Secret Key Generation Based on AoA Estimation for Low SNR Conditions

source of randomness has not been presented in the literature before.

The rest of this paper is organized as follows: In Section II the system model is presented. The AoA estimation is then addressed in section III. Our secret key generation algorithm is presented in Section IV. We evaluate the performance of our algorithm in Section V. The paper is then concluded in section VI.

II. System Model

Let us assume that the two legitimate nodes, Alice and Bob, exchange a signal $s(t)$. Each of Alice's or Bob's receiver is equipped with a smart antenna system consisting of M antenna elements, separated by a fixed separation d and operating at frequency f. When using M receivers, the received and sampled signal $x[n]$ in the matrix notation is:

$$\mathbf{X} = \mathbf{as} + \mathbf{V}, \tag{1}$$

where $\mathbf{X}$ is of size $M \times N$ with N being the total number of received samples, $\mathbf{s}$ is of size $1 \times N$ as seen from each receiver, the steering vector $\mathbf{a}$ is of size $M \times 1$ and $\mathbf{V}$ is the AWGN matrix of size $M \times N$.

When using a single receiver to estimate the AoA as in our newly developed Cross Correlation Switched Beam System (XSBS) presented in [23], the received signal reduces to:

$$\mathbf{x_k} = \mathbf{aS} + \mathbf{v}, \tag{2}$$

where $\mathbf{x_k}$, the received signal from the k^{th} beam, is of size $1 \times N$, where $k \in [1 : K]$, where K is the total number of generated beams, $\mathbf{S}$ is of size $M \times N$ as seen by the M elements of the antenna array and $\mathbf{v}$ is of size $1 \times N$.

Each antenna array has an array response vector also known as *steering vector* $\mathbf{a}(\phi, \theta) \in \mathbb{C}^M$, where ϕ is the azimuth angle and θ is the elevation angle. For a uniform circular array (UCA), $\mathbf{a}(\phi, \theta)$, can be given by [24]:

$$\begin{aligned}\mathbf{a}(\phi,\theta) \;\; = \;\; & [e^{\beta r \sin(\theta)\cos(\phi-\phi_1)}, e^{\beta r \sin(\theta)\cos(\phi-\phi_2)}, \\ & ..., e^{\beta r \sin(\theta)\cos(\phi-\phi_M)}],\end{aligned} \tag{3}$$

where $\beta = \frac{2\pi}{\lambda}$ is the wave number, λ is the wavelength and r is the radius of the antenna array.

$$\phi_m = \frac{2\pi m}{M}, \quad m = 1, 2, .., M, \tag{4}$$

and ϕ ranges between $[0, 2\pi]$ and θ ranges between $[0, \pi]$.

To generate a secret key based on the estimated AoA, the estimated AoA has to be common at both Alice and Bob. In other words, both Alice and Bob estimate the same AoA, whether it is 1-D (Azimuth only) only or 2-D (Azimuth and Elevation). To do so, Both Alice and Bob agree only once on a selected reference, let it be the North, along with a rotation direction, let it be Clockwise as shown in Fig. 1 (a). In this case, the estimated AoA at Alice ϕ_1 is:

$$\phi_1 = \phi_c, \tag{5}$$

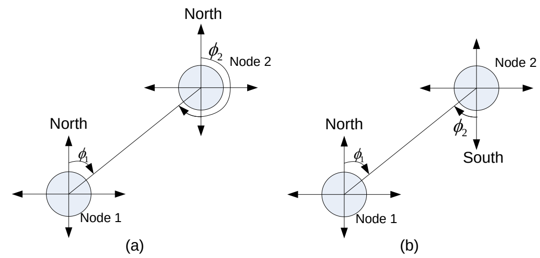

Fig. 1: AoA estimation reference: (a) Both have the same reference, let it be the North and (b) Alice has the reference as the North and Bob has the reference as the South.

where ϕ_c is the common AoA and the estimated AoA at Bob ϕ_2 is:

$$\phi_1 = \phi_c + \pi \tag{6}$$

Therefore, Bob estimates the common AoA, simply, by subtracting π from its estimated AoA ϕ_2. Another approach is that Alice uses the selected reference, let it be the North and Bob uses the opposite reference which is in this case the South. The rotation direction for Both is still the same, let it be Clockwise. As shown in Fig. 1 (b), the estimated AoAs are:

$$\phi_1 = \phi_2 = \phi_c. \tag{7}$$

To generate a sequence of AoA and use that sequence to generate the secret key, at least one of the communication nodes, i.e., either Alice or Bob, is assumed to be mobile.

III. AoA Estimation Techniques

There exists many techniques to estimate the AoA; some of which are: beam switching, classical AoA techniques and subspace techniques [25]–[29]. Subspace based techniques perform better than classical techniques, particularly at low SNR levels. This comes on the cost that they require a higher computational complexity. The most popular AoA estimation subspace based technique is the MUltiple SIgnal Classification (MUSIC) presented in [30]. For 1-D AoA estimation, the elevation angle θ is assumed to be 90 degrees. Therefore, the steering vector for the UCA in (3) reduces to:

$$\begin{aligned}\mathbf{a}(\phi) \;\; = \;\; & [e^{\beta r \cos(\phi-\phi_1)}, e^{\beta r \cos(\phi-\phi_2)}, \\ & ..., e^{\beta r \cos(\phi-\phi_M)}],\end{aligned} \tag{8}$$

The auto-covariance matrix of the received signal, R_{xx} has a dimension $M \times M$, i.e. M receivers are used. R_{xx} is estimated as:

$$\mathbf{R_{xx}} = \frac{1}{N}\left(\mathbf{XX^H}\right) \tag{9}$$

where H denotes the Hermitian matrix operation. The MUSIC algorithm exploits the orthogonality of the signal and noise subspaces. After an eigenvalue decomposition (EVD) on $\mathbf{R_{xx}}$, it can be written as:

$$\mathbf{R_{xx}} \;\; = \;\; \mathbf{a}(\phi)\mathbf{R_{ss}}\mathbf{a^H}(\phi) + \sigma^2 I \tag{10}$$

$$\;\; = \;\; U_s \Lambda_s U_s^H + U_v \Lambda_v U_v^H, \tag{11}$$

where $\mathbf{R_{ss}}$ is the autocovariance matrix of the transmitted signal, σ^2 is the noise variance, I is the unitary matrix, U_s and U_v are the signal and noise subspaces unitary matrices and Λ_s and Λ_v are diagonal matrices of the eigenvalues of the signal and noise. The spatial power spectrum for the MUSIC technique is given by [30], [31]:

$$P_{\text{MUSIC}}(\phi) = \frac{1}{\mathbf{a}^H(\phi) P_v \mathbf{a}(\phi)}, \tag{12}$$

where $P_v = U_v U_v^H$.

Our XSBS collects an omni-directional reference signal, $\mathbf{x_o}$, using a number of antennas in the antenna array with setting the elements of the steering vector $\mathbf{a}(\phi)$, equal to unity at selected elements (the antenna elements used as omni-directional antennas) and equal to zero in the rest. Our XSBS then starts to scan the angular region of interest and collect the signals $\mathbf{x_k}$, for $k \in [1:K]$. The cross correlation coef cient between our omni-directional reference signal and the k^{th} signal, which is our XSBS spatial power spectrum, can be given by:

$$\mathbf{R_{ko}} = \frac{1}{N}\left(\mathbf{x_k}\mathbf{x_o^H}\right) \tag{13}$$

There are several ways to estimate the 2-D AoA as presented in [32]–[34] where they use the cross correlation between the received signal from an L-shaped antenna array. In [35], they estimate the 2-D using a UCA based on the fourth order cumulant of the the received signals. Another example in [36], they use an antenna array that consists of a vertical linear array to estimate θ using the MUSIC algorithm, they then use a circular antenna array with θ fed to the MUSIC algorithm again to estimate ϕ.

Figure 2 shows the simulation results for both the MUSIC algorithm for $M = 16$, and for XSBS for $M = 17$, with ve antenna used as omni-directional antennas to collect $\mathbf{x_o}$ with a separation between each two antennas of $2 * d$ to such that the correlation between the signals received for the selected antenna elements is minimized. The simulation results are for $\phi = 270$ degrees using a UCA and $N = 100$ samples (left), $N = 1000$ samples (middle) and $N = 2000$ samples (right). The simulation is at SNR = - 15 dB. One can see that both algorithms have a remarkable performance at SNR levels as low as -15 dB. The MUSIC algorithm is achieving a peak to oor ratio (PFR) of 3, 10 and 13 for $N = 100$, $N = 1000$ and $N = 2000$, respectively. On the other hand the PFR for the XSBS 15, 19, and 23 for $N = 100$, $N = 1000$ and $N = 2000$, respectively. Increasing the number of samples enhances the performance of both algorithms. For an adequate number of collected samples $N = 1000$, both algorithms will have a decent performance even at very low SNR levels.

IV. Secret Key Generation Algorithm

Both Alice and Bob start exchanging signals to estimate the AoA and consequently generate the secret key. The steps to generate the secret key based on the AoA are:

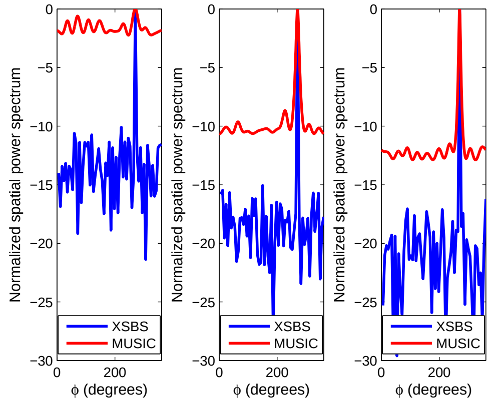

Fig. 2: Spatial power spectrum of MUSIC vs. XSBS for $\phi = 270$ degrees at SNR = -15 dB for $N = 100$ samples (left), $N = 1000$ samples (middle) and $N = 2000$ samples (right).

A. Initialization

Both Alice and Bob agree on the reference as well as the rotation direction, from which the AoA is estimated. This step is performed only once at the beginning of communication between them. It is not required to be applied each time Alice and Bob communicate.

B. AoA Estimation

Both Alice and Bob estimate their AoA and based on the selected reference, they estimate the common source of randomness, i.e. ϕ_c for 1-D or ϕ_c and θ_c for 2-D. The algorithm applied at either Alice or Bob does not necessarily be the same. One can use the MUSIC if it can afford both the computational and hardware complexity. The other can use the XSBS if, for example, it is a portable device and can not afford both computational and hardware complexities. Both Algorithms as we showed earlier can operate in low SNR levels. Other techniques could be used as well after studying their performance at low SNRs to make sure that the generated secret key will have a low BMR.

C. Quantization

Now that we have the common sources of randomness ϕ_c, the third step of our algorithm is to convert it into a bit stream suitable for the secret key generation. The conventional secret key length is between 128 and 512 bits [4]. We use the most popular technique for quantization which is the uniform quantization [37]:

$$z = Q(y) \qquad\qquad y \in (p_i, p_{i+1}) \tag{14}$$

where p is the interval and y is the input, which in this case is estimated AoA. In the uniform quantization, the spaces along the x-axis, i.e., time, is uniformly distributed. Similarly for the spaces in the y-axis, i.e., the estimated AoA. We use n_{quan} bits and therefore $2^{n_{quan}}$ levels to quantize our common sources of randomness and then convert the quantized decimal values into bits.

D. Encoding

Although uniform quantization is easy to implement, increasing the quantization bit number, dramatically degrades the performance of the algorithm since the bit mismatch rate between the two communicating nodes increases. In [3], an encoding algorithm is proposed to tackle this problem where each uniformly quantized value is encoded with multiple values. We encode our most significant bit with n_{encod} bits.

E. Combining the Two Bit Streams

Now that we have measured, quantized and encoded our two common sources of randomness, which are the elevation AoA and the Azimuth AoA, we have two bit streams containing these data. To combine these two bit streams, any logical operation such as AND, OR or concatenation can be applied on the two bit streams to generate a single bit stream containing both Azimuth and Elevation angles information. We choose to use concatenation operation with the two bit streams as the inputs to generate the single bit stream. Before we concatenate, we drop the least significant $n_{quan} - n_{combn}$ bits from each single bit stream, where n_{comb} is the number of bits selected from each bit stream. *It is worth noting that we chose a simple bit operation to be applied on the bit streams for the sake of simplification*. One can apply a more complicated operation at the bit streams such as bit masking or combinations of series and parallel logical gates.

Up to this step, the key is generated and ready to be used to encrypt the transmitted data. The following steps are optional and preferred to be used at very low SNR levels (below -20 dB) where the generated key will have a considerable BMR.

F. Information Reconciliation

The generated bit streams at Alice and Bob might have some discrepancy, particularly at very low SNR levels. This is due to several reasons such as interference, noise and hardware limitations. We adopt the reconciliation protocol presented in [38] to minimize the discrepancy. Both Alice and Bob first permute their bit streams in the same way. Then they divide the permuted bit stream into small blocks. Alice then sends permutations and parities of each block to Bob. Bob then compares the received parity information with the ones he already processed. In case of a parity mismatch, Bob changes his bits in this block to match the received ones.

G. Privacy Amplification

Although information reconciliation protocol leaks minimum information, the eavesdropper can still use this leaked information to guess the rest of the secret key. Privacy amplification solves this issue by reducing the length of the outputted bit stream. The generated bit stream is shorter in length but higher in entropy. To do so, both Alice and Bob apply a universal hash function selected randomly from a set of hash functions known by both Alice and Bob. Alice sends the number of the selected hash function to Bob so that Bob can use the same hash function. Our algorithm is summarized below.

Algorithm 1 Secret Key Generation algorithm

Step 0: Initialization
Alice and Bob agree on the reference and the rotation direction from which they estimate the AoA.
Step 1: AoA Estimation
Alice and Bob estimate the common source(s) of randomness, ϕ_c, or ϕ_c and θ_c, each using its implemented technique.
Step 2: Uniform Quantization
Alice and Bob quantize the ϕ_c or ϕ_c and θ_c using n_{quan} bits to convert the decimal values into bits.
Step 3: Encoding
Alice and Bob encode each uniformly quantized value with multiple values n_{encod}.
Step 4: Combining the Two Bit Streams
Alice and Bob apply concatenate the two bit streams.
Step 5: Information Reconciliation (Optional for very low SNR)
Alice and Bob permute the bit stream and divide them into small blocks.
Alice sends the permutation and parities to Bob.
Bob compares the received parity information with his.
In case of mismatch, Bob corrects his bits accordingly.
Step 6: Privacy Amplification (Optional for very low SNR)
Alice sends the number of the hash function to Bob.
Alice and Bob apply the hash function to the bit stream.

V. PERFORMANCE EVALUATION

To show that the secret key generated based on the estimated AoA will have a low BMR at low SNR levels, we first plot the root mean squared error (RMSE) of the estimated AoA for the two algorithms; the MUSIC and the XSBS. The RMSE is defined as:

$$RMSE = \sqrt{E\left((\hat{\phi}_c - \phi_c)^2\right)} \quad (15)$$

where $E[.]$ denotes the mean operation and $\hat{\phi}_c$ is the actual estimated AoA of the true AoA ϕ_c.

Fig. 3 presents the RMSE for both the MUSIC as well as the XSBS versus SNR for different number of samples for the Azimuth angle. The true Azimuth angle is $\phi_c = 270$ degrees and the RMSE is estimated according to Eq. (15). Table I summarizes the RMSE values for both the MUSIC and the XSBS for different number of samples at different SNR values for the Azimuth angle . Table II summarizes the RMSE values for both the MUSIC and the XSBS at different SNR values for the Elevation angle for $N = 1000$ samples. The true Elevation angle is $\theta_c = 90$ degrees and the RMSE is estimated according to Eq. (15).

From Tables I and II, one can see that both the MUSIC and the XSBS have a low RMSE at low SNR levels. As the SNR decreases, more samples are required to achieve a very low RMSE. The XSBS outperforms the MUSIC algorithms, particularly at very low SNR levels. One can see that when using an adequate number of samples, the RMSE of both

TABLE I: RMSE for MUSIC vs. XSBS for the Azimuth angle.

SNR (dB)	RMSE (degrees)					
	N= 100		N= 1000		N= 2000	
	MUSIC	XSBS	MUSIC	XSBS	MUSIC	XSBS
-10	0	0	0	0	0	0
-15	39	0	0	0	0	0
-20	115	0	29	0	5	0
-25	132	66	114	0	98	0
-30	135	126	131	61	129	20

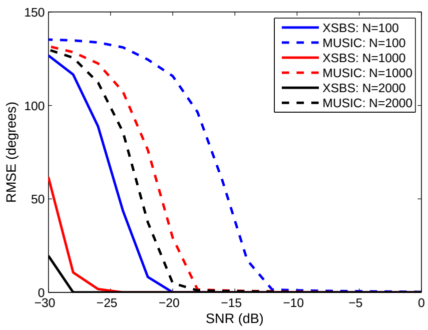

Fig. 3: RMSE vs. SNR for the MUSIC algorithm and for the XSBS.

algorithm will be very low. Consequently, the secret key generated using the estimated AoA as the seed will have a low BMR.

We use the estimated RMSE to generate random Azimuth and Elevation angles and use them as the seed to generate the secret key. We compare the BMR of the generated keys based on AoA with the BMR of the most commonly used physical layer characteristics which are the channel gain and phase. The simulation parameters for the subsequent Figures 4 to 7 are summarized in Table III. Also, the Legends for the curves within the same gures are identi ed in Table IV. We rst use a single characteristic, i.e., amplitude only, phase only, Azimuth angle only and Elevation angle only. We then combine the channel amplitude and phase and combine the Azimuth and Elevation angles to generate the secret key. It's worth noting that the acceptable BMR threshold as presented in [14] is 0.15 to achieve a reliability condition.

For a fair comparison between the different common sources of randomness, we rst scale the sequence of information collected to the same scaling level such that all common sources of randomness used below, i.e., channel amplitude, channel phase, Azimuth angle and Elevation angle uctuate within the same levels.

A. *MUSIC vs. XSBS*

In Fig. 4 we compare the performance of the MUSIC algorithm versus the XSBS in generating the secret key. It can be seen that the algorithm based on XSBS outperforms the MUSIC based algorithm, which was expected since the RMSE for the XSBS is lower than that for the MUSIC. The MUSIC based algorithm can operate within the acceptable range up to - 17 dB, while the XSBS based can operate up to -27 dB.

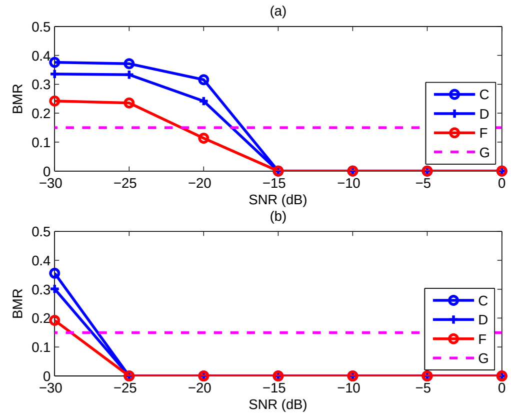

Fig. 4: BMR for (a) MUSIC and (b) XSBS vs. SNR for Azimuth angle, Elevation angle and both angles combined.

TABLE II: RMSE for MUSIC vs. XSBS for the Elevation angle for $N = 1000$ Samples.

SNR (dB)	RMSE (degrees)	
	MUSIC	XSBS
-10	0	0
-15	0	0
-20	8	0
-25	34	0
-30	37	20

B. *Effect of number of quantization bits*

The rst observation aside from the effect of any parameter whether it is the number of quantization bits or the encoding bits, which can be seen from the subsequent Figures, that our AoA based algorithm signi cantly outperforms both the channel amplitude and phase based ones. It is shown that the our algorithm has an operating range below the acceptable threshold which varies according to the testing parameters. Unlike the channel amplitude and phase based algorithm that fail to have an operating range at that low SNR level by achieving a BMR much higher than the acceptable threshold. Also, it is worth noting that the upper bound on the BMR is 0.5 which is equivalent to random guessing. In other words, the highest, i.e., the worst BMR is 0.5.

It is shown from Fig. 5 that as the number of quantization bits increases, the performance of our algorithm deteriorates.

TABLE III: Simulation parameters for the subsequent gures

Figure	Algorithm	Samples	Quan. Bits	Enc. Bits	Comb. Bits
Fig. 4	Both	1000	7	2	2
Fig. 5	MUSIC	1000	6:9	2	5
Fig. 6	MUSIC	1000	7	1:4	5
Fig. 7	MUSIC	1000	7	2	3:6

TABLE IV: Legend

A	B	C	D	E	F	G
Chan. amp.	Chan. phase	Az. angle	Elev. angle	Comb. amp. & ph	Comb. Az. & Elev	Thresh.

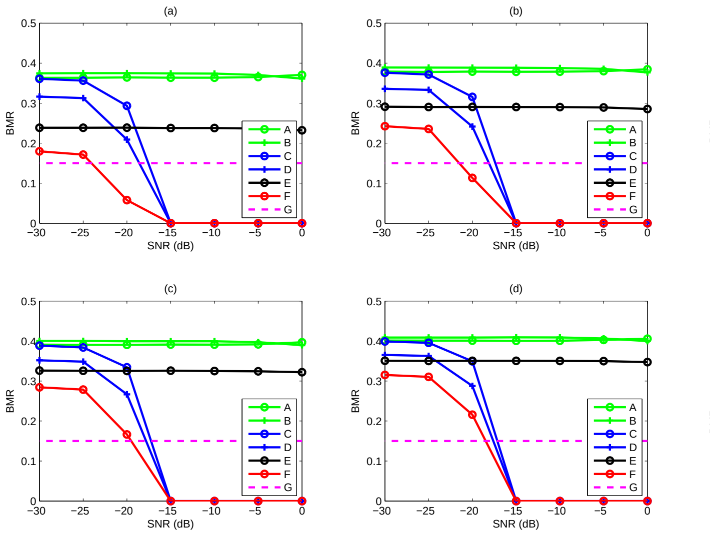

Fig. 5: BMR for the AoA based algorithm vs. channel based for (a) $n_{quan} = 6$ and (b) $n_{quan} = 7$ (c) $n_{quan} = 8$ (d) $n_{quan} = 9$.

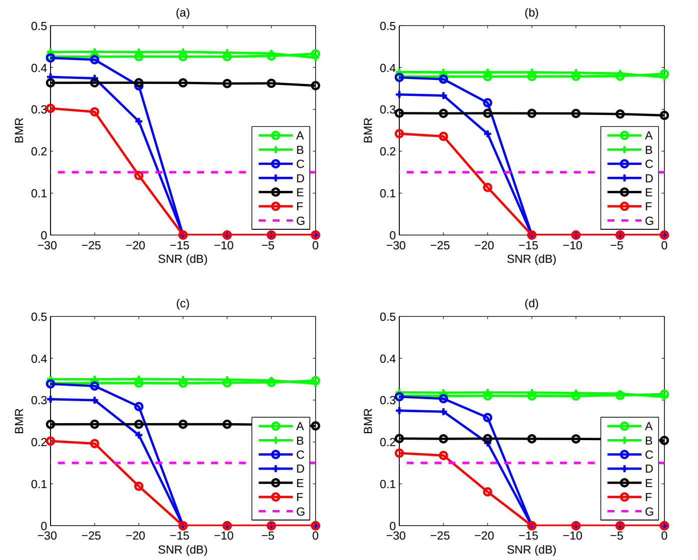

Fig. 6: BMR for the AoA based algorithm vs. channel based for (a) $n_{encod} = 1$ and (b) $n_{encod} = 2$ (c) $n_{encod} = 3$ (d) $n_{encod} = 4$.

This is expected since as the number of quantization b increases, more levels are added. Therefore a smaller misma or error between the estimated AoAs will lead to mor mismatched bit. The acceptable range using $n_{quan} = 7$ is as low as -16 dB using the Azimuth angle, -17 dB using th Elevation angle and -22 using the combination of both of ther

C. Effect of number of Encoding bits

It is shown from Fig. 6 that as the number of encodin bits increases, the performance of our algorithm improve As the number of encoding bits increases, more matched b are added to soothe the effect of quantization. The accepta range using $n_{encod} = 2$ is as low as -16 dB using the Azimuth angle, -17 dB using the Elevation angle and -22 using t combination of both of them.

D. Effect of number of Combining bits

It is shown from Fig. 7 that as the number of combinin bits increases, the performance of our algorithm improves. addition to that, the higher the number of combining bits the longer the generated key which is the main advantage of the concatenation process. The acceptable range using $n_{comb} = 5$ is as low as -16 dB using the Azimuth angle, -17 dB using the Elevation angle and -22 using the combination of both of them.

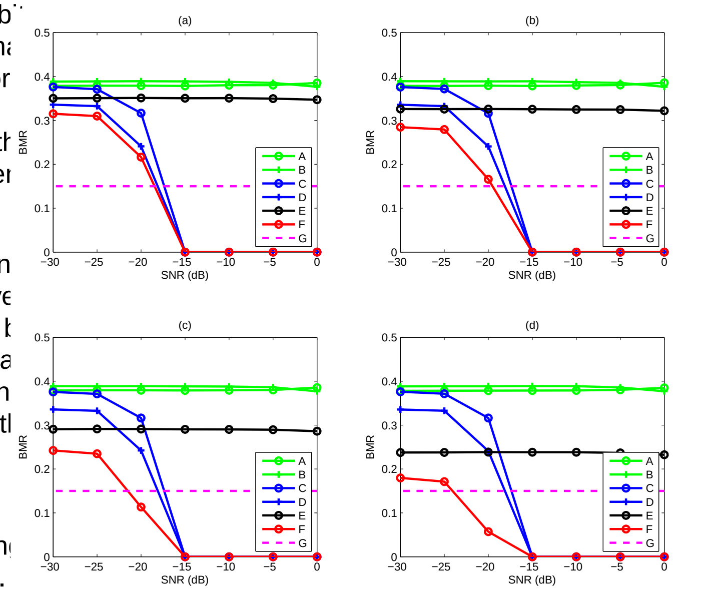

Fig. 7: BMR for the AoA based algorithm vs. channel based for (a) $n_{comb} = 3$ and (b) $n_{comb} = 4$ (c) $n_{comb} = 5$ (d) $n_{comb} = 6$.

VI. Conclusion

In this paper, we proposed a novel secret key generation algorithm that is based on the estimated AoA between the two legitimate nodes. We rst showed that the RMSE for the estimated AoA between Alice and Bob is very low at very low SNR levels. We used both the 1-D AoA information and the 2-D AoA information. Exploiting a second common source of randomness adds an extra degree of freedom to the algorithm since one can use either a single common source or combine both of them in a way that minimizes the BMR. We compared the performance of our algorithm to the most widely used; the channel gain based algorithm. We showed that our algorithm has signi cantly outperformed the channel gain based algorithm at low SNR levels. We also studied the effect of number of quantization bits, number of encoding bit and number of combining bits on the performance of our algorithm.

ACKNOWLEDGMENT

This research was made possible by NPRP 5-559-2-227 grant from the Qatar National Research Fund (a member of The Qatar Foundation). The statements made herein are solely the responsibility of the authors.

REFERENCES

[1] 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*, ser. CCS '07, 2007, pp. 401–410.

[2] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proceedings of the 5th ACM Workshop on Wireless Security*, ser. WiSe '06, 2006, pp. 33–42.

[3] J. Zhang, S. Kasera, and N. Patwari, "Mobility assisted secret key generation using wireless link signatures," in *INFOCOM, 2010 Proceedings IEEE*, 2010, pp. 1–5.

[4] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08, 2008, pp. 128–139.

[5] R. Wilson, D. Tse, and R. Scholtz, "Channel identi cation: Secret sharing using reciprocity in ultrawideband channels," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 3, pp. 364–375, 2007.

[6] N. Patwari, J. Croft, S. Jana, and S. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *Mobile Computing, IEEE Transactions on*, vol. 9, no. 1, pp. 17–30, 2010.

[7] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *Selected Areas in Communications, IEEE Journal on*, vol. 30, no. 9, pp. 1666–1674, October 2012.

[8] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '09, 2009, pp. 321–332.

[9] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *Mobile Computing, IEEE Transactions on*, vol. 12, no. 5, pp. 917–930, 2013.

[10] A. Kitaura, H. Iwai, and H. Sasaoka, "A scheme of secret key agreement based on received signal strength variation by antenna switching in land mobile radio," in *Advanced Communication Technology, The 9th International Conference on*, vol. 3, Feb 2007, pp. 1763–1767.

[11] Y. Wei, C. Zhu, and J. Ni, "Group secret key generation algorithm from wireless signal strength," in *Internet Computing for Science and Engineering (ICICSE), 2012 Sixth International Conference on*, April 2012, pp. 239–245.

[12] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *Wireless Communications, IEEE*, vol. 18, no. 4, pp. 6–12, August 2011.

[13] O. Gungor, F. Chen, and C. Koksal, "Secret key generation from mobility," in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, 2011, pp. 874–878.

[14] O. Güngör, F. Chen, and C. E. Koksal, "Secret key generation from mobility," *CoRR*, vol. abs/1112.2793, 2011.

[15] N. Patwari and A. O. Hero, III, "Using proximity and quantized rss for sensor localization in wireless networks," in *Proceedings of the 2Nd ACM International Conference on Wireless Sensor Networks and Applications*, ser. WSNA '03, 2003, pp. 20–29.

[16] R. Al Alawi, "Rssi based location estimation in wireless sensors networks," in *Networks (ICON), 2011 17th IEEE International Conference on*, 2011, pp. 118–122.

[17] Z. Zhang, C. Law, and Y. Guan, "Ba-poc-based ranging method with multipath mitigation," *Antennas and Wireless Propagation Letters, IEEE*, vol. 4, no. 1, pp. 492–495, 2005.

[18] J.-Y. Lee and R. Scholtz, "Ranging in a dense multipath environment using an uwb radio link," *Selected Areas in Communications, IEEE Journal on*, vol. 20, no. 9, pp. 1677–1683, 2002.

[19] L. Mailaender, "On the geolocation bounds for round-trip time-of-arrival and all non-line-of-sight channels," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, no. 1, p. 584670, 2008.

[20] Y. Qi, H. Kobayashi, and H. Suda, "Analysis of wireless geolocation in a non-line-of-sight environment," *Wireless Communications, IEEE Transactions on*, vol. 5, no. 3, pp. 672–681, 2006.

[21] S. Gezici, Z. Tian, G. Giannakis, H. Kobayashi, A. Molisch, H. Poor, and Z. Sahinoglu, "Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks," *Signal Processing Magazine, IEEE*, vol. 22, no. 4, pp. 70–84, 2005.

[22] M. Dashti, M. Ghoraishi, and J.-i. Takada, "Optimum threshold for ranging based on toa estimation error analysis," in *Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on*, Sept 2009, pp. 988–992.

[23] D. T. T. E. Ahmed Badawy, Tamer Khattab and A. Mohamed, "A simple aoa estimation scheme," *CoRR*, vol. abs/1409.5744, 2014. [Online]. Available: http://arxiv.org/abs/1409.5744

[24] P. Ioannides and C. Balanis, "Uniform circular arrays for smart antennas," *Antennas and Propagation Magazine, IEEE*, vol. 47, no. 4, pp. 192–206, Aug 2005.

[25] T. E. Tuncer and B. Friedlander, *Classical and Modern Direction-of-Arrival Estimation*. Academic Press, 2009.

[26] C. A. Balanis and P. I. Ioannides, "Introduction to smart antennas," *Synthesis Lectures on Antennas*, vol. 2, no. 1, pp. 1–175, 2007.

[27] Z. Chen, G. Gokeda, and Y. Yu, *Introduction to Direction-of-Arrival Estimation*. Artech House, 2010.

[28] S. Chandran, *Advances in Direction-of-Arrival Estimation*. Artech House, 2006.

[29] J. Foutz, A. Spanias, and M. K. Banavar, *Narrowband Direction of Arrival Estimation for Antenna Arrays*. Morgan & Claypool Publishers, 2006.

[30] R. O. Schmidt, "A signal subspace approach to multiple emitter location and spectral estimation," Ph.D. dissertation, Stanford University.

[31] A. Khallaayoun, "A High Resolution Direction of Arrival Estimation Analysis and Implementation in a Smart Antenna System," Ph.D. dissertation, Montana State University.

[32] N.-J. Li, J.-F. Gu, and P. Wei, "Simple and ef cient cross-correlation method for estimating 2-d direction of arrival," in *Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference on*, Sept 2009, pp. 1–4.

[33] Y. Hua, T. Sarkar, and D. Weiner, "An l-shaped array for estimating 2-d directions of wave arrival," *Antennas and Propagation, IEEE Transactions on*, vol. 39, no. 2, pp. 143–146, Feb 1991.

[34] F. Harabi, H. Changuel, and A. Gharsallah, "Estimation of 2-d direction of arrival with an extended correlation matrix," in *Positioning, Navigation and Communication, 2007. WPNC '07. 4th Workshop on*, March 2007, pp. 255–260.

[35] W. Sujuan, D. Jiahao, P. Shuguang, S. Dongning, and D. Xingguang, "The estimation for 2-d direction of arrival based on higher-order cumulant of signals received by circle array," in *Computational Electromagnetics and Its Applications, 2004. Proceedings. ICCEA 2004. 2004 3rd International Conference on*, Nov 2004, pp. 348–351.

[36] Y. Albagory and A. ashour, "Music 2d-doa estimation using split vertical linear and circular arrays," *Computer Network and Information Security (IJCNIS), International Journal of*, vol. 5, no. 8, pp. 12–18, June 2013.

[37] L. Tan, *Digital Signal Processing Fundamentals and Applications*. Academic Press, 2007.

[38] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion." Springer-Verlag, 1994, pp. 410–423.