Physical Layer Privacy in Broadcast Channels

Pin-Hsun Lin†, Christiane Kuhn‡, Thorsten Strufe‡, Eduard A. Jorswieck†
†Chair of Information Theory and Communication Systems Department,
Technische Universität Braunschweig, Braunschweig, Germany
‡Chair of Privacy and Data Security, Computer Science, Technische Universität Dresden, Dresden, Germany
{Lin, Jorswieck}@ifn.ing.tu-bs.de, {christiane.kuhn, thorsten.strufe}@tu-dresden.de

***Abstract*—In industrial IoT scenarios, attackers observe communication systems to find relations between transmitted messages and receivers, in order to conduct impersonation or man-in-the-middle attacks. Therefore, unlinkability and anonymity are desirable properties of the corresponding communications. In this paper, we connect the differential privacy (DP)-based notion, *receiver-message unlinkability* ($RM\bar{L}$), to the physical layer secrecy metrics for a degraded discrete memoryless broadcast channel including two receivers and an external adversary. To characterize this connection, we show that Kullback-Leibler-DP-based $RM\bar{L}$, $(0,\delta)-DP$-based $RM\bar{L}$, strong secrecy, and distinguishing secrecy are equivalent up to a multiplicative constant. We then analyze the achievable rate region of the DP-based $RM\bar{L}$ for the considered model by adapting a coding scheme which can achieve strong secrecy. A numerical comparison of the achievable rate regions of binary symmetric degraded broadcast channels under $RM\bar{L}$, strong secrecy, and a case without secrecy or privacy constraint illustrates the relationship.**

I. Introduction

In future 5G and beyond networks, the potential to explore vertical industries and thereby the creation of a wide array of heterogeneous services requires to support different levels of security and privacy. Therefore, security by design is a key requirement [1] not only for industrial wireless sensor networks [2]. There exist different security notions modeling different security threats and goals, including classical requirements in terms of confidentiality, authenticity, and integrity. Recently, with the massive collection of users' communication data [3], additional privacy-related requirements, like *sender* (or *receiver*) *anonymity*, *unlinkability*, and *unobservability* [4], gained importance.

On higher layers (e.g., network or application layer) different approaches are known as anonymous communication (AC) networks to achieve them (see e.g., [5] for an overview). Naturally, there exist many different privacy requirements in communications, but analysis frameworks like [6] make the variety manageable by formalizing and comparing them. The formalized requirements are called *notions* and are related to differential privacy (DP) [7], a concept originated from a provable privacy-preserving analysis in databases. Additionally, on the lower technological transmission layers, namely the physical layer (PHY), new notions of information-theoretic secure design are considered [8]. They include coding and signal processing techniques for confidential, covert [9], or stealthy data transmission [10].

However, the resulting question on the interplay between privacy notions in communications and information-theoretic approaches remains unanswered. Previous attempts are mainly limited to databases. There, the issue is first modeled and addressed in [11] and further elaborated in at least two recent works. One of those studies the relationships between $(\varepsilon,\delta)-DP$, Kullback-Leibler (KL) divergence*, and mutual information-based DP for databases [12]. The other addresses privacy against an adversary's hypothesis test with applications to smart metering [13].

The objective of the current work is to undertake the first steps for relations in communication privacy. More specifically, we aim to identify the corresponding PHY security mechanisms for the AC privacy notion *receiver-message unlinkability* ($RM\bar{L}$) under a specific system model, namely the degraded broadcast channel. $RM\bar{L}$ protects the privacy of receivers: the adversary is allowed to learn which messages are sent, but not who receives which message. Hiding this connection between a receiver and the received message can be of utmost importance; consider e.g., dissidents communicating via wireless mesh networks that are also used for other purposes. In industrial IoT scenarios, attackers observe the communication system to find relations between the transmitted messages and receivers, in order to design sophisticated impersonation or man-in-the-middle attacks. Therefore, unlinkability and anonymity are desirable properties of corresponding communications. In AC, techniques to achieve $RM\bar{L}$ include broadcast with implicit addressing [14] and anonymous return addresses [15]. The basis for implicit addressing is a public key infrastructure: the sender encrypts the message with the public key of the intended receiver and broadcasts the encryption to everyone. The intended receiver recognizes to be the desired recipient as his/her decryption results in a plausible message (e.g., natural language). In the other technique, the receivers have anonymously contacted the senders before and thereby a private description of the inverse direction, the anonymous return address is constructed with the use of cryptographical primitives.

The contributions of this work are as follows: for a simple one transmitter, two receiver setup (broadcast channel) with an external malicious adversary, we show the equivalence up to a multiplicative constant between the DP notion-based $RM\bar{L}$ and several secrecy metrics. More specifically, we first show that $RM\bar{L}$, formalized by $\varepsilon-KL-DP$ for a discrete memoryless broadcast channel with an external adversary, implies strong secrecy while strong secrecy implies $\varepsilon'-KL-DP$ for $RM\bar{L}$, where $\varepsilon'\neq\varepsilon$. The $\varepsilon-KL-DP$ for $RM\bar{L}$ can be further connected to $(\varepsilon,\delta)-DP$. Secondly, we show the relation between distinguishing secrecy and $(\varepsilon,\delta)-DP$ for $RM\bar{L}$. Based on the above relations, we derive an achievable rate region of the $(\varepsilon,\delta)-DP$ for $RM\bar{L}$ through a modified achievable scheme fulfilling strong secrecy. At the end, we compare the rate regions of the cases including: with $\varepsilon'-KL-DP$ for $RM\bar{L}$, with only the strong secrecy constraint, and

The work of Pin-Hsun Lin was supported in part by DFG LI 2886/2-1 and Fast Secure. The work of Eduard A. Jorswieck was supported in part by the German Research Foundation, within the Collaborative Research Center 912 HAEC.

WIFS'2019, December, 9-12, 2019, Delft, Netherlands.
978-1-7281-3217-4/19/$31.00 ©2019 IEEE.

*In this paper, the KL divergence is used interchangeably with divergence.

without any secrecy or privacy constraint, by numerical results.

The rest of the paper is organized as follows. In Section II we introduce the preliminaries. In Section III we show several relations between secrecy metrics in PHY and the privacy metric $RM\bar{L}$ in AC. In addition, we derive the rate region of $(\varepsilon,\delta)-DP$ for $RM\bar{L}$ with a binary symmetric example. In Section IV we further discuss different assumptions in PHY and AC. Finally, Section V concludes this paper.

Notation: Deterministic and random vectors with length n will be denoted by x^n and X^n, respectively. The mutual information between two random variables is denoted by $I(\cdot;\cdot)$. $X-Y-Z$ means $X, Y,$ and Z form a Markov chain. We denote the probability mass function (PMF) by P. We denote the binary entropy by $H_b(p) = p\log p + \bar{p}\log\bar{p}$, where $0 \le p \le 1/2$, $\bar{p} = 1-p$, and $p*q$ denotes $p\cdot\bar{q}+\bar{p}\cdot q$. Statement A implies statement B is denoted by $A \succeq B$.

II. Preliminaries and Problem Formulation

In order to formalize the different security notions, we introduce a couple of definitions from AC and PHY.

A. Privacy Notions from AC

Databases using DP [7] is an established way to formalize the privacy. DP states that for any two neighboring databases (with the privacy technique applied) the view of the adversary is indistinguishable. Neighboring means that the databases only differ in one entry. The view of the adversary describes what information the adversary gets from the database in the analyzed use case; for example, the answer to a query for some aggregated value. Indistinguishability of views can be defined over different distance metrics, like KL. To make the notion concise, we replace the adversary by Eve.

To apply this concept to communications [6], [16], data transmissions which happen in the system, are used in the role of the database rows. Neighboring defines how the communications can differ, i.e., what is kept private by the used technique, and the view of the Eve is what the assumed Eve can observe, e.g., certain channels.

The following definitions inspired by [6], describe the way of formalizing the privacy goal more detailed. Therefore we first need to define the communications happening in our model. We abstract them as tuples and combine those to a scenario. The tuple (m, rec) denotes that message m is transmitted to the receiver rec. Sets of messages and receivers are denoted by $\mathcal{M}$ and $\mathcal{R}$, respectively.

Definition 1. *Scenario: A Scenario $\mathcal{S}$ is a set of tuples (m, rec) with $m \in \mathcal{M}_1 \cup \mathcal{M}_2$, $rec \in \mathcal{R}$.*

The privacy of the used technique is described in terms of which scenarios Eve can distinguish. For our privacy goal $RM\bar{L}$, Eve shall not be able to learn which receiver received which message. She is, however, allowed to learn which messages are sent. Thus, Eve is not allowed to distinguish any two scenarios where the same messages are sent. We call such scenarios *neighboring*.

Definition 2. *Neighboring Scenarios regarding Receiver-Message Unlinkability ($RM\bar{L}$):* Two scenarios $\mathcal{S}_0$ and $\mathcal{S}_1$ are neighboring scenarios regarding Receiver-Message Unlinkability ($RM\bar{L}$) if there exist messages $m_1 \in \mathcal{M}_1$, $m_2 \in \mathcal{M}_2$ and receivers $Bob, Charlie \in \mathcal{R}$, such that

$$\mathcal{S}_0 = \{(m_1, Bob),\ (m_2, Charlie)\},$$
$$\mathcal{S}_1 = \{(m_1, Charlie),\ (m_2, Bob)\}.$$

$RM\bar{L}$ is illustrated in Fig. 1. Note that in the definition, only two receivers are being compared. As we, however, require in the following definition that Eve cannot distinguish any two neighboring scenarios to protect all receivers. Even for the pair of receivers that Eve can distinguish easiest, she fails.

scenario 0	scenario 1
$m_1 \longrightarrow Bob$	$m_1 \longrightarrow Charlie$
$m_2 \longrightarrow Charlie$	$m_2 \longrightarrow Bob$

Fig. 1: Neighboring Scenarios for Receiver-Message Unlinkability

The ability to distinguish the scenarios is defined as follows.

Definition 3. *Kullback-Leibler-differential privacy (KL-DP): A randomized mechanism $P_{Y|S}$ satisfies ε-KL-DP if for all neighboring scenarios*

$$\mathbb{D}(P_{Y|S=\mathcal{S}_0} || P_{Y|S=\mathcal{S}_1}) \le \varepsilon, \tag{1}$$

where Y is the query response.

Another way to measure how well Eve can distinguish the scenarios is (ε,δ)-closeness. For an interpretation of ε and δ we refer the interested reader to [16, Sec. 4.5].

Definition 4. *(ε,δ)-closeness: Two probability distributions P and Q over the same measurable space $(\Omega, \mathcal{F})$, where Ω is a non-empty set and $\mathcal{F}$ is a σ-algebra on Ω, have (ε,δ)-closeness, denoted as $P \overset{(\varepsilon,\delta)}{\approx} Q$, if*

$$P(A) \le e^{\varepsilon} Q(A) + \delta, \forall A \in \mathcal{F}, \tag{2a}$$
$$Q(A) \le e^{\varepsilon} P(A) + \delta, \forall A \in \mathcal{F}. \tag{2b}$$

As for KL-DP, we define achieving of the privacy goal.

Definition 5. *An encoding scheme achieves (ε,δ)-DP for $RM\bar{L}$ if for all neighboring scenarios $\mathcal{S}_0$ and $\mathcal{S}_1$ regarding the* goal

$$P_{Y|S=\mathcal{S}_0} \overset{(\varepsilon,\delta)}{\approx} P_{Y|S=\mathcal{S}_1}. \tag{3}$$

B. Secrecy Notions from PHY

Several important secrecy concepts in physical layer [17, Chapter 2] are introduced as follows. Note that these definitions can be easily adapted to our system model: M_1 and M_2 denote the messages to receivers 1 and 2, respectively, while Z^n is the observation at Eve.

Definition 6. *Strong secrecy: for arbitrarily small positive valued ε, if*

$$\sigma_{div} := I(M_1, M_2; Z^n) \le \varepsilon. \tag{4}$$

Definition 7. *Total variational distance secrecy: for arbitrarily small positive valued ε, if*

$$\sigma_{var} := \| P_{M_1 M_2 Z^n} - P_{M_1 M_2} P_{Z^n} \| \le \varepsilon, \tag{5}$$

where $\|P-Q\| = \frac{1}{2}\sum_{x\in\mathcal{X}} |P(x)-Q(x)|$ is the total variational distance between P and Q.

Definition 8. *Distinguishing secrecy: for any $\varepsilon > 0$, if*

$$\sigma_{dis} := \max_{\mathcal{S}_k \in S} \left(\max_{\hat{s}} \ Pr(\hat{s}(Z^n|S) = S) - \frac{1}{2} \right) \le \varepsilon, \tag{6}$$

where $S \sim Unif(\{\mathcal{S}_0, \mathcal{S}_1\})$ and $\hat{s}$ is an estimate of S based on the observation Z^n.

Note that we set Z^n as the query response Y in Definition 3.

C. Problem Formulation

In this work we consider a degraded discrete memoryless broadcast channel (DM-BC) with two receivers Bob and Charlie and also one external Eve as shown in Fig. 2. The degradedness is described by a Markov chain $(M_1, M_2) - X - Y_2 - Y_1 - Z$, where X^n is the channel input. Denote the messages to Bob and Charlie by $M_1 \in \mathcal{M}_1 = [1, 2, \cdots, 2^{nR_1}]$ and $M_2 \in \mathcal{M}_2 = [1, 2, \cdots, 2^{nR_2}]$, respectively, where R_1 and R_2 are the corresponding achievable rates. We assume that Eve knows the codebooks and the discrete memoryless channel $p(y_1, y_2, z|x)$.

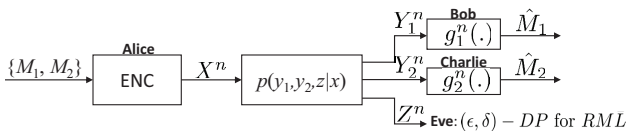

Fig. 2: The considered system model.

Now we give a formal definition of the performance metric used for the considered problem.

Definition 9. *An $RM\bar{L}$ rate pair (R_1, R_2) is (ε, δ)-achievable if there exists a sequence of codes $\mathcal{C}_n$ with encoders f^n and decoders $g_k^n, k = 1, 2$, such that the average error probability*

$$P_e^n = Pr(M_1 \neq g_1^n(Y_1^n) \cup M_2 \neq g_2^n(Y_2^n)) \to 0 \qquad (7)$$

and the (ε, δ)-DP for $RM\bar{L}$

$$P_{Y|S=\mathcal{S}_0} \overset{(\varepsilon,\delta)}{\approx} P_{Y|S=\mathcal{S}_1}.$$

are fulfilled simultaneously as $n \to \infty$.

In this paper we have two main goals: First, we investigate the relations between the privacy notions (DP-based $RM\bar{L}$) from AC and secrecy notions from PHY. Second, we derive the (ε, δ)-achievable $RM\bar{L}$ rate region formed by pairs (R_1, R_2).

III. Main Results

We first show the relations among different secrecy and anonymity metrics in PHY layers and AC. Then we show the corresponding achievable rate region. All proofs are relegated to the appendix.

A. Relations among Different Secrecy and Anonymity Metrics in PHY Layers and AC

In the following, we derive relations among the strong secrecy and $KL - DP$ for $RM\bar{L}$ and further useful notions for the considered model. We first show the condition on the rates R_1 and R_2.

Lemma 1. *For the broadcast model described above to fulfill $RM\bar{L}$, a necessary condition is $R_1 = R_2$.*

Proof. Without loss of generality, assume $R_1 > R_2$. Thus, there must exist a message $m_1 \in \mathcal{M}_1, m_1 \notin \mathcal{M}_2$. We then use this m_1 and an arbitrary $m_2 \in \mathcal{M}_2$ to construct scenarios defined in Sec. II. Hence, we know that in $\mathcal{S}_1$ only one message to Bob is sent, because the one for Charlie fails as $m_1 \notin \mathcal{M}_2$ and hence the codebook does not support sending it. Eve can solely observe whether one or two messages are sent in order to decide on the corresponding bit. Then Eve can win with probability 1. □

To simplify the notation, we define the random message tuple as $\tilde{M} := (M_1, M_2)$. We denote $p_{Z^n|\tilde{M}=(m_1,m_2)}$ and $p_{Z^n|\tilde{M}=(m_2,m_1)}$ by p_{12} and p_{21}, respectively. Define a non-zero $p_{21}^{\min} := \min_{\tilde{m} \in \tilde{\mathcal{M}}} p_{21}(\tilde{m})$, similar to [9, (1)].

Theorem 1. *For a 2-receiver DM-BC with one external passive Eve, the following relations hold for the strong secrecy and $\varepsilon - KL - DP$ for $RM\bar{L}$*

$$I(M_1, M_2; Z^n) \leq \mathbb{D}^{max} \leq \frac{16}{P_{21}^{min}} I(M_1, M_2; Z^n), \qquad (8)$$

where $\mathbb{D}^{max} := \max_{\mathcal{S}_0, \mathcal{S}_1} \mathbb{D}(P_{Z^n|S=\mathcal{S}_0} || P_{Z^n|S=\mathcal{S}_1})$.

Based on Theorem 1, we can derive the following result.

Corollary 1. *For a 2-receiver degraded DM-BC with one external passive Eve, strong secrecy implies $(\varepsilon, \delta) - DP$ for $RM\bar{L}$.*

Theorem 1 and Corollary 1 can be extended to cases with more legitimate receivers and also more eavesdroppers.

Alternatively, we can show an equivalence between distinguishing secrecy to the $(\varepsilon, \delta) - DP$ for $RM\bar{L}$.

Lemma 2. *The distinguishing secrecy is equivalent to the $(\varepsilon, \delta) - DP$ for $RM\bar{L}$.*

B. An $RM\bar{L}$ (ε, δ)-Achievable Rate Region

Theorem 2. *For a 2-receiver DM-BC with an external passive Eve, the following $RM\bar{L}$ (ε, δ)-achievable rate region is (ε, δ)-achievable:*

$$\Big\{(R_1, R_2):\ R_1 \leq R_{DP}, R_2 \leq R_{DP}, R_1 = R_2,$$
$$R_{DP} = \begin{cases} I(X;Y_2|U_1),\ \text{if } I(X;Y_2|U_1) + I(X;Z) \leq I(U_1;Y_1); \\ I(U_1;Y_1) - I(U_1;Z),\ \text{if } I(U_1;Y_1) + I(X;Z) \leq \\ \qquad I(X;Y_2|U_1) + 2I(U_1;Z); \\ \frac{1}{2}(I(U_1;Y_1) + I(X;Y_2|U_1) - I(X;Z)),\ \text{if} \\ \qquad I(X;Y_2|U_1) + 2I(U_1;Z) - I(X;Z) < \\ \qquad I(U_1;Y_1) < I(X;Y_2|U_1) + I(X;Z), \end{cases}$$
$$\Big\}$$

where U_1 is for the first receiver (Bob) forming the Markov chain $U_1 - X - Y_2 - Y_1 - Z$.

Example 1. In this example we show the $RM\bar{L}$ rate region for a 2-receiver binary symmetric degraded BC with an external Eve under $U_1 - X - Y_2 - Y_1 - Z$ with transition probabilities of binary symmetric channels (BSCs) to the legitimate receivers 1, 2, and Eve as P_1, P_2, and P_Z, respectively, where $0 \leq P_2 \leq P_1 \leq P_Z \leq \frac{1}{2}$. Based on Theorem 2, we can derive the (ε, δ)-achievable rate regions as:

$$\Big\{(R_1, R_2):\ R_1 \leq R_{DP}, R_2 \leq R_{DP}, R_1 = R_2,$$
$$R_{DP} = \begin{cases} H_b(\beta * P_2) - H_b(P_2),\ \text{if} \\ H_b(P_2) + H_b(P_Z) \geq H_b(\beta * P_1) + H_b(\beta * P_2); \\ H_b(\beta * P_2) - H_b(\beta * P_1),\ \text{if} \\ H_b(\beta * P_1) + H_b(\beta * P_2) + H_b(P_Z) \geq \\ \qquad 2H_b(\beta * P_Z) + H_b(P_2); \\ \frac{1}{2}(H_b(P_Z) - H_b(\beta * P_1) + H_b(\beta * P_2) - H_b(P_2)), \\ \text{if } (1 + H_b(\beta * P_1))H_b(\beta * P_2) + H_b(P_Z) \leq \\ \qquad H_b(\beta * P_Z). \end{cases}$$
$$\Big\}$$

When there is only secrecy but no $RM\bar{L}$ constraint, we can derive the secrecy rate region as:

$$R_1 \leq H_b(\beta * P_Z) - H_b(\beta * P_1), R_2 \leq H_b(\beta * P_2) - H_b(P_2),$$
$$R_1 + R_2 \leq H_b(\beta * P_2) - H_b(\beta * P_1) - H_b(P_2) + H_b(P_Z).$$

The derivations are relegated to Appendix V. The derived rate regions are shown in Fig. 3 with unit in bit per channel use (bpcu) under the setting $P_1 = 0.2, P_2 = 0.01,$ and $P_Z = 0.3$. The rate region of the case with $RM\bar{L}$ is inside the rate regions with only the secrecy constraint and without $RM\bar{L}$. Rate regions of time sharing are also shown which are enclosed by dashed lines. We conjecture that the derived achievable rate region of $RM\bar{L}$ is close to its capacity region due to the *equivalence up to a multiplicative constant (EMC)*, which will be discussed in the next section.

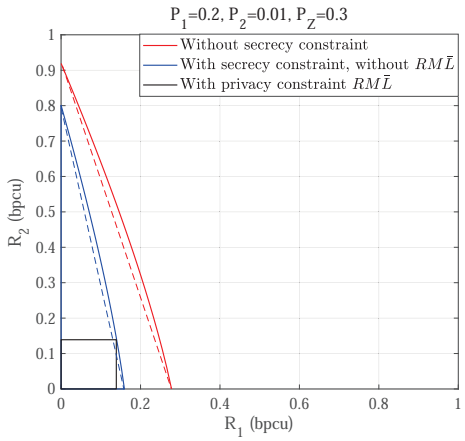

Fig. 3: Comparisons of rate regions of cases with privacy constraint, with only secrecy constraint, and without any constraint under $P_1 = 0.2, P_2 = 0.01, P_Z = 0.3$, where the time sharing regions are enclosed by dashed lines.

IV. Discussion

A. Relations to Other Notions

More detailed relations among different secrecy and DP concepts are shown in Fig. 4, where the notion $\approx$ denotes EMC[†].

Our main contributions in identifying the relations between different notions are twofold: 1) the connection between the strong secrecy and $(\varepsilon, \delta) - DP$ for $RM\bar{L}$ by Theorem 1 and Corollary 1, while (b) in Fig. 4 can be proved by invoking Pinsker's and reverse Pinsker's inequalities as shown in Theorem 1, and (c) is by [12, (20)]. 2) the connection between distinguishing secrecy and $(\varepsilon, \delta) - DP$ for $RM\bar{L}$ by Lemma 2. In addition, from [17, Lemma 2.13] and [17, Lemma 2.15], we have the following relation:

$$\frac{\log e}{2}\sigma_{dis} \leq \frac{\log e}{2}\sigma_{var} \leq \sigma_{div} \leq \sigma_{var} \cdot \log(|\mathcal{M}| - 1) + 1 \leq 2\sigma_{dis} \cdot \log(|\mathcal{M}| - 1) + 1, \tag{10}$$

which shows that σ_{div}, σ_{dis}, and σ_{var} are EMC as (d) and (e), while (f) is by definition. As a special case of semantic secrecy, the distinguishing secrecy can be proved again EMC to the semantic secrecy [17, Lemma 2.14].

B. About Theorem 2

The auxiliary random variable U_1 denotes the code symbol embedding the message M_1 for Bob to decode. Furthermore, these three R_{DP}'s correspond to the following cases: single user rate constraints dominate and $R_1 > R_2$, single user rate constraints dominate and $R_1 \leq R_2$, and sum rate constraint dominate, respectively.

[†]EMC can be formally defined as: two real variables a and b are equivalent up to a multiplicative constant denoted by $a \approx b$, if $a \leq b \leq c \cdot a$ for a finite constat c.

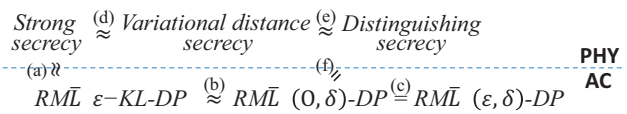

Fig. 4: Comparison of strengths among different secrecy and anonymity concepts, where the upper and lower branches are from PHY and AC, respectively.

The intuition of the coding scheme adapted from [18] is to reuse the messages which are not required to be successfully decoded at a specific receiver as the dummy messages, to protect the secure messages. By this way, the additional binning may be saved, depending on the relation between the sizes of the reused messages and the secure messages for each specific receiver.

C. Towards Comparing Techniques of AC and PHY

Our results allow us to set AC privacy notion $RM\bar{L}$ in relations to the PHY strong secrecy. The next natural question is how existing techniques to achieve the privacy notion from AC, like the implicit addressing and anonymous return addresses from Section I, relate to PHY techniques and their rate regions. This task is challenging as AC and PHY typically start from different assumptions. While solving this challenge completely is out of scope in this work, we want to shed light on the differences we are aware of and present first ideas to compensate them.

There are at least three important differences: 1) the transmission in AC is assumed to be free from noise; 2) for implicit addressing it is assumed that the receiver can distinguish valid messages from random bits and thus the space of valid messages m is $\mathcal{M}' \subsetneq \{0,1\}^{|m|}$; and 3) a computationally restricted adversary is assumed, i.e. it uses only probabilistic, polynomial time algorithms.

To bring both worlds closer, we can do the following adaptions: Assumption 1 can be approximated by adding an error correction code to approach an error free transmission in most cases. Assumption 2 can be compensated with artificially creating this difference by concatenating a sequence of 0-bits to the original message and recognizing this sequence at the intended receiver. Assumption 3 entails a certain choice of the δ parameter in (ε, δ)-differential privacy. AC requirements usually demand δ to be negligible with respect to a *security parameter* λ.[‡] To understand this concept, let us consider encryption [19]: there the security parameter is in the easiest case the key length. Further, the probability that an adversary given an encryption can correctly decide which of two messages was encrypted is required to be at most negligibly better than the probability of a randomly guessing adversary. With this known scaling a threshold in the security parameter is agreed on, for which it is assumed that no adversary on earth can have the computational power to break the encryption in reasonable time.

V. Conclusion

In this paper, we connect the differential privacy-based notion receiver-message unlinkability with the physical layer secrecy concepts for a discrete memoryless broadcast channel with two receivers and an external Eve. For this model, we show the equivalence up to a multiplicative

[‡]Negligibility is therefore defined as $\delta(\lambda)$ being smaller than $\frac{1}{Poly(\lambda)}$ for every λ bigger than a threshold for any positive polynomial *Poly*.

constant relation among strong secrecy, the distinguishing secrecy, the Kullback-Leibler divergence differential privacy for receiver-message unlinkability ($RM\bar{L}$), and the $(\varepsilon,\delta)-DP$ for $RM\bar{L}$. After that, the $RM\bar{L}$ privacy notion is realized by adapting an achievable scheme which can achieve strong secrecy for a degraded broadcast channel with secrecy outside a bounded range. A numerical comparison of the achievable rate regions for binary symmetric degraded broadcast channels under $(\varepsilon,\delta)-DP$ for $RM\bar{L}$, strong secrecy, and a case without secrecy or privacy constraint, illustrates the relationship.

Future works include the extension to continuous alphabets and also further connections to different privacy concepts in anonymous communications community. The converse of the rate region is also interesting to be investigated.

Appendix I. Proof of Theorem 1

The first inequality is proved as follows. For the considered channel, the strong secrecy constraint in Definition 6 can be equivalently expressed by chain rule of divergence [20, Th. 2.2.3] as

$$\mathbb{D}(P_{Z^n|\tilde{M}}||P_{Z^n}\,|P_{\tilde{M}}) \leq \varepsilon, \tag{11}$$

By definition of the conditional divergence [20, Def. 2.2], we can equivalently express the left hand side of (11) as:

$$\begin{aligned}&\sum_{m_1,m_2\in\mathcal{M}^2} P_{\tilde{M}}(m_1,m_2)\mathbb{D}(P_{Z^n|\tilde{M}=(m_1,m_2)}||P_{Z^n})\\ &\overset{(a)}{=} \sum_{m_1,m_2\in\mathcal{M}^2} P_{\tilde{M}}(m_1,m_2)\mathbb{D}(P_{Z^n|\tilde{M}=(m_1,m_2)}||\mathbb{E}_{\tilde{M}}[P_{Z^n|\tilde{M}=(m_2,m_1)}]),\end{aligned} \tag{12}$$

where (a) is by definition of conditional PMF and expectation. Since the divergence is convex with respect to the two input arguments [20, Th. 4.1], we can upper bound the right hand side (RHS) of (a) in (12) by Jensen's inequality:

$$\begin{aligned}&\sum_{m_1,m_2\in\mathcal{M}^2} P_{\tilde{M}}(m_1,m_2)\mathbb{D}(P_{Z^n|\tilde{M}=(m_1,m_2)}||\mathbb{E}_{\tilde{M}}[P_{Z^n|\tilde{M}=(m_2,m_1)}])\\ &\leq \sum_{m_1,m_2\in\mathcal{M}^2} p_{\tilde{M}}(m_1,m_2)\mathbb{E}_{\tilde{M}}[\mathbb{D}(P_{Z^n|\tilde{M}=(m_1,m_2)}||P_{Z^n|\tilde{M}=(m_2,m_1)})]\\ &\overset{(a)}{=} \sum_{m_1,m_2\in\mathcal{M}^2} p_{\tilde{M}}(m_1,m_2)\mathbb{E}_{\tilde{M}}[\mathbb{D}(P_{Z^n|S=\mathcal{S}_0}||P_{Z^n|S=\mathcal{S}_1})] \qquad (13)\\ &\overset{(b)}{\leq} \sum_{m_1,m_2\in\mathcal{M}^2} p_{\tilde{M}}(m_1,m_2)\mathbb{E}_{\tilde{M}}[\mathbb{D}^{max}] \overset{(c)}{=} \mathbb{D}(p^*_{12}||p^*_{21}), \qquad (14)\end{aligned}$$

where (a) is from Definition 1; (b) is by the definition of $\mathbb{D}^{max}$; (c) is from the fact that $\mathbb{D}^{max}$ is a deterministic constant and the re-expression: $\mathbb{D}^{max} := \mathbb{D}(p^*_{12}||p^*_{21})$, to simplify the notation in the following derivation.

The proof of the second inequality is sketched in the following. We can upper bound $\mathbb{D}(p^*_{12}||p^*_{21})$ as:

$$\begin{aligned}\mathbb{D}(p^*_{12}||p^*_{21}) &\overset{(a)}{\leq} \frac{\log e}{p^{\min}_{21}}|p^*_{12}-p^*_{21}|^2\\ &\overset{(b)}{\leq} \frac{\log e}{p^{\min}_{21}}\left(|p^*_{12}-p_{Z^n}|+|p^*_{21}-p_{Z^n}|\right)^2\\ &\overset{(c)}{\leq} \frac{2}{p^{\min}_{21}}\left(\mathbb{D}^{1/2}(p^*_{12}||p_{Z^n})+\mathbb{D}^{1/2}(p^*_{21}||p_{Z^n})\right)^2\\ &\overset{(d)}{\leq} \frac{16\varepsilon}{p^{\min}_{21}},\end{aligned} \tag{15}$$

where (a) is from the reverse Pinsker's inequality [21, (23)]; (b) is from the triangle inequality of total variation distance; (c) is from Pinsker's inequality, and (d) is explained in the following.

Note that the strong secrecy constraint in (11) is an average over $\mathbb{D}(p^*_{12}||p_{Z^n})$ and $\mathbb{D}(p^*_{21}||p_{Z^n})$, with respect to $\forall m_1, m_2$. Therefore, in order to attain the relation that strong secrecy implies $KL-DP$, one way is to transform the upper bound of averaged divergence (11) into the upper bound of the maximum divergence. To achieve this goal, we adopt the technique *codewords expurgation* in Shannon's random coding scheme. More specifically, we re-order $\mathbb{D}(P_{Z^n|\tilde{M}=(m_1,m_2)}||p_{Z^n})$, $\forall m_1, m_2$, in an increasing order with a simplified notation as $0\leq\mathbb{D}_1\leq\cdots\leq\mathbb{D}_{|\mathcal{M}|^2}$. Denote the largest value of the smaller half of $\{\mathbb{D}_k\}_{k=1}^{|\mathcal{M}|^2}$ by $\bar{\mathbb{D}}$. Then following the proof steps of codewords expurgation we can derive:

$$\mathbb{D}(p^*_{12}||p_{Z^n})\leq\bar{\mathbb{D}}\leq 2\varepsilon,\ \mathbb{D}(p^*_{21}||p_{Z^n})\leq\bar{\mathbb{D}}\leq 2\varepsilon \tag{16}$$

with a cost of vanishing rate loss. After substituting (16) into the RHS of (c) in (15), we complete the proof of the second inequality. By combining this two parts, we complete the proof.

Appendix II. Proof of Corollary 1

From [12, (20)] we know that $\varepsilon-KL-DP$ implies (stronger than) $(\varepsilon,\delta)-DP$. Combining with (8), we can easily see that if the strong secrecy is fulfilled, then $(\varepsilon,\delta)-DP$ is fulfilled.

Appendix III. Proof of Lemma 2

From [17, Lemma 2.12] we know (6) is identical to

$$\max_{m_1,m_2\in\mathcal{M}}\frac{1}{2}|P_{Z^n_{\mathcal{S}_0}}-P_{Z^n_{\mathcal{S}_1}}|, \tag{17}$$

which is equivalent to $(0,\delta)-DP$ from Definition 4. With the aid of [12, (20)], which shows $(0,\delta)-DP=(\varepsilon,\delta)-DP$ and then we complete the proof.

Appendix IV. Proof of Theorem 2

We sketch important steps as follows. Due to Theorem 1, we are able to derive the $RM\bar{L}$ rate region by adapting the result of a 4-user case in [18, (6)], which fulfills strong secrecy. More specifically, in the 4-user case in [18] we set both messages for the first and second receivers as null and treat the first receiver as Eve. Meanwhile, the third and fourth messages are secure to Eve by the system model in [18]§, which can be seen from Fig. 5.

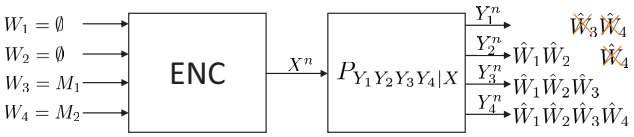

Fig. 5: The adaptation of the 2-user case from the 4-user case in [18].

The intuition of the coding scheme in [18] is to reuse the messages which are not required to be successfully decoded at a specific receiver as the dummy messages, to protect the secure messages. By this way, the additional binning may be saved, depending on the relation between the sizes of the reused messages and the secure messages for each specific receiver.

§In addition, we replace U_3, Y_1, Y_3, and Y_4 in [18, (6)] by U_1, Z, Y_1, and Y_2, respectively, to be consistent to the notation of our model.

Note that we are not able to directly use the three-receiver BC with secrecy outside a bounded range, since the second message in this model [18, Fig. 2] is not secure. On the contrary, we can treat the channel from Alice to Charlie, namely, $W_2(y_2|x)$, as a virtual channel and we can arbitrarily choose $W_2(y_2|x)$ to optimize the rate region of R_1 and R_2 in [18, (6)] as our achievable rate region. It is clear that choosing $W_2(y_2|x)$ such that $I(U_1;Y_1) \geq I(X;Y_2)$ is optimal. Then we obtain an achievable rate region for our case as follows:

$$R_1 \leq I(U_1;Y_1) - I(U_1;Z), R_2 \leq I(X;Y_2|U_1), \quad (18a)$$
$$R_1 + R_2 \leq I(X;Y_2|U_1) + I(U_1;Y_1) - I(X;Z). \quad (18b)$$

Denote the RHS of R_1, R_2, and R_1+R_2 in (18a) and (18b) by R_1^{UB}, R_2^{UB}, and R_{12}^{UB}, respectively. To guarantee the successful decodings at both Bob and Charlie after the message sets are exchanged due to Definitions 2, 5, and 3, we need to fulfill $R_1 \leq R_{DP}, R_2 \leq R_{DP}$, where $\max R_{DP} \leq \min\{R_1^{UB}, R_2^{UB}, R_{12}^{UB}/2\}$. The condition of $R_1 = R_2$ is from Lemma 1. Then we need to consider two cases: whether the right upper corner point of the largest square rate region, which is inside the rectangular rate region formed by (18a), is out of the region (18b) or not.

Case I. If $\frac{R_{12}^{UB}}{2} \geq \min\{R_1^{UB}, R_2^{UB}\}$, then $R_{DP} = \min\{R_1^{UB}, R_2^{UB}\}$: there are two subcases in this case:
Case I-1. If $R_1^{UB} > R_2^{UB}$: it leads to

$$I(X;Y_2|U_1) + I(U_1;Z) \leq I(U_1;Y_1) \text{ and} \quad (19a)$$
$$I(X;Y_2|U_1) + I(X;Z) \leq I(U_1;Y_1). \quad (19b)$$

Due to the Markov chain $U_1 - X - Z$, we know that (19b) dominates.
Case I-2. If $R_1^{UB} \leq R_2^{UB}$: it leads to

$$I(X;Y_2|U_1) + I(U_1;Z) \geq I(U_1;Y_1) \text{ and} \quad (20a)$$
$$I(U_1;Y_1) + I(X;Z) \leq I(X;Y_2|U_1) + 2I(U_1;Z). \quad (20b)$$

We can rearrange (20b) as

$$\begin{aligned} I(U_1;Y_1) &\leq I(X;Y_2|U_1) + I(U_1;Z) + I(U_1;Z) - I(X;Z) \\ &\overset{(a)}{\leq} I(X;Y_2|U_1) + I(U_1;Z), \end{aligned}$$

where (a) is due to the Markov chain $U_1 - X - Z$. Therefore, (20b) dominates.
Case II. If $\frac{R_{12}^{UB}}{2} < \min\{R_1^{UB}, R_2^{UB}\}$, then $R_{DP} = \frac{R_{12}^{UB}}{2}$: there are also two subcases in this case:
Case II-1. If $R_1^{UB} > R_2^{UB}$: it leads to

$$I(X;Y_2|U_1) + I(U_1;Z) \leq I(U_1;Y_1) < I(X;Y_2|U_1) + I(X;Z).$$

Case II-2. If $R_1^{UB} \leq R_2^{UB}$: it leads to

$$I(X;Y_2|U_1) + 2I(U_1;Z) - I(X;Z) < I(U_1;Y_1) < I(X;Y_2|U_1) + I(U_1;Z).$$

Appendix V. Proof of The Rate Regions in Example 1

Since the considered BC is stochastically degraded, we first equivalently transform it into a physically degraded one with four cascading BSCs, for the ease of manipulation. Denote the transition probabilities of the BSCs between Y_2 to Y_1 and Y_1 to Z by α and γ, respectively, where $0 \leq \alpha, \gamma \leq 1/2$. By symmetry we construct another BSC which is between U_1 and X with transition probability β, where $0 \leq \beta \leq 1/2$. Due to symmetry, $U \sim \text{Bern}(1/2)$ maximizes the rates. According to P_1, P_2, P_Z, we can derive $\alpha = (P_1 - P_2)/(1-2P_2)$ and $\gamma = (P_Z - (1-P_2)\alpha + P_2(1-\alpha))/((1-2P_2)(1-2\alpha))$. After some tedious manipulations, we obtain the results.

Taking the union of the upper and lower bounds from Case II-1 and Case II-2, respectively, completes the proof.

References

[1] I. Ahmad, M. Liyanage, M. Ylianttila, S. Shahabuddin, and A. Gurtov, "Design principles for 5G security," *A Comprehensive Guide to 5G Security*, pp. 75–98, 2018.

[2] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4258–4265, Oct 2009.

[3] L. K. Donohue, "Bulk metadata collection: Statutory and constitutional considerations," *Harv. JL & Pub. Pol'y*, vol. 37, pp. 757–900, 2014.

[4] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," TU Dresden, Tech. Rep., 2010.

[5] J. Ren and J. Wu, "Survey on anonymous communications in computer networks," *Computer Communications*, vol. 33, no. 4, pp. 420–431, 2010.

[6] C. Kuhn, M. Beck, S. Schiffner, E. Jorswieck, and T. Strufe, "On privacy notions in anonymous communication," in *PoPETs, the Proceedings on the 19th Privacy Enhancing Technologies Symposium*, 2019, pp. 158–166.

[7] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends® in Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211–407, 2013. [Online]. Available: http://dx.doi.org/10.1561/0400000042

[8] M. R. Bloch and J. Barros, *Physical Layer Security From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[9] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2334–2353, May 2016.

[10] J. Hou and G. Kramer, "Effective secrecy: reliability, confusion and stealth," *aeXiv:1311.1411v3*, Jan. 2014.

[11] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "An information-theoretic approach to privacy," in *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sep. 2010, pp. 1220–1227.

[12] P. Cuff and L. Yu, "Differential privacy as a mutual information constraint," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria*, Oct. 2016, pp. 43–54.

[13] Z. Li, T. J. Oechtering, and D. Gündüz, "Privacy against a hypothesis testing adversary," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1567–1581, June 2019.

[14] A. Pfitzmann and M. Waidner, "Networks without user observability," *Computers & Security*, vol. 6, no. 2, pp. 158–166, 1987.

[15] S. Roos, M. Beck, and T. Strufe, "Anonymous addresses for efficient and resilient routing in f2f overlays," in *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*. IEEE, 2016.

[16] M. Backes, A. Kate, P. Manoharan, S. Meiser, and E. Mohammadi, "Anoa: A framework for analyzing anonymous communication protocols," *Journal of Privacy and Confidentiality*, vol. 7, no. 2, 2016.

[17] P. Narayan and H. Tyagi, *Multiterminal Secrecy by Public Discussion, Foundations and Trends in Communications and Information Theory*. Now Publisher, 2016.

[18] S. Zou, Y. Liang, L. Lai, H. V. Poor, and S. Shamai (Shitz), "Degraded broadcast channel with secrecy outside a bounded range," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 2104–2120, Mar. 2018.

[19] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern, "Rsa-oaep is secure under the rsa assumption," Cryptology ePrint Archive, Report 2000/061, 2000, https://eprint.iacr.org/2000/061.

[20] Y. Polyanskiy and Y. Wu, *Lecture notes on information theory*. http://people.lids.mit.edu/yp/homepage/data/itlecturesv5.pdf, 2017.

[21] I. Sason and S. Verdú, "f-divergence inequalities," vol. 62, no. 11, pp. 5973–6004, Nov. 2016.