Effects of Quantization on the Multiple-Round Secret-Key Capacity

Onur Günlü*, Ueli Maurer†, and João Ribeiro‡
*Chair of Communications Engineering and Security, University of Siegen, Germany, onur.guenlue@uni-siegen.de
†Department of Computer Science, ETH Zurich, Switzerland, maurer@inf.ethz.ch
‡Department of Computing, Imperial College London, United Kingdom, j.lourenco-ribeiro17@imperial.ac.uk

***Abstract*—We consider the strong secret key (SK) agreement problem for the satellite communication setting, where a remote source (a satellite) chooses a common binary phase shift keying (BPSK) modulated input for three statistically independent additive white Gaussian noise (AWGN) channels whose outputs are observed by, respectively, two legitimate receivers (Alice and Bob) and an eavesdropper (Eve). Legitimate receivers have access to an authenticated, noiseless, two-way, and public communication link, so they can exchange multiple rounds of public messages to agree on a SK hidden from Eve. Without loss of essential generality, the noise variances for Alice's and Bob's measurement channels are both fixed to a value $Q > 1$, whereas the noise over Eve's measurement channel has a unit variance, so Q represents a channel quality ratio. The significant and not necessarily expected effect of quantizations at all receivers on the scaling of the SK capacity with respect to a sufficiently large and finite channel quality ratio Q is illustrated by showing 1) the achievability of a constant SK for any finite BPSK modulated satellite output by proposing a thresholding algorithm as an advantage distillation protocol for AWGN channels and 2) the converse (i.e., unachievability) bound for the case when all receivers apply a one-bit uniform quantizer to their noisy observations before SK agreement, for which the SK capacity is shown to decrease quadratically in Q. Our results prove that soft information increases not only the reliability and the achieved SK rate but also the scaling of the SK capacity at least quadratically in Q as compared to hard information.**

I. Introduction

The problem of secret key (SK) agreement consists in legitimate parties that observe dependent random variables to reliably agree on a key that is hidden from an eavesdropper by using a public communication link. We consider the source model for SK agreement where two legitimate parties, called Alice and Bob, and an eavesdropper, called Eve, observe n independent and identically distributed (i.i.d.) realizations of random variables distributed according to a fixed joint probability distribution [1], [2]. The SK capacity, defined as the supremum of all achievable SK rates, is given in [2] for one-way public communication between legitimate parties. General upper and lower bounds on the SK capacity for two-way and multi-round public communication are also given in [1], [2]. Early results on the SK capacity use a weak secrecy-leakage metric that measures the normalized amount of information leaked about the SK to Eve. In [3], [4], lower and upper bounds on the SK capacity with a weak secrecy constraint are shown to be valid also with a strong secrecy constraint that is not normalized by the blocklength. Furthermore, improved lower and/or upper bounds on the SK capacity for general probability distributions are proposed, e.g., in [5]–[8]. A necessary and sufficient condition for the SK capacity to be positive for general probability distributions with two-way and multi-round public communication is provided in [9] and a sufficient condition in terms of Chernoff information is given in [10]. Extensions to multiple parties are discussed in [11]–[15] and capacity regions for SK agreement with privacy and storage rate constraints are given in [16]–[20].

As a binary example that provides interesting insights, SK agreement with a helpful satellite that is a remote source [21, p. 118], [22, p. 78] whose outputs are measured through independent binary symmetric channels (BSCs) is considered in [1], [23]. The satellite setting with BSCs illustrates that two-way and multi-round public communication, unlike one-way public communication, allows to achieve a positive SK rate even when both Alice's and Bob's noisy observations of the satellite outputs have a *lower* quality than Eve's noisy observations. The conditions for this result to hold are that Eve's measurement channel should not be noiseless and Alice's and Bob's measurement channels should have positive channel capacities; see also [24, Section 1.4] for precise definitions.

To achieve a positive SK rate with two-way and multi-round public communication advantage distillation protocols are used, including the repetition protocol [1], the parity check protocol [23], [25], and other protocols such as in [10], [26], [27]. Advantage distillation protocols aim to provide an information-theoretic advantage to the legitimate parties by selecting a subset of their observed symbols for which legitimate parties have an advantage over Eve. To focus on scenarios where advantage distillation is necessary to reliably agree on a SK, a metric called *channel quality ratio* is defined in [24] as the maximum of the ratio of the capacity of the Eve's BSC vs. the capacity of Alice's or Bob's BSC. For the satellite setting with BSCs, the SK capacity is shown to decrease quadratically in the channel quality ratio when it is sufficiently large, achieved by using the parity check protocol [24]. Furthermore, extensions of the satellite setting with BSCs to channels with binary phase shift keying (BPSK) modulated inputs and additive white Gaussian noise (AWGN) components are considered in [5], [28], the former of which proves a

**Alphabetical author order.

sufficient condition to achieve a positive SK rate and the latter proves that using soft information increases the achievable SK rate as compared to a BSC that can be obtained by applying a one-bit uniform quantization at Alice and Bob.

Given the previous significant interest in the satellite setting with binary or Gaussian noise components, we are interested in the following natural question: *How much does one-bit uniform quantization hurt the SK capacity in the AWGN satellite setting as a parameter of the channel quality ratio Q defined below*, which is a ratio of signal-to-noise ratios rather than the ratio of channel capacities defined for BSCs in [24].

We show that the effect of quantization at Alice and Bob on the SK capacity is surprisingly significant. For statistically independent AWGN satellite measurement channels with BPSK modulated inputs and any sufficiently large finite Q, we prove that 1) the SK capacity is bounded from above by a term that decreases quadratically in Q when a one-bit uniform quantization is applied at Alice and Bob before SK agreement; 2) a threshold protocol proposed below suffices to distill an advantage over Eve such that a positive SK rate that is *independent of the channel quality ratio Q* is achievable.

II. Problem Definition and Main Results

Consider a SK agreement problem where Alice and Bob who observe correlated random variables want to agree on a SK by using multiple rounds of public communication without a storage rate constraint such that the SK is hidden from Eve who also observes a correlated random variable. To obtain these correlated random variables we consider the following hidden source model, which is a sensible variation of the satellite setting defined in [1]. Suppose a binary remote source (or satellite) publicly chooses a number $w \in \mathbb{R}^+$ and puts out either the symbol $R = +w$ or $R = -w$, i.e., BPSK modulated symbols, each with probability $1/2$. Without loss of generality, the antipodal satellite output is transmitted to Alice, Bob, and Eve through statistically independent zero-mean additive Gaussian noise channels with variances, respectively, $\sigma_A^2 = \sigma_B^2 = \sigma^2$ and σ_E^2. Thus, we have $P_R(+w) = P_R(-w) = 1/2$, $P_{X|R} \sim \mathcal{N}(0, \sigma^2)$, $P_{Y|R} \sim \mathcal{N}(0, \sigma^2)$, $P_{Z|R} \sim \mathcal{N}(0, \sigma_E^2)$, and Alice, Bob, and Eve observe i.i.d. random variables, respectively, X^n, Y^n, and Z^n, where n is the blocklength.

Define the number of public communication rounds without a public-storage constraint as $\ell \geq 1$, which can be optimized for each parameter set. For $k = 1, 2 \ldots, \ell$, Alice creates public messages F_{2k-1} according to some $P_{F_{2k-1}|X^n, F^{2k-2}}$, where F^0 is a constant, and sends the public messages to Bob. Similarly, Bob creates public messages F_{2k} according to some $P_{F_{2k}|Y^n, F^{2k-1}}$ and sends the public messages to Alice. We remark that to create the random public messages a local source of randomness can be provided by using physical unclonable functions (PUFs), which are unique and unclonable digital circuit outputs that are embodied by a device [29], [30], such as Alice's and Bob's decoders. After ℓ rounds of public communication, Alice generates a SK K_A by using $(X^n, F^{2\ell})$ and Bob generates another SK K_B by using $(Y^n, F^{2\ell})$. Alice and Bob aim to generate the same uniformly distributed key without leaking any information about it to Eve. Fig. 1 illustrates the SK agreement setting with a helpful satellite for, e.g., $\ell = 1$ round of public communication.

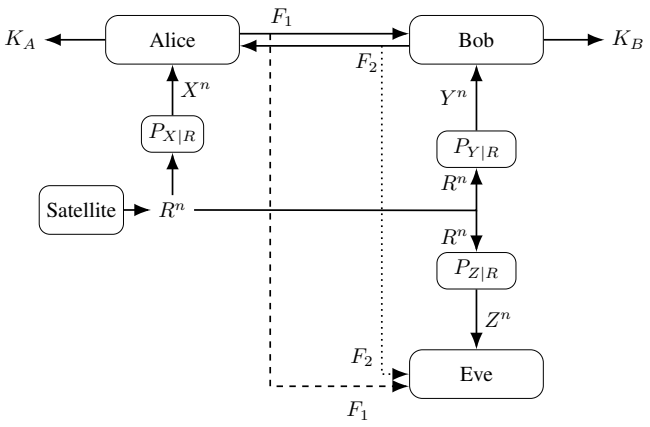

Fig. 1. SK agreement with a helpful satellite for $\ell = 1$ round of public communication.

Without loss of generality, we focus on the setting where the Satellite-to-Eve channel noise component has a variance $\sigma_E^2 = 1$, whereas the Satellite-to-Alice and Satellite-to-Bob channel noise components both have variances $\sigma^2 = Q > 1$. Therefore, for this setting the legitimate receivers Alice and Bob observe X^n and Y^n, respectively, that are *lower* quality versions of the binary satellite outputs R^n as compared to the quality of Eve's observations Z^n. This setting represents the general setting with having Alice, Bob, and Eve scale their observations by $\frac{1}{\sigma_E}$ such that $Q = \frac{\sigma^2}{\sigma_E^2} \geq 1$. Thus, Q represents a *channel quality ratio* between Alice or Bob's channel and Eve's channel, where the quality of Alice's and Bob's observations X_i and Y_i, respectively, of the satellite output R_i as compared to the quality of Eve's observation Z_i degrades as Q increases for all $i = 1, 2, \ldots, n$.

We next define the SK capacities for two scenarios. In Scenario 1, no party quantizes the observed Gaussian symbols X^n, Y^n, and Z^n. For this scenario, we define the *unquantized SK capacity with a helpful satellite*, denoted as $S_{\mathcal{W}}(Q)$. In Scenario 2, all parties apply a one-bit uniform quantizer to its observed Gaussian symbols to obtain X_q^n, Y_q^n, and Z_q^n, where $X_q, Y_q, Z_q \in \{-w, +w\}$ since one-bit uniform quantizers result in $X_{q,i} = w \cdot \mathrm{sgn}(X_i)$, $Y_{q,i} = w \cdot \mathrm{sgn}(Y_i)$, and $Z_{q,i} = w \cdot \mathrm{sgn}(Z_i)$ for all $i = 1, 2, \ldots, n$. For Scenario 2, we define the *quantized SK capacity with a helpful satellite*, denoted as $S_{\mathcal{W}}^q(Q)$.

Definition 1. *Consider Scenario 1 defined above. For the satellite setting depicted in Fig. 1 and for a fixed $w \in \mathcal{W}$ and $Q > 1$, a SK rate $S(w, Q)$ is achievable if, given any $\delta > 0$, there is some $n \geq 1$, an encoder, two decoders, and $\ell \geq 1$ for which $R_K = \dfrac{\log(|\mathcal{K}_A|)}{n}$ and*

$$\Pr[K_A \neq K_B] \leq \delta \qquad (\textit{reliability}) \tag{1}$$

$$H(K_A) \geq n(R_K - \delta) \qquad (\textit{uniformity}) \tag{2}$$

$$I(K_A; F^{2\ell}, Z^n) \leq \delta \qquad (\textit{strong secrecy}). \tag{3}$$

The unquantized SK capacity with a helpful satellite is defined as

$$S_{\mathcal{W}}(Q) = \sup_{w \in \mathcal{W}} S(w, Q). \tag{4}$$

Consider next Scenario 2. The quantized SK capacity with a helpful satellite, i.e., $S^q_{\mathcal{W}}(Q)$, can be defined similarly as defined for Scenario 1 by replacing in (4) the SK rate $S(w,Q)$ with $S^q(w,Q)$ and $S_{\mathcal{W}}(Q)$ with $S^q_{\mathcal{W}}(Q)$, respectively, where $S^q(w,Q)$ corresponds to an achievable SK rate after all parties apply a one-bit uniform quantization to their observations.

In practice, hardware implementations, e.g., of communication networks impose that any modulated symbol R transmitted by the satellite can be chosen from a finite set $\mathcal{W}$, which can be large. Thus, we assume in the following that $\mathcal{W} \subseteq \mathbb{R}^+$ is a finite set.

We next show that quantization *significantly hurts* the SK capacity for the satellite setting shown in Fig. 1. This result follows by providing a lower bound on the SK capacity for Scenario 1 without quantization and an upper bound on the SK capacity for Scenario 2 with quantization. For these results, we consider the case where the channel quality ratio Q is large, which corresponds to the best case for Eve in terms of the respective observed symbol quality. We illustrate for Scenario 1 that one can achieve a constant SK rate in the unquantized setting, whereas for Scenario 2 the SK capacity scales at most by $O\Big(\frac{1}{Q^2}\Big)$, both of which are proved for every sufficiently large finite channel quality ratio Q.

A. Main Results

We next list the main results of this work. The proof of Theorem 1 below follows by proving an upper bound on $S^q_{\mathcal{W}}(Q)$ in Section III and a lower bound on $S_{\mathcal{W}}(Q)$ in Section IV. The proof of Corollary 1 below follows by combining a simple reduction argument with the results of Theorem 1, which is explained below.

Theorem 1. *For every non-empty finite set $\mathcal{W} \subseteq \mathbb{R}^+$, there exists a constant $c > 0$ such that we have $S_{\mathcal{W}}(Q) \geq c$ bits/channel-use for every finite channel quality ratio $Q > 1$ that is sufficiently large, whereas $S^q_{\mathcal{W}}(Q) = O\Big(\frac{1}{Q^2}\Big)$.*

Theorem 1 suggests that for Scenario 1 without quantization the SK capacity scales by $O(1)$, whereas for Scenario 2 with quantization the SK capacity scales at most by $O\Big(\frac{1}{Q^2}\Big)$. This difference illustrates that quantization is significantly hurtful for SK agreement in the satellite setting considered in Fig. 1.

Remark 1. *The bounds on $S_{\mathcal{W}}(Q)$ and $S^q_{\mathcal{W}}(Q)$ given in Theorem 1 directly imply that the same bounds are valid also on, respectively, $S(w,Q)$ and $S^q(w,Q)$ for all $w > 0$ since the bound on the $S^q_{\mathcal{W}}(Q)$ follows for any non-empty finite set $\mathcal{W} \subseteq \mathbb{R}^+$, see Lemma 1 below, and the lower bound on $S_{\mathcal{W}}(Q)$ follows for any non-empty set $\mathcal{W} \subseteq \mathbb{R}^+$, see Lemma 2 below.*

The assumption that Eve has to apply a one-bit uniform quantizer for Scenario 2 is not realistic as a passive attacker cannot be forced to apply a particular decoding method. Thus, we next remove the assumption in Scenario 2 that Eve has to apply any quantization to Z^n, whereas for Scenario 2 Alice and Bob still have to apply a one-bit uniform quantization to X^n and Y^n, respectively. We show that the bound $O\Big(\frac{1}{Q^2}\Big)$ on the quantized SK capacity with a helpful satellite $S^q_{\mathcal{W}}(Q)$ is also a bound for the more realistic version of Scenario 2 with X^n_q, Y^n_q, and Z^n.

Corollary 1. *For every non-empty finite set $\mathcal{W} \subseteq \mathbb{R}^+$ and sufficiently large finite $Q > 1$, the SK capacity for the case where Alice and Bob quantize but Eve does not quantize their corresponding observations can be upper bounded by $O\Big(\frac{1}{Q^2}\Big)$.*

The proof of Corollary 1 follows since allowing Eve to use more information than a one-bit quantizer output cannot increase the SK capacity. Thus, Corollary 1 illustrates that the results of Theorem 1 follow also when we remove the assumption in Scenario 2 that Eve has to apply quantization.

III. Quantized SK Capacity Upper Bound

We first consider the quantized SK capacity with a helpful satellite defined in Definition 1 for Scenario 2, where Alice, Bob, and Eve apply a uniform one-bit quantization to each symbol of their noisy measurements, respectively, X^n, Y^n, and Z^n to obtain X^n_q, Y^n_q, and Z^n_q. We have the following result for $S^q_{\mathcal{W}}(Q)$ when Q is sufficiently large.

Lemma 1. *We have $S^q_{\mathcal{W}}(Q) = O\Big(\frac{1}{Q^2}\Big)$ for every non-empty finite set $\mathcal{W} \subseteq \mathbb{R}^+$ and sufficiently large finite $Q > 1$.*

Proof: Applying a classic upper bound on the SK capacity from [1, Theorem 2] [4, pp. 6], we have

$$S^q(w,Q) \leq I(X_q; Y_q | Z_q).$$

Therefore, it suffices to show that

$$\sup_{w \in \mathcal{W}} I(X_q; Y_q | Z_q) = O\Big(\frac{1}{Q^2}\Big)$$

when $Q \to \infty$. Assuming that w is restricted to an arbitrary finite set $\mathcal{W}$, we can show that

$$S^q_{\mathcal{W}}(Q) \leq \sup_{w \in \mathcal{W}} I(X_q; Y_q | Z_q) \leq \frac{1}{5Q^2} \tag{5}$$

for a sufficiently large Q. To prove a weaker version of (5) for simplicity, we remark that X_q and Y_q correspond to noisy versions of a random bit R measured through a BSC with crossover probability

$$\varepsilon = \frac{1}{2}\Big(1 - \mathrm{erf}\Big(\frac{w}{\sqrt{2Q}}\Big)\Big) \tag{6}$$

whereas Z_q corresponds to a noisy version of the same random bit R measured through another BSC with crossover probability

$$\alpha = \frac{1}{2}\left(1 - \mathrm{erf}\left(\frac{w}{\sqrt{2}}\right)\right) \tag{7}$$

where $\mathrm{erf}(\cdot)$ is the error function defined as $\mathrm{erf}(z) = \frac{2}{\sqrt{\pi}}\int_0^z e^{-t^2}dt$. Thus, using this representation we have

$$\begin{aligned}
&I(X_q;Y_q|Z_q) = I(X_q;Y_q|Z_q=w)\\
&= H(X_q|Z_q=w) - H(X_q|Y_q,Z_q=w)\\
&= H_b(\varepsilon\gamma+(1-\varepsilon)(1-\gamma)) - H(X_q|Y_q,Z_q=w)\\
&= H_b(\varepsilon\gamma+(1-\varepsilon)(1-\gamma))\\
&\quad - (\varepsilon\gamma+(1-\varepsilon)(1-\gamma))\cdot H_b\left(\frac{\varepsilon^2\gamma+(1-\varepsilon)^2(1-\gamma)}{\varepsilon\gamma+(1-\varepsilon)(1-\gamma)}\right)\\
&\quad - (\varepsilon(1-\gamma)+(1-\varepsilon)\gamma)\cdot H_b\left(\frac{\varepsilon(1-\varepsilon)}{\varepsilon(1-\gamma)+(1-\varepsilon)\gamma}\right)
\end{aligned} \tag{8}$$

where $H_b(p) = -p\log(p) - (1-p)\log(1-p)$ is the binary entropy function. Using (8), for every $w > 0$ we have

$$\lim_{Q\to\infty} Q^2 \cdot I(X_{w,Q};Y_{w,Q}|Z_w) = \frac{2w^4\left(1-\mathrm{erf}\left(\frac{w}{\sqrt{2}}\right)^2\right)^2}{\pi^2\ln 2} \tag{9}$$

which can be obtained in a routine manner by combining the following series expansions

$$\varepsilon = \frac{1}{2} - \frac{w}{\sqrt{2\pi Q}} + O\left(\frac{1}{Q^{3/2}}\right) \tag{10}$$

as $Q\to\infty$,

$$\begin{aligned}
H_b(p) =& 1 - \frac{2}{\ln 2}\left(p-\frac{1}{2}\right)^2 - \frac{4}{3\ln 2}\left(p-\frac{1}{2}\right)^4\\
&+ O\left(\left(p-\frac{1}{2}\right)^6\right)
\end{aligned} \tag{11}$$

which is expanded around $p = 1/2$, and

$$\begin{aligned}
&(\varepsilon\gamma+(1-\varepsilon)(1-\gamma))\\
&\quad = \left[\frac{1}{2} - (1-2\gamma)\left(\varepsilon-\frac{1}{2}\right) + O\left(\left(\varepsilon-\frac{1}{2}\right)^4\right)\right],
\end{aligned} \tag{12}$$

$$\begin{aligned}
&\left(\frac{\varepsilon(1-\varepsilon)}{\varepsilon(1-\gamma)+(1-\varepsilon)\gamma}\right)\\
&\quad = \left[\frac{1}{2} - (1-2\gamma)\left(\varepsilon-\frac{1}{2}\right) - 8\gamma(1-\gamma)\left(\varepsilon-\frac{1}{2}\right)^2\right.\\
&\qquad\qquad \left. + O\left(\left(\varepsilon-\frac{1}{2}\right)^3\right)\right],
\end{aligned} \tag{13}$$

$$\begin{aligned}
&\left(\frac{\varepsilon^2\gamma+(1-\varepsilon)^2(1-\gamma)}{\varepsilon\gamma+(1-\varepsilon)(1-\gamma)}\right)\\
&\quad = \left[\frac{1}{2} - (1-2\gamma)\left(\varepsilon-\frac{1}{2}\right) + 8\gamma(1-\gamma)\left(\varepsilon-\frac{1}{2}\right)^2\right.\\
&\qquad\qquad \left. + O\left(\left(\varepsilon-\frac{1}{2}\right)^3\right)\right]
\end{aligned} \tag{14}$$

which are expanded around $\varepsilon = 1/2$. Since $\mathcal{W}$ is finite, applying (10)-(14) to (8) yields (9) for all $w\in\mathcal{W}$. Furthermore, using the following inequality [31], [32]

$$1 - \mathrm{erf}(z) \le e^{-z^2}$$

we obtain

$$1 - 2e^{-z^2} \le \mathrm{erf}(z)^2$$

which gives the inequality

$$(1-\mathrm{erf}(z)^2)^2 \le 4e^{-2z^2}. \tag{15}$$

Applying (15) to the limit in (9) for $z = \frac{w}{\sqrt{2}}$, we obtain the upper bound

$$\lim_{Q\to\infty} Q^2 \cdot I(X_{w,Q};Y_{w,Q}|Z_w) \le \frac{6w^4e^{-w^2}}{\pi^2\ln 2} \tag{16}$$

for all $w\in\mathcal{W}$, which is maximized at $w^* = \sqrt{2}\in\mathcal{W}$ with the value ≈ 0.4748. Using this bound, the proof of Lemma 1 follows. ∎

IV. The threshold protocol with soft information for Unquantized SK Capacity Lower Bound

In this section, we describe and analyze a threshold advantage distillation protocol for Scenario 1 without quantization that achieves a positive SK rate for every sufficiently large finite channel quality ratio $Q > 1$. The proposed protocol can be considered as a special case of the quantization-based protocol from [28] that is applied to Gaussian satellite measurement channels to increase the achieved SK rate. We consider a different parameter set and a different setting than considered in [28], and we use this protocol to prove achievability of a constant positive SK rate rather than to achieve a higher SK rate. We remark that a similar protocol to our threshold protocol was mentioned in [1, Section V] without analysis. Our explicit threshold protocol leads to the following result.

Lemma 2. *For any non-empty set $\mathcal{W}\subseteq\mathbb{R}^+$, there exists a constant $c_{\mathcal{W}} > 0$ such that $S_{\mathcal{W}}(Q) \ge c_{\mathcal{W}}$ bits/channel-use for every sufficiently large finite channel quality ratio $Q > 1$.*

Proof: The threshold protocol is parameterized by $w > 0$, $Q > 1$, and a threshold $\tau \ge 0$. Recall that Alice, Bob, and Eve have access to n i.i.d. samples X_i, Y_i, and Z_i, respectively. An index $i\in\{1,2,\ldots,n\}$ is called *τ-good* if both $|X_i| \ge \tau$ and $|Y_i| \ge \tau$. The threshold protocol proceeds as follows.

1) Alice sends the set $\{i : |X_i| \ge \tau\}$ to Bob;
2) Bob sends the set $\{i : |Y_i| \ge \tau\}$ to Alice;
3) Let $i_1,\ldots,i_k$ denote the τ-good indices, where $\{i_1,\ldots,i_k\} \subseteq \{1,2,\ldots,n\}$. Alice (resp. Bob) sets $\widehat{X}_j = \mathbf{1}_{\{X_{i_j}>0\}}$ (resp. $\widehat{Y}_j = \mathbf{1}_{\{Y_{i_j}>0\}}$) for $j = 1,\ldots,k$;
4) Alice and Bob run information reconciliation and privacy amplification protocols on the pairs $(\widehat{X}_j,\widehat{Y}_j)$ to agree on a SK.

We remark that the pairs $(\widehat{X}_j, \widehat{Y}_j)$ are i.i.d. and independent of $\{Z_i\}_{i\neq i_j}$ conditioned on Z_{i_j}. Thus, if we set $\widehat{Z}_j = Z_{i_j}$, this protocol can achieve a SK rate of

$$\Pr[\{\text{index } i \text{ is } \tau\text{-good}\}] \cdot (I(\widehat{X}_1;\widehat{Y}_1) - I(\widehat{X}_1;\widehat{Z}_1)) \quad (17)$$

which follows from [4, Theorem 4]. It is not clear a priori whether it is possible to set parameters for the threshold protocol such that the SK rate in (17) is a positive constant for every sufficiently large and finite $Q > 1$. We show below that this is the case.

Set $\tau = \alpha_w\sqrt{Q}$ for an appropriate constant $\alpha_w > 0$ that is determined below. We proceed to analyze each term in (17) under this choice of threshold τ. Let N denote a random variable following a standard normal distribution and $\Phi(\cdot)$ denote the cumulative distribution function of N. First, we have

$$\begin{aligned}
&\Pr[\{\text{index } i \text{ is } \tau\text{-good}\}] = \Pr[|X_i| \geq \tau,\ |Y_i| \geq \tau] \\
&\quad = \Pr[|X| \geq \tau]^2 \\
&\quad = (\Pr[X \geq \tau] + \Pr[X \leq -\tau])^2 \\
&\quad = \left(\Pr\left[N \geq \frac{\tau - w}{\sqrt{Q}}\right] + \Pr\left[N \leq -\frac{\tau + w}{\sqrt{Q}}\right]\right)^2 \\
&\quad \overset{(a)}{=} \left(1 - \Phi\left(\alpha_w - \frac{w}{\sqrt{Q}}\right)\right)^2 \cdot \left(1 - \Phi\left(\alpha_w + \frac{w}{\sqrt{Q}}\right)\right)^2
\end{aligned} \quad (18)$$

where (a) follows by the choice $\tau = \alpha_w\sqrt{Q}$. Using (18), we obtain

$$\lim_{Q\to\infty} \Pr[\{\text{index } i \text{ is } \tau\text{-good}\}] = (1 - \Phi(\alpha_w))^4 > 0. \quad (19)$$

Second, the data processing inequality yields

$$I(\widehat{X}_1;\widehat{Z}_1) \leq 1 - H(R|Z). \quad (20)$$

Observe that the conditional entropy term $H(R|Z)$ depends only on w. Thus, since $P_{Z|R}$ is a noisy channel, we have

$$H(R|Z) = \varepsilon_w > 0 \quad (21)$$

for some constant $\varepsilon_w > 0$ that depends only on w. Furthermore, we obtain

$$I(\widehat{X}_1;\widehat{Y}_1) = 1 - H(\widehat{X}_1|\widehat{Y}_1) = 1 - H_b(\Pr[\widehat{X}_1 \neq \widehat{Y}_1]) \quad (22)$$

where

$$\begin{aligned}
&\Pr[\widehat{X}_1 \neq \widehat{Y}_1] = 2\Pr[X \geq \tau,\ Y \leq -\tau] \\
&\quad = \Pr[X \geq \tau | R = w] \cdot \Pr[Y \leq -\tau | R = w] \\
&\qquad + \Pr[X \geq \tau | R = -w] \cdot \Pr[Y \leq -\tau | R = -w] \\
&\quad = 2\Pr[X \geq \tau | R = w] \cdot \Pr[X \leq -\tau | R = w] \\
&\quad \overset{(a)}{=} 2\left(1 - \Phi\left(\alpha_w - \frac{w}{\sqrt{Q}}\right)\right) \cdot \left(1 - \Phi\left(\alpha_w + \frac{w}{\sqrt{Q}}\right)\right)
\end{aligned} \quad (23)$$

where (a) follows by choosing $\tau = \alpha_w\sqrt{Q}$ as in (18)(a). Combining (22) and (23), we obtain

$$\lim_{Q\to\infty} I(\widehat{X}_1;\widehat{Y}_1) = 1 - H_b(2(1 - \Phi(\alpha_w))^2). \quad (24)$$

Since the right-hand side of (24) approaches 1 as $\alpha_w \to \infty$, we can choose $\alpha_w > 0$, depending only on w, such that

$$1 - H_b(2(1 - \Phi(\alpha_w))^2) \geq 1 - \frac{\varepsilon_w}{2}. \quad (25)$$

Therefore, combining (20), (21), (24), and (25) yields

$$\lim_{Q\to\infty} \Big(I(\widehat{X}_1;\widehat{Y}_1) - I(\widehat{X}_1;\widehat{Z}_1)\Big) \geq \frac{\varepsilon_w}{2}. \quad (26)$$

Furthermore, combining (17), (19), and (26) implies that we can achieve a positive constant SK rate of, e.g.,

$$c_w = \frac{1}{2}(1 - \Phi(\alpha_w))^4 \cdot \frac{\varepsilon_w}{2} > 0$$

when Q is sufficiently large. Setting $c_{\mathcal{W}} = \min_{w\in\mathcal{W}} c_w > 0$ for any arbitrary non-empty set $\mathcal{W} \subseteq \mathbb{R}^+$ concludes the proof. ■

Remark 2. *As a concrete example, for $w = 1$ it suffices to set $\tau = 2\sqrt{Q}$ as the threshold protocol allows to achieve a SK rate of 0.2 bits/channel-use for any sufficiently large finite channel quality ratio $Q > 1$.*

ACKNOWLEDGMENT

O. Günlü was supported by the German Federal Ministry of Education and Research (BMBF) within the national initiative for "Post Shannon Communication (NewCom)" under the Grant 16KIS1004.

REFERENCES

[1] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[2] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography - Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[3] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Int. Conf. Theory Appl. Cryptographic Techn.*, Bruges, Belgium, May 2000, pp. 351–368.

[4] U. Maurer, "The strong secret key rate of discrete random triples," in *Communication and Cryptography — Two Sides of One Tapestry*, R. B. et. al, Ed. Kluwer Academic Publishers, 1994, pp. 271–285.

[5] U. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 499–514, Mar. 1999.

[6] R. Renner, J. Skripsky, and S. Wolf, "A new measure for conditional mutual information and its properties," in *IEEE Int. Symp. Inf. Theory*, Yokohama, Japan, June-July 2003, p. 259.

[7] A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals - Part I," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3973–3996, Aug. 2010.

[8] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, "Key rate of quantum key distribution with hashed two-way classical communication," *Physical Rev. A*, vol. 76, no. 3, pp. 032 312–, Sep. 2007.

[9] A. Orlitsky and A. Wigderson, "Secrecy enhancement via public discussion," in *IEEE Int. Symp. Inf. Theory*, San Antonio, TX, Jan. 1993, p. 155.

[10] A. Gohari, O. Günlü, and G. Kramer, "Coding for positive rate in the source model key agreement problem," *IEEE Trans. Inf. Theory*, vol. 66, no. 10, pp. 6303–6323, Oct. 2020.

[11] L. Kusters, O. Günlü, and F. M. Willems, "Zero secrecy leakage for multiple enrollments of physical unclonable functions," in *Symp. Inf. Theory Sign. Process. Benelux*, Twente, The Netherlands, May-June 2018, pp. 119–127.

[12] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[13] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik, "Secret key generation for a pairwise independent network model," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6482–6489, Dec. 2010.

[14] O. Günlü, "Multi-entity and multi-enrollment key agreement with correlated noise," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1190–1202, 2021.

[15] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, "On the optimality of secret key agreement via omniscience," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2371–2389, Apr. 2018.

[16] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[17] T. Ignatenko and F. M. J. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 956–973, Dec. 2009.

[18] H. Tyagi, "Common information and secret key capacity," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5627–5640, Sept. 2013.

[19] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security trade-offs in biometric security systems - Part I: Single use case," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 122–139, Mar. 2011.

[20] O. Günlü and G. Kramer, "Privacy, secrecy, and storage with multiple noisy measurements of identifiers," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2872–2883, Nov. 2018.

[21] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge, U.K.: Cambridge Uni. Press, 2011.

[22] T. Berger, *Rate Distortion Theory: A Mathematical Basis for Data Compression*. Englewood Cliffs, NJ: Prentice-Hall, 1971.

[23] U. Maurer, "Protocols for secret key agreement by public discussion based on common information," in *Int. Cryptology Conf.*, E. F. Brickell, Ed., Santa Barbara, CA, Aug. 1992, pp. 461–470.

[24] D. Jost, U. Maurer, and J. L. Ribeiro, "Information-theoretic secret-key agreement: The asymptotically tight relation between the secret-key rate and the channel quality ratio," in *IACR Theory Cryptography Conf.*, Panaji, Goa, India, Nov. 2018, pp. 345–369.

[25] M. J. Gander and U. Maurer, "On the secret-key rate of binary random variables," in *IEEE Int. Symp. Inf. Theory*, Trondheim, Norway, June-July 1994, p. 351.

[26] J. Muramatsu, K. Yoshimura, and P. Davis, "Secret key capacity and advantage distillation capacity," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 89, no. 10, pp. 2589–2596, Oct. 2006.

[27] S. Liu, H. C. Van Tilborg, and M. Van Dijk, "A practical protocol for advantage distillation and information reconciliation," *Designs, Codes Cryptography*, vol. 30, no. 1, pp. 39–62, Aug. 2003.

[28] M. Naito, S. Watanabe, R. Matsumoto, and T. Uyematsu, "Secret key agreement by soft-decision of signals in Gaussian Maurer's model," *IEICE Trans. Fundam. Electron. Commun. Comp. Sci.*, vol. 92, no. 2, pp. 525–534, 2009.

[29] O. Günlü, "Key agreement with physical unclonable functions and biometric identifiers," Ph.D. dissertation, TU Munich, Germany, Nov. 2018, published by Dr. Hut Verlag in Feb. 2019.

[30] O. Günlü, T. Kernetzky, O. İşcan, V. Sidorenko, G. Kramer, and R. F. Schaefer, "Secure and reliable key agreement with physical unclonable functions," *Entropy*, vol. 20, no. 5, May 2018.

[31] M. Chiani and D. Dardari, "Improved exponential bounds and approximation for the Q-function with application to average error probability computation," in *IEEE Global Telecommun. Conf.*, vol. 2, Taipei, Taiwan, Nov. 2002, pp. 1399–1402.

[32] I. M. Jacobs and J. M. Wozencraft, *Principles of Communication Engineering.*, 1st ed. London, U.K.: Wiley, Jan. 1965.