DOI: 10.61782/fa.2023.0207

ADVANTAGE-DISTILLATION STRATEGIES WITH SIDE INFORMATION FOR UNDERWATER ACOUSTIC CHANNELS

Francesco Ardizzon[1*] **Francesco Giurisato**[1] **Stefano Tomasin**[1,2]

[1] Department of Information Engineering
[2] Department of Mathematics, University of Padua, Italy
and National Inter-University Consortium for Telecommunications (CNIT), Italy

ABSTRACT

Many military and civil applications using underwater acoustic channels (UWACs) are paired with security services, providing, for instance, secrecy and authenticity to the communication. These mechanisms however often require periodically renewed symmetric keys among two communicating devices, namely Alice and Bob. To this end, secret keys can be agreed upon using the physical-layer communication channel, leveraging, in particular, the reciprocity and randomness of the UWAC to extract a common key that remains secret to an attacker (Eve). In this paper, we propose a novel solution for the advantage-distillation part of the secret key generation procedure. After channel probing, the advantage of distillation lets Alice and Bob extract a sequence of bits from their own (analog) measurements. We propose an asymmetric advantage-distillation protocol with two novel features: i) the quantizers used by Alice and Bob are derived maximizing the secret key capacity cooperating through a public channel and ii) Alice transmits a correction over a public authenticated side channel. Numerical results prove the effectiveness of our approach, showing that exchanging a few bits of information before information reconciliation allows extracting more secret bits from the channel.

Keywords: *Secret Key Generation, Physical Layer Security, Underwater Acoustic Communications.*

1. INTRODUCTION

Several applications exploit underwater acoustic channels (UWACs), e.g., seabed monitoring, contamination control, and search-and-survey operations. In these contexts, it is often necessary to have multiple devices on-site communicating among them. Due to the relevance of such communications, it is advisable to protect them with secrecy and authenticity mechanisms, ensuring that no malicious node is infiltrating the network. However, these solutions typically require symmetric keys among legitimate devices that must be periodically reviewed. To this end, the first option could be to directly load the keys into the devices' memory. Still, an attacker may capture a device and endanger the security of the whole network. Secondly, such a solution would make the network non-scalable, since every time a new device joins the network a new set of keys needs to be distributed to the rest of the nodes.

Another solution is instead to generate the keys on the field, after the deployment, resorting to secret key agreement (SKA). This security mechanism lets a pair of users, namely Alice and Bob agree on a common key, which remains secret to any third malicious user, namely Eve. Security mechanisms operating with this strategy can be divided into two main categories: cryptography-based and physical layer-based. Cryptographic-based solutions, such as the Diffie-Hellman key agreement protocol [1, Ch. 11], are computationally secure. However, they have high computational and energy costs, which may be unsuitable for underwater acoustic networks (UWANs). On the other hand, physical layer-based solutions have been initially proposed by Maurer in [2], and by Ahlswede and Csiszar [3], and are information-theoretic secure. These

*[*Corresponding author*: francesco.ardizzon@phd.unipd.it.

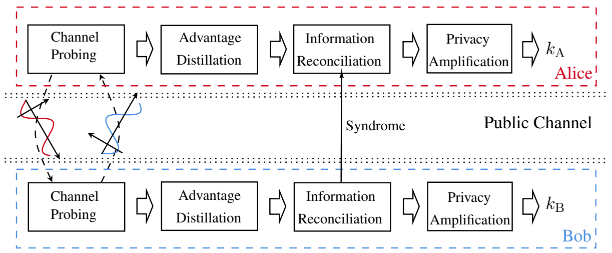


Figure 1: General scheme of a SKA procedure for Alice and Bob.

mechanisms base their security on the physical properties of the channel, such as its reciprocity and unpredictability for third-party devices. Thus, these solutions typically i) require less energy than cryptography-based solutions, and ii) provide security that does not depend on the computational capabilities of the attacker. Indeed, these solutions are said to be quantum-resistant, since these could withstand attacks from quantum computer algorithms, e.g., by using Shor's algorithm [4]. Moreover, such solutions are particularly suitable for the UWAC scenario, where the unpredictability of the channel, e.g., due to large Doppler effect and strong multipath interferences can be exploited to draw more randomness from the channel (i.e. longer or more secure keys). Surveys on the physical-layer SKA protocol, can be found [5] and [6], with a focus on UWACs-based solutions in [7] and [8].

As detailed in [9], a source-model SKA procedure involves four steps: *channel probing*, where the users exchange probing signals and collect the channel measurements from which they will later extract the keys; *advantage distillation* where each user quantizes the measurements to obtain a bit sequence; *information reconciliation*, where Alice and Bob exchange information with the aim of reducing the disagreement between their extracted sequences; lastly, *privacy amplification* where from the bit sequences each user extract a shorter sequence secret to Eve. The SKA procedure is summarized in Fig. 1.

While, typically, only the channel probing and the information reconciliation involve exchanges of information between Alice and Bob (which are also received by Eve), we consider a SKA scheme where some information, i.e., quantization error of Alice, is shared during advantage distillation as well. In [10], later extended in [11], the authors proposed a channel quantization scheme for multiple-input multiple-output (MIMO) channels, where Alice also transmits a quantization correction to Bob. However, the observations are assumed to be Gaussian distributed, with a known mean and variance, therefore the quantizer thresholds are set to output an equal probability sequence, maximizing the entropy of the output bit-sequence. Still, they assume Eve's observations to be spatially decorrelated to Alice's (and Bob's), while we consider a more general case where i) the features' distribution is not known a priori, and ii) the eavesdropper observations are statistically correlated to the legitimate ones.

Concerning channel-model SKA, an advantage-distillation technique where Alice and Bob exchange information and discard the bits associated with a low log-likelihood ratio is proposed in [12]. A technique based instead on code scrambling is proposed in [13]. Still, both approaches actually work on a discrete domain, i.e., after quantization. We propose instead a strategy where the information exchange happens prior to the actual quantization step.

A technique to extract bits from electrocardiograms (ECGs) signals for wireless body area networks (WBANs) was proposed in [14]. Still, they assume that no information is leaked to Eve during the channel probing step, due to the particular nature of the channel. In [15], they propose a quantization strategy for fifth-generation (5G) cellular network wireless channels, based on the received signal strength (RSS) from the fading channels. However, there, Eve is assumed to have sufficient spatial separation to experience a statistically independent fading. Differently from these works, we consider instead a general scenario, where also Eve is taken into consideration.

In [16] and [17] a complete protocol for SKA in UWACs is proposed. Still, the proposed technique exploits a quantizer whose bin size is determined by the standard deviation of each feature, assuming an underlying Gaussian distribution. We make instead no assumption on the actual feature distribution, proposing an optimization of the quantizer based on previously collected datasets.

In this paper, we propose a novel advantage-distillation strategy for the source model SKA, the advantage distillation with quantization correction (ADQC). While in [18], we discussed an advantage-distillation strategy for an ideal scalar Gaussian process, here we consider here a realistic scenario, where two sensors of an UWAN are exploiting the UWACs's measurements to extract the secret key. In particular, the main contributions of this paper are:

- before the actual SKA, first Alice and Bob process the channel features' measurements to obtain a set of uncorrelated measurements;
- next, Alice and Bob optimize their quantizers as-

suming a worst-case scenario where also Eve is able to optimize her own quantizer;

- during advantage distillation, Alice shares with Bob some information so that Bob (partially) corrects the errors without leaking information to Eve;

- the effectiveness of the approach is verified on an experimental dataset, collected during a sea experiment.

The rest of the paper is organized as follows. Section 2 introduces the system model. Section 3 describes the steps of the proposed advantage-distillation protocol. Section 4 presents the numerical results. Section 5 draws the conclusions.

2. SYSTEM MODEL

Two users, namely Alice and Bob, aim at agreeing on a common key that has to stay secret to an eavesdropper, Eve, by using the source-model SKA procedure described in [9]. The key could be stored and later used for security services, e.g., for secrecy or authentication.

We focus on the second step of the SKA procedure, the advantage distillation, assuming that the channel probing step has been already performed. More in detail, Alice and Bob alternatively exchanged pilot signals through the channel and they both estimated the channel power-delay responses h_{BA} and h_{AB}, for Alice and Bob, respectively. Alice extracts from h_{BA} the features $\boldsymbol{x} \in \mathbb{R}^N$, while Bob obtains $\boldsymbol{y} \in \mathbb{R}^N$ from h_{AB}. In detail, each entry of $\boldsymbol{x}$ (or $\boldsymbol{y}$) corresponds to one of the selected channel features. Possible candidates are the number of channel taps, the average tap power, the root mean square (RMS) delay, and the smoothed received power, as discussed in [19,20]. Still, another possible set of channel features is reported instead in [16].

We consider Eve to be a passive attacker that estimates (exploiting pilot signals transmitted by both Alice and Bob) the power delay responses h_{AE} and h_{BE}. Next, Eve exploits the estimated power delay responses to extract $\boldsymbol{z} \in \mathbb{R}^N$.

In general, UWACs are only partially reciprocal, hence features vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ are not identical but strongly correlated with also noise affecting the correlation between the two estimates. Indeed, if Eve is far enough from Alice and Bob, with high probability we have both $\boldsymbol{y} \neq \boldsymbol{z}$ and $\boldsymbol{x} \neq \boldsymbol{z}$. Still, we consider a more challenging scenario where Eve is not too far from the legitimate users, thus her observation $\boldsymbol{z}$ and the legitimate measurements $\boldsymbol{x}$ and $\boldsymbol{y}$ are statistically related.

We assume that a public dataset containing as entries the features measurements ($\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{z}$) is publicly available. Later, this will be exploited to design the user quantizer, used to extract the bit sequence from the feature measurements.

An authenticated side channel is available, over which Alice can broadcast information. A channel coding scheme is exploited on this channel, allowing Bob to detect and correct errors, with an error probability arbitrarily small. We assume that this channel is public, thus any information will be overheard by Eve as well.

3. ADVANTAGE-DISTILLATION PROTOCOL

In this Section, we describe the ADQC advantage-distillation strategy that will be used by Alice and Bob to distill from the measurement the bit sequence, later used to extract the key. Formally, from features x and y each user has to distill the bit string $\boldsymbol{s}_{\mathrm{A}} \in \mathcal{S}$ and $\boldsymbol{s}_{\mathrm{B}} \in \mathcal{S}$ with $\mathcal{S} = \{0,1\}^b$.

However, finding the best function associating a real number, such as the feature measurement, with a binary sequence can be seen as the optimization problem of a quantizer. Indeed, to extract a Q bit sequence, we must partition the input space into $M = 2^b$ intervals, $\mathcal{I}_m$ with $m = 1, \ldots, M$, each associated with one of the M binary sequences belonging to the string space $s_m \in \mathcal{S}$. To ease the reconciliation and the privacy amplification process, the bit sequence $\boldsymbol{s}_m \in \mathcal{S}$ is associated with each interval $\mathcal{I}_m$ by using Gray coding. Thus, for a generic measurement a, collected by the user with quantizer $q(\cdot)$ the bit string will simply be $\boldsymbol{s} = q(a)$.

For instance, Alice extracts the vector of features measurements $\boldsymbol{x}$ from the channel impulse h_{AB}. Note that, in general, the components of the feature measurement vector, $\boldsymbol{x} = [x_1, \ldots, x_N]$ are not independent, thus it would be suboptimal to quantize and process each feature separately. On the other hand, a procedure involving the design (or even the update) of a multidimensional quantizer could be too expensive for many practical applications, where the devices are energy-constrained. We propose a decorrelation step.

As also detailed in [18], the proposed protocol requires also a joint quantizer design and the use of quantization error correction. We remark that the quantizers used by Alice, Bob, and Eve are designed before the actual SKA procedure. Eventually, these can be periodically updated to cope with the channel variability over time. Being the datasets used to compute the quantizers public, we consider a scenario where the quantizers derived from such datasets are publicly known as well. Still, note that the performance of our scheme depends on the secrecy and the randomness of the extracted channel measurements and not on the actual quantizers' choice.

Concerning the quantization correction, during the actual advantage-distillation step of the SKA, Alice will compute $\boldsymbol{s}_m = q_{\mathrm{A}}(\boldsymbol{x})$ and transmit over the side channel a quantization error correction. This is exploited by Bob, and, eventually, by Eve, to correct his own measurement.

In the next Sections, we detail both the decorrelation step, the quantizer design, and the correction computation steps.

3.1 Decorrelation Step

We propose here the decorrelation step that allows computing a vector of independent components from the vector of channel features' measurements. Next, we can quantize each feature independently and concatenate the obtained bit sequences. The procedure involves the inverse sampling method, used also to generate random variables with arbitrarily chosen distribution [21].

While for simplicity, we describe the procedure for Alice's observations, the procedure can directly be used also by Bob (and Eve). First, we assume the distribution of each i-th channel feature to be either known, with cumulative distribution function (CDF) $F_{x_i}(x)$. Next, we compute

$$x'_i = F_{\mathrm{G}}^{-1}(F_{x_i}(x)) \;, \tag{1}$$

where $F_{\mathrm{G}}(x)$ is the CDF of a standard normal distribution. This provides a jointly-Gaussian vector $\boldsymbol{x}'$. Next, we decorrelate these variables by computing

$$\boldsymbol{x}'' = \boldsymbol{V}\boldsymbol{x}' \;, \tag{2}$$

where $\boldsymbol{V}$ is the matrix whose columns are the eigenvectors associated with Alice's dataset. Finally, we remap these values back to the original domain as

$$\tilde{x}_i = F_{x_i}^{-1}(F_{\mathrm{G}}(x)) \;. \tag{3}$$

We remark that after this process the features will have different statistical power, thus affecting the covariance between the features. Moreover, this method is related to the well-known principal component analysis (PCA). Hence for instance, after the decorrelation step, it could be also possible to discard low-power features, thus saving computational power with a minimal impact on the number of extracted secret bits.

3.2 Quantizers Design

Here, we detail the design of the Alice, Bob, and Eve quantizers, i.e., q_{A}, q_{B}, and q_{E}. Since, thanks to the previous step, each feature is statistically independent, we can design a scalar quantizer for each feature, overall obtaining NQ bit per channel measurement. However since the processing does not depend on the specific feature, we detail the procedure for a generic triplet of scalar features (x, y, z) for Alice, Bob, and Eve.

First, note that a generic quantizer q with M quantization intervals is fully defined by the position of $M-1$ thresholds, $\mathcal{T} = \{T_i, i = 0, \ldots, M+1\}$, as the saturation values $T_0 = T_{\min}$ and $T_{M+1} = T_{\max}$ are public and set to match a predefined saturation probability. Samples falling outside the region $[T_{\min}, T_{\max}]$ are remapped to the closest interval. Thus, we define as $\mathcal{T}_{\mathrm{A}}$, $\mathcal{T}_{\mathrm{B}}$, and $\mathcal{T}_{\mathrm{E}}$ the sets of thresholds used for the Alice, Bob, and Eve quantizers, respectively. Our aim is then to find the best thresholds for Alice and Bob, assuming that Eve is able to optimize also her own quantizer, i.e., her own thresholds.

The next step is to introduce a proper optimization metric. Given the pair of quantizers q_{A} and q_{B}, which give as output the bit sequences $\boldsymbol{s}_{\mathrm{A}} = q_{\mathrm{A}}(x)$ and $\boldsymbol{s}_{\mathrm{B}} = q_{\mathrm{B}}(y)$, the mutual information can be computed as

$$I(\boldsymbol{s}_{\mathrm{A}}; \boldsymbol{s}_{\mathrm{B}}) = H(\boldsymbol{s}_{\mathrm{A}}) + H(\boldsymbol{s}_{\mathrm{B}}) - H(\boldsymbol{s}_{\mathrm{A}}, \boldsymbol{s}_{\mathrm{B}}) \;. \tag{4}$$

where $H(\cdot)$ is the entropy of the bit sequence in input. We remark that to estimate the mutual information, it is necessary to know the associated joint probability density function (PDF). This can be either known a priori or estimated a posteriori by using the dataset of observations (x, y, z) as input to the quantizers.

Hence, we use as an optimization metric the lower bound on the secret-key capacity for the source model [2, 9, Ch. 4], i.e.,

$$\begin{aligned} C_{\mathrm{sk}}^{\mathrm{low}}(\mathcal{T}_{\mathrm{A}}, \mathcal{T}_{\mathrm{B}}, \mathcal{T}_{\mathrm{E}}) =& I(\boldsymbol{s}_{\mathrm{A}}; \boldsymbol{s}_{\mathrm{B}}) - \\ & \min\left\{I(\boldsymbol{s}_{\mathrm{A}}; \boldsymbol{s}_{\mathrm{E}}), I(\boldsymbol{s}_{\mathrm{B}}; \boldsymbol{s}_{\mathrm{E}})\right\} \;, \end{aligned} \tag{5}$$

Eq. (5) shows that the quantizers should be designed to increase the reciprocity between Alice and Bob bit sequences, increasing $I(\boldsymbol{s}_{\mathrm{A}}; \boldsymbol{s}_{\mathrm{B}})$, while decreasing the knowledge of Eve about the key, i.e., decreasing instead $I(\boldsymbol{s}_{\mathrm{A}}; \boldsymbol{s}_{\mathrm{E}})$ and $I(\boldsymbol{s}_{\mathrm{B}}; \boldsymbol{s}_{\mathrm{E}})$.

We now introduce the procedure to optimize the quantizers. First, the quantizers are initialized, e.g., by setting the threshold uniformly in the range $[T_0, T_M]$. Next, we consider the following iterative procedure. At the start of each optimization round, Eve chooses the quantizer's thresholds as

$$\hat{\mathcal{T}}_{\rm E} = \arg\min_{\mathcal{T}_{\rm E}} C_{\rm sk}^{\rm low}(\mathcal{T}_{\rm A}, \mathcal{T}_{\rm B}, \mathcal{T}_{\rm E}) \;, \tag{6}$$

with $\mathcal{T}_{\rm A}$ and $\mathcal{T}_{\rm B}$ fixed as in the previous round. Next, Alice and Bob pick as quantizers

$$[\hat{\mathcal{T}}_{\rm A}, \hat{\mathcal{T}}_{\rm B}] = \arg\max_{\mathcal{T}_{\rm A}, \mathcal{T}_{\rm B}} C_{\rm sk}^{\rm low}(\mathcal{T}_{\rm A}, \mathcal{T}_{\rm B}, \hat{\mathcal{T}}_{\rm E}) \;. \tag{7}$$

Finally, Alice, Bob, and Eve set the quantizers $\hat{q}_{\rm A}$, $\hat{q}_{\rm B}$, and $\hat{q}_{\rm E}$, from the new thresholds $\hat{\mathcal{T}}_{\rm A}$, $\hat{\mathcal{T}}_{\rm B}$, and $\hat{\mathcal{T}}_{\rm E}$. The optimizations are performed via numerical methods, such as gradient descent or via genetic algorithm. The procedure is repeated either until convergence is reached or a maximum number of iterations have been performed.

3.3 Shift Computation and Measurement Correction

In this Section, we detail the shift computation and the measurement correction, i.e., what can Alice transmit to Bob to aid his quantization step. We write the observation at Bob as

$$y = x + \epsilon \;, \tag{8}$$

where ϵ represents the channel non-reciprocity.

Next, let c_m be the quantized value at Alice, associated to interval $\mathcal{I}_m$ and with string $\boldsymbol{s}_m$. The resulting quantization error is then

$$\eta \triangleq x - c_m \;, \tag{9}$$

that combined with (8) yields

$$y = c_m + \eta + \epsilon. \tag{10}$$

Ignoring a possible dependency between quantization error and channel reciprocity, (10) shows that y is turned away from the quantization value c_m by both η and ϵ. Thus, to improve the advantage-distillation procedure, Alice communicates over the public (but authenticated) channel the value of the quantization error, η, allowing Bob to compute

$$y' = y - \eta = c_m + \epsilon, \tag{11}$$

and obtain his own bit sequence by quantizing y'.

However, in general, the capacity of the side channel is limited thus Alice cannot send the actual quantization error η, but only B bits per measurement. Hence, we have to quantize η. To this end, each quantization interval $\mathcal{I}_m$ 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, thus Alice transmits

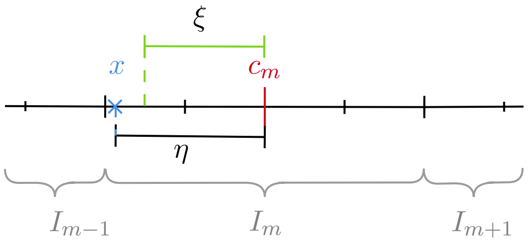


Figure 2: Sketch of the quantization of the error correction, from measurement x (blue cross) and the actual quantization error η to the 2 bit quantized correction ξ.

$$\xi = \left\lceil \eta \frac{K}{L^{(\rm A)}(x)} \right\rceil \;, \tag{12}$$

where $L^{(\rm A)}(x)$ is the length of the quantization interval where x falls. We remark that, if for a non-uniform quantizer $q_{\rm A}(x)$, the value of the correction η may reveal part of the information to Eve, e.g., high values of η suggest that the actual x has fallen in a wide interval. The proposed quantization procedure of (12) instead avoids transmitting the value of η, with ξ not disclosing any information about x.

Upon reception, Bob computes the actual correction from ξ as

$$\eta' = \frac{L^{(\rm B)}(y)}{K}\left(\xi - \frac{1}{2}\right) \;, \tag{13}$$

where $L^{(\rm B)}(y)$ is the length of y. Then, Bob replaces η with η' in (11). Indeed, it may happen that $L^{(\rm A)}(x) \neq L^{(\rm B)}(y)$. Nonetheless, it is reasonable to assume that nearby intervals have a similar length.

4. NUMERICAL RESULTS

In this Section, we present the numerical results obtained by using an augmented dataset.

The dataset has been collected during a designated sea experiment performed in January 2022 in Eilat, Israel. For network communications, we used 7 Succorfish Nanomodem-v3, meausuring 4 cm × 6 cm, and operating in the 24–32 kHz band. Each modem had a source power level of 168 dBm. To obtain the channels' impulse responses, we used Raspberry Pi boards where each trusted node transmits a channel-request and in response receives a message from which the magnitude of the channel's taps is obtained with a resolution of 10 μs. For simplicity, we limit our analysis to the case with $N = 2$ features, namely the average tap power and the RMS delay. To increase the dataset size, we used a dataset augmentation technique based on inverse sampling, with the augmented dataset containing now 10^5 triplets of observations ($\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{z}$). In particular for feature i, the correlation matrix of $\boldsymbol{v}_i = [x_i \, y_i \, z_i]^{\mathrm{T}}$ is

$$\mathbb{E}[\boldsymbol{v}_i \boldsymbol{v}_i^{\mathrm{T}}] = \begin{bmatrix} 1 & \rho_{\mathrm{AB}} & 0.8 \\ \rho_{\mathrm{AB}} & 1 & 0.8 \\ 0.8 & 0.8 & 1 \end{bmatrix} . \tag{14}$$

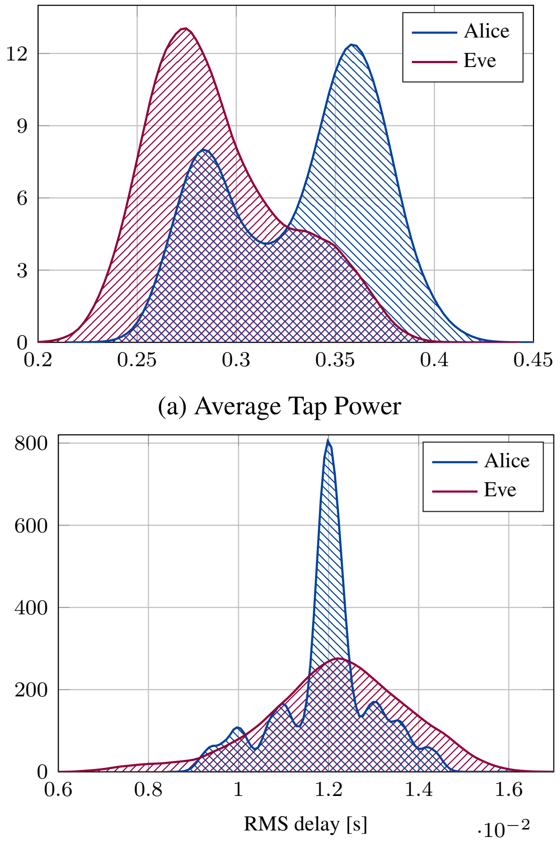
More details about both the experiment and the data augmentation technique can be found in [22].

Fig. 3 reports the (estimated) PDF for the considered features, as measured by two received 100 m apart, acting as Alice and Eve with Bob transmitting. We observe that the distributions do not perfectly overlap and have different shapes, that it is indeed possible to extract secret information out of these measurements. Still, due to the partial overlap, the information needs to be carefully distilled to achieve secrecy.

Fig. 4 shows instead the thresholds obtained in the case b =2 bit for the average tap power. Interestingly, when the correlation between Alice and Bob ρ_{AB} increases, the central thresholds get progressively close to each other. This actually decreases the overall entropy that to be maximized would require equiprobable outputs. On the other hand, the reciprocity is actually not affected for high values of ρ_{AB}, since, Alice's and Bob's measurements end up on the same intervals with high probability, while it is easier for Eve to fall in different intervals.

We consider the measurement after the decorrelation step of Section 3.1. In particular the (feature associated with) the average tap power has unitary power, while the RMS delay has a relative power γ. Thus, $\gamma = 1$ means that the features were independent to begin with, while $\gamma \approx 0$ means that there was an (almost deterministic) function relating average tap power to the RMS delay.

Fig. 5 reports the secret key capacity obtained using average tap power and RMS delay as a function of ρ_{AB}, for various values of γ, with $\rho_{\mathrm{E}} = 0.8$, b =3 bit, and B =1 bit. As γ increases, i.e., with feature initially less correlated, we are able to get more secret bits from the



(a) Average Tap Power

(b) RMS Delay

Figure 3: Estimated features's PDF for Alice and Eve.

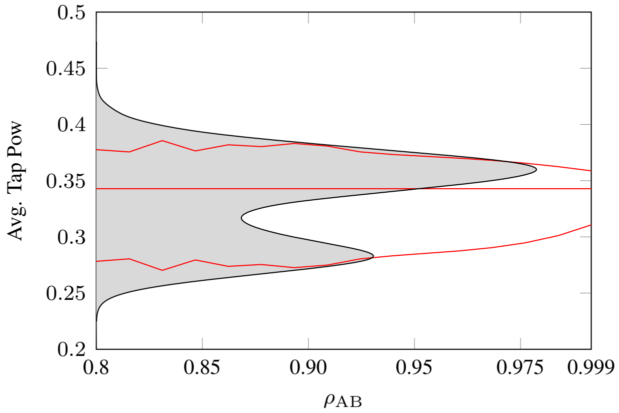


Figure 4: Quantization thresholds $\mathcal{T}_{\mathrm{A}}$, resulting from the proposed optimization as a function of ρ_{AB} for the average tap power for $b = 2$ bit, $B = 1$ bit, and $\rho_{\mathrm{E}} = 0.8$.

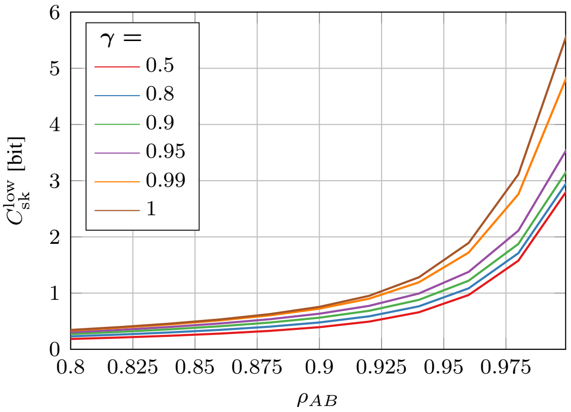


Figure 5: $C_{\text{sk}}^{\text{low}}$ obtained from average tap power and RMS delay as a function of ρ_{AB} for various values of γ, with $\rho_{\text{E}} = 0.8$, $b = 3$ bit, and $B = 1$ bit.

channel achieving up to $C_{\text{sk}}^{\text{low}} \approx 5.66$ bit for $\gamma = 1$ and $\rho_{\text{AB}} = 0.999$.

Fig. 6 shows the $C_{\text{sk}}^{\text{low}}$ obtained from average tap power and RMS delay as a function of ρ_{AB} using either the proposed ADQC or where both Alice, Bob, and Eve use a uniform quantizer, for $\rho_E = 0.8$, $b = 4$ bit, and $\gamma = 0.8$. The number of bits describing the quantization error shared over the public channel during the distillation phase is either $B = 1$ or 2 bit. Indeed, the proposed strategy is advantageous to the uniform quantizer, even when only a few bits of correction are shared via the side channel.

5. CONCLUSION

In this paper, we have proposed an advantage-distillation technique for physical layer-based SKA for UWACs. The proposed protocol, the ADQC, is asymmetric and has two main features. The quantizers used by Alice and Bob are optimized using the lower bound on the secret-key capacity as a metric. Before the actual advantage distillation, we process the features to decorrelate them, thus obtaining two independent features. This allows us to process each feature separately, with a (cheaper) scalar quantizer.

Next, during the actual advantage-distillation procedure, Alice quantizes her measurement and sends a message with partial information on the position of the measurement in the quantization interval over an authenticated public side channel. The partial information is used by Bob to quantize his measurement and obtain a bit sequence more in agreement with that of Bob.

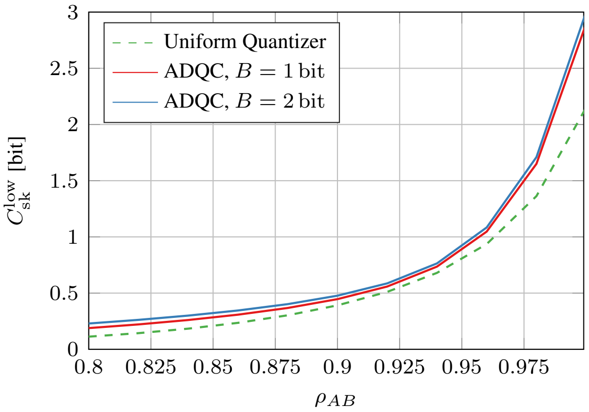


Figure 6: $C_{\text{sk}}^{\text{low}}$ obtained from average tap power and RMS delay as a function of ρ_{AB}, using the uniform quantizer and ADQC, with either $B = 1$ or 2 bit, when $\rho_E = 0.8$, $b = 4$ bit, and $\gamma = 0.8$.

We have tested the performance of the proposed strategies using data collected from a sea experiment. Results show that both the quantizer optimization and the correction transmission contribute to increasing the lower bound of the secret key capacity, even considering the worst-case scenario where Eve exploits the knowledge on Alice's and Bob's quantizer to optimize her own.

6. ACKNOWLEDGMENTS

This work was sponsored in part by the NATO Science for Peace and Security Programme under grant no. G5884 (SAFE-UComm).

7. REFERENCES

[1] D. R. Stinson, *Cryptography: Theory and Practice*. USA: CRC Press, Inc., 4th ed., 1995.

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

[3] 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, 1993.

[4] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proc. of FOCS*, pp. 124–134, 1994.

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

[6] 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, 2019.

[7] S. Jiang, "On securing underwater acoustic networks: A survey," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 1, pp. 729–752, 2019.

[8] W. Aman, S. Al-Kuwari, M. Muzzammil, M. M. U. Rahman, and A. Kumar, "Security of underwater and air–water wireless communication: State-of-the-art, challenges and outlook," *Ad Hoc Networks*, vol. 142, p. 103114, 2023.

[9] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[10] C. Chen and M. A. Jensen, "Improved channel quantization for secret key establishment in wireless systems," in *Proc. of ICWITS*, pp. 1–4, 2010.

[11] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mob. Comput.*, vol. 10, pp. 205–215, Feb. 2011.

[12] S. Tomasin, F. Trentini, and N. Laurenti, "Secret key agreement by LLR thresholding and syndrome feedback over AWGN channel," *IEEE Commun. Lett*, vol. 18, no. 1, pp. 26–29, 2014.

[13] S. Park and H. Son, "Near-perfect code scrambling with limited key information for wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13410–13423, 2020.

[14] A. V. Guglielmi, A. Muraro, G. Cisotto, and N. Laurenti, "Information theoretic key agreement protocol based on ECG signals," in *Proc. of GLOBECOM*, pp. 1–6, 2021.

[15] 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, Jan. 2021.

[16] K. Pelekanakis, S. A. Yıldırım, G. Sklivanitis, R. Petroccia, J. Alves, and D. Pados, "Physical layer security against an informed eavesdropper in underwater acoustic channels: Feature extraction and quantization," in *Proc. of UComms*, 2021.

[17] G. Sklivanitis, K. Pelekanakis, S. A. Yıldırım, R. Petroccia, J. Alves, and D. A. Pados, "Physical layer security against an informed eavesdropper in underwater acoustic channels: Reconciliation and privacy amplification," in *Proc. of UComms*, 2021.

[18] F. Ardizzon, F. Giurisato, and S. Tomasin, "Secret-key-agreement advantage distillation with quantization correction," *arXiv*, Apr. 2023.

[19] R. Diamant, P. Casari, and S. Tomasin, "Cooperative authentication in underwater acoustic sensor networks," *IEEE Trans. Wirel. Commun.*, vol. 18, no. 2, pp. 954–968, 2019.

[20] L. Bragagnolo, F. Ardizzon, N. Laurenti, P. Casari, R. Diamant, and S. Tomasin, "Authentication of underwater acoustic transmissions via machine learning techniques," in *Proc. of COMCAS*, pp. 255–260, 2021.

[21] L. Devroye, *Non-Uniform Random Variate Generation*. Springer New York, 1986.

[22] F. Ardizzon, R. Diamant, P. Casari, and S. Tomasin, "Machine learning-based distributed authentication of UWAN nodes with limited shared information," in *Proc. of UComms*, pp. 1–5, 2022.