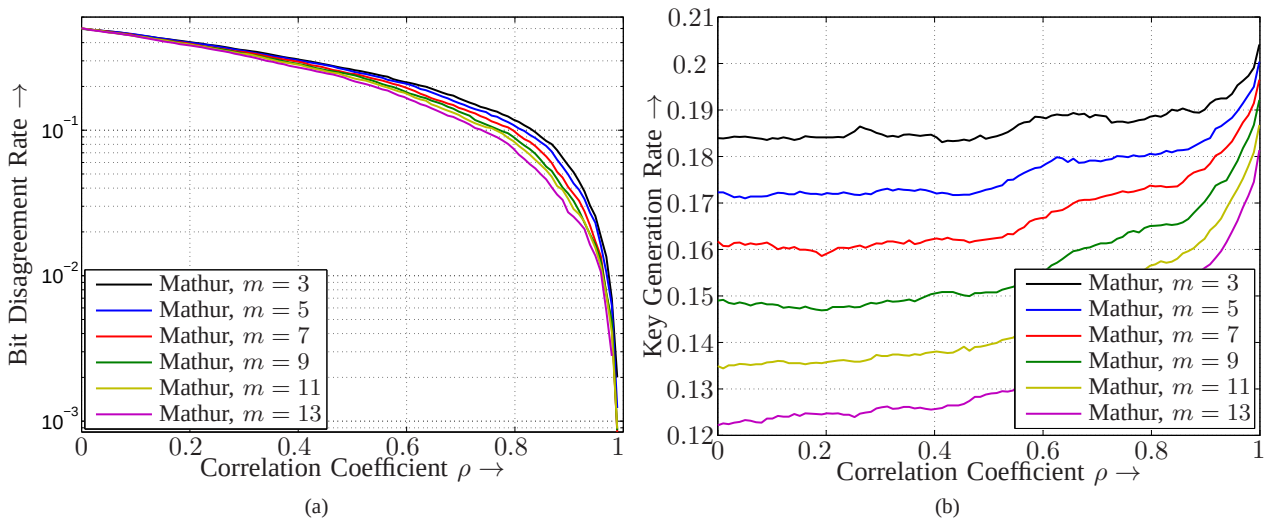

Fig. 6. For different protocol parameters of the quantization scheme proposed by Mathur et al. [3] we present the following simulation results: (a) Bit disagreement rate versus correlation coefficient. (b) Initial key generation rate versus correlation coefficient.

for extracting the resulting entropy, such as an universal hash function, is required. As a result, attackers possible eavesdropping-knowledge is considered.

V. Conclusion

We present a method for evaluating quantization schemes applied for secret key generation. It is shown that robust quantization schemes heavily affect the system's vulnerability to eavesdropping. Given the Pearson correlation coefficients of real world channel measurements (of Alice, Bob, and Eve), designers of PHY-based security system are able to verify and define security thresholds (e.g., the correction strength of an information reconciliation stage should not support an attackers purpose). The proposed evaluation method is also applicable to multicarrier systems and helps choosing an appropriate subcarrier spacing under consideration of the coherence bandwidth.

VI. Acknowledgement

This work is supported by the Federal Ministry for Education and Research (BMBF) within the project *Providing Physical Layer Security for the Internet of Things (Prophylaxe)* (16KIS0006 and 16KIS0010).

References

[1] P. Tuyls, B. Škorić, S. Stallinga, A. H. Akkermans, and W. Ophey, "Information-theoretic security analysis of physical uncloneable functions," in *Financial Cryptography and Data Security*, pp. 141–155, Springer, 2005.

[2] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *Wireless Communications, IEEE*, vol. 18, no. 2, pp. 66–74, 2011.

[3] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *MobiCom '08*, pp. 128–139, ACM, 2008.

[4] S. Jana, S. Premnath, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *MobiCom '09*, pp. 321–332, ACM, 2009.

[5] 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, pp. 17–30, Jan 2010.

[6] 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*, CCS '07, (New York, NY, USA), pp. 401–410, ACM, 2007.

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

[8] R. Ramachandran and S. Shetty, "Blind channel estimation based robust physical layer key generation in mimo networks," in *Circuits and Systems (ISCAS), Proceedings of 2010 IEEE International Symposium on*, pp. 2522–2525, May 2010.

[9] A. Ambekar, M. Hassan, and H. Schotten, "Improving channel reciprocity for effective key management systems," in *ISSSE 2012*, pp. 1–4, Oct 2012.

[10] A. Kitaura and H. Sasaoka, "A scheme of private key agreement based on the channel characteristics in OFDM land mobile radio," *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, vol. 88, no. 9, 2005.

[11] S. Yasukawa, H. Iwai, and H. Sasaoka, "Adaptive key generation in secret key agreement scheme based on the channel characteristics in ofdm," in *Information Theory and Its Applications, 2008. ISITA 2008. International Symposium on*, pp. 1–6, Dec 2008.

[12] W. C. Jakes, "Microwave mobile communications," 1975.

[13] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.

[14] J. Hershey, A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *Communications, IEEE Transactions on*, vol. 43, pp. 3–6, Jan 1995.

[15] J. Wallace, C. Chen, and M. Jensen, "Key generation exploiting mimo channel evolution: Algorithms and theoretical limits," in *EuCAP 2009*, pp. 1499–1503, March 2009.

[16] M. Tope and J. McEachen, "Unconditionally secure communications over fading channels," in *MILCOM 2001. IEEE*, vol. 1, pp. 54–58 vol.1, 2001.

[17] 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 Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, 2005.

[18] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, "A practical man-in-the-middle attack on signal-based key generation protocols," in *Computer Security–ESORICS 2012*, pp. 235–252, Springer, 2012.

[19] G. H. Golub and C. F. Van Loan, *Matrix computations*, vol. 3. JHU Press, 2012.