Experimental Investigation of MIMO Reciprocal Channel Key Generation

Jon W. Wallace and Rajesh K. Sharma

School of Engineering and Science, Jacobs University Bremen
Campus Ring 1, 28759 Bremen, Germany
E-mail: wall@ieee.org, ra.sharma@jacobs-university.de

***Abstract*— There is growing interest in physical-layer key generation schemes that provide very strong or even perfect security in wireless communication systems. One such scheme is reciprocal channel key generation, where two nodes quantize reciprocal channel state information to generate keys. Although the use of multiple-input multiple-output (MIMO) techniques is interesting in this case since the number of random parameters available for rapid key generation is increased, MIMO techniques may also provide more information to an eavesdropper. This work presents a new MIMO measurement campaign performed in LOS and NLOS indoor environments that studies the correlation of the channel between legitimate users with the eavesdropper channel, revealing what key generation rates can be attained in practice and what fraction of generated key bits are safe from eavesdroppers. The effect of eavesdropper separation, number of antennas, eavesdropper advantage, and covariance separability are studied.**

I. Introduction

Physical layer security is a method for enhancing the security of existing wireless systems and networks by exploiting the random nature of the physical propagation channel, possibly providing perfect information theoretic security in some cases. In reciprocal channel key generation (RCKG), legitimate nodes observe a common fluctuating channel [2] to generate keys that are safe from the eavesdropper (Eve), in contrast to existing physical layer approaches that transmit random information through the channel and distill common randomness at Alice and Bob that is unobservable by Eve [1]. Advantages of RCKG are that perfect secrecy is attained without needing to estimate Eve's channel quality, full channel variability is available for key generation since channel state information (CSI) is never fed back between Alice and Bob, keys can be generated using buffered CSI data in contrast to methods that adapt transmission to the immediate channel state, and existing TDD systems could already support RCKG without any changes to the PHY or MAC.

In previous work [5], [6], we derived expressions for the available key bits and those safe from an eavesdropper for MIMO systems with correlated complex Gaussian statistics and presented extensions to existing channel quantization (CQ) that dramatically reduce symbol error rate (SER). In this paper, we build on this foundation to investigate key generation limits and the performance of CQ methods for real LOS and NLOS scenarios based on new MIMO measurements in an indoor environment, revealing the true rate at which key bits can be generated as well as the required eavesdropper separation required for key bits to be secure.

II. Information Theoretic Limits and Key Generation Methods

Here we briefly list a number of important results from [5], [6] that are needed for this experimental investigation. Figure 1 depicts our system model, where Alice and Bob are legitimate users and Eve is a potential eavesdropper. Reciprocal vector channels $\mathbf{h}_a = \mathbf{h}_{a'}$ are referred to as the *forward* and *reverse* channels that are estimated by Bob and Alice, respectively, while channels $\mathbf{h}_b$ and $\mathbf{h}_c$ are estimated by Eve. The nodes have imperfect channel estimates

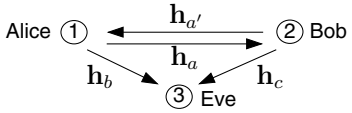

Fig. 1. System model for a wireless communications scenario

$$\hat{\mathbf{h}}_a = \mathbf{h}_a + \boldsymbol{\epsilon}_2, \;\; \hat{\mathbf{h}}_{a'} = \mathbf{h}_{a'} + \boldsymbol{\epsilon}_1, \;\; \hat{\mathbf{h}}_b = \mathbf{h}_b + \boldsymbol{\epsilon}_3, \;\; \hat{\mathbf{h}}_c = \mathbf{h}_c + \boldsymbol{\epsilon}_3', \tag{1}$$

where $\boldsymbol{\epsilon}_i$ is zero-mean complex Gaussian estimation error at node i having variance σ_i^2, which can be due to thermal noise, interference, time-variation of the channel, slight non-reciprocities, etc. Channel vectors contain general CSI quantities, such as MIMO and OFDM channel coefficients.

Channels are zero-mean spatially correlated complex Gaussian random processes, characterized by covariance matrices

$$\mathbf{R}_{p_1 p_2} = \mathrm{E}\left\{\mathbf{h}_{p_1}\mathbf{h}_{p_2}^H\right\} \;\; \hat{\mathbf{R}}_{p_1 p_2} = \mathrm{E}\left\{\hat{\mathbf{h}}_{p_1}\hat{\mathbf{h}}_{p_2}^H\right\}, \tag{2}$$

where $p_1, p_2 \in \{a, a', b, c\}$. It is assumed that temporal correlation of channel estimates has been removed by pre-whitening or decimation of the CSI stream.

The available key bits that can be extracted by Alice and Bob from noisy reciprocal MIMO channel estimates is

$$I_{\mathrm{K}} = \log_2 |\mathbf{R}_{aa}\mathbf{R}_{\sigma}^{-1} + \mathbf{I}|, \tag{3}$$

$$\mathbf{R}_{\sigma} = (\sigma_1^2 + \sigma_2^2)\mathbf{I} + \sigma_1^2\sigma_2^2\mathbf{R}_{aa}^{-1}. \tag{4}$$

This paper focuses on a worst-case scenario where Eve is near one of the legitimate nodes (chosen to be Alice), and the number of secure key bits is

$$I_{\mathrm{SK}} = \log_2 \frac{|\hat{\mathbf{R}}_{AC}||\hat{\mathbf{R}}_{A'C}|}{|\hat{\mathbf{R}}_{C}||\hat{\mathbf{R}}_{AA'C}|}, \tag{5}$$

where a covariance with uppercase subscripts is that of the named vectors stacked into an aggregate vector or

$$\hat{\mathbf{R}}_{P_1 P_2 \ldots P_M} = \mathrm{E}\left\{[\hat{\mathbf{h}}_{p_1}^H\hat{\mathbf{h}}_{p_2}^H \ldots \hat{\mathbf{h}}_{p_M}^H]^H[\hat{\mathbf{h}}_{p_1}^H\hat{\mathbf{h}}_{p_2}^H \ldots \hat{\mathbf{h}}_{p_M}^H]\right\}. \tag{6}$$

In [6] two channel quantization methods were presented. In channel quantization with guardband (CQG), Alice and Bob divide the space of observable channels into N rectangular quantization sectors (QSs) with equal probability and

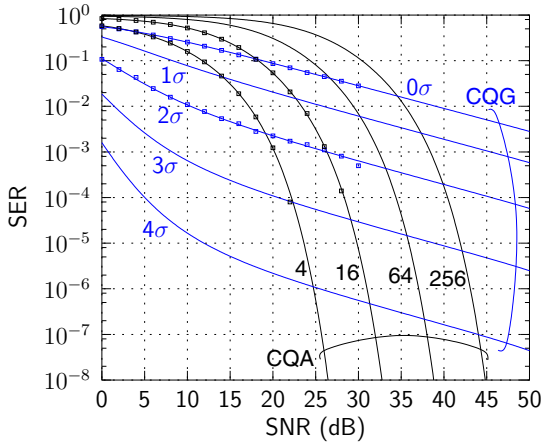

Fig. 2. Exact SER performance of CQ methods, where results verified with Monte-Carlo are shown as boxes, and σ is the estimation error variance

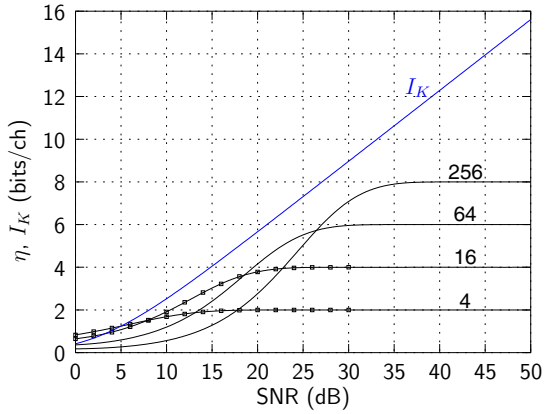

Fig. 3. Exact efficiency η of CQA, where results verified with Monte-Carlo are shown as boxes

specified guardband g between sectors. Although SER can be reduced significantly with CQG, the efficiency suffers. In channel quantization alternating (CQA), QSs are formed in a similar way, but alternate interleaved maps are used instead of guardband. By adapting the QSs to the channel observation, SER similar to CQG can be obtained, but with no reduction in efficiency. Figure 2 plots the exact symbol error rate of CQA (varying order N) and CQG ($N = 4$ QSs) for a single complex scalar channel with unit variance, estimation error σ^2, and SNR=$1/\sigma^2$. Due to superior performance at moderate SNR, only CQA will be considered hereafter, whose exact efficiency is plotted in Figure 3. Here, efficiency is defined as the number of good bits per channel observation, or $\eta = (1-P_e)\log_2(N)$, where P_e is the probability of a symbol error.

III. MIMO Security Measurements

MIMO measurements were taken on the first floor of the Research I building on the Jacobs University Bremen Campus, consisting mainly of classrooms and laboratories, which is depicted in Figure 4. Measurements were performed with a custom MIMO channel sounder fabricated at Jacobs University that is functionally equivalent to the switched array architecture presented in [7].

MIMO channels were measured with 23 dBm transmit power using a multitone signal consisting of $N_F = 8$ discrete frequencies with 10 MHz separation and centered at 2.55 GHz. Transmit (TX) and receive (RX) employed 8-element monopole antennas equivalent to those in [7]. At TX, the monopoles were attached to a ground plane having a pre-drilled hexagonal grid of holes, and the antenna positions were chosen to form a nearly uniform 8-element circular array (5.7 cm=0.47λ interelement spacing, where λ is the free-space wavelength at 2.55 GHz). In subsequent analysis, only 4 of the TX elements are usually considered (a semi-circle of adjacent elements), simulating Alice and Bob with the same number of antennas.

Unlike usual single-link MIMO measurements, the RX antennas were partitioned into two separate 4-element square arrays (5 cm=0.43λ interelement spacing) to represent Alice and Eve, where each sub-array consisted of 4 antennas in a separate 15 cm×15 cm ground plane. Although truly bi-directional measurements (simultaneous measurement of $\mathbf{h}_a$, $\mathbf{h}_c$ *and* $\mathbf{h}'_a$) is perhaps of interest, due to limitations of measurement equipment, only $\mathbf{h}_a$ and $\mathbf{h}_c$ are measured, and $\mathbf{h}'_a = \mathbf{h}_a$ is assumed. The goals of this work are not significantly hindered by this limitation, since non-reciprocity could be mitigated by careful system design and residual error can be lumped into channel estimation error.

The sub-arrays were fixed to a long wooden plank with mounting holes drilled at regular intervals, and Alice-Eve separation distances d of 10 cm, 25 cm, 1 m, and 2 m were investigated. Both TX and RX arrays were approximately 1.6 m off the ground (shoulder height). TX and RX were placed on carts, where the TX remained stationary throughout the measurement and the RX was pushed along a straight path at approximately 0.3 m/s to obtain a time-varying channel response. Given the channel measurement repetition rate of 1 snapshot/3 ms, the spatial sampling resolution along the path is 130 snapshots/λ, sufficient to ensure quasi-static channel conditions for a single switched snapshot. For each TX/RX position, 8 measurements were taken, consisting of 2 trials for each of the 4 different Alice-Eve separations.

The raw channel snapshot for the ith receiver, jth transmitter, fth frequency, and nth temporal sample is denoted $h^{(f,n)}_{\text{raw},ij}$, where $i \in [1,4]$ is Alice, $i \in [5,8]$ is Eve, and j is Bob's antenna index. $\mathbf{H}^{(f,n)}_{\text{raw}}$ is normalized and possibly processed (described later) to obtain $\mathbf{H}^{(f,n)}$. A time series of channel covariances is obtained by dividing temporal snapshots into 10λ blocks having N_B=1297 samples each, and computing the full channel covariance for block n as

$$r^{(n)}_{ij,k\ell} = \frac{1}{N_B N_F} \sum_{f=1}^{N_F} \sum_{m=(n-1)N_B+1}^{nN_B} h^{(f,m)}_{ij} h^{(f,m)*}_{k\ell}. \quad (7)$$

IV. Key Generation Limits of Measured Channels

Figure 5(a) plots example temporal variation of I_{K} and I_{SK} for the raw channels acquired for Location 1B with four antennas at Alice, Bob, and Eve. Here, channels are normalized collectively to give an average SISO SNR of 15 dB, although instantaneous SNR can be higher or lower at each position since path loss differences are preserved. In this LOS scenario, RX approaches TX and the number of available and safe key bits both increase with increasing SNR. Also, increasing Alice-Eve separation (d) weakly increases safe key bits.

Instead of processing raw data in this way, we will simulate a realistic system with power control, where average SISO gain in each block is normalized to 1. Since for LOS scenarios the dominant non-fading component is not very secure for generating keys and violates the zero-mean Gaussian assumption,

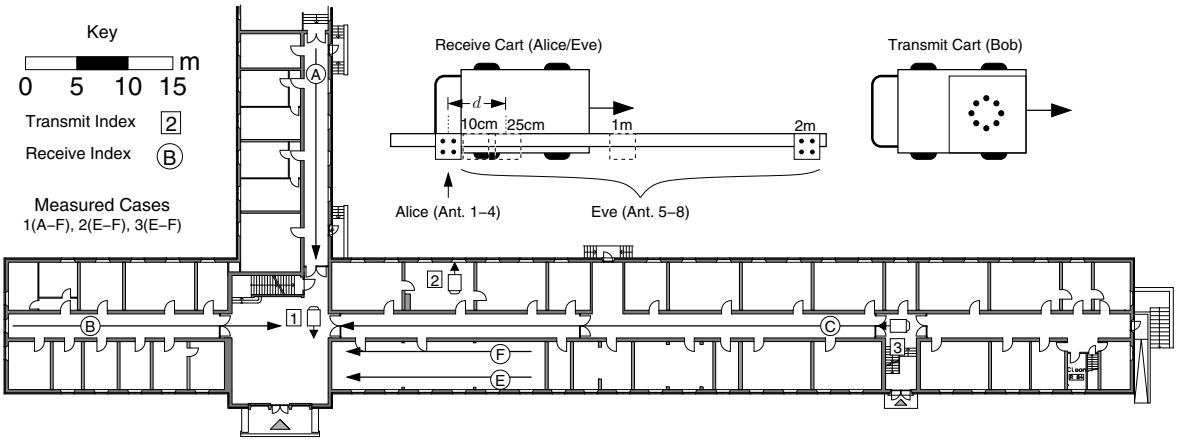

Fig. 4. Indoor measurement scenario on the ground floor of Research I on the Jacobs University Bremen campus. Boxed numbers indicate stationary transmit (Bob) positions, while circled letters indicate moving paths for the receiver (Alice/Eve).

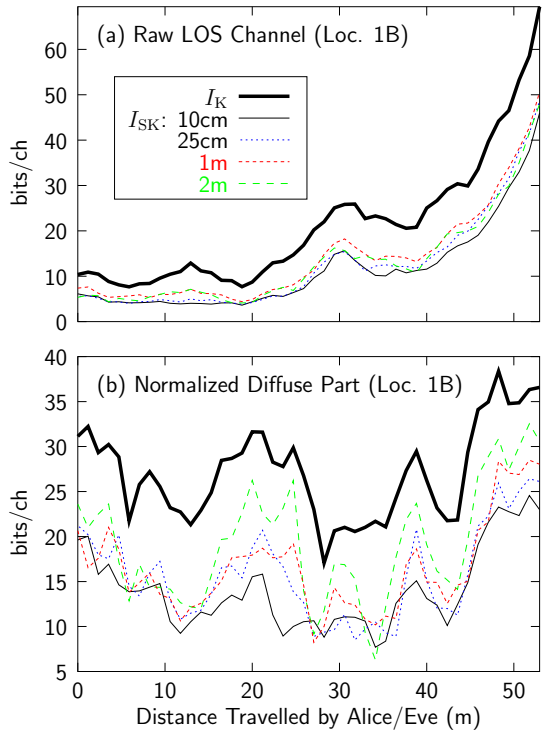

Fig. 5. Available (I_K) and secret (I_{SK}) key bits for LOS Location 1B: computed for (a) raw channels, and (b) normalized channels with DCR

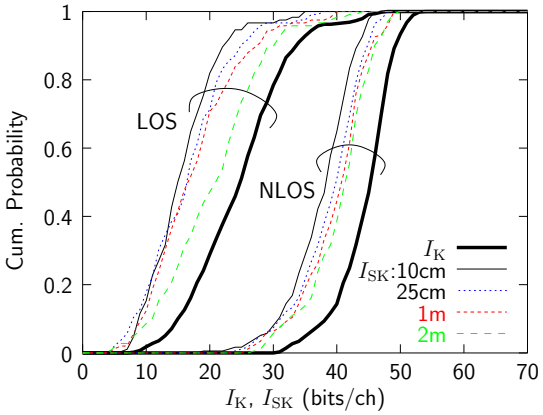

Fig. 6. CDFs for I_K and I_{SK} averaged over all LOS and NLOS scenarios

we approximately remove its effect using dominant component removal (DCR). We can only briefly explain that DCR works by performing a higher-order singular value decomposition (HOSVD) on the tensor covariance [8] in each block and forming the dominant component as the outer product of the dominant singular vectors for transmit and receive. Each channel within that block is then projected onto the dominant component and the result is subtracted from the channel. Observations confirm that this simple method transforms LOS data with marginal Rician statistics to marginal Gaussian statistics as desired.

Figure 5(b) plots I_K and I_{SK} for Location 1B for normalized channels after DCR for 15 dB SNR. Compared to the raw channels in Figure 5(a), the dynamic range of key generation rates is reduced. The number of available key bits varies between 20 and 40 bits/ch, which is around half of the theoretical value for rich multipath channels [6]. Note that the highest I_K occurs at the end of the path, where the receiver transitions from the hallway to an open foyer. At positions in the hallway with high I_K, values for I_{SK} depend more strongly on eavesdropper separation d, similar to observations in [6], where more paths give higher key generation rates, but require larger Alice-Eve separation to be secure.

A. Environmental Effects: LOS vs. NLOS

Figure 6 plots the key generation statistics for I_K and I_{SK} for LOS and NLOS scenarios with $N = 4$ antennas for Alice, Bob, and Eve and SNR=15 dB. LOS channels exhibit about half of the available key bits compared to NLOS, likely due to power control (equal SNR) and power reduction by DCR. Although for the widest separation of 2 m, there is still a gap of around 4 bits/ch between I_{SK} and I_K, this is only 10-20% of the total available key bits, indicating that most key bits are actually safe under practical conditions.

B. Dependence on Number of Antennas

Figure 7 plots key generation statistics for varying numbers of antennas for NLOS scenarios only, where curves for (N_1, N_2) indicate N_1 antennas each at Alice and Eve and

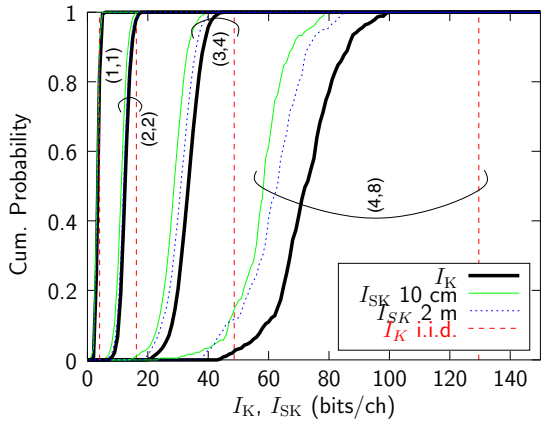

Fig. 7. CDFs for I_K and I_{SK} for NLOS scenarios with varying number of antennas

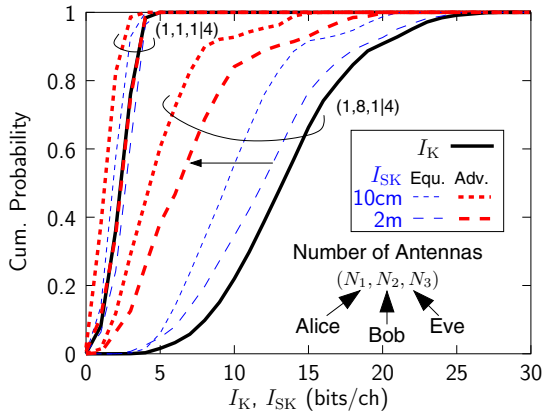

Fig. 8. CDFs when Eve has equal SNR and antennas as Alice (Equ.) or SNR and array size advantage (Adv.)

N_2 at Bob. For few antennas at Alice and Bob, I_K is near the theoretical maximum for i.i.d. Gaussian channels and most key bits are safe ($I_{SK} \approx I_K$). However, for increasing numbers of antennas, the gap between ideal i.i.d. I_K and actual I_K widens dramatically, which is reasonable since increasing antennas for limited multipath will lead to high correlation. Also, the gap between I_K and I_{SK} increases moderately with additional antennas. Similar trends are seen for LOS scenarios.

C. Effect of Eavesdropper Advantage

Eavesdroppers with a significant SNR and/or array size advantage may limit the security of key generation when Eve's channel is correlated with the Alice-Bob channel. Figure 8 depicts statistics for LOS scenarios with SNR=15 dB for two cases, illustrating where eavesdropper advantage appears to have minimum and maximum effect. Advantage appears to have minimal effect for small arrays that are balanced at Alice and Bob ($N_1 = N_2 = 1$). In this case the plot shows that at 2 m separation, a larger array ($N_3 = 4$) and SNR advantage (35 dB) help Eve negligibly. On the other hand, for unbalanced arrays ($N_1 = 1$, $N_2 = 8$), having more antennas at Eve reduces security significantly, as depicted by the arrow. Note that for slightly larger balanced arrays ($N_1 = 2$, $N_2 = 2$, and $N_3 = 2$ or $N_3 = 4$) we observe (not plotted) that the impact of eavesdropper antenna advantage is small, similar to the single antenna case.

These results are logical, since for a larger array Eve can estimate more multipath components and obtain a better estimate of the Alice-Bob channel. In general, we have observed that having an antenna advantage appears to help Eve more than even a very large SNR advantage.

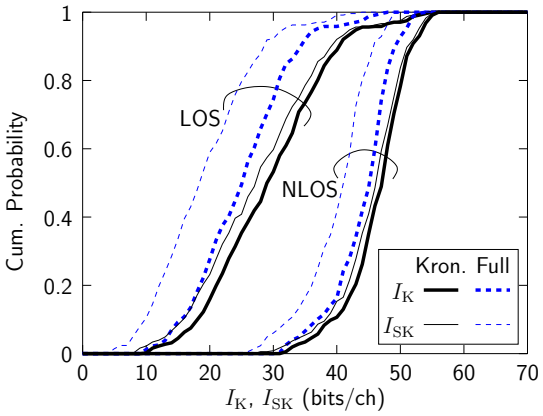

Fig. 9. Comparison of key generation CDFs for LOS and NLOS cases using Kronecker (solid) or full (dashed) covariance for 15 dB SNR

D. Impact of Using Separable Covariances

In real systems with limited CSI, separate (Kronecker) transmit and receive covariances are more easily computed than full covariance. Figure 9 shows how I_K and I_{SK} computed with Kronecker covariances compare with the true values computed with the full covariance, where each node has 4 antennas, 15 dB SNR, and I_{SK} is the average value for 1 and 2 m separation. Although the Kronecker model somewhat overestimates the number of available key bits, perhaps more importantly it suggests that nearly all key bits are secure, when a significant gap is present for the full covariance. This result is in harmony with previous MIMO capacity studies that show that the Kronecker model creates spurious non-physical paths that inflate the richness (diversity order) of channels.

V. Key Generation using Measured Channels

Section IV indicated that between 10 and 50 bits/channel are available for a 4-antenna system in the indoor channel. It is of interest to study how many bits can be generated with the CQA method using a practical implementation. In this section, we briefly outline one possible adaptive CQA protocol, followed by an investigation of its performance using the measured data.

A. Key Generation Protocol

The adaptive CQA method can be briefly outlined as

1) Raw CSI is subdivided into blocks large enough to have sufficient intra-block fading (10λ distance used here).
2) The decorrelation sample lag n_d (where temporal autocorrelation drops to $1/e$ of its maximum value) is estimated, and CSI data is decimated at this interval.
3) Full spatial covariance is estimated in each block using all remaining time/frequency samples of CSI.
4) The eigenvalue decomposition (EVD) is used to spatially decorrelate CSI samples, where the SNR of the resulting parallel channels streams is given by the eigenvalues.
5) For a maximum target SER, the highest quantization order N for each parallel stream is chosen considering Figure 2 and stream SNRs.
6) Parallel streams are normalized to have unit variance.

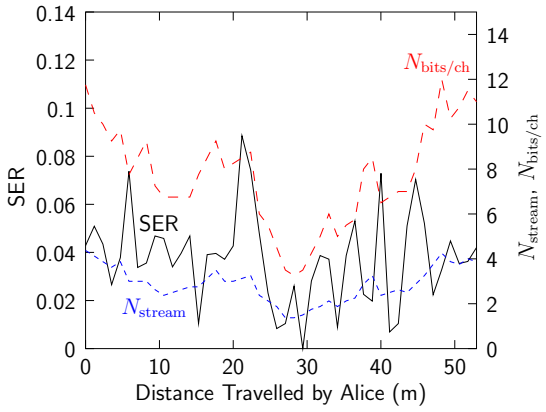

Fig. 10. Key generation statistics with movement for Location 1B for $N_1 = N_2 = 4$ antennas, 15 dB SNR, and target SER of 0.1

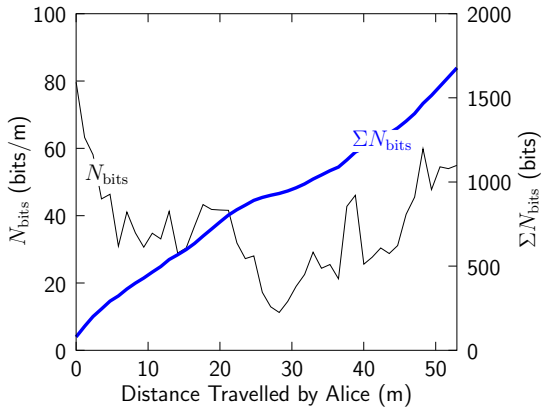

Fig. 11. Key generation rates and accumulated key bits of the key generation protocol for Location 1B

7) Alice and Bob quantize CSI streams based on pre-computed CQA maps, order chosen for each parallel stream, and the QM index [6] sent from Alice to Bob.
8) Appropriate symbol bits are added to keys.

Alice chooses n_d and order N in each block, which information is also known by Bob. This combined with error control coding would likely require some additional overhead in a real system. In our opinion, this key-generation protocol is the most obvious way of applying adaptive CQA to time-varying MIMO channels, and in future work we will consider refined protocols possibly providing higher performance.

Figure 10 shows variation of the protocol's key generation statistics with movement for LOS Location 1B averaged over the 8 runs on the path, assuming four antennas at Alice and Bob, 15 dB SNR, a single frequency bin, and maximum SER of 0.1. Here, $N_{\text{bits/ch}}$ is the number of bits generated per decimated (independent) CSI sample and N_{stream} is the number of spatial streams in use.

Figure 11 shows the key generation per distance, taking into account the number of decimated CSI samples per data block, where N_{bits} is the instantaneous rate of key bit generation (per meter) in each block, while ΣN_{bits} shows accumulation over the whole path. The result indicates that even for LOS channels, very long keys can be generated, allowing frequent key renewal. Since the result is for just one frequency bin, wideband CSI introduces another multiplication factor. Although not plotted, autocorrelation of key symbols for this case exhibit a maximum correlation of around 0.2 for nonzero lag, indicating good independence of key bits.

TABLE I
AVERAGE KEY GENERATION RATES

	bits/ch		bits/m	
	LOS	NLOS	LOS	NLOS
I_{K} (all)	22.9	43.9	95.7	302.8
(used)	13.4	29.7	56.7	205.3
Achieved Rate	7.3	16.9	31.1	116.5

Although seemingly high key generation rates are possible with the protocol, there is still a significant performance gap compared to the upper bound I_{K}. Table I lists the average key generation rates for all LOS and NLOS scenarios as well as I_{K}, where "all" and "used" indicate I_{K} for all parallel spatial channels and only those which had sufficient SNR for CQA, respectively. The table indicates ample room for improvement in CQ protocols since only 30-40% of the available I_{K} is captured.

VI. CONCLUSION

This paper explored the idea of secret key generation exploiting reciprocal MIMO channel fluctuations in an indoor environment, indicating that such methods are both secure and practical. LOS and NLOS measurements were performed for eavesdropper separations ranging from 10 cm to 2 m. The data was used to compute the actual number of available and secret key bits, where the effects of array size, eavesdropper separation and advantage, and covariance model were investigated. Even though for moderately sized arrays (4 elements or less) the number of available key bits is somewhat smaller than for i.i.d. channels, most bits are safe for reasonable eavesdropper separation, even with eavesdropper advantage. Although application of a sample key-generation protocol to the measured data indicated that very long keys can be generated in practice, only 30-40% of the available rate was captured, indicating room for future improvement.

ACKNOWLEDGMENT

This work was supported in part by a grant from the German Science Foundation (DFG) under the COIN program.

REFERENCES

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2515–2534, June 2008.
[2] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, pp. 3–6, Jan. 1995.
[3] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, pp. 3776–3784, Nov. 2005.
[4] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. 2008 IEEE Intl. Conf. Acoustics, Speech, and Signal Processing*, Las Vegas, NV, Mar. 31-Apr. 4, 2008, pp. 3013 – 3016.
[5] J. Wallace, C. Chen, and M. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *3rd European Conference on Antennas and Propagation (EuCAP '09)*, Berlin, Germany, Mar. 23-27, 2009, pp. 1499 – 1503.
[6] J. Wallace, "Secure physical layer key generation schemes: Performance and information theoretic limits," in *IEEE International Conference on Communications (ICC '09)*, Dresden, Germany, June 14-18, 2009, pp. 1–5.
[7] B. T. Maharaj, J. W. Wallace, M. A. Jensen, and L. P. Linde, "A low-cost open-hardware wideband multiple-input multiple-output (MIMO) wireless channel sounder," *IEEE Trans. Instrum. Meas.*, vol. 57, pp. 2283 – 2289, Oct. 2008.
[8] J. Wallace and B. Maharaj, "Accurate MIMO channel modeling: Correlation tensor vs. directional approaches," in *Proc. 2007 IEEE Global Telecomm. Conf.*, Washington, D.C., 26-30 Nov., 2007, pp. 3750–3754.