Information Theoretic Security Based on Bounded Observability

Jun Muramatsu, Kazuyuki Yoshimura, and Peter Davis

NTT Communication Science Laboratories, NTT Corporation
Hikaridai 2-4, Soraku-gun, Seika-cho, Kyoto 619-0237, Japan
{pure,kazuyuki,davis}@cslab.kecl.ntt.co.jp

Abstract. Under the condition that all users can observe a common object, each using an observation function independently chosen from the same limited set of observation functions, we show necessary and sufficient conditions for users to be able to generate secret keys by public discussion.

Keywords: Bounded observability, bounded storage model, information theoretic security, satellite scenario, secret key agreement by public discussion.

1 Introduction

As proven by Maurer [1], when two users have access to correlated random variables, it is possible for them to create a shared secret key, which is information theoretically secure, by exchanging messages over a public channel. A scenario known as the Satellite Scenario has been presented as an example of how in principle such a scheme could be implemented. In the satellite scenario, a common random signal is received by all users, but the signal received by each user is corrupted by independent noise. On the other hand, a model known as the Bounded Storage Model [2][3] has been used to show that secret key agreement is possible if the memory space of the attacker is bounded. In this model, all users have noise-free access to a huge common data source before the public discussion for secret key agreement.

In this paper, we study the problem where there is a common source as in the satellite scenario, but instead of considering limitation on user information due to noise error or bounded memory, we consider limitation on observation. We show necessary and sufficient conditions for creating secret keys in this case. Specifically, we suppose that the object of observation is an unpredictable information source, prepared by a separate legitimate entity, or by a legitimate user. Also, we suppose that there exist multiple observation functions which map states of the object to various different observation values, and each user must independently choose just one of these multiple observation functions to observe the object, before revealing his choice of function in a public discussion. Furthermore, we assume that knowledge of the whole state cannot be obtained using any single observation function, and different observation values may be

K. Kurosawa (Ed.): ICITS 2009, LNCS 5973, pp. 128–139, 2010.

obtained using different observation functions, but users observe the same result if they use the same observation function.

Intuitively, it is easy to understand that secret key agreement is impossible if a user can obtain complete knowledge of the state of the object from the observation. In the Bounded Storage Model, it was shown that secure key agreement is possible when the attacker's memory is bounded so that they cannot store all the information from the source. In this paper, we generalize this by considering limitations on the observation functions, and show necessary and sufficient conditions for creating secret keys.

We consider this scenario to be physically plausible. Imagine that some physical instrument, corresponding to an observation function, is used to observe a random physical phenomenon. It is physically plausible that knowledge of the whole physical state cannot be obtained by using any single physical observation method available to the users, but users can observe the same result if they use the same observation method. The results of this paper show that it is possible to create secret keys in this scenario.

2 Formal Description of Problem

In this section, we provide a formal description of the problem. We assume that two legitimate users Alice and Bob and an eavesdropper Eve can observe an object prepared by a legitimate entity. Formally, we define the following terminology.

Definition 1. *We call a member of a set $\mathcal{S}$ the state of an object and assume that the state of an object is decided at random according to a probability distribution μ_S, where S represents a random variable on $\mathcal{S}$.*

Definition 2. *Let $\overline{\mathcal{M}}$ be the set of all functions with the domain $\mathcal{S}$, and let $\mathcal{V}_f$ be the range of a function $f \in \overline{\mathcal{M}}$. We call a member of $\overline{\mathcal{M}}$ an observation function, and we call $f(s) \in \mathcal{V}_f$ the observed value of a state $s \in \mathcal{S}$.*

Note that an observed value $f(s)$ is determined uniquely depending on the state $s \in \mathcal{S}$ of the observed object.

Now, to specify the situation described in the introduction, we assume that the following conditions hold.

1. **Unknown State:** The state $s \in \mathcal{S}$ of an object is completely unknown before observation and can be observed only through an observation function. The probability distribution μ_S can be set only by a legitimate entity.
2. **Passive Observation:** Every user observes the same state $s \in \mathcal{S}$ and the state cannot be changed by observation.
3. **Limited Observation:** For each observation, each user independently selects *a single* observation function f, where the selection is restricted to a subset $\mathcal{M}$ of $\overline{\mathcal{M}}$, i.e., $\mathcal{M} \subset \overline{\mathcal{M}}$. The observation is completed before the public discussion, and the same state cannot be observed after the public discussion.

4. **Public Discussion:** Alice and Bob can use a public authenticated error-free channel, which may be monitored by Eve.

The restriction on the observation functions is the key idea behind our problem. Let us comment briefly on these assumed conditions. First, the assumption of passive observation is different from the conditions of quantum cryptography [4], where the effect of observation on the state is a key aspect of the scheme. Next, let us consider the physical meaning of a limited observation. We rely on the limit of observation technology. We could consider the fundamental physical limit of observability of quantum states, but we have excluded this with our passive observation assumption. So we assume a technological limit rather than an absolute physical limit. We assume the existence of physical phenomena that are too fast, or too large, or too noisy or too complex to be completely observed with current technology. We also note that the addition of noise during the observation is not an essential part of the scheme. Of course, in actual implementations this may affect the performance e.g. the key generation rate. Finally, we note that Alice and Bob are free to adopt an arbitrary key agreement protocol using the knowledge of the probability distribution μ_S and the set $\mathcal{M}$ of observation functions. Also, Eve is free to adopt an optimal strategy using the public knowledge of μ_S, $\mathcal{M}$ and the protocol designed by Alice and Bob.

Next, we define a protocol for public discussion, which is used in Section 5, and then define the secret key capacity introduced by Maurer [1].

Definition 3. *Let X and Y be two sources available to Alice and Bob, respectively. A protocol $(C, \widehat{X}, \widehat{Y})$ for (X^n, Y^n) with step t is composed of a sequence of random variables $C = (C_1, \ldots, C_t)$, which represents communication between a sender and a receiver, and random variables $\widehat{X}$ and $\widehat{Y}$, which are generated by the computations of the sender and the receiver, respectively, such that*

- *When $1 \leq i \leq t$ is odd, Alice sends C_i which is calculated deterministically from X^n and $(C_1, \ldots, C_{t-1})$, where $(C_1, \ldots, C_{i-1})$ is a null sequence when $i = 1$.*
- *When $2 \leq i \leq t$ is even, Bob sends C_i which is calculated deterministically from Y^n and $(C_1, \ldots, C_{i-1})$.*
- *After the public discussion, Alice obtains $\widehat{X}$, which is calculated deterministically from X^n and $(C_1, \ldots, C_t)$. Bob obtains $\widehat{Y}$, which is calculated deterministically from Y^n and $(C_1, \ldots, C_t)$.*

Definition 4. *Let X, Y, and Z be three sources available to Alice, Bob, and Eve, respectively. A secret key agreement protocol (C, K, K') for (X, Y, Z) with a rate $R \geq 0$ is composed of two-way communication $C^t = (C_1, \ldots, C_t)$ and computations of secret keys $K, K' \in \mathcal{K}$ such that for all $\varepsilon > 0$ and all sufficiently large n*

$$\frac{H(K)}{n} \geq R - \varepsilon$$

$$\Pr[K \neq K'] \leq \varepsilon$$

$$I(K; Z^n C^t) \leq \varepsilon$$
$$H(K) \geq \log |\mathcal{K}| - \varepsilon,$$

where $|\cdot|$ denotes the cardinality of a set. The secret key capacity $\mathsf{S}(X; Y\|Z)$ of the sources is defined as the least upper bound of such R for all possible key agreement protocols.

3 Relationship with Maurer's Secret Key Agreement from Correlated Source Outputs

Our problem setting is motivated by the satellite scenario introduced by Maurer [1], where a satellite broadcasts a signal, and all users are allowed to access the signal through respective noisy receivers. In this setting, the satellite signal corresponds to the state of an object, and the noisy receivers correspond to the observations. When the channels between the satellite and the receivers are binary symmetric, we can let $\mathcal{S} \equiv \{0, 1\}$ and the following two deterministic maps

$$f_0(s) \equiv s$$
$$f_1(s) \equiv \bar{s}$$

are selected randomly depending on the random noise, where $\bar{s}$ denotes the reverse symbol of $s \in \{0, 1\}$. Let $F_A, F_B, G \in \{f_0, f_1\}$ be random variables that represent noise between the satellite signal and Alice, Bob, and Eve, respectively. Then the random variable corresponding to the correlated sources is represented by $(F_A(S), F_B(S), G(S))$. The possibility of a secret key agreement corresponds to the fact that $(F_A(S), F_B(S), G(S))$ has the positive secret key capacity defined above. The necessary and sufficient condition for the possibility of a secret key agreement has been clarified by [5] when $\mathcal{S}$ is binary. However, it is still an open problem for a general case. It should be noted that our setting is different from the setting in Maurer's satellite scenario because we assume that Alice, Bob, and Eve can each choose their respective observation functions *freely*. We do not discuss the case where Alice, Bob, and Eve are forced to select observation functions.

4 Necessary and Sufficient Conditions for Possibility of Secret Key Agreement Based on Limited Observation

In this section, we present the necessary and sufficient conditions for the possibility of a secret key agreement based on limited observation.

We describe the strategy of Alice and Bob. Alice and Bob determine a finite set $\mathcal{M}_{AB} \subset \mathcal{M}$. We can consider the set $\mathcal{M}_{AB}$ as the specification of a physical sensing device and $f \in \mathcal{M}_{AB}$ as a parameter that represents the input of this device. First, Alice and Bob choose one of the observation functions independently. Next they observe the state of an object by using their respective observation functions. Finally, they agree on a secret key by using public discussion. On the other hand, we assume that Eve can choose one of the observation functions in the superset $\mathcal{M}$ of $\mathcal{M}_{AB}$, where Eve may know the set $\mathcal{M}_{AB}$ and the secret key agreement protocol. Furthermore, we assume that all users are allowed to choose their respective observation functions independently at random. This implies that the possible strategies of Alice, Bob, and Eve can be represented by their respective probability distributions. Let $F_A, F_B \in \mathcal{M}_{AB}$ and $G \in \mathcal{M}$ be random variables corresponding to the random choice of the respective observation functions. Then the respective observation values form correlated sources $((F_A, F_A(S)), (F_B, F_B(S)), (G, G(S)))$ and the secret key capacity of these sources is described by $\mathsf{S}(F_A, F_A(S); F_B, F_B(S) \| G, G(S))$.

We consider the following two situations, which differ with respect to the identity of the legitimate entity who prepares the state of the observed object.

1. The probability distribution μ_S of the state of an object is set *a priori* by a legitimate entity other than Alice, Bob or Eve. Alice, Bob, and Eve choose observation functions F_A, F_B, and G, respectively, so that the random variables $\{S, F_A, F_B, G\}$ are mutually independent. Then the secret key capacity can be represented by the equilibrium point of a game (see [6])
$$\sup_{F_A, F_B} \inf_{G} \mathsf{S}(F_A, F_A(S); F_B, F_B(S) \| G, G(S)).$$
2. Alice sets the probability distribution μ_S, including the possibility that F_A is correlated with S. Bob, and Eve choose observation functions F_B and G, respectively, so that the random variables $\{(S, F_A), F_B, G\}$ are mutually independent. Then the secret key capacity can be represented by the equilibrium point of a game (see [6])
$$\sup_{S, F_A, F_B} \inf_{G} \mathsf{S}(F_A, F_A(S); F_B, F_B(S) \| G, G(S)).$$

In the following, we assume that the observation functions are measurable. Also, for simplicity, we assume throughout the paper that $\mathcal{S}$, $\mathcal{V}_f$ $(f \in \mathcal{M})$ are discrete sets. We believe the results can be extended to continuous sets under suitable technical assumptions.

In the above two situations, the condition for the existence of the possibility of a secret key agreement is equivalent to the condition whereby the equilibrium point of the game has a positive value. We have the following theorem which provides the necessary and sufficient condition for the possibility of a secret key agreement based on bounded observability. The proof is presented in the Appendix.

Theorem 1. *When a probability distribution μ_S is given a priori and random variables $\{S, F_A, F_B, G\}$ are mutually independent, the following conditions are equivalent.*

(C1) The secret key agreement is possible for Alice and Bob, that is,

$$\sup_{F_A, F_B} \inf_{G} \mathsf{S}(F_A, F_A(S); F_B, F_B(S) \| G, G(S)) > 0.$$

(C2) The triplet $(\mu_S, \mathcal{M}_{AB}, \mathcal{M})$ *satisfies*

$$\inf_{g \in \mathcal{M}} \max_{f \in \mathcal{M}_{AB}} H(f(S)|g(S)) > 0. \tag{1}$$

(C3) For any $g \in \mathcal{M}$*, there are* $f \in \mathcal{M}_{AB}$ *and* $u, u', v \in \mathcal{V}$ *such that*

$$u \neq u' \tag{2}$$

$$\mathrm{Prob}(f(S) = u, g(S) = v) > 0 \tag{3}$$

$$\mathrm{Prob}(f(S) = u', g(S) = v) > 0, \tag{4}$$

where Prob *denotes the probability with respect to the random variable* S*.*

When a probability distribution μ_S *is given by Alice and random variables* $\{(S, F_A), F_B, G\}$ *are mutually independent, the following conditions are equivalent.*

(C'1) The secret key agreement is possible for Alice and Bob, that is,

$$\sup_{S, F_A, F_B} \inf_{G} \mathsf{S}(F_A, F_A(S); F_B, F_B(S) \| G, G(S)) > 0.$$

(C'2) There is a probability distribution μ_S *such that* $(\mu_S, \mathcal{M}_{AB}, \mathcal{M})$ *satisfies (1).*

(C'3) For any $g \in \mathcal{M}$*, there are* $f \in \mathcal{M}_{AB}$ *and* $s, s' \in \mathcal{S}$ *such that*

$$g(s) = g(s') \tag{5}$$

$$f(s) \neq f(s'). \tag{6}$$

Remark 1. In the first situation, we could also assume, as in the second situation, that Alice chooses an observation function F_A correlated with S, and Bob and Eve choose observation functions F_B and G, respectively, so that the random variables $\{(S, F_A), F_B, G\}$ are mutually independent. This is a more general but less realistic situation.

We note that condition (1) is equivalent to

$$\sup_{g \in \mathcal{M}} \min_{f \in \mathcal{M}_{AB}} I(f(S); g(S)) < H(f(S)). \tag{7}$$

We propose that conditions (1) and (7) can be called “bounded observability.”

Let us remark on the intuitive meaning of these conditions. Condition (1) corresponds to the fact that there is no universal observation function $g \in \mathcal{M}$ that allows the determination of the observation value for all functions $f \in \mathcal{M}_{AB}$. Conditions (2)–(4) correspond to the fact that Alice and Bob can choose f such that there are two or more possibilities for Eve with respect to the observation value even by the best choice of g. Conditions (5) and (6) correspond to the fact that Eve cannot distinguish two states s and s', which can be distinguished by using the observation function f, by using the observation function g. It should be noted that the existence of $s, s' \in \mathcal{S}$ satisfying (5) and (6) is equivalent to the existence of $v \in \operatorname{Im} g$ such that

$$|f(g^{-1}(v))| \geq 2,$$

where $|\cdot|$ denotes the cardinality of a set.

From the above theorem, we have the following corollary, which is intuitively trivial.

Corollary 1. *If the invertible function (e.g. identity) $g : \mathcal{S} \to \mathcal{V}_g$ is included in $\mathcal{M}$, then a secret key agreement is impossible using any μ_S and $\mathcal{M}_{AB}$.*

Proof. For any $f \in \mathcal{M}$, we have

$$H(f(S)|g(S)) \leq H(f(S)|g^{-1}(g(S))) = H(f(S)|S) = 0.$$

This implies that

$$\inf_{g\in\mathcal{M}} \max_{f\in\mathcal{M}_{AB}} H(f(S)|g(S)) = 0$$

for any S and $\mathcal{M}_{AB} \subset \mathcal{M}$. From the theorem, we have the fact that a secret key agreement is impossible by using any μ_S and $\mathcal{M}_{AB}$. □

5 Advantage Distillation and Information Reconciliation Protocol

In this section, we introduce an advantage distillation and information reconciliation protocol (cf. [7]) for a secret key agreement based on bounded observability. This protocol is used to prove Theorem 1. We assume that there is a finite set $\mathcal{M}_{AB}$ satisfying (1).

1. Alice and Bob choose $f_A, f_B \in \mathcal{M}_{AB}$ independently and uniformly at random, and observe the state S by using their respective observation functions. Let F_A and F_B be random variables corresponding to their respective choices of functions. Then Alice and Bob obtain the observed values $F_A(S)$ and $F_B(S)$, respectively.
2. After Eve obtains a value $g(S)$ using an observation function g, Alice and Bob exchange the information F_A and F_B via a public channel.
3. Alice and Bob calculate X and Y, respectively, defined as

$$X \equiv \begin{cases} F_A(S), & \text{if } F_A = F_B \\ \phi, & \text{if } F_A \neq F_B \end{cases}$$

$$Y \equiv \begin{cases} F_B(S), & \text{if } F_B = F_A \\ \phi, & \text{if } F_B \neq F_A, \end{cases}$$

where ϕ denotes the erasure symbol.

It should be noted that $X = Y$ holds and the secret key generation rate is given by

$$\begin{aligned}&I(X;Y) - I(X;F_A,F_B,G,G(S))\\&= H(X|F_A,F_B,G,G(S))\\&= \mathrm{Prob}(F_A = F_B)H(F_A(S)|F_A,G,G(S)) + \mathrm{Prob}(F_A \neq F_B)\cdot 0\\&= \frac{H(F_A(S)|F_A,G,G(S))}{|\mathcal{M}_{AB}|}.\end{aligned}$$

6 Bounded Storage Model

In this section, we investigate the bounded storage model introduced in [2][3] from the viewpoint of bounded observability. Let n be a sufficiently large number and let $\mathcal{S} \equiv \{0,1\}^n$. We define the set of observation functions $\mathcal{M}$ as the following.

$$\mathcal{M} \equiv \left\{ f_{\mathcal{I}} : \begin{array}{l} \mathcal{I} \subset \{1,2,\ldots,n\} \\ |\mathcal{I}| \leq m < n \\ f_{\mathcal{I}}(\boldsymbol{s}) \equiv (v_1,v_2,\ldots,v_n), \\ \text{where } v_i \equiv \begin{cases} s_i & \text{if } i \in \mathcal{I} \\ v_i = \phi & \text{if } i \neq \mathcal{I} \end{cases} \end{array} \right\}$$

It should be noted that $f_{\mathcal{I}} \in \mathcal{M}$ is characterized by a set $\mathcal{I} \subset \{1,2,\ldots,n\}$. By using an observation function $f \in \mathcal{M}$, all users can observe at most $m(< n)$ bits of $\boldsymbol{s} \in \mathcal{S}$. The parameter m corresponds to the bound of storage space for Eve in the context of the bounded storage model.

Assume that Alice and Bob define the set $\mathcal{M}_{AB} \subset \mathcal{M}$ as

$$\mathcal{M}_{AB} \equiv \left\{ f_i : \begin{array}{l} i \in \{1,2,\ldots,n\} \\ f_i(\boldsymbol{s}) \equiv (v_1,v_2,\ldots,v_n), \\ \text{where } v'_i \equiv \begin{cases} s'_i & \text{if } i' = i \\ \phi & \text{if } i' \neq i \end{cases} \end{array} \right\}.$$

This set corresponds to a situation where Alice and Bob observe only one bit of $\boldsymbol{s} \in \mathcal{S}$. Let $(v_1,v_2,\ldots,v_n)$ and $(v'_1,v'_2,\ldots,v'_n)$ be sequences of $f_i(\boldsymbol{s})$ and $f_{\mathcal{I}'}(\boldsymbol{s})$, respectively. Then we have

$$\begin{gathered} v_i = v'_i = s_i \text{ if } i \in \mathcal{I}' \\ v_i = s_i \text{ and } v'_i = \phi \text{ if } i \notin \mathcal{I}' \end{gathered}$$

for all $f_i \in \mathcal{M}_{AB}$ and $f_{\mathcal{I}'} \in \mathcal{M}$. By letting $\mu_S(s^n) \equiv 1/2^n$, we have the fact that for any $f_{\mathcal{I}'} \in \mathcal{M}$ there is $i \notin \mathcal{I}'$ such that

$$H(f_i(S)|f_{\mathcal{I}'}(S)) = 1.$$

This implies that

$$\min_{f_{\mathcal{I}'}\in\mathcal{M}} \max_{f_i\in\mathcal{M}_{AB}} H(f_i(S)|f_{\mathcal{I}'}(S)) = 1 > 0.$$

Then, from the theorem, we have the fact that Alice and Bob can agree on a secret key. On the other hand, the corollary implies that it is impossible for Alice and Bob to agree on any secret key when $f_{\{1,2,\ldots,n\}} \in \mathcal{M}$ because this function is the identity function.

7 Conclusion

We introduced the information theoretically secure key generation based on bounded observability and derived the necessary and sufficient conditions for the secret key agreement. We also show that the Bounded Storage Model can be formulated within the framework of the bounded observability model.

Acknowledgements

Authors wishes to thank Dr. Harayama for constructive comments.

References

1. Maurer, U.M.: Secret key agreement by public discussion from common information. IEEE Transactions on Information Theory IT-39(3), 733–742 (1993)
2. Chachin, C., Maurer, U.M.: Unconditional security against memory-bounded adversaries. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 292–306. Springer, Heidelberg (1997)
3. Aumann, Y., Ding, Y.Z., Rabin, M.O.: Everlasting security in the bounded storage model. IEEE Transactions on Information Theory IT-48(6), 1668–1680 (2002)
4. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, pp. 175–179 (1984)
5. Maurer, U.M., Wolf, S.: Unconditionally secure key agreement and the intrinsic conditional information. IEEE Transactions on Information Theory IT-45(2), 499–514 (1999)
6. von Neumann, J., Morgenstern, O.: Theory of Games and Economic Behavior. Princeton University Press, Princeton (1944)
7. Bennett, C.H., Brassard, G., Crepeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Transactions on Information Theory IT-41(6), 1915–1923 (1995)
8. Muramatsu, J., Yoshimura, K., Davis, P.: Secret key capacity and advantage distillation capacity. IEICE Transactions on Fundamentals E89-A(10), 2589–2596 (2006)

Appendix: Proof of Theorem

First, we prepare the following lemma.

Lemma 1. *If* (S, F_A, G) *and* F_B *are independent and* $H(F_B(S)|F_B, G, G(S)) = 0$*, then*

$$\mathsf{S}(F_A, F_A(S); F_B, F_B(S) \| G, G(S)) = 0.$$

Proof. It is enough to show $\mathsf{S}(F_A, F_A(S); F_B, F_B(S) \| G, G(S)) \leq 0$, because $\mathsf{S}(F_A, F_A(S); F_B, F_B(S) \| G, G(S)) \geq 0$ is trivial. Since (S, F_A, G) and F_B are independent, we have

$$\begin{aligned} H(F_B, F_B(S)|G, G(S)) &= H(F_B|G, G(S)) + H(F_B(S)|G, G(S), F_B) \\ &= H(F_B|G, G(S)) \\ &= H(F_B) \end{aligned}$$

and

$$\begin{aligned} &H(F_B, F_B(S)|F_A, F_A(S), G, G(S)) \\ &= H(F_B|F_A, F_A(S), G, G(S)) + H(F_B(S)|F_A, F_A(S), G, G(S), F_B) \\ &= H(F_B|F_A, F_A(S), G, G(S)) \\ &= H(F_B). \end{aligned}$$

Then we have

$$\begin{aligned} &\mathsf{S}(F_A, F_A(S); F_B, F_B(S) \| G, G(S)) \\ &\leq I(F_A, F_A(S); F_B, F_B(S)|G, G(S)) \\ &= H(F_B, F_B(S)|G, G(S)) - H(F_B, F_B(S)|F_A, F_A(S), G, G(S)) \\ &= 0, \end{aligned}$$

where the first inequality comes from [1, Theorem 2]. □

Now, we prove the main theorem by showing

$$\text{(C1)} \Leftrightarrow \text{(C2)} \Leftrightarrow \text{(C3)}$$
$$\text{(C'2)} \Rightarrow \text{(C'1)} \Rightarrow \text{(C'3)} \Rightarrow \text{(C'2)}.$$

First, we show the fact that (C1) does not hold for a given μ_S if (C2) does not hold; that is, a secret key agreement is impossible if $(\mu_S, \mathcal{M}_{AB}, \mathcal{M})$ does not satisfy (1). This fact implies (C1) ⇒ (C2). When (C2) does not hold, we have

$$\inf_{g \in \mathcal{M}} \max_{f \in \mathcal{M}_{AB}} H(f(S)|g(S)) = 0.$$

This implies that Eve can use $g \in \mathcal{M}$, which satisfies $H(f(S)|g(S)) = 0$ for any $f \in \mathcal{M}_{AB}$. By letting G be a random variable taking value g with probability one, G satisfies $H(F_B(S)|F_B, G, G(S)) = 0$ for any (F_A, F_B). From Lemma 1, we have

$$\sup_{F_A,F_B} \inf_{G} \mathsf{S}(F_A, F_A(S); F_B, F_B(S)\|G, G(S)) = 0.$$

Next, we show (C2)⇒(C1) for a given μ_S; that is, a secret key agreement is possible when $(\mu_S, \mathcal{M}_{AB}, \mathcal{M})$ satisfies (1). The proof of (C'2)⇒(C'1) is the same as the following. Assume that the function g satisfies $P_G(g) > 0$. From the assumption, there is $f_g \in \mathcal{M}_{AB}$ such that $H(f_g(S)|g(S)) > 0$. Let $(X, Y, (F_A, F_B, G, G(S)))$ be the correlated random variables obtained after the advantage distillation protocol introduced in Section 5. We have

$$\begin{aligned}
&\mathsf{S}(F_A, F_A(S); F_B, F_B(S)\|G, G(S))\\
&\geq \mathsf{S}(X, Y\|F_A, F_B, G, G(S))\\
&\geq I(X;Y) - I(X; F_A, F_B, G, G(S))\\
&= H(X|F_A, F_B, G, G(S))\\
&= \mathrm{Prob}(F_A = F_B)H(F_A(S)|F_A, G, G(S)) + \mathrm{Prob}(F_A \neq F_B)\cdot 0\\
&\geq P_{F_A}(f_g)P_{F_B}(f_g)P_G(g)H(f_g(S)|g(S))\\
&> 0,
\end{aligned}$$

where the first inequality comes from [8, Theorem 1] and the second inequality comes from [1, Theorem 3]. Since this inequality holds for any g satisfying $P_G(g) > 0$, we have the fact that a secret key agreement is possible from $(\mu_S, \mathcal{M}_{AB}, \mathcal{M})$ satisfying (1).

Next, we show the fact that (C2) does not hold if (C3) does not hold; that is, if there is $g \in \mathcal{M}$ such that at least one of (2)–(4) does not hold for $f \in \mathcal{M}_{AB}$ and $u, u', v \in \mathcal{V}$, then g satisfies

$$\max_{f\in\mathcal{M}_{AB}} H(f(S)|g(S)) = 0. \tag{8}$$

This implies (C2)⇒(C3). Assume that (3) holds for $u, v \in \mathcal{V}$ satisfying $\mathrm{Prob}(g(S) = v) > 0$. Then, we have the fact that

$$\mathrm{Prob}(f(S) = u', g(S) = v) = 0$$

for any $u' \neq u$ because (C3) does not hold. This implies that

$$\begin{aligned}
\mathrm{Prob}(f(S) = u|g(S) = v) &= \frac{\sum_u \mathrm{Prob}(f(S) = u, g(S) = v)}{\mathrm{Prob}(g(S) = v)}\\
&= 1
\end{aligned}$$

for any $u, v \in \mathcal{V}$ satisfying $\mathrm{Prob}(g(S) = v) > 0$. Then we have

$$H(f(S)|g(S)) = 0$$

for any $f \in \mathcal{M}_{AB}$ and

$$0 \leq \max_{f\in\mathcal{M}_{AB}} H(f(S)|g(S)) = 0,$$

which implies (8).

Next, we show (C'3)⇒(C'2); that is, μ_S satisfying (1) exists if for any $g \in \mathcal{M}$ there are $f_g \in \mathcal{M}_{AB}$ and $s_g, s'_g \in \mathcal{S}$ satisfying (5) and (6). Let μ_S be a probability distribution that assigns a positive probability for every $s \in \mathcal{S}$. Since

$$\begin{aligned}\mathrm{Prob}(f_g(S) = u_g, g(S) = v_g) &\geq \mathrm{Prob}(S = s_g) > 0\\ \mathrm{Prob}(f_g(S) = u'_g, g(S) = v_g) &\geq \mathrm{Prob}(S = s'_g) > 0\end{aligned}$$

by letting

$$\begin{aligned}u_g &\equiv f_g(s_g)\\ u'_g &\equiv f_g(s'_g)\\ v_g &\equiv g(s_g) = g(s'_g),\end{aligned}$$

we have

$$\mathrm{Prob}(g(S) = v_g) > 0 \tag{9}$$
$$0 < \mathrm{Prob}(f_g(S) = u_g | g(S) = v_g) < 1 \tag{10}$$
$$0 < \mathrm{Prob}(f_g(S) = u'_g | g(S) = v_g) < 1 \tag{11}$$

where (10) and (11) come from the fact that $u_g \neq u'_g$. Then we have

$$\begin{aligned}H(f_g(S)|g(S)) &= \sum_{u,v} \mathrm{Prob}(f_g(S) = u, g(S) = v) \log \frac{1}{\mathrm{Prob}(f_g(S) = u | g(S) = v)}\\ &\geq \mathrm{Prob}(f_g(S) = u_g, g(S) = v_g) \log \frac{1}{\mathrm{Prob}(f_g(S) = u_g | g(S) = v_g)}\\ &\quad + \mathrm{Prob}(f_g(S) = u'_g, g(S) = v_g) \log \frac{1}{\mathrm{Prob}(f_g(S) = u'_g | g(S) = v_g)}\\ &> 0,\end{aligned}$$

where the last inequality comes from (9)—(11). Then we have the fact that

$$\max_{f \in \mathcal{M}_{AB}} H(f(S)|g(S)) \geq H(f_g(S)|g(S)) > 0$$

for any $g \in \mathcal{M}$. This implies (1). Similarly, we can show (C3)⇒(C2) because (9)–(11) can be shown immediately from (2)–(4).

Finally, we show that if (C'3) does not hold then (C'1) does not hold; that is,

$$\mathsf{S}(F_A, F_A(S); F_B, F_B(S) \| G, G(S)) = 0 \tag{12}$$

for any independent random variables (S, F_A) and F_B if there is a random variable $G \in \mathcal{M}$ such that at least one of (5) and (6) does not hold for any $f \in \mathcal{M}_{AB}$ and $s, s' \in \mathcal{S}$. This fact implies (C'1)⇒(C'3). Since $g(s) = g(s') = v$ for any $v \in \mathrm{Im}\, g$ and $s, s' \in g^{-1}(v)$, we have $f(s) = f(s')$ for any $f \in \mathcal{M}_{AB}$ from the assumption. This implies that $|f(g^{-1}(v))| = 1$ for any $v \in \mathrm{Im}\, g$ and $f \in \mathcal{M}_{AB}$. Let $u(f, v)$ be the unique element of $f(g^{-1}(v))$. Then we have the fact that $F_B(S) = u(F_B, g(S))$, which implies $H(F_B(S)|F_B, G, G(S)) = 0$, for any S and F_B. From Lemma 1, we have (12). □