
\end{aligned}
$$

Consequently,

$$1/n\ I(f, \varphi; g, \psi|\, X^n_3, C) < \delta(\mathcal{E})\ \text{----------(12)}$$

Thus, (6) and (12) are sufficient conditions that guarantee the secrecy requirement (5).

The rate pair at point P is given by (I(X1; X0X2|X3), H(X2|X1X3) − H(X2|X0X3)). To achieve this rate pair, we set the binning rates as follows:

$$R\tilde{}\ 1 = H(X1|X0X2X3) + Ɛ, \text{---------- (14)}$$

$$R1 = I(X1; X0X2|X3) - 2\delta(Ɛ) - 2\,Ɛ, \text{------(15)}$$

$$R\tilde{}\ 2 = H(X2|X0X3) + Ɛ, \text{----------(16)}$$

$$R2 = H(X2|X1X3) - H(X2|X0X3) - 2\delta(Ɛ) - 2, \text{-- (17)}$$

$$R\tilde{}\ 3 = H(X3|X0) + Ɛ \text{ ----------(18)}$$

It is easy to verify that the above rates satisfy the Slepian-Wolf conditions, and the sufficient conditions (6) and (12) for secrecy.

EXTENSION

- Internet of Things is one of the results of advancing network and telecommunications technology.
- This technology is expected to connect millions of home devices, vehicles, and industrial environments. It is conceivable that millions of devices will be equipped with various sensors and be connected to the internet through various heterogeneous networks.
- IoT, therefore, can be said as a system that allows the transfer of data between interconnected devices without human interaction.
- IoT infrastructure is connected to a communication network to collect and exchange information between devices.
- Referring to the basic character of wireless media, data aggregation through wireless communication is very vulnerable to eavesdropping.
- Using equipment like Raspberry PI 3 and making the terminals motionless with a distance between each of them secret key can be generated which can be hidden from eavesdropping.

CONCLUSION

- The problem of generating a pair of keys for a cellular source model with a helper is studied.
- We have established the full key capacity region for four models with different secrecy requirements.
- The models mentioned here consist of four terminals, which are more complicated to analyze than three-terminal models studied previously.
- Because the cut-set outer bound takes more cases due to different source distributions.
- Instead of designing a specific achievable scheme for each case one by one, a unified strategy has been developed, which achieves corner points for all cases, and hence significantly reduces the complexity of the achievability proof.