Multi-Key Generation over a Cellular Model with a Helper

A Project Report Submitted in partial fulfilment of
the requirements for the award of the degree of

Master of Science in Computer Science (M.S.C.S)

By

Pakalapati Sri Lakshmi Prasanna Kumar (WSU ID: W845T858)

Revanth Chowdary Chaganti (WSU ID: Q929B649)

Ajay Kumar Mengani (WSU ID: Y955T859)

Multi-Key Generation over a Cellular Model with a Helper

Abstract:

As a part of an investigation of issues including normal randomness at far off locations, creating a typical random key at four terminals without allowing a eavesdropper to acquire data about the key, is thought of in this project. In the model considered, there are four terminals, X0, X1, X2, and X3, every one of which notices one part of a vector source. Terminal X0 wishes to produce two mystery keys K1 and K2 individually with terminals X1 and X2 under the assistance of terminal X3. All terminals are permitted to impart over a public channel. A eavesdropper is expected to approach the public conversation. Both asymmetric and symmetric key production are thought of. In symmetric key production models, model 1a (with a confided in partner) necessitates that the two keys are hidden from the snoop, and model 1b (with an untrusted assistant) further necessitates that the two keys are hidden from the aide notwithstanding the eavesdropper. The generation of asymmetric key models 2a and 2b are equivalent to generation of symmetric key models 1a and 1b, separately, then again, actually the key K2 is additionally required to be covered from terminal X1. For all models considered, the key limit district is set up by planning a bound together attainable technique to accomplish the cut set external limits.

Table of Contents

List of figures

CHAPTER- 1:

Introduction:

Security is a prominent issue in remote communications. These days secure remote data exchange depends basically on encryption, the most common way of encoding data in such a way that main the beneficiary with the mysterious key can interpret it. It is broadly acknowledged that a cryptosystem ought to be secure as far as data hypothetical security, which originates from Shannon's perfect secrecy. Wonderful mystery is accomplished A secrecy framework is characterized conceptually as a bunch of changes of one space into a subsequent space. Every specific change of the set compares to enciphering with a specific key. The changes are assumed reversible non-particular) so special interpreting is conceivable when the key is known. Each key and accordingly every change is expected to have a deduced likelihood related with it—the likelihood of picking that key. Likewise every conceivable message is accepted to have a related deduced likelihood, dictated by the basic stochastic cycle.

These probabilities for the different keys and messages are really the foe cryptanalyst's deduced probabilities for the decisions being referred and address his deduced information of the circumstance. To utilize the framework a key is first chosen and shipped off the starting point. The decision of a key decides a specific change in the set framing the framework. Then, at that point, a message is chosen and the specific change relating to the chose key applied to this message to create a cryptogram. This cryptogram is communicated to the getting point by a channel furthermore, might be captured by the " eavesdropper." Whereas at the receiving end the opposite of the specific change is applied to the cryptogram to recuperate the unique message. On the off chance that the foe captures the cryptogram he can ascertain from it the deduced probabilities of the different potential messages and keys which may have delivered this cryptogram. This arrangement of deduced probabilities establishes his insight into the key and message after the capture attempt. "Information" is consequently related to a bunch of suggestions having related probabilities. The estimation of the deduced probabilities is the summed up issue of cryptanalysis.

Different Types of Eavesdropping Attacks:

Ciphertext-just Assault/Attacks: Eve (the Eavesdropper) is accepted to approach the ciphertext. The objective for Eve is to attempt the recovery of the secret key, the plaintext, or perhaps some incomplete data about the plaintext. This is the most vulnerable type of an assault/attack that we consider.

Known-plaintext Assault/Attacks: Eve (the Eavesdropper) knows the plaintext and the ciphertext. She attempts to recover the secret key. Then again, she may know a piece of the plaintext along with the full ciphertext, and she attempts to recover the part which is unknown of the plaintext (or just some halfway data about it). It ought to be noticed that a known-plaintext assault is a fundamental assault that all cryptographic natives ought to be safe against. For instance, Eve ought not have the option to recuperate the key from a known plaintext and the relating ciphertext. It is exceptionally normal the situation in genuine applications that a few information known to Eve is encoded. So, the known-plaintext assault isn't unreasonable in any way.

Picked/Chosen plaintext Assault/Attacks: Not just does Eve (the Eavesdropper) know the plaintext however she can pick it herself. She gets the comparing ciphertext. Her objective is to recuperate the secret key. As in the past, we can likewise consider an assault/attack when she picks a piece of the plaintext and attempts to recuperate another obscure piece of it. This assault/attack situation is obviously less practical contrasted with the assaults referenced previously. Notwithstanding, there are a few applications when this is likewise a practical assault/attack. One such model is when Eve is assaulting a crude executed in an ensured gadget (example smart card). She may approach the gadget furthermore, can give self-assertive info and notice the output.

Picked ciphertext Assault/Attacks: Eve (the Eavesdropper) is accepted to approach a decoding calculation and can take care of it with a discretionary ciphertext, noticing the plaintext which is corresponding. Once more Sometimes we people do think about likewise related-key assault/attack. Here plaintexts have been scrambled by distinctive keys that are practically indistinguishable (they might vary in just the slightest bit). Eve (the Eavesdropper) attempts to recuperate one of the keys. A significant situation in specific applications is the space of side channel assault/attack. Here Eve approaches a gadget performing encryption or unscrambling and gets extra data from side channels. This could be the means by which the gadget overwhelm power during its execution, the time it takes the devise to perform various activities, and so on Eve (the Eavesdropper) is assaulting the execution of a calculation and not simply the calculation. However, the outcomes of a execution rely a great deal upon the actual algorithm.

HELPER:

We concentrate on the issue of deciding the most extreme measure of generation of secret key which can be produced by separate terminals under indicated conditions and which might include secrecy necessities. The generation of secret key can be founded on randomness addressed by the results of corresponded sources accessible at the terminals (source-type models), or on randomness presented by channel noise (channel-type models), or on both. The helper is introduced by the role so called a "third party" (e.g., a trusted server or centralized server), which works with the production of secret key by client terminals by outfitting them extra connected data. Additionally, the idea of an helper has expected importance for functional plans for the generation of key by at least three or more than three terminals, wherein the various users can alternate roles as helper in progressive rounds of generation of Key. In addition to this, we inspect models for the generation of mystery or non-mystery key with rate imperatives forced on admissible transmissions, portraying data transfer capacity constraints related with the utilization of shared public channels.

CHAPTER- 2:

Literature review

Paper 1:

U. M. Maurer. Secrete key agreement by public discussion based on common information. IEEE Trans. Inform. Theory, 39(5):733–742, May 1993.

Inference:

This paper speaks about key dispersion and encryption: a common mystery key produced. by one of our conventions can be utilized as the key succession in the above mentioned referenced one-time cushion, along these lines accomplishing (for all intents and purposes) awesome secrecy of the communicated messages.

Paper 2:

R. Ahlswede and I. Csiszar. Common randomness in information theory and cryptography Part I: Secret sharing. IEEE Trans. Inform. Theory, 39(4):1121–1132, July 1993.

Inference:

Paper speaks about the generating common randomness (CR), by two client terminals with help from a "helper" terminal. Every terminal notices an alternate part of a discrete memoryless various source. The partner helps the clients by sending data to them over a silent public channel subject to a rate requirement. Moreover, one of the clients is permitted to send to the next client over a public channel under a comparable rate limitation.

The above 2 papers shown that a particularly secret key can be set up between two distant terminals if every terminal approaches to a part of a vector source arrangement and the two terminals which are used can communicate with each other by means of a public channel. The produced key can be kept secure from the EVE (eavesdropper), which has full admittance to the public channel. The vital limit with regards to the two-terminal source model has been set up in these examinations.

Paper 3:

A. A. Gohari and V. Anantharam. Information-theoretic key agreement of multiple terminalsPart I. IEEE Trans. Inform. Theory, 56(8):3973–3996, Aug 2010.

Inference:

In the secret key generation issue, the prerequisite toward the finish of the communication is certifiably not a secret key, yet that every one of the terminals become roughly all-knowing about each other's arbitrary variables. The objective is to limit the correspondence rate needed to accomplish this This paper works on the characterization of more extensive thought of communication. Also they developed another single letter lower bound for the secrecy rate which, in the instance of two terminals, rigorously enhances the one which is the limit of the two single direction secret key rates. The bound is demonstrated by following the intuitive correspondence stage by stage and cautious accounting of the development of the secret key rate by controlling the measure of decrease of mystery key rate developed in before stages because of the communication that took place in later stage.

Paper 4:

H. Zhang, L. Lai, Y. Liang, and H. Wang. The secret key-private key generation over three terminals: Capacity region. In Proc. IEEE Int. Symp. Information Theory (ISIT), Honolulu, HI, USA, June 2014

Inference:

The above paper speaks about the transmission of de-evaluated message sets with two layers over a three-receiver BC under various secrecy requirements. It also speaks about typical message communicated to every one of the three recipients/terminals, a confidential normal message to the two real beneficiaries and two confidential individual messages to the two authentic collectors, where every beneficiary is just keen on one them, while being completely discerning of the other one.

CHAPTER- 3:

THEORETICAL ANALYSIS:

Challenges:

Apparently, so far, the multi-key limit region is described as it were for three-terminal frameworks. It is hence important to explore whether it is feasible to describe the multi-key limit area for frameworks with multiple terminals i.e., more than three terminals.
Such investigation needs to resolve two challenging issues.

- Although the key limit region for the three-terminal model was demonstrated to be equivalent to the cut set bound, it is not satisfactory at the beginning whether the cut-set bound can in any case be accomplished for models with distinctive secrecy prerequisites and for four-terminal models with an extra aide helper. In addition to it, cut-set bound is more uncertain attainable as the framework gets more convoluted.

- For the three-terminal model, there are three cuts for producing two keys, and plans can be intended to accomplish corner points of the cut-set destined for each instance of the source circulation. Apart from that, for four-terminal models with an helper, there are six cuts for producing two keys, also, these six cuts yield eight potential instances of the cut-set bound because of various source appropriations. It isn't certain whether there exists a brought together plan to accomplish the cut-set destined for all cases.

Developing the Framework:

Attributes:

X0 - Terminal

X1- Terminal

X1- Terminal

X3- Terminal

K1- Key

K2- Key

Model 1a- Symmetric key generation with a trusted helper

Model 1b- Symmetric key generation with an untrusted helper

Model 1c- Asymmetric key generation with a trusted helper

Model 1d- Asymmetric key generation with an untrusted helper

Our commitment in this paper lies in setting up key limit regions for four source models of producing a couple of keys, and our outcomes give 2 certifiable responses to both of the above challenges that we see. As part of all models, there are four terminals, and every terminal notices one component of the vector source which is a connected. Terminals X0 and X1 wish to concur on a key K1, and terminals X0 and X2 wish to concede to another key K2 which is independent. The four terminals are permitted to convey over a public channel, and an Eve (eavesdropper) is assumed to approach the public conversation without uncertainty. The four models vary from one another because of secrecy constraints.

Models 1a and 1b speaks about generation of symmetric key, in which secrecy prerequisites for two keys are something similar. Model 1a (with a helper that can be trusted) requires that the two keys are covered from the Eve (eavesdropper), furthermore, model 1b (with an helper which is untrusted) further requires that the two keys are disguised from terminal X3 in addition to the Eve (eavesdropper).

In the case of helper which is untrusted, we expect that the helper is interested however legit. To elaborate the helper tries to gather the data about the keys that are generated yet it follows the protocol.

Models 2a and 2b (with a trusted and an untrusted helper) have similar secrecy prerequisites for the two keys as models 1a and 1b, but actually the key K2 is additionally needed to be disguised from terminal X1 for the two models. Consequently, models 2a and 2b both speaks generation of asymmetric key.

For all of the over four models, we set up the cut-set bound to be the key limit area by showing that the cut-set bound is to be indeed feasible. Besides, in this project a reachable system is brought to accomplish the corner points of the cut-set bound relating to all instances of source distributions. The plans to accomplish various cases change just in the rate at which every terminal uncovers data to public. Consequently, the attainability confirmation is fundamentally rearranged. All the more explicitly, the achievable technique depends on irregular binning and in addition to it joint decoding.

Given a unified system, we infer the Slepian-Wolf conditions that ensure right key understanding and infer adequate conditions that ensure the secrecy requirements. Then, at that point, for every individual case, it is adequate to confirm the public transmission paces of terminals which satisfies the inferred Slepian-Wolf conditions and mystery conditions, which can be performed without any problem.

CHAPTER- 4:

Experimental Investigations:

Model 1A:

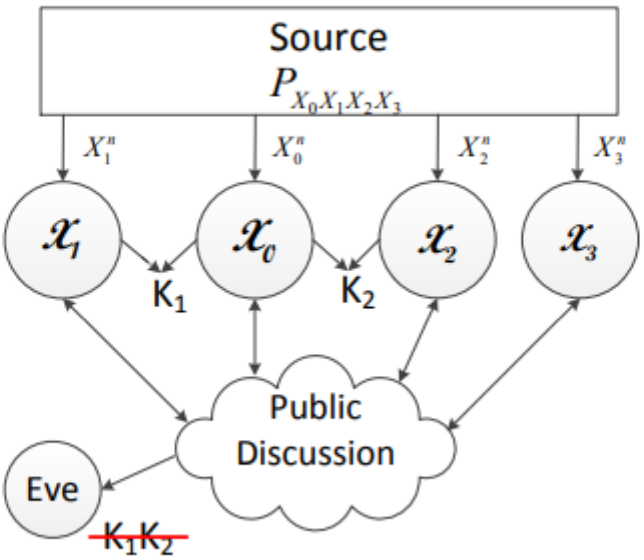

Figure 4.1-Model 1a. Symmetric key generation with a trusted helper

In this project there are four models and in all four models there are four terminals, each and every terminal notices one part of an associated vector source. Among the four Terminals X0 and X1 wish to concede to a key K1, and in addition to it terminals X0 and X2 wish to concur on key K2 which is independent. The four terminals that are present are permitted to have communication over a public channel, and in the meanwhile EVE (eavesdropper) is expected to approach the public conversation without equivocalness. The four models do differ from one another because of secrecy limitations.

Models 1a speaks about generation of symmetric key, in which secrecy necessities for two keys are something similar. Model 1a (with a helper which is trusted) requires that the two keys are hidden from the Eve(eavesdropper).

Model 1B:

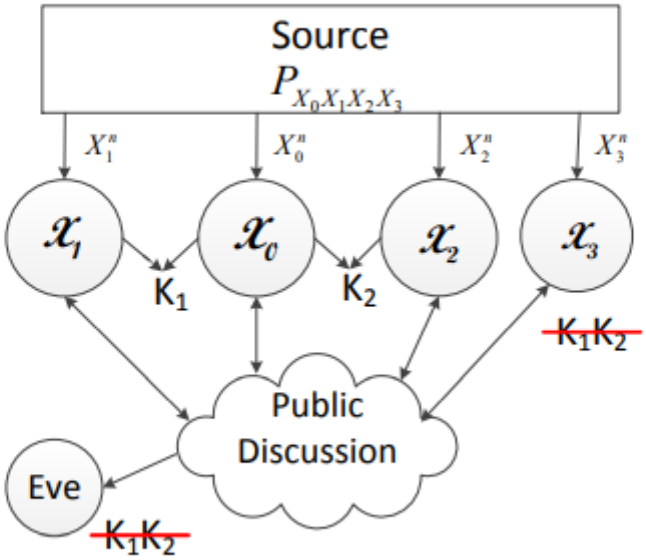

Figure 4.2- Model 1b. Symmetric key generation with an untrusted helper

Among the four Terminals X0 and X1 wish to concede to a key K1, and in addition to it terminals X0 and X2 wish to concur on key K2 which is independent. The four terminals that are present are permitted to have communication over a public channel, and in the meanwhile EVE (eavesdropper) is expected to approach the public conversation without equivocalness. The four models do differ from one another because of secrecy limitations.

Model 1b (with a helper which is not trustable) requires that the two keys are covered from terminal X3 with respect to the EVE (eavesdropper). In the case of untrusted helper, we expect that the helper is interested however fair, the partner tries to derive the data about the keys that are generated yet at the same time it also follows the protocols.

Model 2A:

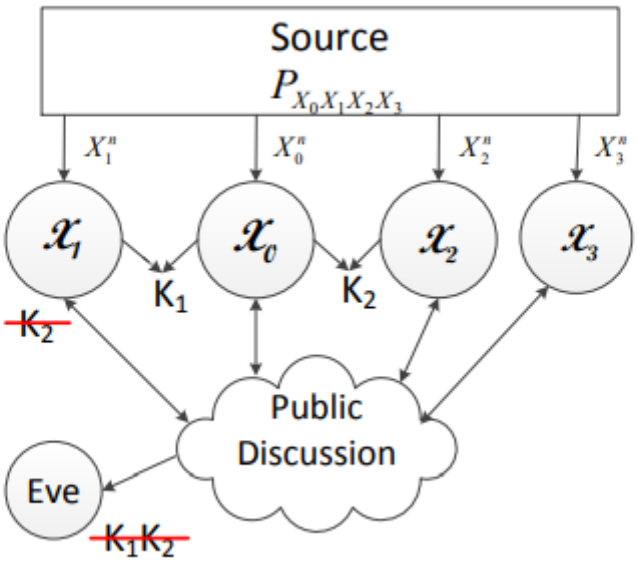

Figure 4.3- Model 2a. Generation of Asymmetric key with a trusted helper

Models 2a (with a helper which is a trusted one) have similar secrecy requirements as of the two keys in models 1a and 1b. But what differs is the key K2 is additionally needed to be hidden from terminal X1 for the model 2A. In this manner, models 2a speaks about the generation of asymmetric key.

The four terminals in all the models can communicate by means of a public channel by neglecting rate requirements. The public channel is quite noiseless as in every one of the four terminals and an EVE (eavesdropper) can get to the public conversation without equivocalness. We accept that the EVE (eavesdropper) doesn't notice any additional data, for example, source arrangements.

Model 2B:

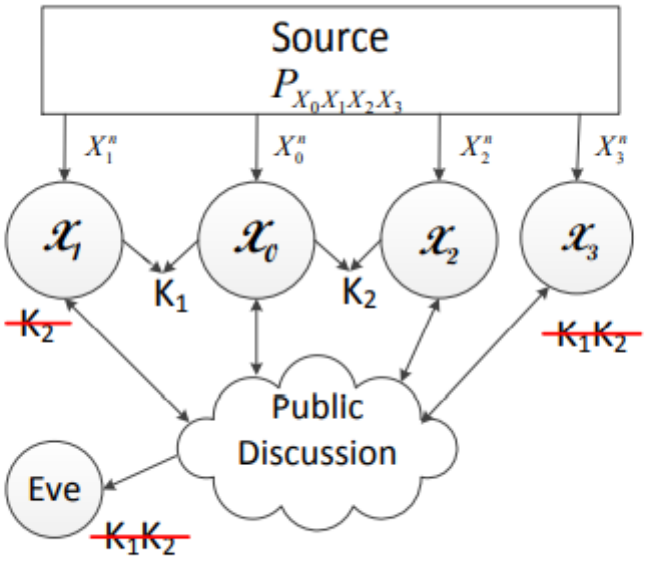

Figure 4.4 Model 2b. Generation of Asymmetric key with an Untrusted helper

Models 2b (with a helper which is a untrusted one) have similar secrecy requirements as of the two keys in models 1a and 1b. But what differs is the key K2 is additionally needed to be hidden from terminal X1 for the model 2A. In this manner, models 2b speaks about the generation of asymmetric key with the help of an untrusted helper.

For all the over four models, we set up the cut-set bound to be the critical limit area by showing that the cut-set bound is to be sure attainable. Moreover, we build a brought together feasible methodology to accomplish the corner points of the cut-set bound relating to all instances of source dispersions. The plans to accomplish various cases change just in the rate at which every terminal uncovers data to public. In this manner, the attainability verification is essentially improved.

.

CHAPTER- 5:

Experiment results:

1. Generation of Symmetric Key with a Trusted Helper

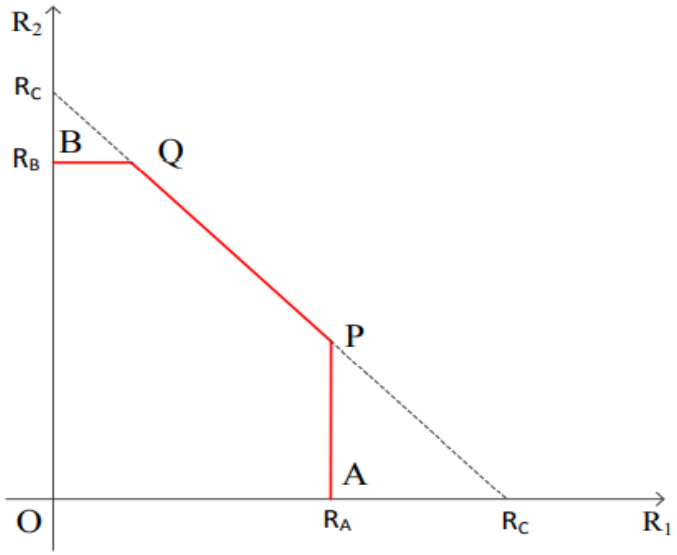

Figure 5.1: **The key capacity region for symmetric key generation with a trusted helper**.

As the secrecy limitations on K1 and K2 are symmetric, the limits on R1 and R2 are likewise symmetric. These limits can be naturally perceived as cut-set limits. Specifically, the upper bound on R1 in is because of two cuts isolating X0 and X1 for producing K1 (two more limits on R1 because of the other two cuts isolating X0 and X1 become repetitive due to the aggregate rate bound). The upper bound on R2 in is because of two cuts isolating X0 and X2 for creating K2 (two additional limits on R2 because of the other two cuts isolating X0 and X1 become repetitive because of the total rate bound). The total rate bound is because of the two cuts isolating X0 and (X1, X2) for creating the two keys K1 and K2 one after another.

The design of the key limit region is shown above in the figure 5.1 as the pentagon O-A-P-Q-B-O. We next portray developing an attainable plan to accomplish the key limit region. It does the trick to show the feasibility of P and Q points. Since the secrecy requirements on K1 and K2 are symmetric, it is adequate to show that the corner point P is attainable, and afterward the feasibility of the point Q follows by balance. We expect to be that RA < RC, on the grounds that generally the point P would implode to the point A.

The key rate pair of the point P is given by R1 = RA also, R2 = RC − RA. Comparing to various source disseminations, every one of RA and RC can take one of the two shared data terms yielded. Henceforth, the directions of the point P can take four structures, i.e., case 1 with RA = I(X1; X0X2X3) and RC = I(X0; X1X2X3), case 2 with RA = I(X1; X0X2X3) and RC = I(X0X3; X1X2), case 3 with RA = I(X1X3; X0X2) and RC = I(X0; X1X2X3), and case 4 with RA = I(X1X3; X0X2) also, RC = I(X0X3; X1X2).

Here a unified scheme is made in order to achieve the rate point P for all cases. In the unified scheme, terminals X1, X2, and X3 shows enough information to public so that terminal X0 can recover Xn 1, Xn 2 and Xn 3. Key K1 is generated with the help of terminals X0 and X1 by depending on Xn 1 , and Key K2 is generated with the help of terminals X0 and X2 depending on Xn 2. Let R˜ 1, R˜ 2 and R˜ 3 indicate the rates upon which terminals X1, X2 and X3 that reveal data to public.

Case 1. The key rate pair of the point P is given by (I(X1; X0X2X3), H(X2X3|X1) − H(X2X3|X0)). As the rate of K1 needs to be maximized, terminal X1 should expose as little information as possible. Therefore, terminals X2 and X3 first expose information at the rate R˜ 2 + R˜ 3 = H(X2X3|X0) so that terminal X1 needs to release only at the rate R˜ 1 = H(X1|X0X2X3) in order for X0 to recover Xn 1 . Thus, the rate of K1 can be as large as I(X1; X0X2X3).

As the K1 generation already makes use of information contained in Xn 1, generation of K2 can be done only based on information that is contained in Xn 2 and Xn 3 given Xn 1. Thus, R2 can be as large as $H(X2X3|X1) - H(X2X3|X0)$, where the subtraction is due to public discussion at the rate $\tilde{R} 2 + \tilde{R} 3 = H(X2X3|X0)$.

Case 2. The key rate pair of the point P is given by $(I(X1; X0X2X3), H(X2|X1) - H(X2|X0X3))$. The argument for R1 is the same as that for case 1. In case 2, $RC = I(X0X3; X1X2)$, which implies that $I(X0X3; X1X2) \leq I(X0; X1X2X3)$. This further implies $I(X1X2; X3) \leq I(X0; X3)$. Thus, in order for terminal X0 to recover Xn 2 and Xn 3, it is more efficient to let X3 reveal information first at the rate $\tilde{R} 3 = H(X3|X0)$, and then let X2 reveal information at the rate $\tilde{R} 2 = H(X2|X0X3)$. Since in this case X2 does not recover Xn 3, the key rate $R2 = H(X2|X1) - H(X2|X0X3)$.

Case 3. The key rate pair of the point P is given by $(I(X0X2; X1X3), H(X2|X1X3) - H(X2|X0))$. The case conditions $RA = I(X0X2; X1X3)$ and $RC = I(X0; X1X2X3)$ implies that X0 and X2 have high correlation, and X1 and X3 have high correlation. Thus, a natural idea for public discussion is to let terminal X0 recover Xn 2 and let X1 recover Xn 3 first, and then generate K1 between terminals X0 and X1 to achieve $R1 = I(X0X2; X1X3)$. Since Xn 1 and Xn 3 have been fully used for generating K1, then K2 can achieve the rate $R2 = H(X2|X1X3) - H(X2|X0)$, where the subtraction is due to the public transmission of terminal X2 to let X0 recover Xn 2.

Case 4. This case does not exist because of the contradiction induced by setting $RA = I(X0X2; X1X3)$ and $RC = I(X0X3; X1X2)$.

2. Generation of Symmetric Key with an Untrusted Helper

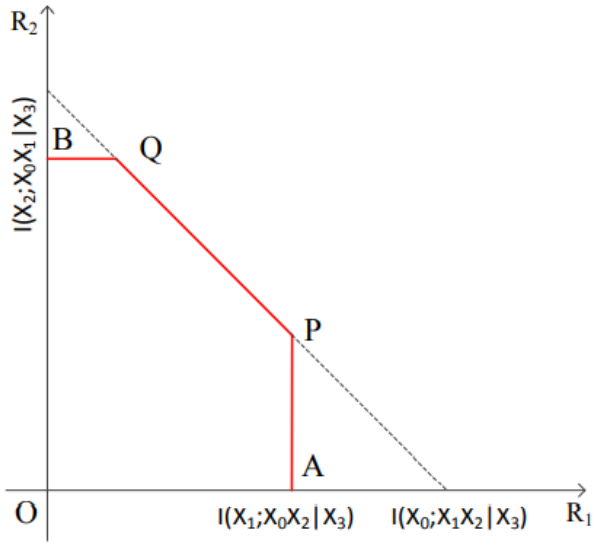

Figure 5.2 The key capacity region for symmetric key generation with an untrusted helper

The key capacity region for generation of symmetric key with an untrusted helper is contained in the key capacity region for generation of symmetric key with a trusted helper, because it holds that I(X1; X0X2|X3) ≤ RA, I(X2; X0X1|X3) ≤ RB and I(X0; X1X2|X3) ≤ RC. This is reasonable due to the additional requirement for the keys to be concealed from the helper when the helper is untrusted. In order to justify the achievability of the region, by symmetry, it is sufficient to show the achievability of the point P. The rate pair at point P is given by (I(X1; X0X2|X3), H(X2|X1X3) − H(X2|X0X3)). The idea to achieve the point P follows the 9 unified strategy i.e., public discussion first guarantees that terminal X0 recovers Xn 1, Xn 2 and Xn 3 correctly, and then K1 is generated by terminals X0 and X1 based on Xn 1 and K2 is generated by terminals X0 and X2 based on Xn 2.

Since the generated keys should be concealed from the helper terminal X3, Xn 3 cannot be used as random resource for generating the keys, although the helper can still participate the public discussion to assist the recovery of source sequences. More specifically, since the rate of K1 needs to be maximized, terminal X1 should reveal as little information as possible. Hence, terminals X2 and X3 first reveal information at the rate R˜ 2 + R˜ 3 = H(X2X3|X0) so that terminal X1 needs to release only at the rate R˜ 1 = H(X1|X0X2X3) in order for X0 to recover Xn 1. Thus, the rate of K1 can be as large as I(X1; X0X2|X3). Since X3 is an untrusted helper, it can reveal information at any rate. Hence, R˜ 2 can be set to be H(X2|X0X3). Consequently, R2 = H(X2|X1X3) − H(X2|X0X3). Since the generation of K1 already uses up information contained in Xn 1s, K2 can be generated only based on information contained in Xn 2 given Xn 1 and Xn 3.

3. Asymmetric Key Generation with a Trusted Helper:

The key capacity region is represented as the pentagon O-A-P-Q-B-O in figure 5.3. Since the secrecy requirements for the two keys are different, achievable schemes need to be designed in order to achieve the points P and Q separately. Corresponding to different source distributions, the rate pairs of the points P and Q can take different forms. Interestingly, the same unified strategy described for the previous models can achieve the points P and Q for all cases. Namely, terminals X1, X2 and X3 reveal information to public such that terminal X0 can recover (Xn 1, Xn 2, Xn 3) correctly. Then K1 is generated based on Xn 1 and K2 is generated based on Xn 2. The schemes for different cases vary only in the rate at which each terminal reveals information to public. Here, we still use R˜ 1, R˜ 2 and R˜ 3 to denote the rates at which terminals X1, X2 and X3 reveal information to public, respectively.

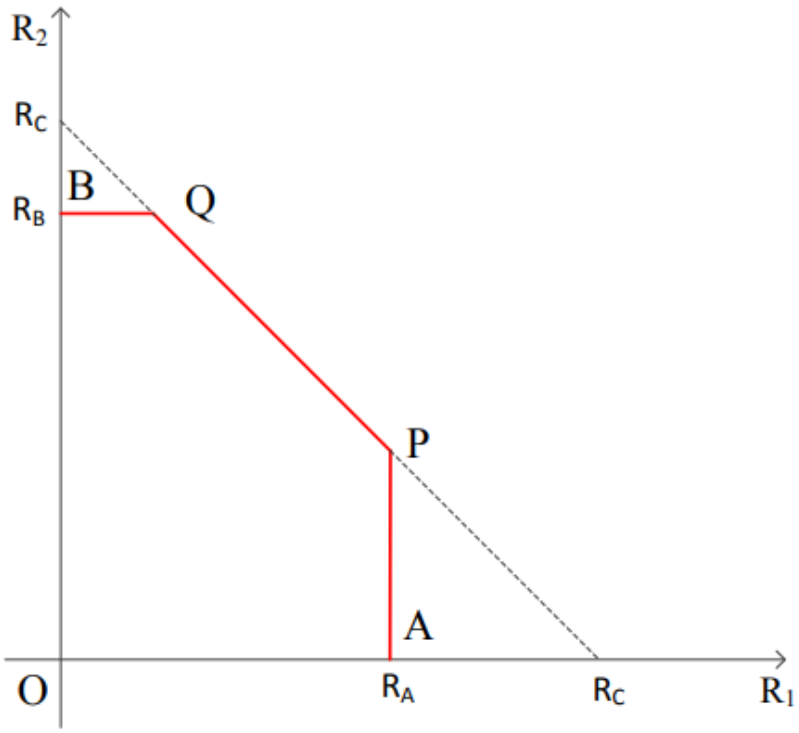

Figure 5.3 The key capacity region for asymmetric key generation with a trusted helper

For the point P, it can be observed that its rate coordinates are exactly the same as symmetric key generation with a trusted helper. This is because both models should reach the same maximum rate R1 of K1 due to the same secrecy requirement for K1. Furthermore, since both models should exhaust all random resource in Xn 1 for generating K1, K2 should be generated from random resource independent from Xn 1 even if it is not required to be concealed from terminal X1 in symmetric key generation. Thus, the two models also 11 have the same rate R2 at the point P. For the point Q, the rate coordinates are given by (RC − R0 B, R0 B). Corresponding to different source distributions, each of RC and R0 B can take one of the two mutual information terms. Hence, the coordinates of the point Q can take four forms, i.e., case 1 with RC = I(X0; X1X2X3) and R0 B = I(X0; X2X3|X1); case 2 with RC = I(X0; X1X2X3) and R0 B = I(X2; X0X3|X1); case 3 with RC = I(X0X3; X1X2) and R0 B = I(X0; X2X3|X1); and case 4 with RC = I(X0X3; X1X2) and R0 B = I(X2; X0X3|X1). The achievable designs for the following cases are different due to the source distributions that determine these cases.

Case 1. The key rate pair of the point Q is given by (I(X0; X1), I(X0; X2X3|X1)). In order to generate K1 at the rate I(X0; X1), terminal X1 can reveal information at the rate R˜ 1 = H(X1|X0). Then terminal X0 can recover Xn 1 correctly. In order for terminal X0 to further recover (Xn 2, Xn 3), terminals X2 and X3 jointly release information at the sum rate R˜ 2 + R˜ 3 = H(X2X3|X0X1). Since the resource to generate K2 should be contained in (Xn 2, Xn 3) given Xn 1, the key rate R2 should satisfy R2 = H(X2X3|X1)−R˜ 2−R˜ 3 which yields R2 = I(X0; X2X3|X1).

Case 2. The key rate pair of the point Q is given by (I(X0; X1X3)−I(X2; X3|X1), I(X2; X0X3|X1)). Terminals X1 and X3 first jointly reveal information at the sum rate R˜ 1+R˜ 3 = H(X1X3|X0). Then terminal X0 recovers Xn 1 and Xn 3 correctly. Terminal X2 needs to release information only at the rate R˜ 2 = H(X2|X0X1X3) and then Xn 2 can be successfully recovered at X0. Thus, K2 can be generated at the rate H(X2|X1) − H(X2|X0X1X3), which yields R2 = I(X2; X0X3|X1). In order to generate K1 at the rate R1 = I(X0; X1X3)−I(X2; X3|X1), R˜ 1 should be chosen to be R˜ 1 = H(X1X3|X0) − H(X3|X1X2), and then R˜ 3 = H(X3|X1X2).

Case 3. This case does not exist because of the contradiction induced by setting RC = I(X0X3; X1X2) and R0 B = I(X0; X2X3|X1).

Case 4. The key rate pair of the point Q is given by (I (X1; X0X3), I (X2; X0X3|X1)). Still, terminals X1 and X3 first reveal information at the sum rate R˜ 1+R˜ 3 = H(X1X3|X0). Due to the case conditions, X3 has high correlation with X0 and hence let X3 reveal its information at the rate R˜ 3 = H(X3|X0). Then X1 reveals its information at the rate R˜ 1 = H(X1|X0X3), and finally X2 reveals its information at the rate R˜ 2 = H(X2|X0X1X3) in order for X0 to recover (Xn 1, Xn 2, Xn 3). Thus, the key rate R2 = I(X0X3; X2|X1), and the rate R1 = I(X0X3; X1).

It has been noted that for generating asymmetric key with a trusted helper, the point Q achieves the same sum rate as that for generation of symmetric key with the help of trusted helper. This is because even if the rate of K2 decreases in the asymmetric model due to the additional secrecy requirement for K2 to be concealed from X1, the random resource contained in Xn 1 can still be used for generating K1 so that there is no loss in the sum rate.

4. Generation of Asymmetric Key with an Untrusted Helper

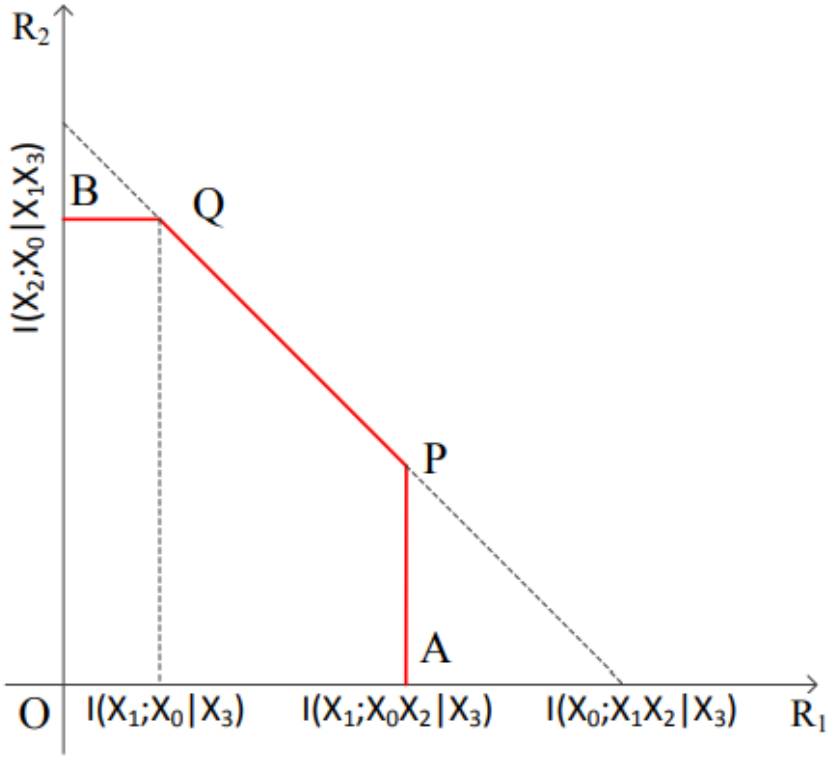

Figure 5.4 The key capacity region for asymmetric key generation with an untrusted helper.

Similarly to the symmetric case, it is clear that the key capacity region for asymmetric key generation with an untrusted helper is contained in that for the asymmetric key generation with a trusted helper, because it always holds that I(X1; X0X2|X3) ≤ RA, I(X2; X0|X1X3) ≤ R0 B and I(X0; X1X2|X3) ≤ RC. This is anticipated due to the additional requirement for the keys to be concealed from the helper. The key capacity region is illustrated in Fig. 5.4 as the pentagon O-A-P-Q-B-O. It can be shown that the point P can be achieved by the same scheme as that for achieving the point P in symmetric key generation with an untrusted helper in Section 3.2. We next describe the idea to achieve the point Q. The rate pair of the point Q is given by (I(X0; X1|X3), I(X2; X0|X1X3)). Terminals X1 and X3 first reveal information at the rate R˜ 1+R˜ 3 = H(X1X3|X0) so that terminal X0 can recover Xn 1 and Xn 3 correctly. Then terminal X2 needs to release only at the rate R˜ 2 = H(X2|X0X1X3) for X0 to recover Xn 2. Thus, the rate of K2 can be as large as I(X2; X0|X1X3). Since X3 is an untrusted helper, it can reveal information at any rate. Hence, R˜ 1 can be set to be H(X1|X0X3). Consequently, R1 = H(X1|X3) − H(X1|X0X3) = I(X0; X1|X3).

CHAPTER- 6:

CONCLUSION:

In this project, we have concentrated on the issue of creating a couple of keys for a cell source model with a helper. We have set up the full key limit region for four models with distinctive mystery necessities. The models considered here comprise of four terminals, which are more convoluted to break down than three-terminal models concentrated already, on the grounds that the cut-set external bound takes more cases because of various source distributions. Rather than planning a particular reachable plan for each case individually, we have fostered a bound together procedure, which accomplishes corner points in all cases, and thus fundamentally diminishes the complexity of the attainability evidence. It will be of future interest to sum up the investigations here to cell models with multiple mobile terminals, in which every terminal wishes to create a key with the base station terminal. In such a case, a unified methodology is alluring to work with attainable investigation. As another course, it will be fascinating to concentrate on this kind of generation of various key with rate limitations on the public conversation. For such a case, past investigations of the source model with the helper subject to limited rate imperatives and of vector Gaussian source model with public conversation topic to limited rate imperatives in give helpful procedures.

CHAPTER- 7:

REFERENCES:

[1] Simultaneously generating multiple keys in many to one networks.
L. Lai and L. Huie. In Proc. IEEE Int. Symp. Information Theory (ISIT),
Istanbul, Turkey, July 2013. 30

[2] The secret key-private key capacity region for three terminals.
C. Ye and P. NarayanIn Proc. IEEE Int. Symp. Information Theory (ISIT),
Adelaide, Australia, September 2005.

[3]Common randomness in information theory and cryptography Part II: CR capacity.
R. Ahlswede and I. Csisz´ar IEEE Trans. Inform. Theory, 44(1):225–240, January 1998.

[4] Common randomness and secret key generation with a helper. IEEE Trans. Inform. Theory,
46(2):344–366,
March 2000, I. Csisz´ar and P. Narayan.

[5] Secrecy capacities for mulitple terminals. IEEE Trans. Inform. Theory, 50(12):3047–3061,
December 2004.
I. Csisz´ar and P. Narayan

[6] Information-theoretic key agreement of multiple terminals-Part I. IEEE Trans. Inform. Theory,
56(8):3973–3996,
Aug 2010. A. A. Gohari and V. Anantharam.

[7] Mutual dependence for secret key agreement. In Proc. Conf. on Information Sciences and Systems
(CISS), Princeton University, NJ, USA, March 2010.
C. Chan and L. Zheng.

[8] Common randomness in information theory and cryptography-Part I: Secret sharing. IEEE Trans.
Inform. Theory, 39(4):1121–1132, July 1993.
R. Ahlswede and I. Csisz´ar

[9] The secret key-private key generation over three terminals: Capacity region. In Proc. IEEE Int.
Symp. Information Theory (ISIT), Honolulu, HI, USA, June 2014.
H. Zhang, L. Lai, Y. Liang, and H. Wang.

[10] The capacity region of the source-type model for secret key and private key generation. IEEE
Trans. Inform. Theory, 60(10):6389–6398, October 2014.
H. Zhang, L. Lai, Y. Liang, and H. Wang

[11] Secrete key agreement by public discussion based on common information. IEEE Trans. Inform.
Theory, 39(5):733–742, May 1993.
U. M. Maurer.