Secret-Key-Agreement Advantage Distillation With Quantization Correction

Francesco Ardizzon, *Member, IEEE*, Francesco Giurisato, and Stefano Tomasin, *Senior Member, IEEE*

***Abstract*— We consider a physical layer-based secret-key-agreement (SKA) scenario where Alice and Bob aim at extracting a common bit sequence, which should remain secret to Eve, by quantizing a random number obtained from measurements of their communication channel. We propose an asymmetric advantage distillation protocol where i) Alice quantizes her measurement and sends partial information on it over an authenticated public side channel, and ii) Bob (and Eve) quantizes his measurement by exploiting the partial information. The partial information on the position of the measurement in the quantization interval allows Bob to obtain a quantized value closer to that of Alice. Such strategies are shown to increase the lower bound of the secret key rate.**

***Index Terms*— Advantage distillation, secret-key-agreement, physical layer security.**

I. Introduction

SECRET-KEY-AGREEMENT (SKA) is a security mechanism by which two users, namely Alice and Bob, agree on a common key while keeping it secret from any third malicious user, namely Eve. The secret key can then be used for other security services, e.g., symmetric key encryption or authentication.

Initially proposed by Maurer [1], Ahlswede, and Csiszar [2], physical-layer-based SKA schemes are information-theoretic secure, and their security is based on the physical properties of the channel itself. A source-model SKA procedure involves four steps [3]: *channel probing*, where Alice and Bob transmit in turn probing signals and all agents (including Eve) collect the channel measurements later used to extract the key; *advantage distillation*, by which each agent extracts a bit sequence from his/her measurement; *information reconciliation*, where Alice and Bob exchange information with the aim of reducing the disagreement among the bit sequences; finally, *privacy amplification*, where Alice and Bob extract from the bit sequences the secret key, typically by using universal hashing (for further details see surveys [4] and [5]).

In this letter, we focus on the advantage distillation step. Following the definition of [3], the basic approach requires quantizing the measurement obtained from channel probing. A channel quantization scheme for multiple-input multiple-output channels is proposed in [6], [7], and [8]. In particular, in the strategy of [6] Alice transmits a quantization correction to Bob, the observations have a (known) Gaussian distribution, and the quantizer thresholds are set to provide equiprobable bit sequences (with maximum entropy). However, Eve's observations are assumed to be independent of those of Bob. We consider here instead a more realistic scenario, where the observations' distribution is not known a priori, and Eve's observations are statistically correlated to those of both Alice and Bob.

In [9] a bi-directional advantage distillation is proposed. However, that work focuses only on the last part of advantage distillation, rather than the quantization step. Moreover, we consider a scenario where the agents have limited communication capabilities, therefore it may not be feasible to exploit such a two-way scheme.

Observing that points falling close to the margins of quantization intervals are often responsible for quantization mismatches between Alice and Bob bit sequences after advantage distillation, in [10] the quantization intervals are separated by guard bands (GBs) and samples falling in these regions are discarded. This approach increases the probability of agreement, at the expense of fewer extracted bits. A related approach is also proposed in [11], where the quantizer thresholds are set to assure that each sequence is equiprobable, maximizing the output entropy. An advantage distillation strategy for frequency division duplexing systems has been proposed in [12], where a non-linear transform remaps the measurements to make them uniformly distributed. Next, a uniform quantizer extracts the bit sequence with the aim of maximizing the output entropy. In both works, legitimates' and Eve's channels are considered to be uncorrelated, thus she has no information about the actual bit sequence obtained by Alice and Bob, making the SKA design trivial.

Recently, a technique to extract bits from electrocardiogram signals for wireless body area network has been proposed in [13]. The quantizer thresholds are optimized to maximize both the entropy and the matching rate of the extracted bits. Still, even in this case, no information is leaked to Eve during the channel probing step.

In this letter, we propose a novel advantage distillation strategy for a source-model SKA, where Alice and Bob obtain each a random number and optimize their quantizers to obtain bit sequences providing the highest secret key rate (through a lower bound). We consider the case wherein Eve is observing a channel correlated to that of Alice and Bob, and Eve also overhears any public discussion between Alice and Bob. Then, they coordinate the quantization of the observed feature with

Manuscript received 7 June 2023; revised 7 July 2023; accepted 26 July 2023. Date of publication 1 August 2023; date of current version 12 September 2023. This work was sponsored in part by the NATO Science for Peace and Security Programme under grant no. G5884 (SAFE-UComm). The associate editor coordinating the review of this letter and approving it for publication was P. K. Upadhyay. *(Corresponding author: Francesco Ardizzon.)*

Francesco Ardizzon and Francesco Giurisato are with the Department of Information Engineering, Università degli Studi di Padova, 35131 Padua, Italy (e-mail: francesco.ardizzon@phd.unipd.it; francesco.giurisato@studenti.unipd.it).

Stefano Tomasin is with the Department of Information Engineering, Università degli Studi di Padova, 35131 Padua, Italy, and also with the National Inter-University Consortium for Telecommunications (CNIT), 43124 Parma, Italy (e-mail: stefano.tomasin@unipd.it).

Digital Object Identifier 10.1109/LCOMM.2023.3300462

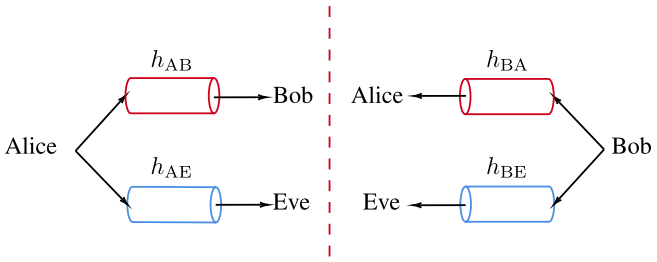

Fig. 1. Scheme of a channel probing procedure.

a discussion over a public authenticated channel. In particular, Alice quantizes her measurement and sends the position of the measurement in the quantization interval over an authenticated public side channel. In turn, Bob (and Eve) quantizes his measurement by exploiting the partial information. We denote the proposed advantage distillation technique as advantage distillation with quantization correction (ADQC). We show that such a strategy allows the extraction of more secret bits from the channel measurements. Finally, with respect to the existing literature, we show that a careful design of the quantizers used during advantage distillation and the transmission of quantization error correction over a public channel allows Alice and Bob to obtain a secret key, even in those harsh scenarios where Eve is close to one of the other agents.

The rest of the letter is organized as follows. Section II introduces the system model. Section III describes the step of the proposed advantage distillation protocol. Section IV presents the numerical results. Section V draws the conclusions.

II. System Model

We consider a scenario where Alice and Bob aim at agreeing on a common bit sequence, which has to remain secret from Eve, using a source model SKA procedure [3]. First, they probe their channel, as shown in Fig. 1: Alice and Bob alternatively send pilot signals through the connecting wireless channel to enable their partner to estimate the channel, so that Alice obtains the estimated channel h_{BA} and Bob obtains estimated channel h_{AB}.

We assume Alice and Bob have already agreed on a feature selection and extraction function such that Alice extracts x from h_{BA}, while Bob extracts y from h_{AB}. We focus on the scalar case where x and y are real numbers, although the SKA will operate on sequences of x and y, thus using longer observation sequences. We remark that, in general, the channels are only partially reciprocal, therefore x and y will be strongly correlated but not identical.

Eve is modeled as a passive attacker. Assuming that pilot signals and feature extraction procedures are publicly known, from the pilot exchange, Eve estimates channels h_{AE} and h_{BE}, from Alice and Bob, respectively. Eve uses an extraction function to obtain her estimate z of channel feature x. However, since Eve is not in the same position as neither Alice nor Bob, z will differ from both x and y. In particular, thanks to the (partial) channel reciprocity, we have that x and y are more similar (i.e., higher mutual information) than z and x (or y).

Still, if Eve is not too far from Alice or Bob, there exists a non-negligible correlation between z and both x and y.

We assume that the statistics of x, y, and z are not known in close form, but a dataset of measurements (x, y, z) is available to Alice, Bob, and Eve, used for the design of the SKA procedure.

An authenticated public side channel is also available, over which Alice and Bob can exchange information, while Eve overhears any communication. Channel coding is used on this side channel, allowing Bob to detect and correct, with arbitrarily small error probability, any error of publicly exchanged information.

Note that since the side channel is public, data transmitted on it will not be confidential to Alice and Bob. Moreover, we consider a rate limitation on this channel.

III. Advantage Distillation With Quantization Correction

We now describe the ADQC technique. Let us introduce the binary space $\mathcal{S} = \{0, 1\}^b$ containing $M = 2^b$ different binary sequences, each of b bits. Alice and Bob aim at drawing two sequences, $\boldsymbol{s}_{\mathrm{A}} \in \mathcal{S}$ and $\boldsymbol{s}_{\mathrm{B}} \in \mathcal{S}$, by processing the observed channel features x and y, respectively.

The problem of associating a real number (in this case, the feature measurement) to a binary sequence can be seen as a quantization problem that partitions the set of real numbers into M intervals so that the m-th interval is associated with the sequence $\boldsymbol{s}_m \in \mathcal{S}$. A quantizer q provides a (real) number, $\tilde{x} = q(x)$, and each of the M outputs is mapped to a binary sequence $\boldsymbol{s}$.

First, note that the quantizers used by Alice, Bob, and Eve are chosen before the actual key agreement protocol, as will be detailed later. Moreover, we consider a worst-case scenario where all quantizers are publicly known. However, both the secrecy and the randomness of the scheme still lie in the extracted channel measurements.

Now, we aim to obtain an advantage distillation process such that $\boldsymbol{s}_{\mathrm{A}}$ is as close as possible to $\boldsymbol{s}_{\mathrm{B}}$ without revealing information to Eve. We can write Bob's measurements as Alice's measurements corrupted by an error ϵ, i.e.,

$$y = x + \epsilon. \tag{1}$$

Let $q_{\mathrm{A}}(x)$ be the quantized value at Alice, and let $\eta = x - q_{\mathrm{A}}(x)$ be the quantization error at Alice. Then, from (1) we have

$$y = q_{\mathrm{A}}(x) + \eta + \epsilon. \tag{2}$$

In general, note that η and ϵ are statistically dependent. However, ignoring this dependency, we have that y is turned away from the quantization value $q_{\mathrm{A}}(x)$ by both errors η and ϵ. Thus, to improve the advantage distillation procedure, in ADQC Alice communicates over the public channel the value of the quantization error η so that Bob computes

$$y' = y - \eta = q_{\mathrm{A}}(x) + \epsilon, \tag{3}$$

and quantizes y' with his quantizer $q_{\mathrm{B}}(\cdot)$ to obtain the bit sequence $\boldsymbol{s}_{\mathrm{B}}$. Note that, even with this adjustment, we have $y' \neq q_{\mathrm{A}}(x)$, due to the error ϵ.

If Alice uses B bits to feedback η over the public channel, we must quantize η. To this end, each quantization interval is split into $K = 2^B$ sub-intervals of equal length, and (a binary representation) of the index of the sub-interval in which η is falling is transmitted over the public channel. Then, Alice transmits

$$\xi = \left\lceil \eta \frac{K}{L^{(\mathrm{A})}(x)} \right\rceil \in [1, K] , \tag{4}$$

where $L^{(\mathrm{A})}(x)$ is the length of the quantization interval of x.

Upon reception of ξ, Bob computes

$$\eta' = \frac{L^{(\mathrm{B})}(y)}{K} \left(\xi - \frac{1}{2} \right) , \tag{5}$$

where $L^{(\mathrm{B})}(y)$ is the length of quantization interval of y. Then Bob uses η' instead of η in (3) to quantize y' with $q_{\mathrm{B}}(\cdot)$.

Eve applies the same procedure of Bob, by computing its own correction factor η'' and applying it to its measurement z before quantizing it with $q_{\mathrm{E}}(\cdot)$ to obtain sequence $\boldsymbol{s}_{\mathrm{E}}$. However, there will be a higher probability that $z' = z - \eta''$ falls in another interval than x, thus the correction factor won't provide the same benefit on the sequence extraction of Bob. Moreover, since ξ is a normalized version of η with respect to $L_{\mathrm{A}}(x)$, it does not reveal any information on the interval of the quantized value $q_{\mathrm{A}}(x)$.

A. Quantizer Design

We are now left with the design of the Alice, Bob, and Eve quantizers, i.e., q_{A}, q_{B}, and q_{E}, respectively.

Note that a quantizer q with M quantization intervals is fully defined by the position of $M + 1$ thresholds, $\mathcal{T} = \{T_i, i = 0, \ldots, M\}$, where the saturation values $T_0 = T_{\min}$ and $T_M = T_{\max}$ are set to match a predefined saturation probability.[1] Let $\mathcal{T}_{\mathrm{A}}$, $\mathcal{T}_{\mathrm{B}}$, and $\mathcal{T}_{\mathrm{E}}$ be sets of thresholds used for the three quantizers. The design metric is the lower bound on the secret-key capacity for the source model [1], [3, Ch. 4], i.e.,

$$C_{\mathrm{sk}}^{\mathrm{low}}(\mathcal{T}_{\mathrm{A}}, \mathcal{T}_{\mathrm{B}}, \mathcal{T}_{\mathrm{E}}) = I(\boldsymbol{s}_{\mathrm{A}}; \boldsymbol{s}_{\mathrm{B}}) - \min \{ I(\boldsymbol{s}_{\mathrm{A}}; \boldsymbol{s}_{\mathrm{E}}), I(\boldsymbol{s}_{\mathrm{B}}; \boldsymbol{s}_{\mathrm{E}}) \} , \tag{6}$$

where $I(\boldsymbol{v}_1; \boldsymbol{v}_2)$ is the mutual information between the bit sequences $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$. Alice and Bob aim at designing the quantizers q_{A} and q_{B} to increase $C_{\mathrm{sk}}^{\mathrm{low}}$, i.e., by increasing the agreement between Alice's and Bob's extracted bit sequences, while limiting the amount of information revealed to Eve. Eve in turn aims at minimizing $C_{\mathrm{sk}}^{\mathrm{low}}(\mathcal{T}_{\mathrm{A}}, \mathcal{T}_{\mathrm{B}}, \mathcal{T}_{\mathrm{E}})$ with a proper choice of her quantizer q_{E}.

The quantizers are then designed using the following iterative procedure. Starting from uniform quantizers on a predefined range, at each iteration Eve optimizes her quantizer

$$\hat{\mathcal{T}}_{\mathrm{E}} = \arg\min_{\mathcal{T}_{\mathrm{E}}} C_{\mathrm{sk}}^{\mathrm{low}}(\mathcal{T}_{\mathrm{A}}, \mathcal{T}_{\mathrm{B}}, \mathcal{T}_{\mathrm{E}}) , \tag{7}$$

with $\mathcal{T}_{\mathrm{A}}$ and $\mathcal{T}_{\mathrm{B}}$ fixed. Next, Alice and Bob optimize their own

$$[\hat{\mathcal{T}}_{\mathrm{A}}, \hat{\mathcal{T}}_{\mathrm{B}}] = \arg\max_{\mathcal{T}_{\mathrm{A}}, \mathcal{T}_{\mathrm{B}}} C_{\mathrm{sk}}^{\mathrm{low}}(\mathcal{T}_{\mathrm{A}}, \mathcal{T}_{\mathrm{B}}, \hat{\mathcal{T}}_{\mathrm{E}}) . \tag{8}$$

[1]Samples eventually falling outside the region $[T_{\min}, T_{\max}]$ are remapped to the closest interval.

We remark that, since $C_{\mathrm{sk}}^{\mathrm{low}} \leq I(\boldsymbol{s}_{\mathrm{A}}, \boldsymbol{s}_{\mathrm{B}}) \leq H(s_{\mathrm{A}})$ (or $H(s_{\mathrm{B}})$), i.e., the entropy of $\boldsymbol{s}_{\mathrm{A}}$ (or $\boldsymbol{s}_{\mathrm{B}}$), we are also implicitly taking into account also the actual bit-sequence output distribution when maximizing (8), thus avoiding quantizers that lead to a low bit-sequence entropy.

Alice, Bob, and Eve set the quantizers $\hat{q}_{\mathrm{A}}$, $\hat{q}_{\mathrm{B}}$, and $\hat{q}_{\mathrm{E}}$, from the new thresholds $\hat{\mathcal{T}}_{\mathrm{A}}$, $\hat{\mathcal{T}}_{\mathrm{B}}$, and $\hat{\mathcal{T}}_{\mathrm{E}}$. The optimizations are performed via numerical methods, e.g., by using the genetic algorithm, as neither (7) nor (8) are convex, therefore the solutions obtained are, in general, only locally optimal. Thus, the procedure is repeated either until convergence is reached or a maximum number of iterations has been performed.

Finally, notice that maximizations (7) and (8) require the evaluation of the mutual information, thus the output bit sequence distributions which, in turn, depends on the input measurements' distributions that is not known a priori, thus algorithms relying instead on a single-sample metric (e.g., the Euclidean distance in the Linde-Buzo'Gray algorithm), are not suitable for this problem.

B. Advantage Distillation Vs Information Reconciliation With Limited-Rate Public Channel

When the public channel has no rate limitations, a large number of bits, B describing the quantization error can be used to improve the agreement between the bit sequences extracted by Alice and Bob. We consider now a scenario where the side-channel rate is limited. The same channel is used for both advantage distillation (to share the error correction) and information reconciliation. Hence, we must allocate the number of bits to be used for both processes, in a trade-off between the quality of the advantage distillation and information reconciliation phases.

For ADQC, B bits are transmitted for each quantized sample. On the other hand, for information reconciliation, we consider the linear error-correcting code (k, n)-based strategy proposed in [14], where the extracted sequence $\boldsymbol{s}_{\mathrm{A}}(x)$ of $n > k$ bits obtained from advantage distillation is considered a corrupted codeword of the linear code and, during reconciliation, Bob shares $n - k$ redundancy bits over the public channel. Then, Alice and Bob use the redundancy bits to correct their sequences. Thus, the number of bits shared on the public channel for each bit of the extracted bit sequence $\boldsymbol{s}_{\mathrm{A}}(x)$ is $\beta \triangleq B/b$, with $\beta = 0$ when no information is shared during advantage distillation, in what we will denote as no error correction (NEC) technique.

Now, thanks to Shannon's theorem on channel capacity (with input $\boldsymbol{s}_{\mathrm{B}}$ and output $\boldsymbol{s}_{\mathrm{A}}$), for $n \to \infty$ and assuming perfect coding, Alice and Bob will recover the same codeword with high probability when the following relation is satisfied

$$\frac{k}{n} \geq \frac{I(\boldsymbol{s}_{\mathrm{A}}; \boldsymbol{s}_{\mathrm{B}})}{b} = C_{\mathrm{AB}}. \tag{9}$$

In the following, we will consider the value of k that satisfies (9) at the equality.

We introduce now the cost function γ representing the ratio between the numbers of bits shared on the side channel for the ADQC and the NEC techniques. For the same number of measurements (thus for the same n), the ADQC and

NEC techniques generate $k^{(\mathrm{ADQC})}$ and $k^{(\mathrm{NEC})}$ secret-key bits, respectively. Then, γ is computed as

$$\gamma \triangleq \frac{n - k^{(\mathrm{ADQC})} + \beta n}{n - k^{(\mathrm{NEC})}} = \frac{1 + \beta - C_{\mathrm{AB}}^{(\mathrm{ADQC})}}{1 - C_{\mathrm{AB}}^{(\mathrm{NEC})}}, \tag{10}$$

where $C_{\mathrm{AB}}^{(\mathrm{ADQC})}$ and $C_{\mathrm{AB}}^{(\mathrm{NEC})}$ are the (scaled) mutual information between Alice and Bob bit sequences for the ADQC and NEC techniques, respectively. This relation will be used in Section IV to evaluate the efficiency of the ADQC in the limited-rate public channel.

IV. Numerical Results

In this Section, we report the performance of the ADQC technique and compare it with both the NEC and the GB technique [10]. We considered NEC with both uniform and optimized quantizers, where the thresholds are chosen to maximize the output entropy [12].

Vector $\boldsymbol{v} = [x\, y\, z]^{\mathrm{T}}$ of Alice's, Bob's, and Eve's measurements is a jointly Gaussian vector having zero-mean and covariance

$$\boldsymbol{\Sigma} = \mathbb{E}[\boldsymbol{v}\boldsymbol{v}^{\mathrm{T}}] = \begin{bmatrix} 1 & \rho_{\mathrm{AB}} & 0.8 \\ \rho_{\mathrm{AB}} & 1 & 0.8 \\ 0.8 & 0.8 & 1 \end{bmatrix}, \tag{11}$$

where we fixed the correlation between legitimates and Eve features to $\rho_{\mathrm{AE}} = \rho_{\mathrm{BE}} = 0.8$. Next, we let ρ_{AB} varying in the interval $\rho_{\mathrm{AB}} \in [0.8, 1]$. The saturation thresholds are set at $T_{\max} = -T_{\min} = 6$, yielding a saturation probability $P_{\mathrm{sat}} \leq 2 \cdot 10^{-9}$.

We considered $B = 1$ and $2\,\mathrm{bit}$ of quantization error correction. For both ADQC and NEC techniques, quantizers are either optimized as described in the previous section or uniform, with $M - 1$ thresholds, placed uniformly in $[-T_{\min}, T_{\max}]$. For the GB technique, the quantizer is uniform and guard bands are set to 0.85, to maximize the secret key capacity lower bound.

Fig. 2 shows the Alice quantizer's thresholds $\mathcal{T}_A$ obtained using the ADQC for $\rho_{\mathrm{AB}} \in [0.8, 1]$ and $\rho_{\mathrm{AE}} = \rho_{\mathrm{BE}} = 0.8$. We also report the Gaussian PDF of the channel measurements (in gray), which does not depends on ρ_{AB}. Interestingly, for high values of correlation ρ_{AB} it is more convenient for Alice and Bob to decrease the length of the interval in the middle, enlarging instead the external ones. Each region corresponds to one s_m, associated to one of the M bit possible bit sequences in $\mathcal{S}_{\mathrm{A}}$.

Fig. 3 shows $C_{\mathrm{sk}}^{\mathrm{low}}$ for the considered SKA techniques when extracting $b = 3\,\mathrm{bit}$ per sample. We remark that the GB technique discards samples falling on the guard bands, reducing the observation rate (and in general the secret key rate). The best performance is in fact achieved by ADQC with optimized quantizers, thus, sharing information during the advantage distillation is advantageous. In particular, optimizing the quantizers and using ADQC yields on average a 60% improvement of the secrecy capacity, more than doubling it for low correlation values, i.e., when $\rho_{\mathrm{AB}} \approx \rho_{\mathrm{AE}} = \rho_{\mathrm{BE}} = 0.8$. We remark that this last scenario, actually models the case where the channel measured by the attacker is almost equal to that of the legitimate user, a situation occurring, e.g., when the attacker is close to one of the users. Note that even the NEC technique with optimized quantizers yields a higher $C_{\mathrm{sk}}^{\mathrm{low}}$ with respect to both [10] and NEC with uniform quantizers.

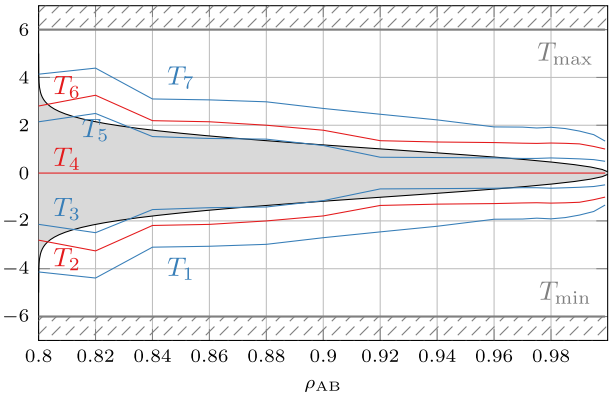

Fig. 2. Optimal Alice thresholds $\mathcal{T}_{\mathrm{A}}$ using ADQC, as function of ρ_{AB} and for $\rho_{AE} = 0.8$, $b = 3\,\mathrm{bit}$, and $B = 1\,\mathrm{bit}$. The saturation values set to $T_{\max} = -T_{\min} = 6$. The Gaussian PDF of the channel measurements is reported in filled gray.

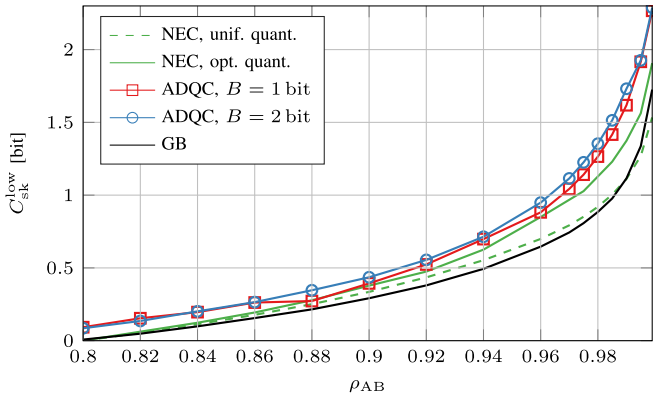

Fig. 3. Lower-bound of the secret-key capacity for $b = 3\,\mathrm{bit}$, $\rho_{\mathrm{AB}} \in [0.8, 1]$ and $\rho_{\mathrm{AE}} = \rho_{\mathrm{BE}} = 0.8$, achieved when Alice, Bob, Eve use uniform quantizers, the GB method, and the ADQC with no quantization error correction transmission, $B = 2$ and $3\,\mathrm{bit}$.

TABLE I

Lower Bound of the Secret-Key Capacity Achieved With ADQC, for $\rho_{\mathrm{AB}} \in [0.8, 1]$, $\rho_{\mathrm{AE}} = \rho_{\mathrm{BE}} = 0.8$, $B = 2\,\mathrm{bit}$, and $b = 2$, 3, and $4\,\mathrm{bit}$

b [bit]	$C_{\mathrm{sk}}^{\mathrm{low}}$ [bit]									
	0.80	0.84	0.88	0.90	0.92	0.94	0.96	0.98	0.99	0.995
2	0.084	0.185	0.297	0.377	0.486	0.601	0.764	1.010	1.199	1.305
3	0.086	0.202	0.347	0.436	0.555	0.714	0.949	1.354	1.731	1.896
4	0.095	0.247	0.314	0.414	0.577	0.779	1.039	1.455	1.867	2.305

Table I shows the performance of the ADQC with $B = 2\,\mathrm{bit}$ used for quantization error correction and for $b = 2$, 3, and $4\,\mathrm{bit}$ extracted bits per measurement. Increasing the number of bits extracted from the channel yields a higher $C_{\mathrm{sk}}^{\mathrm{low}}$, even sharing just $B = 2\,\mathrm{bit}$ of error correction.

We now consider the case of limited side-channel rate, described in Section III-B, focusing on the NEC and ADQC techniques, both with optimized quantizers. Fig. 4 shows γ as a function of the correlation ρ_{AB}, with $b = 2$, 3, or $4\,\mathrm{bit}$, and $B = 1$ or $2\,\mathrm{bit}$. We first note that for $B = 1\,\mathrm{bit}$

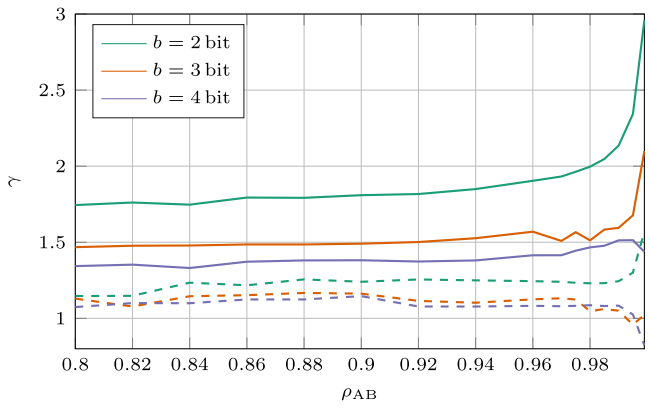

Fig. 4. Cost γ vs correlation ρ_{AB} with $\rho_{\mathrm{AE}} = \rho_{\mathrm{BE}} = 0.8$, for scenarios $B = 1$ bit (dashed lines) and $B = 2$ bit (solid lines), with $b = 2$, 3, and 4 bit.

(thus a very limited side-channel overhead due to quantization error correction) the number of bits exchanged on the side channel is very close for both ADQC and NEC schemes (i.e., $\gamma \approx 1$). Indeed, for high values of ρ_{AB} the ADQC technique requires even fewer bits than NEC (for $b = 3$ and 4 bit) since the extracted bit sequences are more similar and information reconciliation is less demanding. Instead, when we consider $B = 2$ bit, we note that the data rate of the side channel increases by a factor of 3 (for highly correlated channels) to obtain however a higher secrecy capacity as from Fig. 3.

V. Conclusion

We have proposed an advantage distillation technique for physical layer-based SKA, where Alice transmits via a publicly authenticated channel a correction that is exploited by Bob and eventually, by Eve to correct their measurements. Numerical results show that both the quantizer optimization and the correction transmission allow Alice and Bob to achieve a higher lower bound of the secret key capacity, even when Eve optimizes her quantizers as well. Additionally, we showed that the lower bound of the secrecy key rate per bit shared on the public channel is higher when correction is used, revealing an efficient use of the public channel by this technique.

References

[1] U. M. 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. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[3] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[4] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the uncertainty: Authentication and confidentiality by physical-layer processing," *Proc. IEEE*, vol. 103, no. 10, pp. 1702–1724, Oct. 2015.

[5] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao, and A. Hu, "Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities," *Entropy*, vol. 21, no. 5, p. 497, May 2019.

[6] C. Chen and M. A. Jensen, "Improved channel quantization for secret key establishment in wireless systems," in *Proc. IEEE Int. Conf. Wireless Inf. Technol. Syst.*, Aug. 2010, pp. 1–4.

[7] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, Feb. 2011.

[8] J. W. Wallace, C. Chen, and M. A. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *Proc. 3rd Eur. Conf. Antennas Propag.*, Mar. 2009, pp. 1499–1503.

[9] Y. Feng, X.-Q. Jiang, J. Hou, H.-M. Wang, and Y. Yang, "An efficient advantage distillation scheme for bidirectional secret-key agreement," *Entropy*, vol. 19, no. 9, p. 505, Sep. 2017.

[10] O. Graur, N. Islam, and W. Henkel, "Quantization for physical layer security," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2016, pp. 1–7.

[11] M. Adil, S. Wyne, and S. J. Nawaz, "On quantization for secret key generation from wireless channel samples," *IEEE Access*, vol. 9, pp. 21653–21668, 2021.

[12] E. O. Torshizi and W. Henkel, "Reciprocity and secret key generation for FDD systems using non-linear quantization," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2022, pp. 927–932.

[13] A. V. Guglielmi, A. Muraro, G. Cisotto, and N. Laurenti, "Information theoretic key agreement protocol based on ECG signals," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2021, pp. 1–6.

[14] E. Biham, M. Boyer, P. Boykin, T. Mor, and V. Roychowdhury, "A proof of the security of quantum key distribution," *J. Cryptol.*, vol. 19, pp. 381–439, Oct. 2006.

Open Access funding provided by 'Università degli Studi di Padova' within the CRUI CARE Agreement