

This Report is Submitted on

Multi-Key Generation over a Cellular Model with a Helper

Master's in computer science

Submitted By

Pakalapati Sri Lakshmi Prasanna Kumar WSUID: W845T858

Chaganti Revanth Chowdary WSUID: Q929B649

Mengani Ajay Kumar WSUID: 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 an eavesdropper to acquire data about the key, is thought of in this project. In the model considered, there are four terminals, X_0 , X_1 , X_2 , and X_3 , every one of which notices one part of a vector source. Terminal X_0 wishes to produce two mystery keys K_1 and K_2 individually with terminals X_1 and X_2 under the assistance of terminal X_3 . 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 K_2 is additionally required to be covered from terminal X_1 . 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

| | TOPIC | Page No |
|-----------|-----------------------------|----------------|
| 1 | Introduction | 5-7 |
| 2 | Literature review | 8-9 |
| 3 | Theoretical Analysis | 10-12 |
| 4 | Investigations | 13-16 |
| 5 | Results | 17-24 |
| 6 | Proof Of Theorems | 25-44 |
| 7 | Weak Points | 45 |
| 8 | Strong Points | 46 |
| 9 | Extension | 47 |
| 10 | Conclusion | 48 |
| 11 | References | 49-50 |

List of figures

| Chapter number | Figure number | Description |
|----------------|---------------|--|
| 4 | 4.1 | Model 1a- Symmetric key generation with a trusted helper |
| | 4.2 | Model 1b- Symmetric key generation with an untrusted helper |
| | 4.3 | Model 1c- Asymmetric key generation with a trusted helper |
| | 4.4 | Model 1d- Asymmetric key generation with an untrusted helper |
| 5 | 5.1 | The key capacity region for symmetric key generation with a trusted helper |
| | 5.2 | The key capacity region for symmetric key generation with an untrusted helper |
| | 5.3 | The key capacity region for asymmetric key generation with a trusted helper |
| | 5.4 | The key capacity region for asymmetric key generation with an untrusted helper |

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 device 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 an 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 a 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. Csisz'ar. 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 approach 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 terminals Part 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 of 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 a 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 above challenges that we see. As part of all models, there are four terminals, and every terminal notice 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 a 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 the key K_2 is additionally needed to be disguised from terminal X_1 for the two models. Consequently, models 2a and 2b both speak generation of asymmetric key.

For all 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. Even more explicitly, the achievable technique depends on irregular binning and in addition to its 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 rates of terminals which satisfies the inferred Slepian-Wolf conditions and mystery conditions, which can be performed without any problem.

CHAPTER- 4:

Investigations:

Model 1A:

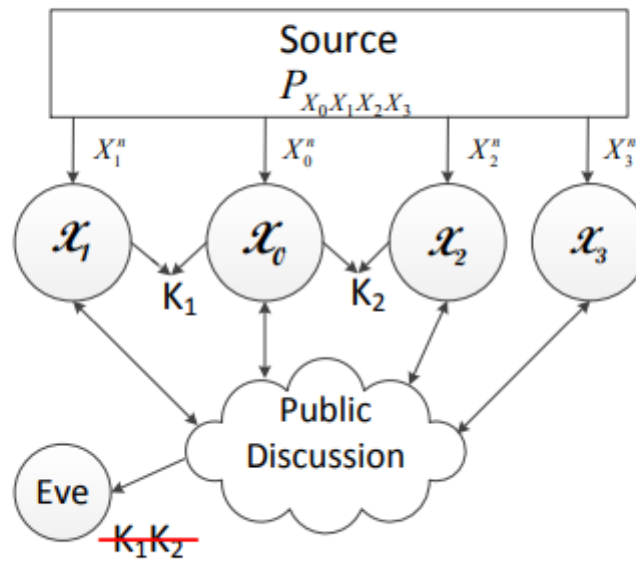


Figure 4.1-Model 1a. Symmetric key generation with a trusted helper

In this project there are four models and in all four models there are four terminals, each and every terminal notice one part of an associated vector source. Among the four Terminals X_0 and X_1 wish to concede to a key K_1 , and in addition to it terminals X_0 and X_2 wish to concur on key K_2 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 equivocallness. 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:

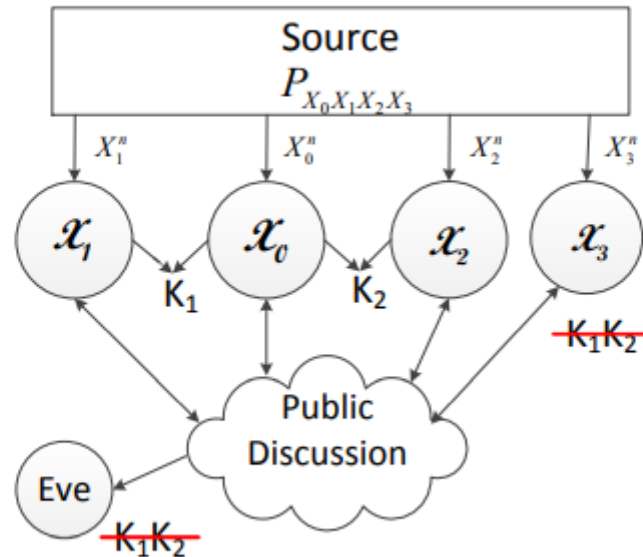


Figure 4.2- Model 1b. Symmetric key generation with an untrusted helper

Among the four Terminals X_0 and X_1 wish to concede to a key K_1 , and in addition to it terminals X_0 and X_2 wish to concur on key K_2 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 equivocality. 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 X_3 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:

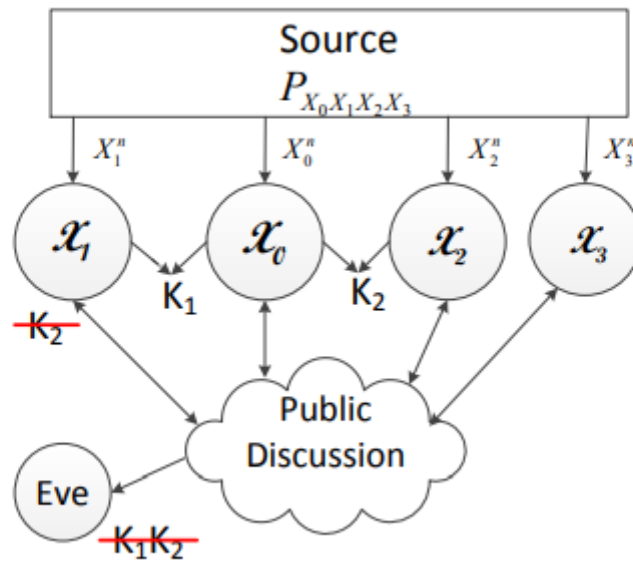


Figure 4.3- Model 2a. Generation of Asymmetric key with a trusted helper

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 K_2 is additionally needed to be hidden from terminal x_1 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 equivocality. We accept that the EVE (eavesdropper) doesn't notice any additional data, for example, source arrangements.

Model 2B:

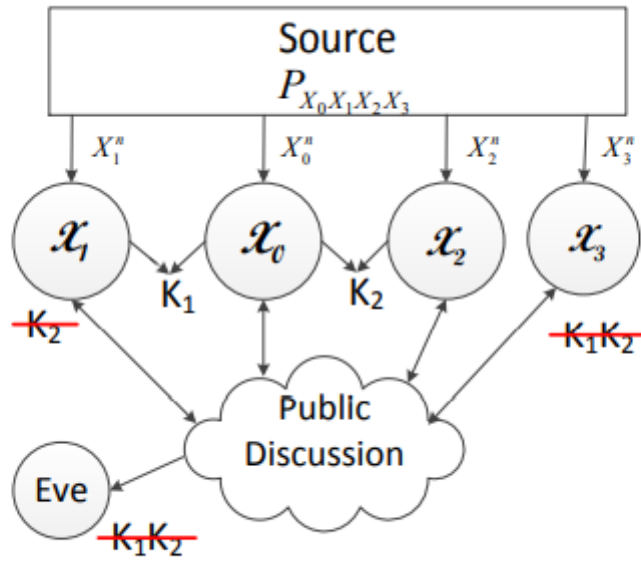


Figure 4.4 Model 2b. Generation of Asymmetric key with an Untrusted helper

Models 2b (with a helper which is an untrusted one) have similar secrecy requirements as of the two keys in models 1a and 1b. But what differs is the key K_2 is additionally needed to be hidden from terminal X_1 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:

Results:

1. Generation of Symmetric Key with a Trusted Helper

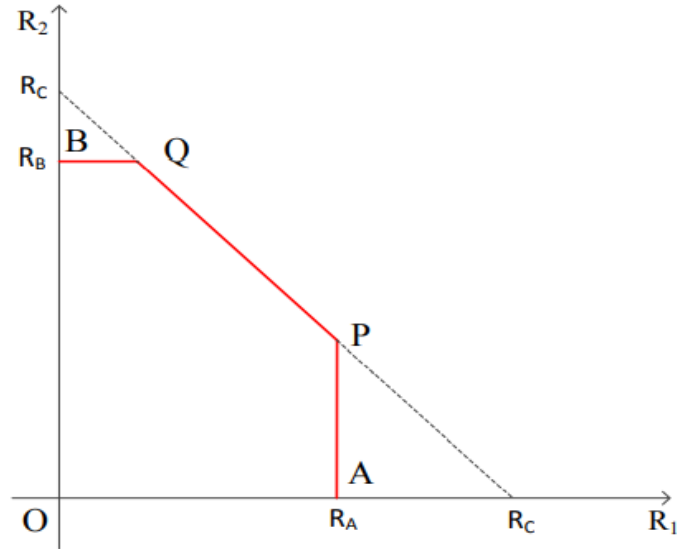


Figure 5.1: The key capacity region for symmetric key generation with a trusted helper.

As the secrecy limitations on K_1 and K_2 are symmetric, the limits on R_1 and R_2 are likewise symmetric. These limits can be naturally perceived as cut-set limits. Specifically, the upper bound on R_1 is because of two cuts isolating X_0 and X_1 for producing K_1 (two more limits on R_1 because of the other two cuts isolating X_0 and X_1 become repetitive due to the aggregate rate bound). The upper bound on R_2 is because of two cuts isolating X_0 and X_2 for creating K_2 (two additional limits on R_2 because of the other two cuts isolating X_0 and X_1 become repetitive because of the total rate bound). The total rate bound is because of the two cuts isolating X_0 and (X_1, X_2) for creating the two keys K_1 and K_2 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 X_{n1} , X_{n2} and X_{n3} . Key K1 is generated with the help of terminals X0 and X1 by depending on X_{n1} , and Key K2 is generated with the help of terminals X0 and X2 depending on X_{n2} . Let \tilde{R}_1 , \tilde{R}_2 and \tilde{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 $\tilde{R}_2 + \tilde{R}_3 = H(X2X3|X0)$ so that terminal X1 needs to release only at the rate $\tilde{R}_1 = H(X1|X0X2X3)$ in order for X0 to recover X_{n1} . Thus, the rate of K1 can be as large as $I(X1; X0X2X3)$.

As the K1 generation already makes use of information contained in $X_n 1$, generation of K2 can be done only based on information that is contained in $X_n 2$ and $X_n 3$ given $X_n 1$. Thus, R_2 can be as large as $H(X_2X_3|X_1) - H(X_2X_3|X_0)$, where the subtraction is due to public discussion at the rate $\tilde{R}_2 + \tilde{R}_3 = H(X_2X_3|X_0)$.

Case 2. The key rate pair of the point P is given by $(I(X_1; X_0X_2X_3), H(X_2|X_1) - H(X_2|X_0X_3))$. The argument for R_1 is the same as that for case 1. In case 2, $R_C = I(X_0X_3; X_1X_2)$, which implies that $I(X_0X_3; X_1X_2) \leq I(X_0; X_1X_2X_3)$. This further implies $I(X_1X_2; X_3) \leq I(X_0; X_3)$. Thus, in order for terminal X_0 to recover $X_n 2$ and $X_n 3$, it is more efficient to let X_3 reveal information first at the rate $\tilde{R}_3 = H(X_3|X_0)$, and then let X_2 reveal information at the rate $\tilde{R}_2 = H(X_2|X_0X_3)$. Since in this case X_2 does not recover $X_n 3$, the key rate $R_2 = H(X_2|X_1) - H(X_2|X_0X_3)$.

Case 3. The key rate pair of the point P is given by $(I(X_0X_2; X_1X_3), H(X_2|X_1X_3) - H(X_2|X_0))$. The case conditions $R_A = I(X_0X_2; X_1X_3)$ and $R_C = I(X_0; X_1X_2X_3)$ implies that X_0 and X_2 have high correlation, and X_1 and X_3 have high correlation. Thus, a natural idea for public discussion is to let terminal X_0 recover $X_n 2$ and let X_1 recover $X_n 3$ first, and then generate K1 between terminals X_0 and X_1 to achieve $R_1 = I(X_0X_2; X_1X_3)$. Since $X_n 1$ and $X_n 3$ have been fully used for generating K1, then K2 can achieve the rate $R_2 = H(X_2|X_1X_3) - H(X_2|X_0)$, where the subtraction is due to the public transmission of terminal X_2 to let X_0 recover $X_n 2$.

Case 4. This case does not exist because of the contradiction induced by setting $R_A = I(X_0X_2; X_1X_3)$ and $R_C = I(X_0X_3; X_1X_2)$.

2. Generation of Symmetric Key with an Untrusted Helper

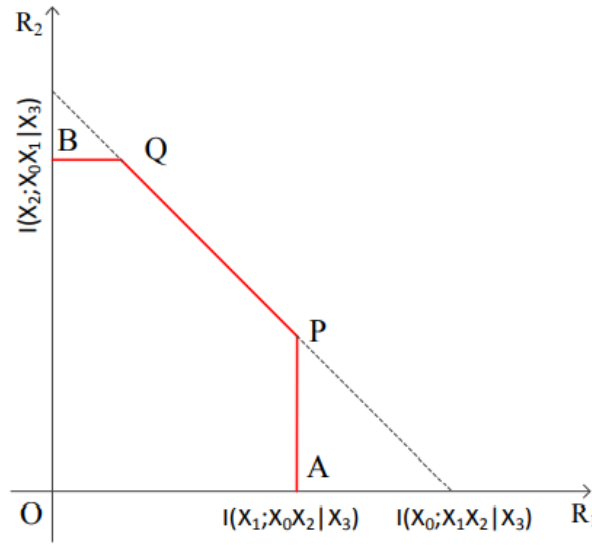


Figure 5.2 The key capacity region for symmetric key generation with an untrusted helper

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 $I(X_1; X_0X_2|X_3) \leq R_A$, $I(X_2; X_0X_1|X_3) \leq R_B$ and $I(X_0; X_1X_2|X_3) \leq R_C$. 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 $(I(X_1; X_0X_2|X_3), H(X_2|X_1X_3) - H(X_2|X_0X_3))$. The idea to achieve the point P follows the 9 unified strategy i.e., public discussion first guarantees that terminal X_0 recovers X_{n1} , X_{n2} and X_{n3} correctly, and then K_1 is generated by terminals X_0 and X_1 based on X_{n1} , and K_2 is generated by terminals X_0 and X_2 based on X_{n2} .

Since the generated keys should be concealed from the helper terminal X_3 , X_{n-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 K_1 needs to be maximized, terminal X_1 should reveal as little information as possible. Hence, terminals X_2 and X_3 first reveal information at the rate $R_2 + R_3 = H(X_2X_3|X_0)$ so that terminal X_1 needs to release only at the rate $R_1 = H(X_1|X_0X_2X_3)$ in order for X_0 to recover X_{n-1} . Thus, the rate of K_1 can be as large as $I(X_1; X_0X_2|X_3)$. Since X_3 is an untrusted helper, it can reveal information at any rate. Hence, R_2 can be set to be $H(X_2|X_0X_3)$. Consequently, $R_2 = H(X_2|X_1X_3) - H(X_2|X_0X_3)$. Since the generation of K_1 already uses up information contained in X_{n-1} , K_2 can be generated only based on information contained in X_{n-2} given X_{n-1} and X_{n-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 X_1 , X_2 and X_3 reveal information to public such that terminal X_0 can recover $(X_{n-1}, X_{n-2}, X_{n-3})$ correctly. Then K_1 is generated based on X_{n-1} and K_2 is generated based on X_{n-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 X_1 , X_2 and X_3 reveal information to public, respectively.

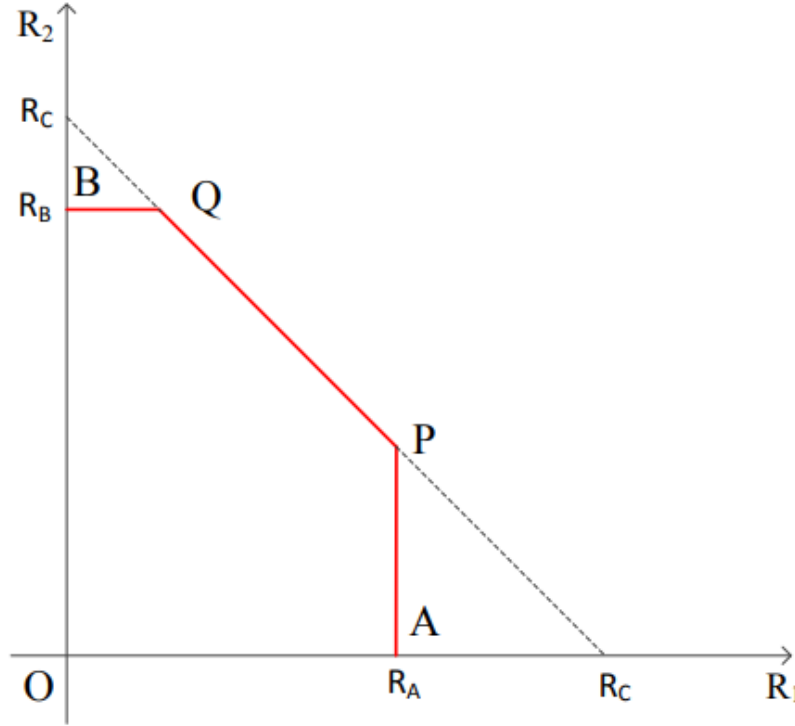


Figure 5.3 The key capacity region for asymmetric key generation with a trusted helper

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 R_1 of K_1 due to the same secrecy requirement for K_1 . Furthermore, since both models should exhaust all random resource in X_{n-1} for generating K_1 , K_2 should be generated from random resource independent from X_{n-1} even if it is not required to be concealed from terminal X_1 in symmetric key generation.

Thus, the two models also have the same rate R_2 at the point P. For the point Q, the rate coordinates are given by $(R_C - R_0 B, R_0 B)$. Corresponding to different source distributions, each of R_C and $R_0 B$ 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 $R_C = I(X_0; X_1 X_2 X_3)$ and $R_0 B = I(X_0; X_2 X_3 | X_1)$; case 2 with $R_C = I(X_0; X_1 X_2 X_3)$ and $R_0 B = I(X_2; X_0 X_3 | X_1)$; case 3 with $R_C = I(X_0 X_3; X_1 X_2)$ and $R_0 B = I(X_0; X_2 X_3 | X_1)$; and case 4 with $R_C = I(X_0 X_3; X_1 X_2)$ and $R_0 B = I(X_2; X_0 X_3 | X_1)$. 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 $(I(X_0; X_1), I(X_0; X_2X_3|X_1))$. In order to generate K_1 at the rate $I(X_0; X_1)$, terminal X_1 can reveal information at the rate $R_1 = H(X_1|X_0)$. Then terminal X_0 can recover X_{n1} correctly. In order for terminal X_0 to further recover (X_{n2}, X_{n3}) , terminals X_2 and X_3 jointly release information at the sum rate $R_2 + R_3 = H(X_2X_3|X_0X_1)$. Since the resource to generate K_2 should be contained in (X_{n2}, X_{n3}) given X_{n1} , the key rate R_2 should satisfy $R_2 = H(X_2X_3|X_1) - R_2 - R_3$ which yields $R_2 = I(X_0; X_2X_3|X_1)$.

Case 2. The key rate pair of the point Q is given by $(I(X_0; X_1X_3) - I(X_2; X_3|X_1), I(X_2; X_0X_3|X_1))$. Terminals X_1 and X_3 first jointly reveal information at the sum rate $R_1 + R_3 = H(X_1X_3|X_0)$. Then terminal X_0 recovers X_{n1} and X_{n3} correctly. Terminal X_2 needs to release information only at the rate $R_2 = H(X_2|X_0X_1X_3)$ and then X_{n2} can be successfully recovered at X_0 . Thus, K_2 can be generated at the rate $H(X_2|X_1) - H(X_2|X_0X_1X_3)$, which yields $R_2 = I(X_2; X_0X_3|X_1)$. In order to generate K_1 at the rate $R_1 = I(X_0; X_1X_3) - I(X_2; X_3|X_1)$, R_1 should be chosen to be $R_1 = H(X_1X_3|X_0) - H(X_3|X_1X_2)$, and then $R_3 = H(X_3|X_1X_2)$.

Case 3. This case does not exist because of the contradiction induced by setting $R_C = I(X_0X_3; X_1X_2)$ and $R_{0B} = I(X_0; X_2X_3|X_1)$.

Case 4. The key rate pair of the point Q is given by $(I(X_1; X_0X_3), I(X_2; X_0X_3|X_1))$. Still, terminals X_1 and X_3 first reveal information at the sum rate $R_1 + R_3 = H(X_1X_3|X_0)$. Due to the case conditions, X_3 has high correlation with X_0 and hence let X_3 reveal its information at the rate $R_3 = H(X_3|X_0)$. Then X_1 reveals its information at the rate $R_1 = H(X_1|X_0X_3)$, and finally X_2 reveals its information at the rate $R_2 = H(X_2|X_0X_1X_3)$ in order for X_0 to recover (X_{n1}, X_{n2}, X_{n3}) . Thus, the key rate $R_2 = I(X_0X_3; X_2|X_1)$, and the rate $R_1 = I(X_0X_3; X_1)$.

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 K_2 decreases in the asymmetric model due to the additional secrecy requirement for K_2 to be concealed from X_1 , the random resource contained in X_{n1} can still be used for generating K_1 so that there is no loss in the sum rate.

4. Generation of Asymmetric Key with an Untrusted Helper

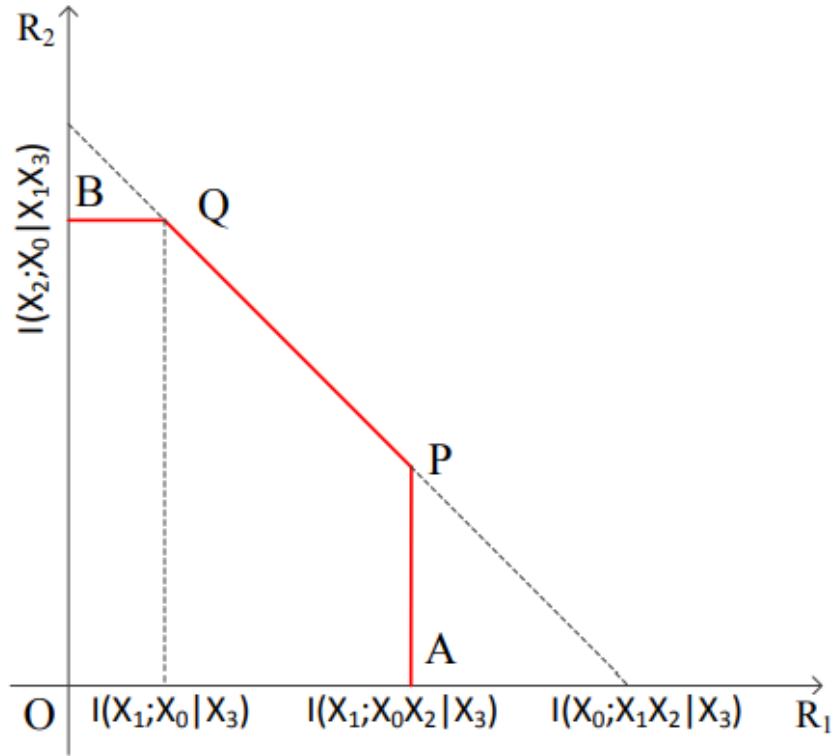


Figure 5.4 The key capacity region for asymmetric key generation with an untrusted helper.

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 $I(X_1; X_0X_2|X_3) \leq R_A$, $I(X_2; X_0|X_1X_3) \leq R_0$ and $I(X_0; X_1X_2|X_3) \leq R_C$. 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 $(I(X_0; X_1|X_3), I(X_2; X_0|X_1X_3))$. Terminals X_1 and X_3 first reveal information at the rate $R_1 + R_3 = H(X_1X_3|X_0)$ so that terminal X_0 can recover X_1 and X_3 correctly. Then terminal X_2 needs to release only at the rate $R_2 = H(X_2|X_0X_1X_3)$ in order for X_0 to recover X_2 . Thus, the rate of K_2 can be as large as $I(X_2; X_0|X_1X_3)$. Since X_3 is an untrusted helper, it can reveal information at any rate. Hence, R_1 can be set to be $H(X_1|X_0X_3)$. Consequently, $R_1 = H(X_1|X_3) - H(X_1|X_0X_3) = I(X_0; X_1|X_3)$.

CHAPTER- 6:

Proof of Theorem 1:

Proof of Converse. First, if we need only to generate K_1 , the model reduces to the secret key generation problem, the key capacity is shown to be $\min \{R_A, R_C\}$, which provides an upper bound (10) on R_1 . Similarly, if we dedicate to generate K_2 , the key capacity is shown to be $\min \{R_B, R_C\}$, which provides an upper bound (11) on R_2 . For the sum rate bound, we consider an enhanced model by replacing terminals X_1 and X_2 with a super terminal X_s that observes both X_{n1} and X_{n2} . The secret key rate between X_0 and X_s is upper bounded by R_C .

Proof of Achievability. We design an achievable scheme to achieve the key capacity region plotted as the pentagon O-A-P-Q-B-O, where the coordinates of the points A and B are $(\min \{R_A, R_C\}, 0)$ and $(0, \min \{R_B, R_C\})$, respectively. The corner point A is achieved by letting X_2 be a dedicated helper to generate K_1 following the omniscience scheme. Similarly, the corner point B is achieved by letting X_1 be a dedicated helper to generate K_2 . We note that the point P would collapse to the point A if $R_C \leq R_A$ and the point Q would collapse to the point B if $R_C \leq R_B$. It is thus sufficient to show that the points P and Q are achievable whenever they are different from the points A and B, respectively. Then the entire pentagon can be achieved by time sharing.

We note that since the secrecy constraints on K_1 and K_2 are symmetric, it is sufficient to show that the corner point P is achievable, and the achievability of the point Q follows by symmetry. We assume that $R_A < R_C$, because otherwise the point P would collapse to the point A and has been justified to be achievable. The key rate pair of the point P can take different forms due to different source distributions. In the following, we first describe a unified scheme that is applicable to all cases, and then study each case one by one. In general, our scheme is based on random binning and joint decoding.

Codebook Generation: At terminal X_1 , randomly and independently assign a bin index f to each sequence $x_{n1} \in X_{n1}$, where $f \in [1: 2^{nR_1}]$. We use $f(x_{n1})$ to denote the bin index of the sequence x_{n1} , and use $B_1(f)$ to denote the bin indexed by f . Then randomly and independently assign a sub-bin index ϕ to each sequence in each nonempty bin $B_1(f)$, where $\phi \in [1: 2^{nR_1}]$. We further use $B_1(f, \phi)$ to denote the sub-bin indexed by ϕ within the bin $B_1(f)$. At terminal X_2 , randomly and independently assign a bin index g to each sequence $x_{n2} \in X_{n2}$, where $g \in [1: 2^{nR_2}]$. We use $g(x_{n2})$ to denote the bin index of the sequence x_{n2} , and use $B_2(g)$ to denote the bin indexed by g .

Then randomly and independently assign a sub-bin index ψ to each sequence in each nonempty bin $B_2(g)$, where $\psi \in [1: 2^{nR_2}]$. We further use $B_2(g, \psi)$ to denote the sub-bin indexed by ψ within the bin $B_2(g)$. At terminal X_3 , randomly and independently assign a bin index l to each sequence $x_{n3} \in X_{n3}$, where $l \in [1: 2^{nR_3}]$. We use $l(x_{n3})$ to denote the bin index of the sequence x_{n3} , and use $B_3(l)$ to denote the bin indexed by l . The codebook is revealed to all parties, i.e., terminals X_0, X_1, X_2, X_3 and the eavesdropper.

Encoding and Transmission: Given a sequence x_{n1} , terminal X_1 finds the index pair (f, ϕ) such that $x_{n1} \in B_1(f, \phi)$. Then it reveals the index $f = f(x_{n1})$ over the public channel to all parties. Given a sequence x_{n2} , terminal X_2 finds the index pair (g, ψ) such that $x_{n2} \in B_2(g, \psi)$. Then it reveals the index $g = g(x_{n2})$ over the public channel to all parties. Given a sequence x_{n3} , terminal X_3 finds the index l such that $x_{n3} \in B_3(l)$. Then it reveals the index $l = l(x_{n3})$ over the public channel to all parties.

Decoding: The decoding scheme is based on joint typicality. Terminal X_0 , given x_{n0} and the bin indexes f, g and l , claims $\hat{x}_{n1}, \hat{x}_{n2}$ and \hat{x}_{n3} are observations of terminals X_1, X_2 and X_3 , respectively, if there exists a unique tuple of sequences $(\hat{x}_{n1}, \hat{x}_{n2}, \hat{x}_{n3})$ such that $\hat{x}_{n1} \in B_1(f), \hat{x}_{n2} \in B_2(g), \hat{x}_{n3} \in B_3(l)$, and $(x_{n0}, \hat{x}_{n1}, \hat{x}_{n2}, \hat{x}_{n3}) \in T_{\epsilon}(n)(P_{X_0 X_1 X_2 X_3})$.

Based on Slepian-Wolf coding theorem [5, 15], the decoding error can be arbitrarily small if the rates R_1, R_2 and R_3 satisfy the following Slepian-Wolf conditions:

$$R_1 > H(X_1|X_0 X_2 X_3), \quad (23)$$

$$R_2 > H(X_2|X_0 X_1 X_3), \quad (24)$$

$$R_3 > H(X_3|X_0 X_1 X_2), \quad (25)$$

$$R_1 + R_2 > H(X_1 X_2|X_0 X_3), \quad (26)$$

$$R_1 + R_3 > H(X_1 X_3|X_0 X_2), \quad (27)$$

$$R_2 + R_3 > H(X_2 X_3|X_0 X_1), \quad (28)$$

$$R_1 + R_2 + R_3 > H(X_1 X_2 X_3|X_0). \quad (29)$$

Key Generation: Terminal X1 sets $K_1 = \varphi(X_{n1})$. Terminal X2 sets $K_2 = \psi(X_{n2})$. Terminal X0 sets $\hat{K}_1 = \varphi(\hat{X}_{n1})$ and $\hat{K}_2 = \psi(\hat{X}_{n2})$. If the decoding error vanishes asymptotically (i.e., (23)-(29) are satisfied), we have

$$\Pr\{K_1 = \hat{K}_1\} > 1 - \epsilon, \quad (30)$$

$$\Pr\{K_2 = \hat{K}_2\} > 1 - \epsilon. \quad (31)$$

Secrecy: We derive the sufficient conditions for achieving the secrecy requirement (4). Then these sufficient conditions need to be verified for each of the four cases later on. We evaluate the key leakage rates averaged over the random codebook ensemble. Let $f := f(X_{n1})$, $g := g(X_{n2})$ and $l := l(X_{n3})$. Then it is clear that $F = \{f, g, l\}$. We further let $\varphi := \varphi(X_{n1})$ and $\psi := \psi(X_{n2})$. Hence, $K_1 = \varphi$ and $K_2 = \psi$. We first derive

$$\begin{aligned} I(K_1 K_2; F|C) &= I(\varphi, \psi; f, g, l|C) \\ &= I(\psi; f, g, l|C) + I(\varphi; f, g, l|\psi, C) \\ &\leq I(\psi; g|C) + I(\psi; f, l|g, C) + I(\varphi; f, g, \psi, l|C) \\ &\leq I(\psi; g|C) + I(g, \psi; f, l|C) + I(\varphi; f|C) + I(\varphi; g, \psi, l|f, C) \\ &\leq I(\psi; g|C) + I(g, \psi; f, l|C) + I(\varphi; f|C) + I(f, \varphi; g, \psi, l|C). \end{aligned}$$

(32) We next consider each of the four terms in (32). If

$$\tilde{R}_1 + R_1 < H(X_1) - 2\delta(\epsilon), \quad (33)$$

$$\frac{1}{n} I(\phi; f|C) < \delta(\epsilon); \quad (34)$$

$$\tilde{R}_2 + R_2 < H(X_2) - 2\delta(\epsilon), \quad (35)$$

$$\frac{1}{n} I(\psi; g|C) < \delta(\epsilon). \quad (36)$$

In order to bound the second term in (32), we have the following derivation:

$$\begin{aligned} I(g, \psi; f, l|C) &\leq I(X_{n2}, g, \psi; f, l|C) \\ &= I(X_{n2}; f, l|C) \\ &= I(X_{n2}; X_{n1}, X_{n3}|C) - I(X_{n2}; X_{n1}, X_{n3}|f, l, C) \\ &= H(X_{n1}, X_{n3}|C) - H(X_{n1}, X_{n3}|X_{n2}, C) - H(X_{n1}, X_{n3}|f, l, C) \\ &\quad + H(X_{n1}, X_{n3}|X_{n2}, f, l, C) \\ &\leq H(X_{n1}, X_{n3}|C) - H(X_{n1}, X_{n3}|X_{n2}, C) \\ &\quad - [H(X_{n1}, X_{n3}|C) - n\tilde{R}_1 - n\tilde{R}_3] + H(X_{n1}, X_{n3}|X_{n2}, f, l, C) \\ &\leq n[\tilde{R}_1 + \tilde{R}_3 - H(X_1 X_3|X_2)] + H(X_{n1}, X_{n3}|X_{n2}, f, l, C). \end{aligned}$$

It can be shown that if

$$\tilde{R}_1 + \tilde{R}_3 \leq H(X_1 X_3 | X_2) - 2\delta(\epsilon), \quad (37)$$

then

$$\limsup_{n \rightarrow \infty} \frac{1}{n} H(X_1^n, X_3^n | X_2^n, f, l, C) < H(X_1 X_3 | X_2) - \tilde{R}_1 - \tilde{R}_3 + \delta(\epsilon). \quad (38)$$

Consequently,

$$\frac{1}{n} I(g, \psi; f, l | C) < \delta(\epsilon). \quad (39)$$

Next, we consider the last term in (32) as follows:

$$\begin{aligned} I(f, \phi; g, \psi, l | C) &\leq I(X_{n-1}; g, \psi, l | C) \\ &= I(X_{n-1}; X_{n-2}, X_{n-3}, g, \psi, l | C) - I(X_{n-1}; X_{n-2}, X_{n-3} | g, \psi, l, C) \\ &= I(X_{n-1}; X_{n-2}, X_{n-3} | C) - I(X_{n-1}; X_{n-2}, X_{n-3} | g, \psi, l, C) \\ &= H(X_{n-2}, X_{n-3} | C) - H(X_{n-2}, X_{n-3} | X_{n-1}, C) - H(X_{n-2}, X_{n-3} | g, \psi, l, C) \\ &\quad + H(X_{n-2}, X_{n-3} | X_{n-1}, g, \psi, l, C) \\ &\leq n [\tilde{R}_2 + R_2 + \tilde{R}_3 - H(X_2 X_3 | X_1)] + H(X_{n-2}, X_{n-3} | X_{n-1}, g, \psi, l, C). \end{aligned} \quad (40)$$

It can be shown that if

$$\tilde{R}_2 + R_2 + \tilde{R}_3 < H(X_2 X_3 | X_1) - 2\delta(), \quad (41)$$

then

$$\limsup_{n \rightarrow \infty} \frac{1}{n} H(X_{n-2}, X_{n-3} | X_{n-1}, g, \psi, l, C) < H(X_2 X_3 | X_1) - \tilde{R}_2 - R_2 - \tilde{R}_3 + \delta().$$

Consequently,

$$\frac{1}{n} I(f, \phi; g, \psi, l | C) < \delta(\epsilon). \quad (42)$$

Therefore, (33), (35), (37) and (41) are sufficient conditions that guarantee the secrecy requirement (4)

Uniformity: Uniformity of keys is due to properties of random binning and typicality. We next show the achievability of the point P with rate coordinates $R_1 = R_A$ and $R_2 = R_C - R_A$. Corresponding to different source distributions, each of R_A and R_C can take one of the two mutual information terms given in (9a) and (9c), respectively. Hence, the coordinates of the point P can take four forms.

Which are case 1 with $RA = I(X_1; X_0X_2X_3)$ and $RC = I(X_0; X_1X_2X_3)$, case 2 with $RA = I(X_1; X_0X_2X_3)$ and $RC = I(X_0X_3; X_1X_2)$, case 3 with $RA = I(X_0X_2; X_1X_3)$ and $RC = I(X_0; X_1X_2X_3)$, and case 4 with $RA = I(X_0X_2; X_1X_3)$ and $RC = I(X_0X_3; X_1X_2)$. For each case, it is sufficient to set the rates $\tilde{R}_1, R_1, \tilde{R}_2, R_2$ and \tilde{R}_3 to satisfy the Slepian-Wolf conditions (23)-(29) for guaranteeing correct key agreement and to satisfy the sufficient conditions (33), (35), (37) and (41) for guaranteeing secrecy.

Case 1:

$RA = I(X_1; X_0X_2X_3)$ and $RC = I(X_0; X_1X_2X_3)$, which imply

$$H(X_3|X_0X_2) < H(X_3|X_1), \quad (43)$$

$$H(X_3|X_1X_2) < H(X_3|X_0). \quad (44)$$

Moreover, $RA < RC$ implies

$$H(X_2X_3|X_0) < H(X_2X_3|X_1). \quad (45)$$

The rate pair at the point P is given by $(I(X_1; X_0X_2X_3), H(X_2X_3|X_1) - H(X_2X_3|X_0))$. To achieve this rate pair, we set the binning rates in the achievable strategy as follows:

$$\tilde{R}_1 = H(X_1|X_0X_2X_3) + \epsilon, \quad (46)$$

$$R_1 = I(X_1; X_0X_2X_3) - 2\delta(\epsilon) - 2\epsilon, \quad (47)$$

$$\tilde{R}_2 = H(X_2X_3|X_0) - \tilde{R}_3 + \epsilon, \quad (48)$$

$$R_2 = H(X_2X_3|X_1) - H(X_2X_3|X_0) - 4\delta(\epsilon) - 3\epsilon, \quad (49)$$

$$\tilde{R}_3 = \min\{H(X_3|X_2), H(X_3|X_0)\} - 2\delta(\epsilon) - 2\epsilon. \quad (50)$$

It can be verified that the above rates satisfy the Slepian-Wolf conditions (23)-(29) if $\tilde{R}_3 > H(X_3|X_0X_1X_2)$. Otherwise, either the Markov chain $X_3 - X_0 - X_1X_2$ or the Markov chain $X_3 - X_2 - X_0X_1$ holds and thus the rate pair can be easily achieved without the 18 helper's assistance. It can also be verified that the above rates (46)-(50) satisfy the sufficient conditions (33), (35), (37) and (41) for secrecy.

Case 2:

$RA = I(X_1; X_0X_2X_3)$ and $RC = I(X_0X_3; X_1X_2)$, which imply the following two inequalities:

$$H(X_3|X_0X_2) < H(X_3|X_1), \quad (51)$$

$$H(X_3|X_0) < H(X_3|X_1X_2). \quad (52)$$

Here, $RA < RC$ is equivalent to

$$H(X_2|X_0X_3) < H(X_2|X_1). \quad (53)$$

The key rate pair at the point P in this case is given by $(I(X_1; X_0X_2X_3), H(X_2|X_1) - H(X_2|X_0X_3))$.

To achieve this rate pair, we set the binning rates in the achievable strategy as follows:

$$\tilde{R}_1 = H(X_1|X_0X_2X_3) + \epsilon, \quad (54)$$

$$R_1 = I(X_1; X_0X_2X_3) - 2\delta(\epsilon) - 2\epsilon, \quad (55)$$

$$\tilde{R}_2 = H(X_2|X_0X_3) + \epsilon, \quad (56)$$

$$R_2 = H(X_2|X_1) - H(X_2|X_0X_3) - 2\delta(\epsilon) - 2\epsilon, \quad (57)$$

$$\tilde{R}_3 = H(X_3|X_0) + \epsilon. \quad (58)$$

It can be verified that the above rates satisfy the Slepian-Wolf conditions (23)-(29) and the sufficient conditions (33), (35), (37) and (41) for secrecy. In particular, (37) holds due to (52) as follows:

$$\begin{aligned} \tilde{R}_1 + \tilde{R}_3 &= H(X_1|X_0X_2X_3) + H(X_3|X_0) + 2\epsilon \\ &< H(X_1|X_2X_3) + H(X_3|X_1X_2) - 2\delta(\epsilon) \\ &< H(X_1X_3|X_2) - 2\delta(\epsilon), \end{aligned}$$

and (41) holds due to (52) as follows:

$$\begin{aligned} \tilde{R}_2 + R_2 + \tilde{R}_3 &= H(X_3|X_0) + H(X_2|X_1) - 2\delta(\epsilon) - \epsilon \\ &< H(X_3|X_1X_2) + H(X_2|X_1) - 2\delta(\epsilon) \\ &< H(X_2X_3|X_1) - 2\delta(\epsilon). \end{aligned}$$

Case 3: $R_A = I(X_0X_2; X_1X_3)$ and $R_C = I(X_0; X_1X_2X_3)$, which imply the following two inequalities:

$$H(X_3|X_0X_2) > H(X_3|X_1), \quad (59)$$

$$H(X_3|X_0) > H(X_3|X_1X_2), \quad (60)$$

Here, $R_A < R_C$ is equivalent to

$$H(X_2|X_0) < H(X_2|X_1X_3). \quad (61)$$

The rate pair of the point P is given by $(I(X_0X_2; X_1X_3), H(X_2|X_1X_3) - H(X_2|X_0))$. To achieve this rate pair, we set the binning rates as follows:

$$\tilde{R}_1 = H(X_1X_3|X_0X_2) - H(X_3|X_1) + \epsilon, \quad (62)$$

$$R_1 = I(X_0X_2; X_1X_3) - 2\delta(\epsilon) - 2\epsilon, \quad (63)$$

$$\tilde{R}_2 = H(X_2|X_0) + \epsilon, \quad (64)$$

$$R_2 = H(X_2|X_1X_3) - H(X_2|X_0) - 2\delta(\epsilon) - 2\epsilon, \quad (65)$$

$$\tilde{R}_3 = H(X_3|X_1) + \epsilon. \quad (66)$$

It can be verified that the above rates satisfy the Slepian-Wolf conditions (23)-(29). It is also easy to verify that the rate settings (62)-(66) satisfy the sufficient conditions (33), (35) and (41) for secrecy. Furthermore, the condition (37) is satisfied if

$$H(X_1X_3|X_0X_2) < H(X_1X_3|X_2). \quad (67)$$

Otherwise, the Markov chain $X_1X_3 - X_2 - X_0$ holds. To show the secrecy, we derive a new condition to replace (37) to guarantee that $I(g, \psi; f, l|C)$ is asymptotically small as follows.

$$\begin{aligned} I(g, \psi; f, l|C) &\leq I(g, \psi; X_{n-1}, X_{n+3}|C) \\ &= I(X_{n+2}; X_{n-1}, X_{n+3}|C) - I(X_{n+2}; X_{n-1}, X_{n+3}|g, \psi, C) \\ &= H(X_{n+2}|C) - H(X_{n+2}|X_{n-1}, X_{n+3}, C) - H(X_{n+2}|g, \psi, C) \\ &\quad + H(X_{n+2}|X_{n-1}, X_{n+3}, g, \psi, C) \\ &\leq n[R_2 + R_2 - H(X_2|X_1X_3)] + H(X_{n+2}|X_{n-1}, X_{n+3}, g, \psi, C). \end{aligned}$$

It can be shown that if

$$\tilde{R}_2 + R_2 \leq H(X_2|X_1X_3) - 2\delta(\epsilon), \quad (68)$$

then

$$\limsup_{n \rightarrow \infty} \frac{1}{n} H(X_2^n|X_1^n, X_3^n, f, l, \mathcal{C}) < H(X_2|X_1X_3) - \tilde{R}_2 - R_2 + \delta(\epsilon). \quad (69)$$

Thus, $I(g, \psi; f, l|C) < \delta()$. It is clear that the rates given in (62)-(66) satisfy (68) and hence secrecy is guaranteed.

Case 4: $R_A = I(X_0X_2; X_1X_3)$ and $R_C = I(X_0X_3; X_1X_2)$, which imply the following two inequalities:

$$H(X_3|X_0X_2) > H(X_3|X_1), \quad (70)$$

$$H(X_3|X_1X_2) > H(X_3|X_0), \quad (71)$$

Then, we have $H(X_3|X_1) < H(X_3|X_0X_2) \leq H(X_3|X_0) < H(X_3|X_1X_2)$, which yields a contradiction.

Thus, this case does not exist.

Proof of Theorem 2

Proof of Converse. First, if we need only to generate K_1 , the model reduces to the private key generation problem. The key capacity is shown to be

$$R_1 = \min \{I(X_1; X_0X_2|X_3), I(X_0; X_1X_2|X_3)\}, \quad (13)$$

which provides an outer bound (13) on R_1 . Similarly, if we dedicated to generating K_2 , the key capacity is shown to be $R_2 = \min \{I(X_2; X_0X_1|X_3), I(X_0; X_1X_2|X_3)\}$, which provides an outer bound (14) on R_2 . For the sum rate bound, we consider an enhanced model by replacing terminals X_1 and X_2 with a super terminal X_s which observes both X_{n1} and X_{n2} . The rate of the private key between X_0 and X_s concealed from terminal X_3 is upper bounded by $I(X_0; X_1, X_2|X_3)$, which yields the sum rate bound (15).

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 $\min \{I(X_1; X_0X_2|X_3), I(X_0; X_1X_2|X_3)\}$ and $\min \{I(X_2; X_0X_1|X_3), I(X_0; X_1X_2|X_3)\}$, respectively. The corner point A can be achieved by letting X_2 be a dedicated helper to generate K_1 following the omniscience. The corner point B can be achieved by letting X_1 be a dedicated helper to generate K_2 .

We note that the point P would collapse to the point A if $I(X_0; X_1X_2|X_3) \leq I(X_1; X_0X_2|X_3)$ and the point Q would collapse to the point B if $I(X_0; X_1X_2|X_3) \leq I(X_2; X_0X_1|X_3)$. 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 K_1 and K_2 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 $I(X_1; X_0X_2|X_3) < I(X_0; X_1X_2|X_3)$, which implies

$$H(X_2|X_0X_3) < H(X_2|X_1X_3), \quad (72)$$

because otherwise the point P would collapse to the point A and has been justified to be achievable. The rate pair at the point P is given by $(I(X_1; X_0X_2|X_3), H(X_2|X_1X_3) - H(X_2|X_0X_3))$. The idea to achieve the point P follows the same achievable strategy. The steps of codebook generation, encoding and transmission, decoding and key generation are the same as the corresponding steps, and are omitted here. In particular, Slepian-Wolf conditions (23)-(29) also guarantee the correct key establishment here.

The secrecy requirement (5) here is different from that for symmetric key generation with a trusted helper. Hence, we next develop the sufficient conditions that guarantee (5) and then choose the binning rates to satisfy these sufficient conditions.

Secrecy: We evaluate the key leakage rates averaged over the random codebook ensemble. 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 $\phi := \phi(X_n 1)$ and $\psi := \psi(X_n 2)$. Hence, $K_1 = \phi$ and $K_2 = \psi$. We first derive

$$\begin{aligned}
& I(K_1, K_2; X_{n-3}, F|C) \\
&= I(\phi, \psi; f, g, l, X_{n-3} | C) \\
&= I(\phi; f, g, X_{n-3} | C) + I(\psi; f, g, X_{n-3} | \phi, C) \\
&\leq I(\phi; f|C) + I(\phi, f; g, X_{n-3} | C) + I(\psi; \phi, f, g, X_{n-3} | C) \\
&\leq I(\phi; f|C) + I(\phi, f; g, X_{n-3} | C) + I(\psi; g|C) + I(\psi, g; \phi, f, X_{n-3} | C) \\
&\leq I(\phi; f|C) + I(\phi, f; X_{n-3} | C) + I(\phi, f; g|X_{n-3}, C) \\
&\quad + I(\psi; g|C) + I(\psi, g; X_{n-3} | C) + I(\psi, g; \phi, f|X_{n-3}, C). \quad (73)
\end{aligned}$$

We consider each of the six terms in (73). Similarly, to the techniques, it can be shown that if

$$\tilde{R}_1 + R_1 < H(X_1) - 2\delta(\epsilon), \quad (74)$$

$$\text{then} \quad \frac{1}{n} I(\phi; f|C) < \delta(\epsilon); \quad (75)$$

$$\text{and if} \quad \tilde{R}_2 + R_2 < H(X_2) - 2\delta(\epsilon), \quad (76)$$

$$\text{then} \quad \frac{1}{n} I(\psi; g|C) < \delta(\epsilon). \quad (77)$$

In order to bound the second term in (73), we have the following derivation:

$$\begin{aligned}
& I(\phi, f; X_{n-3} | C) \\
&= I(X_{n-1}; X_{n-3} | C) - I(X_{n-1}; X_{n-3} | \phi, f, C) \\
&= H(X_{n-1} | C) - H(X_{n-1} | X_{n-3}, C) - H(X_{n-1} | \phi, f, C) + H(X_{n-1} | \phi, f, X_{n-3}, C) \\
&\leq n[R_1 + R_1 - H(X_1|X_3)] + H(X_{n-1} | \phi, f, X_{n-3}, C).
\end{aligned}$$

It can be shown as in [10, Appendix A] that if

$$\tilde{R}_1 + R_1 \leq H(X_1|X_3) - 2\delta(\epsilon), \quad (78)$$

$$\text{then} \quad \limsup_{n \rightarrow \infty} \frac{1}{n} H(X_1^n | \phi, f, X_3^n, C) < H(X_1|X_3) - \tilde{R}_1 - R_1 + \delta(\epsilon). \quad (79)$$

$$\text{Consequently,} \quad \frac{1}{n} I(\phi, f; X_3^n | C) < \delta(\epsilon). \quad (80)$$

Similarly, it can be shown that if

$$\tilde{R}_2 + R_2 \leq H(X_2|X_3) - 2\delta(\epsilon), \quad (81)$$

$$\text{then} \quad \frac{1}{n} I(\psi, g; X_3^n | C) < \delta(\epsilon). \quad (82)$$

By noting that $I(\varphi, f; g|X_{n-3}, C) \leq I(\psi, g; \varphi, f|X_{n-3}, C)$, it is sufficient to bound the latter term:

$$\begin{aligned}
& I(\psi, g; \varphi, f|X_{n-3}, C) \\
& \leq I(\psi, g; X_{n-1}|X_{n-3}, C) \\
& = I(X_{n-2}; X_{n-1}|X_{n-3}, C) - I(X_{n-2}; X_{n-1}|g, \psi, X_{n-3}, C) \\
& = H(X_{n-2}|X_{n-3}, C) - H(X_{n-2}|X_{n-1}, X_{n-3}, C) - H(X_{n-2}|g, \psi, X_{n-3}, C) \\
& \quad + H(X_{n-2}|g, \psi, X_{n-1}, X_{n-3}, C) \\
& \leq n[R_2 + R_2 - H(X_2|X_1X_3)] + H(X_{n-2}|g, \psi, X_{n-1}, X_{n-3}, C). \quad (83)
\end{aligned}$$

$$\tilde{R}_2 + R_2 < H(X_2|X_1X_3) - 2\delta(\epsilon), \quad (84)$$

then

$$\limsup_{n \rightarrow \infty} \frac{1}{n} H(X_2^n|g, \psi, X_1^n, X_3^n, C) < H(X_2|X_1X_3) - \tilde{R}_2 - R_2 + \delta(\epsilon).$$

Consequently,

$$\frac{1}{n} I(f, \phi; g, \psi|X_3^n, C) < \delta(\epsilon). \quad (85)$$

Thus, (78) and (84) are sufficient conditions that guarantee the secrecy requirement (5). The rate pair at point P is given by $(I(X_1; X_0X_2|X_3), H(X_2|X_1X_3) - H(X_2|X_0X_3))$. To achieve this rate pair, we set the binning rates as follows:

$$\tilde{R}_1 = H(X_1|X_0X_2X_3) + \epsilon, \quad (86)$$

$$R_1 = I(X_1; X_0X_2|X_3) - 2\delta(\epsilon) - 2\epsilon, \quad (87)$$

$$\tilde{R}_2 = H(X_2|X_0X_3) + \epsilon, \quad (88)$$

$$R_2 = H(X_2|X_1X_3) - H(X_2|X_0X_3) - 2\delta(\epsilon) - 2\epsilon, \quad (89)$$

$$\tilde{R}_3 = H(X_3|X_0) + \epsilon. \quad (90)$$

It is easy to verify that the above rates satisfy the Slepian-Wolf conditions (23)-(29), and the sufficient conditions (78) and (84) for secrecy.

Proof of Theorem 3

Proof of Converse.

First, if we need only to generate K_1 , the model reduces to the secret key generation problem. The key capacity is shown to be $\min \{R_A, R_C\}$ which provides an upper bound on R_1 . Next, if we dedicate to generate K_2 , the model reduces to the private key generation problem over multiple terminals as the private key model.

The key capacity is shown to be $R_0 B$ which serves as an upper bound (18) on R_2 . For the sum rate bound, we consider an enhanced model, which replaces terminals X_1 and X_2 with a super terminal X_s that observes both X_{n1} and X_{n2} . Then, the secret key rate between X_0 and X_s is upper bounded by R_C as given in [5] for the secret key model, which yields the sum rate bound (19).

Proof of Achievability. The key capacity region is plotted as the pentagon $O-AP-Q-B-O$, where the coordinates of the points A and B are $(\min \{R_A, R_C\}, 0)$ and $(0, R_0 B)$, respectively. The corner point A is achieved by letting X_2 be a dedicated helper to generate K_1 following [5]. The corner point B is achieved by letting X_1 be a dedicated helper to generate K_2 following [5]. We note that the point P may collapse to the point A if $R_C \leq R_A$, and the point Q may collapse to the point B if $R_C \leq R_B$. It is thus sufficient to show the achievability of the points P and Q whenever they are different from the points A and B , respectively.

Then the entire pentagon can be achieved by time sharing. For the point P , it can be observed that its rate coordinates are exactly the same, can be shown to be achievable by the same scheme designed in Appendix A for symmetric key generation with a trusted helper. The idea to achieve the point Q follows the same achievable strategy as in Appendix A.

Hence, the steps of codebook generation, encoding and transmission, decoding and key generation are the same as the corresponding steps in Appendix A, and are omitted here. In particular, Slepian-Wolf conditions (23)-(29) guarantee the correct key establishment. The secrecy requirement (6) here is different. Hence, we next derive sufficient conditions for achieving secrecy requirement (6). Then these sufficient conditions need to be verified for the point Q in all cases.

Secrecy: We evaluate the key leakage rates averaged over the random codebook ensemble. 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, $K_1 = \varphi$ and $K_2 = \psi$. We first derive

$$\begin{aligned} I(K_1; F|C) &= I(\varphi; f, g, l|C) \\ &= I(\varphi; f|C) + I(\varphi; g, l|f, C) \\ &\leq I(\varphi; f|C) + I(\varphi, f; g, l|C), \end{aligned} \quad (91) \text{ and}$$

$$\begin{aligned} I(K_2; F, X_{n-1}|C) &= I(\psi; f, g, l, X_{n-1}|C) \\ &= I(\psi; g, l, X_{n-1}|C) \\ &= I(\psi; g|C) + I(\psi; l, X_{n-1}|g, C) \\ &\leq I(\psi; g|C) + I(\psi, g; l|C) + I(\psi, g, l; X_{n-1}|C). \end{aligned} \quad (92)$$

If

$$\tilde{R}_1 + R_1 < H(X_1) - 2\delta(\epsilon), \quad (93)$$

then

$$\frac{1}{n}I(\phi; f|C) < \delta(\epsilon); \quad (94)$$

and if

$$\tilde{R}_2 + R_2 < H(X_2) - 2\delta(\epsilon), \quad (95)$$

then

$$\frac{1}{n}I(\psi; g|C) < \delta(\epsilon). \quad (96)$$

Furthermore,

$$\begin{aligned} &I(g, \psi; l|C) \\ &\leq I(g, \psi, X_{n-2}; l|C) \\ &= I(X_{n-2}; l, X_{n-3}|C) - I(X_{n-2}; X_{n-3}|l, C) \\ &= I(X_{n-2}; X_{n-3}|C) - I(X_{n-2}; X_{n-3}|l, C) \\ &= H(X_{n-3}|C) - H(X_{n-3}|X_{n-2}, C) - H(X_{n-3}|l, C) + H(X_{n-3}|X_{n-2}, l, C) \\ &\leq H(X_{n-3}|C) - H(X_{n-3}|X_{n-2}, C) - [H(X_{n-3}|C) - n\tilde{R}^3] \\ &\quad + H(X_{n-3}|X_{n-2}, l, C) \\ &= n(\tilde{R}^3 - H(X_3|X_2)) + H(X_{n-3}|X_{n-2}, l, C) \end{aligned}$$

where we used the fact that $H(X_{n-3} | X_{n-2}, C) = nH(X_3|X_2)$ due to the assumption of discrete memoryless source.

If

$$\tilde{R}_3 \leq H(X_3|X_2) - 2\delta(\epsilon), \quad (97)$$

then

$$\limsup_{n \rightarrow \infty} \frac{1}{n} H(X_3^n | X_2^n, l, \mathcal{C}) < H(X_3|X_2) - \tilde{R}_3 + \delta(\epsilon). \quad (98)$$

Consequently,

$$\frac{1}{n} I(g, \psi; l | \mathcal{C}) < \delta(\epsilon). \quad (99)$$

We next consider the last term in (92):

$$\begin{aligned} & I(\psi, g, l; X_{n-1} | \mathcal{C}) \\ &= I(g, \psi, l, X_{n-2}, X_{n-3}; X_{n-1} | \mathcal{C}) - I(X_{n-2}, X_{n-3}; X_{n-1} | g, \psi, l, \mathcal{C}) \\ &= I(X_{n-2}, X_{n-3}; X_{n-1} | \mathcal{C}) - I(X_{n-2}, X_{n-3}; X_{n-1} | g, \psi, l, \mathcal{C}) \\ &\leq n(\tilde{R}_2 + R_2 + \tilde{R}_3 - H(X_2 X_3 | X_1)) + H(X_{n-2} X_{n-3} | X_{n-1}, g, \psi, l, \mathcal{C}). \end{aligned}$$

Similarly, it can be shown as that if

$$\tilde{R}_2 + R_2 + \tilde{R}_3 < H(X_2 X_3 | X_1) - 2\delta(\epsilon), \quad (100)$$

then

$$\limsup_{n \rightarrow \infty} \frac{1}{n} H(X_2^n X_3^n | X_1^n, g, \psi, l, \mathcal{C}) < H(X_2 X_3 | X_1) - \tilde{R}_2 - R_2 - \tilde{R}_3 + \delta(\epsilon).$$

Consequently,

$$\frac{1}{n} I(g, \psi, l; X_1^n | \mathcal{C}) < \delta(\epsilon). \quad (101)$$

Thus, (93), (95), (97) and (100) are sufficient conditions that guarantee the secrecy requirements in (6).

Uniformity: Uniformity of keys is due to properties of random binning and typicality.

We next show the achievability of the point Q, whose rate coordinates are given by $(R_C - R_0 B, R_0 B)$. Corresponding to different source distributions, each of R_C and $R_0 B$ can take one of the two mutual information terms given in (19) and (18), respectively.

Hence, the coordinates of the point Q can take four forms, i.e., case 1 with $R_C = I(X_0; X_1 X_2 X_3)$ and $R_0 B = I(X_0; X_2 X_3 | X_1)$; case 2 with $R_C = I(X_0; X_1 X_2 X_3)$ and $R_0 B = I(X_2; X_0 X_3 | X_1)$; case 3 with $R_C = I(X_0 X_3; X_1 X_2)$ and $R_0 B = I(X_0; X_2 X_3 | X_1)$; and case 4 with $R_C = I(X_0 X_3; X_1 X_2)$ and $R_0 B = I(X_2; X_0 X_3 | X_1)$.

For each case, it is sufficient to set the rates $\tilde{R}_1, R_1, \tilde{R}_2, R_2$ and \tilde{R}_3 to satisfy the Slepian-Wolf conditions (23)-(29) for guaranteeing correct key agreement and to satisfy the sufficient conditions (93), (95), (97) and (100) for guaranteeing secrecy.

Case 1: $R_C = I(X_0; X_1 X_2 X_3)$ and $R_0 B = I(X_0; X_2 X_3 | X_1)$, which imply

$$H(X_3 | X_1 X_2) < H(X_3 | X_0), \quad (102)$$

$$H(X_3 | X_1 X_2) < H(X_3 | X_0 X_1). \quad (103)$$

The rate pair at the point Q is given by $(I(X_0; X_1), I(X_0; X_2 X_3 | X_1))$. To achieve this rate pair, we set the binning rates in the achievable strategy as follows:

$$\tilde{R}_1 = H(X_1 | X_0) + \epsilon, \quad (104)$$

$$R_1 = I(X_0; X_1) - 2\delta(\epsilon) - 2\epsilon, \quad (105)$$

$$\tilde{R}_2 = H(X_2 X_3 | X_0 X_1) - H(X_3 | X_1 X_2) + 2\delta(\epsilon) + 2\epsilon, \quad (106)$$

$$R_2 = I(X_0; X_2 X_3 | X_1) - 4\delta(\epsilon) - 3\epsilon, \quad (107)$$

$$\tilde{R}_3 = H(X_3 | X_1 X_2) - 2\delta(\epsilon) - \epsilon. \quad (108)$$

It can be verified that the above rates satisfy the Slepian-Wolf conditions (23)-(29) if $\tilde{R}_3 > H(X_3 | X_0 X_1 X_2)$. Otherwise, the rate pair can be easily achieved without the helper's assistance.

It can also be verified that the above rates (104)-(108) satisfy the secrecy conditions (93), (95), (97) and (100).

Case 2: $R_C = I(X_0; X_1X_2X_3)$ and $R_0 = I(X_2; X_0X_3|X_1)$, which imply

$$H(X_3|X_1X_2) < H(X_3|X_0), \quad (109)$$

$$H(X_3|X_0X_1) < H(X_3|X_1X_2). \quad (110)$$

The rate pair at the point Q is given by $(I(X_0; X_1X_3) - I(X_2; X_3|X_1), I(X_2; X_0X_3|X_1))$. To achieve this rate pair, we set the binning rates in the achievable strategy as follows:

$$\tilde{R}_1 = H(X_1X_3|X_0) - H(X_3|X_1X_2) + \epsilon, \quad (111)$$

$$R_1 = I(X_0; X_1X_3) - I(X_2; X_3|X_1) - 2\delta(\epsilon) - 2\epsilon, \quad (112)$$

$$\tilde{R}_2 = H(X_2|X_0X_1X_3) + \epsilon, \quad (113)$$

$$R_2 = I(X_2; X_0X_3|X_1) - 4\delta(\epsilon) - 3\epsilon, \quad (114)$$

$$\tilde{R}_3 = H(X_3|X_1X_2) + \epsilon. \quad (115)$$

It can be verified that the above rates satisfy the Slepian-Wolf conditions (23)-(29). In particular, $\tilde{R}_1 > H(X_1|X_0X_2X_3)$ and $\tilde{R}_1 + \tilde{R}_2 > H(X_1X_2|X_0X_3)$ hold due to (109), and $\tilde{R}_2 + \tilde{R}_3 > H(X_2X_3|X_0X_1)$ holds due to (110).

It can also be verified that the above rates (111)-(115) satisfy the secrecy conditions (93), (95), (97) and (100). In particular, (97) holds under the following assumption

$$H(X_2|X_0X_1X_3) < H(X_2|X_1) - 2\delta(\epsilon) - 2\epsilon. \quad (116)$$

If the above assumption does not hold, then the Markov chain $X_2 - X_1 - X_0X_3$ holds, which implies $R_2 = I(X_2; X_0X_3|X_1) = 0$. The point Q coincides with the point B, which has been justified to be achievable.

Case 3: $R_C = I(X_0X_3; X_1X_2)$ and $R_0 = I(X_0; X_2X_3|X_1)$, which imply

$$H(X_3|X_0) \leq H(X_3|X_1X_2), \quad (117)$$

$$H(X_3|X_1X_2) \leq H(X_3|X_0X_1). \quad (118)$$

Then, we have $H(X_3|X_0) \leq H(X_3|X_1X_2) \leq H(X_3|X_0X_1)$, which yields contradiction. Thus, this case does not exist.

Case 4: $R_C = I(X_0X_3; X_1X_2)$ and $R_0 B = I(X_2; X_0X_3|X_1)$, which imply

$$H(X_3|X_0) \leq H(X_3|X_1X_2), \quad (119)$$

$$H(X_3|X_0X_1) < H(X_3|X_1X_2). \quad (120)$$

The rate pair at the point Q is given by $(I(X_1; X_0X_3), I(X_2; X_0X_3|X_1))$. To achieve this rate pair, we set the binning rates in the achievable strategy as follows:

$$\tilde{R}_1 = H(X_1|X_0X_3) + \epsilon, \quad (121)$$

$$R_1 = I(X_1; X_0X_3) - 2\delta(\epsilon) - 2\epsilon, \quad (122)$$

$$\tilde{R}_2 = H(X_2|X_0X_1X_3) + \epsilon, \quad (123)$$

$$R_2 = I(X_2; X_0X_3|X_1) - 2\delta(\epsilon) - 2\epsilon, \quad (124)$$

$$\tilde{R}_3 = H(X_3|X_0) + \epsilon. \quad (125)$$

It is easy to verify that the above rates satisfy the Slepian-Wolf conditions (23)-(29) and the secrecy conditions (93), (95), (97) and (100).

Proof of Theorem 4

Proof of Converse. First, if we need only to generate K_1 , the model reduces to the private key generation problem over multiple terminals. The key capacity is shown to be $\min \{I(X_1; X_0X_2|X_3), I(X_0; X_1X_2|X_3)\}$, which serves as an upper bound (20) on R_1 . Next, if we dedicate to generate K_2 , it also reduces to the private key model.

The key capacity is shown to be $I(X_2; X_0|X_1X_3)$, which serves an upper bound (21) on R_2 . For the sum rate bound, we consider an enhanced model which replaces terminals X_1 and X_2 with a super terminal X_s that observes both X_{n1} and X_{n2} . Then, the private key rate between X_0 and X_s is upper bounded by $I(X_0; X_1, X_2|X_3)$ due to the private key model, which yields the sum rate bound (22).

Proof of Achievability. The key capacity region as the pentagon O-AP-Q-B-O, where the coordinates of the points A and B are $(\min \{I(X_0; X_1X_2|X_3), I(X_1; X_0X_2|X_3)\}, 0)$ and $(0, I(X_0; X_2|X_1X_3))$, respectively. The corner point A is achieved by letting X_2 be a dedicated helper to generate K_1 following [5]. The corner point B is achieved by letting X_1 be a dedicated helper to generate K_2 following [5]. We note that the point P would collapse to the point A if $I(X_0; X_1X_2|X_3) \leq I(X_1; X_0X_2|X_3)$, and the point Q would collapse to the point B if $I(X_0; X_1X_2|X_3) \leq I(X_2; X_0|X_1X_3)$. It is thus sufficient to show the achievability of the points P and Q whenever they are different from the points A and B, respectively. Then the entire pentagon can be achieved by time sharing.

The idea to achieve the points P and Q follows the same achievable strategy described. The steps of codebook generation, encoding and transmission, decoding and key generation are the same as those in Appendix A, and are omitted here. In particular, Slepian-Wolf conditions (23)-(29) guarantee the correct key establishment. Since the secrecy requirements given in (7) are different, we next develop the sufficient conditions that guarantee (7), and then choose the binning rates to satisfy these sufficient conditions.

Secrecy: We evaluate the key leakage rates averaged over the random codebook ensemble. 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 $\phi := \phi(X_{n-1})$ and $\psi := \psi(X_{n-2})$. Hence, $K_1 = \phi$ and $K_2 = \psi$. We first derive

$$\begin{aligned} I(K_1; X_{n-3}, F|C) &= I(\phi; f, g, l, X_{n-3} | C) \\ &= I(\phi; f|C) + I(\phi; g, X_{n-3} | f, C) \\ &\leq I(\phi; f|C) + I(\phi, f; g, X_{n-3} | C) \\ &\leq I(\phi; f|C) + I(\phi, f; X_{n-3} | C) + I(\phi, f; g|X_{n-3}, C), \end{aligned} \quad (126)$$

and

$$\begin{aligned} I(K_2; X_{n-1}, X_{n-3}, F|C) &= I(\psi; f, g, l, X_{n-1}, X_{n-3} | C) \\ &= I(\psi; g, X_{n-1}, X_{n-3} | C) \\ &\leq I(\psi; g|C) + I(\psi, g; X_{n-1}, X_{n-3} | C). \end{aligned} \quad (127)$$

We next bound each of the five terms in (126) and (127).

If

$$\tilde{R}_1 + R_1 < H(X_1) - 2\delta(\epsilon), \quad (128)$$

$$\frac{1}{n}I(\phi; f|\mathcal{C}) < \delta(\epsilon); \quad (129)$$

$$\tilde{R}_2 + R_2 < H(X_2) - 2\delta(\epsilon), \quad (130)$$

--

then

$$\frac{1}{n}I(\psi; g|\mathcal{C}) < \delta(\epsilon). \quad (131)$$

To bound the second term in (126), we have

$$\begin{aligned} I(\phi, f; X_{n-3} | \mathcal{C}) &= I(X_{n-1}; X_{n-3} | \mathcal{C}) - I(X_{n-1}; X_{n-3} | \phi, f, \mathcal{C}) \\ &= H(X_{n-1} | \mathcal{C}) - H(X_{n-1} | X_{n-3}, \mathcal{C}) - H(X_{n-1} | \phi, f, \mathcal{C}) + H(X_{n-1} | \phi, f, X_{n-3}, \mathcal{C}) \\ &\leq n[R_1 + R_1 - H(X_1|X_3)] + H(X_{n-1} | \phi, f, X_{n-3}, \mathcal{C}). \end{aligned}$$

If

$$\tilde{R}_1 + R_1 \leq H(X_1|X_3) - 2\delta(\epsilon), \quad (132)$$

then

$$\limsup_{n \rightarrow \infty} \frac{1}{n}H(X_1^n | \phi, X_3^n, \mathcal{C}) < H(X_1|X_3) - R_1 + \delta(\epsilon), \quad (133)$$

and consequently,

$$\frac{1}{n}I(\phi, f; X_3^n | \mathcal{C}) < \delta(\epsilon). \quad (134)$$

We observe that $I(\phi, f; g | X_{n-3}, \mathcal{C}) \leq I(X_{n-1} | X_{n-3}; \psi, g | \mathcal{C})$ by simple calculation. Thus, it is sufficient to only bound the last term in (127):

$$\begin{aligned} I(\psi, g; X_{n-1}, X_{n-3} | \mathcal{C}) &= I(X_{n-2}; X_{n-1}, X_{n-3} | \mathcal{C}) - I(X_{n-2}; X_{n-1}, X_{n-3} | \psi, g, \mathcal{C}) \\ &= H(X_{n-2} | \mathcal{C}) - H(X_{n-2} | X_{n-1}, X_{n-3}, \mathcal{C}) - H(X_{n-2} | \psi, g, \mathcal{C}) \\ &\quad + H(X_{n-2} | g, X_{n-1}, X_{n-3}, \mathcal{C}) + H(X_{n-2} | \psi, g, X_{n-1}, X_{n-3}, \mathcal{C}) \\ &\leq n[R_2 + R_2 - H(X_2|X_1X_3)] + H(X_{n-2} | \psi, g, X_{n-1}, X_{n-3}, \mathcal{C}). \end{aligned} \quad (135)$$

Similarly, it can be shown that if

$$\tilde{R}_2 + R_2 \leq H(X_2|X_1X_3) - 2\delta(\epsilon), \quad (136)$$

then

$$\limsup_{n \rightarrow \infty} \frac{1}{n} H(X_2^n|g, X_1^n, X_3^n, \mathcal{C}) < H(X_2|X_1X_3) - \tilde{R}_2 + \delta(\epsilon), \quad (137)$$

and consequently,

$$\frac{1}{n} I(\psi, g; X_1^n, X_3^n | \mathcal{C}) \leq \delta(\epsilon). \quad (138)$$

Hence, (132) and (136) are the sufficient conditions that guarantee the secrecy requirements given in (7).

We next show the achievability of the points P and Q. It can be shown that the binning rates chosen to achieve the point P in Appendix B for symmetric key generation with a 29 untrusted helper is applicable here to achieve the point P. To achieve the point Q, whose coordinates are given by $(I(X_0; X_1|X_3), I(X_0; X_2|X_1X_3))$, we set the binning rates in the achievable strategy as follows:

$$\tilde{R}_1 = H(X_1|X_0X_3) + \epsilon, \quad (139)$$

$$R_1 = I(X_0; X_1|X_3) - 2\delta(\epsilon) - 2\epsilon, \quad (140)$$

$$\tilde{R}_2 = H(X_2|X_0X_1X_3) + \epsilon, \quad (141)$$

$$R_2 = I(X_0; X_2|X_1X_3) - 2\delta(\epsilon) - 2\epsilon, \quad (142)$$

$$\tilde{R}_3 = H(X_3|X_0) + \epsilon. \quad (143)$$

It can be verified that the above rates satisfy the Slepian-Wolf conditions (23)-(29) and the secrecy conditions (132) and (136).

CHAPTER-7:

WEAK POINTS

- 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.

CHAPTER-8:

STRONG POINTS

- 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

CHAPTER-9:

EXTENSION

- Internet of Things is one of the consequences of propelling network and media communications innovation. This innovation is relied upon to associate huge number of home gadgets, vehicles, and modern conditions. It is possible that millions of many gadgets will be furnished with different sensors and be associated with the web through different heterogeneous organizations.
- IoT, hence, can be said as a framework that permits the exchange of information between interconnected gadgets without human communication. IoT foundation is associated with a correspondence organization to gather and trade data between gadgets.
- Alluding to the fundamental character of remote media, information conglomeration through remote correspondence is entirely powerless against listening in.
- Utilizing hardware like Raspberry PI 3 and making the terminals still with a distance between every one of them secret key can be created which can be stowed away from eavesdropping.

CHAPTER- 10:

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- 9:

REFERENCES:

- [1] Simultaneously generating multiple keys in many to one network.
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. Narayan In 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 multiple 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.

- [12] Key capacity region for a cellular source model. In Proc. IEEE Information Theory Workshop (ITW), Hobart, Tasmania, Australia, November 2014.
H. Zhang, Y. Liang, and L. Lai.
- [13] From weak to strong information-theoretic key agreement. In Proc. IEEE Int. Symp. Information Theory (ISIT), page 18, Sorrento, Italy, June 2000.
U. M. Maurer and S. Wolf.
- [14] Secret key agreement from vector gaussian sources by rate limited public communication. IEEE Trans. Inform. Forensics and Security, 6(3):541–550, September 2011.
S. Wantanabe and Y. Oohama.
- [15] Noiseless coding of correlated information sources. IEEE Trans. Inform. Theory, IT-19:471–480, 1973.
D. Slepian and J. K. Wolf.