A Novel Physical Layer Authenticated Encryption Protocol Exploiting Shared Randomness

Cornelius Saiki, Arsenia Chorti

A Novel Physical Layer Authenticated Encryption Protocol Exploiting Shared Randomness

Cornelius Saiki and Arsenia Chorti
School of Computer Science and Electronic Engineering, University of Essex
Wivenhoe Park, Colchester, CO4 3SQ, UK
Email: {cosaik, achorti}@essex.ac.uk

***Abstract*—The topic of physical layer authenticated encryption using high rate key generation through shared randomness is investigated in this work. First, a physical layer secret key generation scheme is discussed exploiting channel reciprocity in wireless systems. In order to address the susceptibility of this family of schemes to active attacks, a novel physical layer authentication encryption protocol is presented along with its extension to multi-node networks in the presence of active adversaries. Secondly, in order to increase the key generation rate, a multi-level quantization algorithm with public feedback is discussed. It is demonstrated that the proposed scheme is superior to direct information distillation approaches and can substantially increase the key generation rates even at low and medium SNRs.**

I. Introduction

One of the most promising topics in the area of physical layer security is the generation of secret keys via public discussion, based on either the so-called *source* model or the so-called *channel* model. Regarding the former, the potential for generating secret keys at a source and a destination in the presence of passive eavesdroppers through the exchange of correlated sequences was examined in [1]. In [2] single letter characterizations of the channel key capacity were derived while it was demonstrated that the secret keys can be generated without any information leakage to a passive adversary. On the other hand, the channel model alternatively exploits the inherent correlation of the channel gains in the wireless transmission medium due to reciprocity [3]. A straightforward application of the channel model was proposed in [4]. In [5] the shared randomness of the multipath wireless channel was exploited to generate a common secret key between a source and an intended destination assuming that the adversarial channel is uncorrelated with the main channel between the legitimate nodes.

Traditionally, secret key generation from wireless channel estimates includes three distinct phases [6]:
- *Advantage distillation*: Alice and Bob obtain estimates of their reciprocal channel state information (CSI) and pass them through a suitable quantizer [5], [7]–[9].
- *Information reconciliation*: Discrepancies in the quantizer local outputs due to imperfect channel estimation are reconciled through public discussion.
- *Privacy amplification*: Applying universal hash functions to the reconciled information ensures that the generated keys are uniformly distributed and completely unpredictable by Eve.

In the present work, we use the phase of the local CSI estimates for information distillation. Following this approach the estimation error is shown to be approximately Gaussian while the phase estimates at the adversary are uncorrelated to those at the legitimate nodes. We propose a novel *adaptive* quantization scheme with multi-level public feedback, acting in essence as the interface between the advantage distillation and the information reconciliation phases. The proposed quantizer achieves a particularly high information distillation rate at the two legitimate nodes and allows a substantial reduction in the complexity of the reconciliation process. Finally, the generated secret keys are employed in a novel *physical layer authenticated encryption* protocol (PLAE). The complexity of the proposed scheme is minimal in comparison to public key encryption schemes , rendering it a compelling approach for establishing secure links in ad-hoc networks and device-to-device communication.

The rest of the paper is organized as follows. Section II introduces the system model and the achievable secret key rate. Our key generation algorithm along with a detailed description of secure error reconciliation process is discussed in Section III. In section IV the PLAE scheme is described. A feedback quantizer with an improved information distillation rate (IDR) is discussed in Section V. Finally, the paper conclusions are drawn in Section VI.

II. System Model and Achievable Secret Key Rates

A. System Model

The system model is shown in Fig.1 with Alice and Bob denoting legitimate nodes and Eve an active adversary. The channel between Alice and Bob is assumed to be reciprocal and stationary during each transmission cycle and to change independently from one transmission cycle to the next. Each cycle includes the transmission of two consecutive probe signals, from Alice to Bob and from Bob to Alice. During the i-th cycle Alice obtains an estimate $h_A(i)$ and Bob an

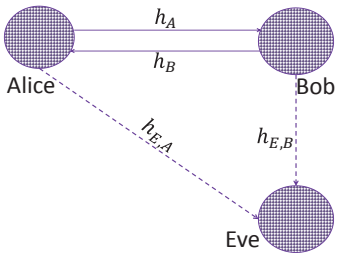

Fig. 1. Wireless system model.

estimate $h_B(i)$ respectively of their reciprocal CSI, denoted by $h_0(i)$, so that,

$$\begin{aligned} h_A(i) &= h_0(i) + \Delta h_A(i), && (1)\\ h_B(i) &= h_0(i) + \Delta h_B(i), && (2)\\ h_0(i) &= x_0(i) + jy_0(i), && (3)\\ \Delta h_A(i) &= \Delta x_A(i) + j\Delta y_A(i), && (4)\\ \Delta h_B(i) &= \Delta x_B(i) + j\Delta y_B(i), && (5) \end{aligned}$$

where $x_0(i)$ and $y_0(i)$ are zero mean Gaussian random variables distributed as $\sim \mathcal{N}(0,\sigma^2)$ and $\Delta x_A(i)$, $\Delta y_A(i)$, $\Delta x_B(i)$ and $\Delta y_B(i)$ are zero mean unit variance Gaussian random variables, $\sim \mathcal{N}(0,1)$. Using this modelling the variance σ^2 of $x_0(i)$ and $y_0(i)$ is equal to the channel SNR. Finally, Eve's channel to Alice and Bob is uncorrelated with either $h_A(i)$ and $h_B(i)$.

We focus on a single transmission cycle and drop related time indices. The central scope of the remainder of this section is to discuss the achievable key rates that can be generated at Alice and Bob from the angles of the estimated channel coefficients, i.e., the effective distillation of the common parts of the correlated random variables θ_A and θ_B, which are calculated locally at Alice and Bob, respectively, as:

$$\begin{aligned} \theta_A &= \angle h_A = \tan^{-1}\left(\frac{y_0+\Delta y_A}{x_0+\Delta x_A}\right), && (6)\\ \theta_B &= \angle h_B = \tan^{-1}\left(\frac{y_0+\Delta y_B}{x_0+\Delta x_B}\right). && (7) \end{aligned}$$

In the following we investigate in further detail the distribution of θ_A (respectively of θ_B). Based on the assumption that $\sigma^2 \gg 1$, the following approximation holds:

$$\begin{aligned} \frac{y_0+\Delta y_A}{x_0+\Delta x_A} &= \frac{y_0}{x_0+\Delta x_A} + \frac{\Delta y_A}{x_0+\Delta x_A}\\ &\simeq \frac{y_0}{x_0} + \frac{\Delta y_A}{x_0}. && (8) \end{aligned}$$

Furthermore, exploiting the fact that the Taylor series expansion of $\tan^{-1}(x+y)$ around $y=0$ can be written as

$$\tan^{-1}(x+y) = \tan^{-1}(x) + \frac{y}{x^2+1} + O(y^2), \quad (9)$$

we can establish the following approximations for small values of $\frac{\Delta y_A}{x_0} \ll 1$, $\frac{\Delta y_B}{x_0} \ll 1$ (these conditions are satisfied with very high probability when $\sigma^2 \ll 1$, i.e., for medium and high SNRs):

$$\begin{aligned} \theta_A &\simeq \theta_0 + \Delta\theta_A, && (10)\\ \theta_B &\simeq \theta_0 + \Delta\theta_B, && (11) \end{aligned}$$

where,

$$\begin{aligned} \theta_0 &= \tan^{-1}\left(\frac{y_0}{x_0}\right), && (12)\\ \Delta\theta_A &= \frac{\Delta y_A}{x_0}\frac{x_0^2}{x_0^2+y_0^2}, && (13)\\ \Delta\theta_B &= \frac{\Delta y_B}{x_0}\frac{x_0^2}{x_0^2+y_0^2}. && (14) \end{aligned}$$

The pdf of the ratio $r = \frac{y_0}{x_0}$ follows the standard Cauchy distribution and as a result $\theta_0 = \tan^{-1}(r)$ is uniformly distributed in the range $(-\frac{\pi}{2}, \frac{\pi}{2})$ with zero-mean and variance $\frac{\pi}{12}$:

$$p_{\Theta_0}(\theta_0) = \begin{cases} \frac{1}{\pi}, & \theta_0 \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right],\\ 0 & \text{otherwise.} \end{cases} \quad (15)$$

On the other hand, the random variable $\Delta\theta_A$ ($\Delta\theta_B$ respectively) is the product of two *dependent* random variables; (i) of $v_A = \frac{\Delta y_A}{x_0}$ which follows a Cauchy distribution with location parameter 0 and scale parameter $\frac{1}{\sigma}$ and (ii) of $u = \frac{x_0^2}{x_0^2+y_0^2}$ which follows an arcsine distribution with mean $\frac{1}{4}$ and variance $\frac{1}{8}$:

$$\begin{aligned} p_V(v_A) &= \frac{\sigma}{\pi(1+\sigma v_A)^2}, && (16)\\ p_U(u) &= \begin{cases} \frac{1}{\pi\sqrt{u(1-u)}}, & u \in (0,1),\\ 0 & \text{otherwise.} \end{cases} && (17) \end{aligned}$$

while the corresponding analysis holds for $\Delta\theta_B$ as well.

During each transmission cycle and for a particular realization of the channel, the phase estimate θ_A (respectively θ_B) of the common phase θ_0 is a Gaussian random variable with mean θ_0 and variance σ_t^2, which is given as:

$$\sigma_t^2 = \mathbb{E}_{X_0,Y_0}\left[\left(\frac{x_0}{x_0^2+y_0^2}\right)^2\right] - \mathbb{E}_{X_0,Y_0}\left(\left[\frac{x_0}{x_0^2+y_0^2}\right]\right)^2, \quad (18)$$

as a function of the channel SNR σ^2. As a result of this discussion, the quantities $\Delta\theta_A$ and $\Delta\theta_B$ will in the following be approximated by zero-mean Gaussian random variables with variance σ_t^2.

B. Secret Key Capacity and Achievable Key Rates

The maximum rate at which Alice and Bob can extract identical secret bits from θ_A and θ_B, is denoted hereafter as the phase secret key capacity $C_k^{(\phi)}$ and is upper bounded by the mutual information of θ_A and θ_B in the channel model

[2]. Based on the previous discussion, the phase secret key capacity can be expressed as:

$$\begin{aligned} C_k^{(\phi)} &= I(\theta_A;\theta_B) = h(\theta_A) + h(\theta_B) - h(\theta_A,\theta_B) \\ &= 2\log_2\left(2\pi e\left(\frac{\pi^2}{12}+\sigma_t^2\right)\right) \\ &\quad - \log_2\left((2\pi e)^2\left[\left(\frac{\pi^2}{12}+\sigma_t^2\right)^2 - \left(\frac{\pi^2}{12}\right)^2\right]\right) \\ &= \log_2\left(1+\frac{\pi^2/12}{2\sigma_t^2+\frac{\sigma_t^4}{\pi^2/12}}\right). \end{aligned} \tag{19}$$

$C_k^{(\phi)}$ is only achievable if infinite blocklength encoders are employed at the information reconciliation stage to correct for any discrepancies between θ_A and θ_B. In the realistic scenario in which finite blocklength encoders are used instead, we can estimate the achievable phase secret key rate, denoted by $R_k^{(\phi)}$, for any blocklength n and non zero (output) error probability ϵ by employing the results of [10]. The achievable phase secret key rate can then be expressed as:

$$R_k^{(\phi)}(n,\epsilon) = C_k^{(\phi)} - \sqrt{\frac{V}{n}}Q^{-1}(\epsilon) + \frac{1}{2n}\log n. \tag{20}$$

In (20) V denotes the channel dispersion–a quantity which describes the backoff from capacity in the finite blocklength regime; using the additive white Gaussian model, [10]–eqs. (292-293), the channel dispersion with respect to $C_k^{(\phi)}$ can be expressed as

$$V = \frac{\left(\pi^4+48\sigma_t^2\pi^2+288\sigma_t^4\right)\pi^4}{(\pi^4+24\sigma_t^2\pi^2+144\sigma_t^4)^2}\log_2^2 e. \tag{21}$$

In (20) $Q = \int_x^\infty \frac{1}{\sqrt{2\pi}}e^{-t^2/2}dt$, ϵ is the error probability, $0<\epsilon<1$, and n is the blocklength.

Finally, in a direct application of the previous results, the required blocklength n is evaluated with respect to a target fractional rate $\eta = R_k^{(\phi)}/C_k^{(\phi)}$. For illustration purposes, the required blocklength as a function of ϵ is depicted for $\eta = 0.5$ and $\eta = 0.9$ in Fig 2.

III. Key Generation Protocol

A. Information Distillation

Based on our estimate of σ^2 we split the range from $(-\frac{\pi}{2},\frac{\pi}{2})$ to quantization levels of width at most $l\sigma_t$ (e.g. $l=4$). The number of quantization intervals, Q, is given by

$$Q = \left\lfloor \frac{\pi}{l\sigma_t} \right\rfloor, \tag{22}$$

where $\lfloor\cdot\rfloor$ denotes the floor function. The phase estimate θ_A (respectively of θ_B) is mapped to quantization interval $q \in \{1,\ldots,\log_2(Q)\}$ using the mapping:

$$\lfloor x \rceil = q \text{ if } x \in \left[\frac{\pi(q+1)}{Q},\frac{\pi q}{Q}\right) - \frac{\pi}{2}, q = 0,2,\ldots,Q-1, \tag{23}$$

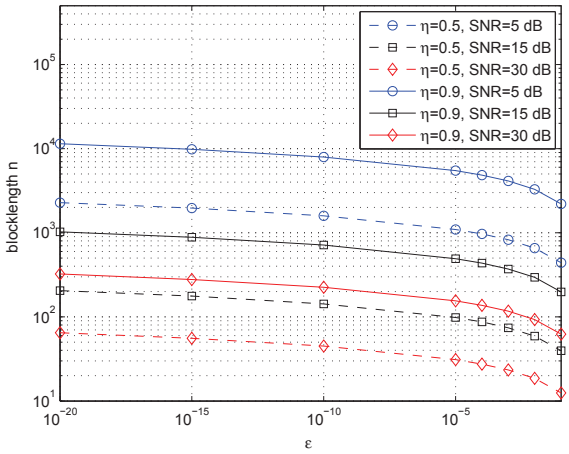

Fig. 2. Blocklength n required to achieve desired fractional rate $\eta = R_k^{(\phi)}/C_k^{(\phi)}$ as a function of the error rate ϵ for various SNRs.

where $\lfloor\cdot\rceil$ denotes quantization. In the present protocol we employ this straightforward approach of a quantizer with no feedback while later in Section V we will discuss an improved design using public feedback.

B. Information Reconciliation Phase Using FEC

A low complexity information reconciliation approach is built using standard linear block codes as follows: Alice and Bob use length n buffers to store length n-tuples at the output of the quantizer. These n-tuples are here denoted by k_A and k_B respectively. Subsequently, using a predetermined block code they estimate locally their respective syndromes, denoted by s_A and s_B and the corresponding error patterns e_A and e_B so that

$$k_A = k_0 \oplus e_A, \tag{24}$$
$$k_B = k_0 \oplus e_B. \tag{25}$$

In essence, k_A and k_B correspond to θ_A and θ_B respectively, k_0 to θ_0 and e_A, e_B to $\Delta\theta_A$ and $\Delta\theta_B$ respectively.

For Bob to derive an estimate of k_A, it is required that Alice communicates her syndrome s_A to Bob via public discussion as will be explained later. In Section IV we will demonstrate that although the syndrome will be sent in the clear, the key generation scheme combined with an authenticated encryption (A.E) protocol can still be robust to active attackers. At present, we concentrate on how Alice and Bob can establish a common secret key. Bob, given s_A can derive an estimate of $\hat{k}_A$ of k_A as:

$$\hat{k}_A = k_0 \oplus e_A = k_B \oplus e_B \oplus e_A. \tag{26}$$

It is important to note that by communicating s_A in the clear, Eve by mere interception can also estimate e_A. The following Lemma discusses the related information leakage.

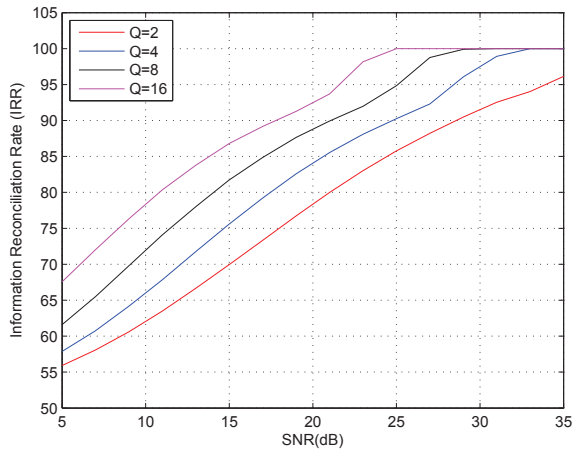

Fig. 3. Information reconciliation rate (IRR) for the quantizer without feedback.

Lemma 1: Using the key distillation scheme discussed in (24)-(26), the transmission of the syndrome s_A in the clear does not leak more than $n-k$ bits of information with respect to k_A.

Proof: s_A can be used to obtain e_A. On the other hand k_0 and e_A are independent because they correspond to the quantization of two independent continuous random variables, namely of θ_0 and $\Delta\theta_A$. As a result, we have that

$$H(k_A) = n, \quad (27)$$

$$H(k_A|s_A) = H(k_A|e_A) = H(k_0) = k. \quad (28)$$

Therefore, the transmission of s_A does not leak more than $n-k$ bits of information as claimed. ■

As a result of Lemma 1, the effective size of the key space of k_A is 2^k and its entropy is k bits. As result appropriate hashing of the encoder output to remove redundant bits is required and is performed in the privacy amplification stage (details are omitted due to space limitations). The overall key generation rate can be estimated as the product of the IDR, the IRR and the rate of the FEC. As an example, we have used a BCH code with rate $\frac{513}{1023}$ and length-1023 bit codewords in our error reconciliation stage. The choice of this encoder stems from the analysis in Fig. 2 in order to achieve a negligible ϵ across all SNRs. In Fig. 3 the IRR is depicted for a simple quantizer $l = 4$ is shown.

Finally, further exploiting the use of public feedback, it is possible to design a key validation process as follows. First, Bob transmits to Alice his estimated syndrome s_B which Alice uses to derive e_B. Using (26), Alice can then estimate $\hat{k}_A$ and check that $\hat{k}_A = k_A$. Blocks which fail the validation test are subject to further processing or are discarded.

IV. Physical Layer Authenticated Encryption

Assuming that the key generation protocol is publicly available and that Eve is an active eavesdropper, the threat model is summarized as follows:
- Eve can intercept all information exchanges between Alice and Bob, i.e., Eve can mount chosen plaintext attacks [11].
- Eve can modify the transmitted signals in a predetermined manner, i.e., Eve can mount chosen ciphertext attacks [11] and can act as a man-in-the-middle.

Existing literature on shared randomness exclusively focuses on key generation for data confidentiality applications in the presence of passive adversaries. On the other hand, secure communication in the presence of an active adversary without any pre-shared secret (i.e., a pre-established key at both Alice and Bob) is currently solely based on the use of public key encryption schemes (PKE) [11] that employ trapdoor functions such as the RSA (Rivest-Shamir-Adleman) or the DH (Diffie Hellman) with asymmetric key lengths of at least 1024 or 2048 bits. However, the computational resources required to encrypt and decrypt using PKE are substantial; as a result, PKE can limit the performance of ad-hoc or device-to-device networks in which the nodes join or leave the network frequently.

To overcome such limitations, in this section we alternatively propose a PLAE scheme that instead of computationally demanding trapdoor functions employs the low complexity scheme described in section Section II to generate pair-wise keys. To begin with, we assume that Alice wishes to transmit a secret message m to Bob without having access to a public key infrastructure. We build a PLAE protocol using the following elements:
1) A physical layer key seed generation scheme employing the simple quantizer without feedback described in section II. The scheme will in the following be denoted by $F_{Gen}(h_A, h_B) = \{s_A, s_B, e_A, e_B, k_A, k_B\}$.
2) A semantically secure hash function (random oracle) denoted by $H(x) = k$ where $k = \{k_e, k_i\}$ is a pair of keys. k_e is to be employed by a symmetric encryption algorithm and k_i is the key to be used by a message authentication code (MAC).
3) A semantically secure A.E scheme (e.g. an encrypt-then-MAC protocol) [11] that comprises four algorithms: an encryption algorithm denoted by $E_s(k_e, m) = c$, a decryption algorithm denoted by $D_s(k_e, c) = m$, a signing algorithm denoted by $S(k_i, m) = t$ and a verification algorithm denoted by $V(k_i, m, t) = v \in \{m, \perp\}$.

A. Two Node PLAE Protocol

- F_{Gen} **scheme**: During cycle 1 Alice transmits a probe signal to Bob who evaluates $s_B(1), e_B(1), k_B(1)$. Subsequently, Bob transmits a probe signal to Alice who evaluates $s_A(1), e_A(1), k_A(1)$. This procedure is repeated until suitable length tuples $s_A, e_A, k_A, s_B, e_B, k_B$ are generated from the concatenation of successively generated parameters, i.e., $s_A = [s_A(1)||, \ldots, ||s_A(n)]$, $e_A = [e_A(1)||, \ldots, ||e_A(n)]$, $k_A = [k_A(1)||, \ldots, ||k_A(n)]$, $s_B = [s_B(1)||, \ldots, ||s_B(n)]$, $e_B = [e_B(1)||, \ldots, ||e_B(n)]$ and

$k_B = [k_B(1)||, \ldots, ||k_B(n)]$ where $||$ denotes concatenation. The number of cycles depends on the required key entropy according to the specifications of the A.E. algorithms.

- **Hashing and A.E.**: Alice generates a secret key $k = \{k_e, k_i\} = H(k_A)$ and encrypts the message as $c = E_s(k_e, m)$. Subsequently, she signs the ciphertext c using the signing algorithm $t = S(k_i, c)$ and transmits to Bob the extended ciphertext.

$$C = [s_A||c||t] \tag{29}$$

- **Integrity check and decryption**: Bob checks the integrity of the received data as follows: from s_A he evaluates k_A and obtains $k = \{k_e, k_i\} = H(k_A)$. Subsequently, Bob evaluates $V(k_i, c, t)$, which is either equal to $\perp$ if the integrity test of the A.E. failed or c if the integrity test of the A.E. was successful. The integrity test will fail if any part of C was modified; for example, if s_A was modified during the transmission then Bob would have evaluated a wrong key k and the integrity test would have failed. If the integrity test was successful then Bob decrypts $m = D_s(k_e, c)$. Using standard chosen ciphertext attack and chosen plaintext attack semantic security proofs, it is straightforward to demonstrate that the proposed scheme achieves semantic security and integrity.

B. Multi-node Key Generation Scheme

Generalizing the PLAE protocol to a wireless network with multiple nodes can have many different flavors depending on the application of the F_{Gen} function. In this paper we briefly present a scheme suitable for a network of N nodes who want to establish a *common* key k. We note that generating a common secret key using the RSA or the DH schemes is an open problem for networks with $N > 3$.

The procedure comprises two phases. In the first phase, the F_{Gen} scheme is applied pairwise between node 1 and the remaining nodes 2 to N. In this phase, the nodes sequentially transmit suitable probe signals one after the other and obtain estimates of the pairwise CSIs $h_{1,i}$ and $h_{i,1}$, $i = 2, \ldots, N$. At the end of this procedure node 1 generates $N-1$ pairwise syndromes $s_{1,i}, i = 2, \ldots, N$ while the remaining nodes generate syndromes $s_2, \ldots, s_N$. The syndromes $s_{1,i}$ correspond to the error pattern from the key seed k_1 extracted from $h_{1,2}$ to key seeds extracted from $h_{1,i}, i = 3, \ldots, N$. Finally the syndromes $s_i, i = 2, \ldots, N$ correspond to error patterns of key seeds $k_2, \ldots, k_N$, extracted from $h_{i,1}, i = 2, \ldots, N$. At the second phase, node 1 generates a key $k = H(k_1)$ and *broadcasts* its extended syndrome $s_1 = [s_{1,1}||, \ldots ||s_{1,N}]$ so that nodes 2 to N can regenerate the common secret key k using $k = k_i \oplus e_i \oplus e_{1,N}$, for $i = 2, \ldots, N$.

V. Improving the Key Generation Rate Using Information Distillation with Feedback

After discussing the PLAE protocol, we re-focus our attention to the IDR phase and discuss an improved scheme with feedback. In future work, this will be incorporated in the PLAE protocol. In order to increase the information distillation rate at the output of the quantizer, we propose the following public feedback approach: each quantization interval is split into n slots as shown in Fig. 4. Alice determines the quantization interval and the slot index $i_A \in \{1, \ldots, n\}$ of her estimated phase sample; the latter is transmitted to Bob. Similarly, Bob identifies the quantization interval and the slot index $i_B \in \{1, \ldots, n\}$ of his own estimate. Based on the public feedback received by Alice he then computes the likelihood that his own estimate is in the same quantization interval as Alice's. According to a slot agreement (SA)-disagreement (SD) protocol he announces the retaining or rejection of the current output of the quantizer. No useful information is revealed to Eve when Alice and Bob exchange slot indices. This is due to the fact that irrespective of the quantization level, all slots are equiprobable. Below we explain alternative $SA-SD$ protocols for a quantizer with eight slots $(n = 8)$ in each quantization interval.

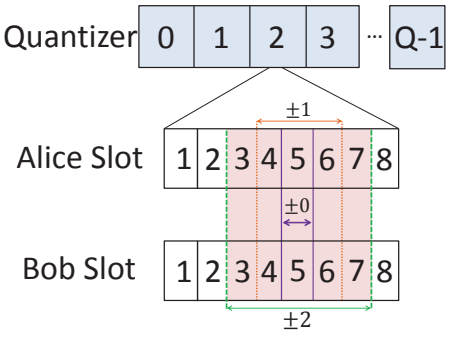

Fig. 4. Proposed quantizer with public feedback

$SA-SD(0)$ **: Hard decision (same slot)**
In this approach Alice and Bob must be in the same slot, otherwise the output of the quantizer is discarded, i.e.,

$$SA-SD(0) = \begin{cases} 1, \text{ if } i_A = i_B, i_A, i_B \in \{1 \ldots, n\} \\ \perp, \text{ otherwise,} \end{cases} \tag{30}$$

where $\perp$ denotes `rejected`. In Fig. 5 the information distillation rate (IDR) for the $SA-SD(0)$ approach is depicted.

$SA-SD(d)$ **: Soft decision ±d slot indices:**
Alice and Bob must be at most one slot apart otherwise the observed phase sample is discarded, i.e.,

$$SA-SD(d) = \begin{cases} 1, \text{ if } |i_A - i_B| \leq d, i_A, i_B \in \{1 \ldots, n\} \\ \perp, \text{ otherwise.} \end{cases} \tag{31}$$

As an example, for d=1, if Alice is in slot with index $i_A = 5$ as shown in Fig. 4, the quantizer output is retained only when Bob is in a slot with indices $i_B = 4, 5$ or 6. Unlike the $SA-SD(0)$, this approach has an increased IDR. Fig. 5 shows the IDR for $d = 1$ and $d = 2$.

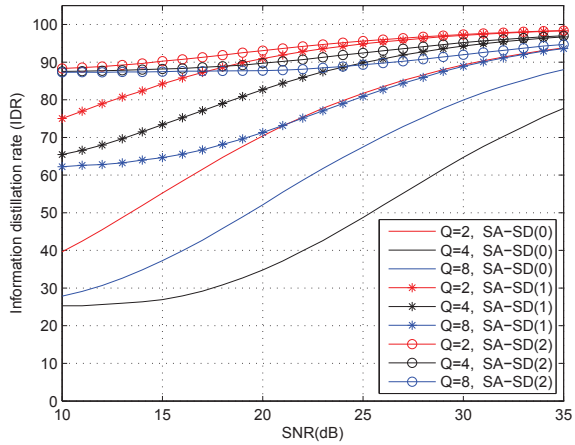

Fig. 5. Information distillation rate for the $SA-SD(0)$, $SA-SD(1)$ and $SA-SD(2)$ approaches for 8 slot division.

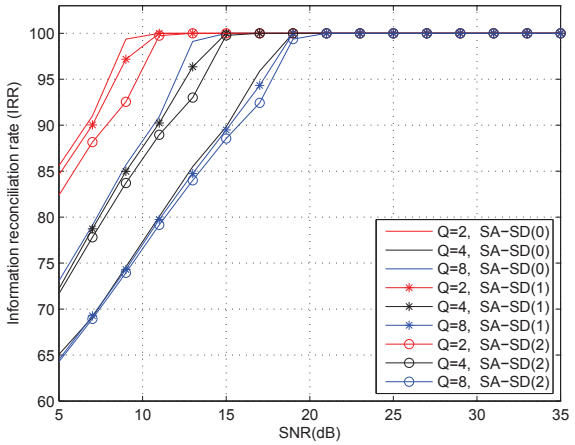

Fig. 6. Information reconciliation rate (IRR) for the $SA-SD(0)$, $SA-SD(1)$ and $SA-SD(2)$ approaches for 8 slot division.

Increasing the number of slots within each quantization interval decreases the complexity of the subsequent reconciliation phase.

Using the FEC described in Section III-B, discrepancies in the quantizer output are reconciled. An IRR of 100% is achieved at SNRs of 14.6 dB, 15.5 dB and 18 dB for $SA-SD(0)$, $SA-SD(1)$ and $SA-SD(2)$ respectively when $Q=4$ and $l=4$. These results are shown in Fig. 6.

A. Probability of Error at the Information Distillation Process

Let Alice's and Bob's quantizers generate $\log_2 Q$-tuples denoted by q_A and q_B respectively. In the outlined approaches an error (disagreement in the quantizer outputs at Alice and Bob) occurs when $SA-SD=1$ & $q_A \neq q_B$. In more detail, for the $SA-SD(0)$ approach the probability of error can be expressed as:

$$\begin{aligned} P_e &= \sum_{\substack{q=1 \\ q \neq \log 2(q_B)}}^{Q} \int_{q_l}^{q_u} \int_{-\infty}^{\infty} \frac{1}{\sigma_t\sqrt{2\pi}} \exp - \frac{(\theta-\theta_0)^2}{2\sigma_t^2} d\theta \\ &= \frac{Q-1}{n}, \end{aligned} \tag{32}$$

where

$$q_l = l\sigma_t \left(i_A - 1 + \frac{i-1}{n} \right) \frac{\pi}{Q} - \frac{\pi}{2}, \tag{33}$$

$$q_u = l\sigma_t \left(i_A - 1 + \frac{i}{n} \right) \frac{\pi}{Q} - \frac{\pi}{2} = q_l + \frac{1}{n}\frac{\pi}{Q}. \tag{34}$$

Extending this analysis, the probability of error can be estimated as a function of the number of the slots n, according to the approach employed:

$$\pm d \ \text{ slots} : P_e = (Q-1)\frac{1+2d}{n}. \tag{35}$$

VI. Conclusions

In this paper a physical layer approach for secure secret key generation in wireless networks with passive and active adversaries were investigated. Using a simple version of the proposed key generation scheme we developed a novel physical layer authenticated encryption (PLAE) scheme, employing standard semantically secure algorithms. The proposed PLAE scheme offers a compelling alternative to computationally demanding PKE schemes and can be employed in the setup of secure sessions in wireless networks. Due to its low computational complexity it can be particularly attractive in resource limited networks (e.g. sensor networks) or dynamic settings (e.g. ad hoc and device-to-device networks). We have extended earlier physical layer key generation approaches by proposing a novel key extraction scheme with multi-level feedback that allow for a substantial reduction of complexity in the information reconciliation phase.

References

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

[2] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. Part I: secret sharing," *IEEE Trans. Information Theory*, vol. 39, no. 4, 1993.

[3] G. Smith, "A direct derivation of a single-antenna reciprocity relation for the time-domain," *IEEE Trans. Antennas Propagation*, vol. 52, no. 6, pp. 1568–1577, Jun. 2004.

[4] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Communications*, vol. 43, no. 1, pp. 3–6, 1995.

[5] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Las Vegas, NV, Mar. 30 Apr. 4 2008, pp. 3013– 3016.

[6] C. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," *IEEE Trans. Information Theory*, vol. 50, no. 2, pp. 394–400, Feb. 1995.

[7] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proceedings of the 14th ACM conference on Computer and communications security*. ACM, 2007, pp. 401–410.

[8] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM International Conference on Mobile Computing and networking*. ACM, 2008, pp. 128–139.

[9] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE INFOCOM*. IEEE, 2011, pp. 1422–1430.

[10] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *Information Theory, IEEE Transactions on*, vol. 56, no. 5, pp. 2307–2359, 2010.

[11] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed. Boca Raton FL 33487-2742: CRC Press, 2007.