A USRP implementation of wiretap lattice codes

Lu, Jinlong; Harshan, J.; Oggier, Frédérique

2014

Lu, J., Harshan, J., & Oggier, F. (2014). A USRP implementation of wiretap lattice codes. 2014 IEEE Information Theory Workshop (ITW), 316-320.

https://hdl.handle.net/10356/79492

https://doi.org/10.1109/ITW.2014.6970845

A USRP Implementation of Wiretap Lattice Codes

Jinlong Lu, J. Harshan, Frédérique Oggier
Division of Mathematical Sciences
Nanyang Technological University, Singapore
Email: kerin_lu@ntu.edu.sg,jharshan@ntu.edu.sg,frederique@ntu.edu.sg

***Abstract*— A wiretap channel models a communication channel between a legitimate sender Alice and a legitimate receiver Bob in the presence of an eavesdropper Eve. Confidentiality between Alice and Bob is obtained using wiretap codes, which exploit the difference between the channels to Bob and to Eve. This paper discusses a first implementation of wiretap lattice codes using USRP (Universal Software Radio Peripheral), which focuses on the channel between Alice and Eve. Benefits of coset encoding for Eve's confusion are observed, using different lattice codes in small dimensions, and varying the position of the eavesdropper.**

I. Introduction

The wiretap channel is a discrete memoryless communication channel introduced by Wyner [1] to model transmission between two legitimate players Alice and Bob in the presence of an eavesdropper Eve. The main assumption is that the channel from Alice to Eve is "worse" than the channel from Alice to Bob, and randomness is used by Alice to increase Eve's confusion. Thus Wyner's seminal work is the root of two important ideas: (1) unconditional security (with Shannon's work [2]), or how to obtain security using randomness instead of computational complexity, and (2) physical layer security, which introduces security mechanisms together with coding, rather than on top of it. The wiretap channel model was extended to additive white Gaussian noise (AWGN) channels in [3]. Recent years have witnessed a renewed interest in wiretap channels, especially in the context of wireless communications. Information theoretical results (e.g. in terms of achievable rates or capacity) are summarized in [4], while standard explicit wiretap coding strategies are compiled in [5].

A related line of research is addressing the practicality of physical layer security schemes through experiments, e.g., wireless one-time pads have been proposed and experimentally tested in [6], while wireless key exchanges have been studied, and also experimented using software radios in [7]. Finally, physical layer security in the presence of an eavesdropper is the main product proposed by whisper communication [8].

In this paper, we start to address the practicality of wiretap lattice codes, as proposed in [9] for the Gaussian channel, or [10] for fading channels. Both works rely heavily on (1) lattice coset encoding and its effect on Eve's probability of correctly decoding, and (2) on assumptions on Eve's channel, which is actually the most critical parameter which enables physical layer security. This motivates to prototype a wiretap testbed, which allows measurements on Eve's channel, to evaluate the confidentiality brought by wiretap lattice coding.

In this paper, we report the progress made towards the setting of a wiretap lattice testbed, using USRP (Universal Software Radio Peripheral). We focus on the channel between Alice and Eve, and as a first step, we test the key component of wiretap lattice coding, that is, lattice coset encoding, recalled in Section II. We compare it with traditional encoding, using lattices in different small dimensions. We provide details of the experiments set up in Section III. Experiment results, provided in Section IV, confirm the theory so far, namely: coded transmissions outperform uncoded ones, the code performance improves with the dimension, and coset encoding does provide confusion, for the different USRP positions considered.

II. Wiretap Lattice Codes

A *lattice* Λ of dimension L is a discrete set of points in $\mathbb{R}^L$, conveniently described by a generator matrix M as $\Lambda = \{\mathbf{x} = \lambda M | \lambda \in \mathbb{Z}^L\}$, where M is an $L \times L$ real matrix, whose L rows form a basis of Λ. A *lattice constellation* is obtained by carving a finite subset of points of Λ. Lattice constellations are commonly used for transmission over Additive White Gaussian Noise (AWGN) channels and fading channels.

A. Wiretap Channel Model

A wiretap channel consists of a broadcast channel, where Alice, a legitimate sender, transmits to both a legitimate receiver Bob and an eavesdropper Eve through channels typically of the same nature. In our case, we consider block fading channels, that is transmission occurs over a frame length of n, and we suppose a coherence time of n, namely

$$\begin{aligned} \mathbf{Y} &= h_B\mathbf{X} + \mathbf{Z}_B \in \mathbb{C}^n \\ \mathbf{Z} &= h_E\mathbf{X} + \mathbf{Z}_E \in \mathbb{C}^n \end{aligned} \tag{1}$$

where the subscripts B and E refers to Bob and Eve respectively. The coefficients h_B and h_E are complex Gaussian random variables representing respectively the channel gain to Bob and Eve, while the coefficients of $\mathbf{Z}_B$ and $\mathbf{Z}_E$ are i.i.d zero mean complex Gaussian random variables.

To transmit lattice points of dimension L, we suppose that L divides n, and (1) can be seen as n/L instances of

$$\begin{aligned} \mathbf{y} &= h_B\mathbf{x} + \mathbf{z}_B \in \mathbb{C}^L \\ \mathbf{z} &= h_E\mathbf{x} + \mathbf{z}_E \in \mathbb{C}^L \end{aligned} \tag{2}$$

with h_B, h_E as in (1). When $h_B = h_E = 1$, we get usual AWGN channels.

They key idea behind wiretap coding is to introduce randomness at the transmitter, such that it increases the confusion at the eavesdropper. This is concretely done via coset encoding, namely: a message to be sent by Alice is not mapped to

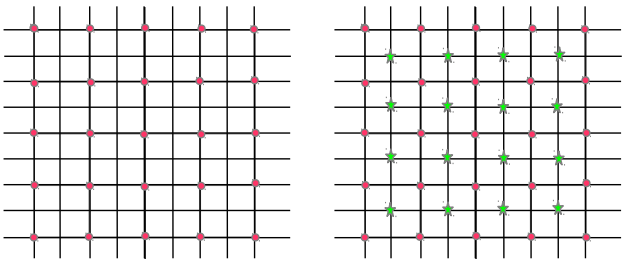

Fig. 1. Coset Encoding: on the left, the lattice $\mathbb{Z}^2$ and its sublattice $2\mathbb{Z}^2$. On the right, the sublattice $2\mathbb{Z}^2$ (dots) and its coset $2\mathbb{Z}^2 + (1,1)$ (stars).

one codeword, it is mapped to a coset, after which a random point within the coset is actually transmitted. To perform lattice coset encoding, consider two nested lattices $\Lambda_E \subset \Lambda_B$, where Λ_B is the lattice chosen for the transmission between Alice and Bob. A message to be sent is then mapped to a coset of Λ_E, and a random point $\mathbf{x}$ within this coset is transmitted over (2). This is illustrated in Figure 1. The lattice $\Lambda_B = \mathbb{Z}^2$ can be partitioned into 4 cosets of $\Lambda_E = 2\mathbb{Z}^2$, namely $2\mathbb{Z}^2 + (0,0), 2\mathbb{Z}^2 + (0,1), 2\mathbb{Z}^2 + (1,0), 2\mathbb{Z}^2 + (1,1)$. Thus a two bit message can be sent (the two bits are used to label each of the 4 cosets).

B. Construction A

A classical way to obtain coset encoding of lattices is via the so-called Construction A of lattices from linear codes [11]. Let $\rho : \mathbb{Z}^L \to \mathbb{F}_2^L$ denote the componentwise reduction modulo 2 ($\mathbb{F}_2$ denotes the binary field $\{0,1\}$), which maps an integer vector $\mathbf{x}$ to a binary vector $\mathbf{x} \pmod 2$. Let $C \subset \mathbb{F}_2^L$ be a linear (L,k) code, that is a code of dimension k and length L. Then $\rho^{-1}(C) = 2\mathbb{Z}^L + C$ is a lattice, we use it for Λ_B while $\Lambda_E = 2\mathbb{Z}^L$, and codewords from C are coset representatives.

The example of Figure 1 in fact fits this setting of Construction A. Indeed, take C to be the universe code of length 2, that is $C = \{(0,0),(0,1),(0,1),(1,1)\}$. Then

$$\mathbb{Z}^2 = 2\mathbb{Z}^2 + C$$

that is $\mathbb{Z}^2 = (2\mathbb{Z}^2 + (0,0)) \cup (2\mathbb{Z}^2 + (0,1)) \cup (2\mathbb{Z}^2 + (1,0)) \cup (2\mathbb{Z}^2 + (1,1))$.

Another example is the 2-dimensional checkerboard lattice D_2, which can be constructed using the 2-dimensional repetition code $C = \{(0,0),(1,1)\}$, namely

$$D_2 = 2\mathbb{Z}^2 + C = (2\mathbb{Z}^2 + (0,0)) \cup (2\mathbb{Z}^2 + (1,1)). \quad (3)$$

The 4-dimensional Schäffli lattice D_4 is also obtained via Construction A as

$$D_4 = 2\mathbb{Z}^4 + (4,3,2) \quad (4)$$

where $(4,3,2)$ denotes the binary parity check code of length 4, dimension 3, and minimum distance 2 (which is also the Reed-Muller code RM(1,2)).

The lattice E_8 is (with the normalization $\frac{1}{\sqrt{2}}\rho^{-1}(C)$)

$$\sqrt{2}E_8 = 2\mathbb{Z}^8 + (8,4,4), \quad (5)$$

using the Reed-Muller code of length 8 and dimension 4.

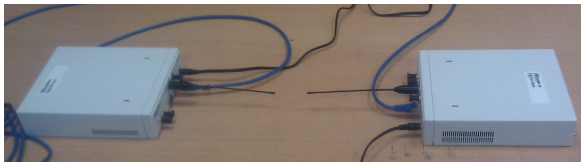

Fig. 2. USRP Testbed

III. Experiment Setup: USRP Testbed

We use NI USRP-2920 devices (with Windows 7, Matlab R2013b and its USRP radio support package) to implement a testbed, which focuses at the moment on Eve's channel. Figure 2 shows the configuration of the USRP testbed. The experiments are carried out by placing the USRP corresponding to Eve at different positions. We fix the transmitter and receiver gains (18 and 31 dB, respectively) and then vary the positions to capture different signal-to-noise ratio (SNR) values. The center frequency of the two devices is preset to 2.42E+09 with LO offset of 0 Hz.

A. Encoding and Transmission

Communication between the two USRP devices takes place over a sequence of frames where each frame constitutes $n = 100$ complex symbols in baseband representation. Among the 100 symbols, the first 13 symbols are QPSK modulated pilot symbols which are constructed by identically placing a 13-length binary Barker code sequence [12] on the in-phase and quadrature components. These pilot symbols are essential for the timing recovery and frame synchronization operations at the receiver. The rest of the 87 locations in the frame are allocated for data transmission. For the uncoded scheme, 87 binary symbols (from the set $\{0,1\}$) are embedded into the frame, while for the coded scheme, these locations are loaded with uniformly chosen codewords from an underlying lattice code (carved from Λ_B, with $\Lambda_B \in \{D_2, D_4, E_8\}$). For the coded schemes, since the codewords do not fill the 87 symbols completely, the remainder locations are loaded with dummy symbols. Further, note that the codewords of lattice codes in $\mathbb{Z}, D_2, D_4$ and E_8 have components with only non-negative real values. Hence, for implementation purpose, the symbols are appropriately shifted around the origin to reduce the average transmit power.

Our method to transmit the lattice codewords of $\mathbb{Z}$, D_2, D_4 and E_8 is as follows. Irrespectively of whether the strategy is conventional encoding or coset encoding, for any $\mathbf{x} \in \{0,1,\ldots,M-1\}^L$, where L is the dimension of the lattice, the transmitted codeword is of the form

$$\mathbf{x}_t = \frac{e^{-i\frac{\pi}{4}}}{\sqrt{E_{avg}}}\left(\mathbf{x} - \frac{M-1}{2}\right) \in \mathbb{C}^L, \quad (6)$$

where E_{avg} is the average energy of the shifted constellation $\{-\frac{M-1}{2}, -\frac{M-1}{2}+1, \ldots, \frac{M-1}{2}-1, \frac{M-1}{2}\}$. Using the scale and the shift operation in (6), each component of $\mathbf{x}_t$ takes value from a complex constellation with unit average energy. For the experiment, we use the carrier frequency compensation and

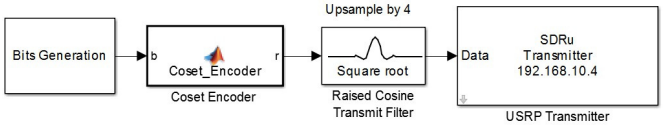

Fig. 3. Transmitter side baseband operations.

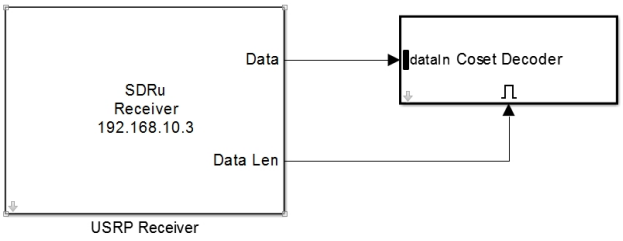

Fig. 4. Receiver block

timing recovery blocks that are tailor-made for QPSK signal sets [14]. Hence, to facilitate this reuse, the real lattice points are rotated by -45 degrees.

Once a frame constituting Barker code symbols and lattice codewords $\{\mathbf{x}_t\}$ is generated, it is subsequently upsampled by 4 and then passed through a square-root raised cosine filter (with roll-off factor 0.5) for pulse shaping purpose (see Fig. 3 for the transmitter side baseband operations). Finally, the filtered samples are forwarded to the USRP device (with interpolation factor 500) for passband transmission.

B. Reception and Decoding

At the receiver, the passband signal is down-converted and appropriately sampled by the USRP hardware. Then these samples are forwarded to the simulink block (with decimation factor 500) for baseband processing (see Fig. 4 and 5 for the receiver side baseband operations).

A total of 4000 samples (equivalent to 10 received frames) are processed batch-wise in order to facilitate frame synchronization and timing recovery operations. For accurate synchronization, the received samples are passed through an Automatic Gain Control (AGC) block before it is filtered using a square-root raised cosine receive filter (with identical parameters as that of the transmit filter). Subsequently, the filtered output is forwarded to the frequency compensation and timing recovery blocks. In the timing recovery block, the Barker code sequence is independently generated, using which the beginning of the received frames is detected through cross-correlation operations. Finally, the *aligned* frames are forwarded to the data decoding block (either conventional or

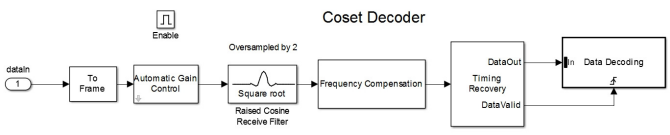

Fig. 5. Receiver side baseband operations

coset), which assuming the frame synchronization is accurate, estimates the channel gain using the Barker code symbols on the first 13 locations. Since the AGC gain values may vary across successive frames, we use the estimated channel gain locally within a frame but not across frames. The received lattice codewords by Eve (see (2)) of the form $\mathbf{y} = h_E\mathbf{x}+\mathbf{z}_E \in \mathbb{C}^L$ are extracted from the frame to carry out the decoding process. Here, the scalar h_E is the complex channel gain (for Eve) and $L \in \{1, 2, 4, 8\}$ is the block length of the lattice code. Using $\mathbf{y}$ and $\hat{h}_E$ (the estimated channel gain), the most likely transmitted lattice point is computed using the Maximum Likelihood (ML) decoder as

$$\hat{\mathbf{x}}_{int} = \arg\min_{\mathbf{x}\in\mathcal{C}} ||\mathbf{y} - \hat{h}_E \frac{e^{-i\frac{\pi}{4}}}{\sqrt{E_{avg}}}(\mathbf{x} - c)||^2, \qquad (7)$$

where the offset $c = \frac{M-1}{2}$ when the underlying constellation is $\{0, 1, \ldots, M-1\}$. In our experiments, since the codes under consideration have short length and are also small in size, we perform brute-force ML decoding to recover the information bits. However, for codes in larger dimension, sphere decoder [13] can be used to speed up the decoding process. For conventional encoding, the code $\mathcal{C}$ is a subset of $\{0, 1\}^L$, and hence, the intermediate latice codeword $\hat{\mathbf{x}}_{int}$ in (7) is the end result, i.e., $\hat{\mathbf{x}} = \hat{\mathbf{x}}_{int}$. However, for coset encoding, the code $\mathcal{C}$ is a subset of either $\{0, 1, 2, 3\}^L$ or $\{0, 1, 2, \ldots, 7\}^L$, and hence, the decoding operation is continued as $\hat{\mathbf{x}} = \hat{\mathbf{x}}_{int} \bmod 2$, to obtain the end result. We repeat this procedure for all the codewords in the frame. A frame is said to be in error if at least one codeword in that frame is incorrectly decoded. To quantify the error performance of conventional and coset encoding methods, we repeat the experiment for 10000 frames to compute the frame error rate. In the following section, we report some observations and results from these experiments.

IV. Experiment Results and Analysis

For the experiments, we fix the transmitter USRP position and then vary the receiver USRP position at 4 different locations, referred to as Placement 1, 2, 3 and 4 (in the order of increasing distance). In Fig. 6, 7 and 8, we plot the received symbols $\{r\}$ (available at the input of the data decoding block) when symbols from the constellation $\{0, 1\}, \{0, 1, 2, 3\}$ and $\{0, 1, 2, \ldots, 7\}$ are transmitted. Fig. 6 highlights that for Placement 1, the SNR at Eve is too high to cause degradation in the error performance with both conventional encoding and coset encoding with 1 bit confusion. However, for the same placement, coset encoding with 2 bits confusion can potentially introduce errors since the decision regions overlap. Similarly, for other placements (which corresponds to lower SNR values), it can be seen that coset encoding can potentially result in more errors for Eve.

For the four placements, we compute the corresponding baseband SNR values by transmitting unit energy training sequences. The received symbols are used to compute the SNR as $\frac{\mathbb{E}[|\hat{h}_E|^2]}{\mathbb{E}[|r|^2]-\mathbb{E}[|\hat{h}_E|^2]}$, where $\mathbb{E}[|\hat{h}_E|^2]$ indicates the average signal power and $\mathbb{E}[|r|^2]-\mathbb{E}[|\hat{h}_E|^2]$ is indicative of the average

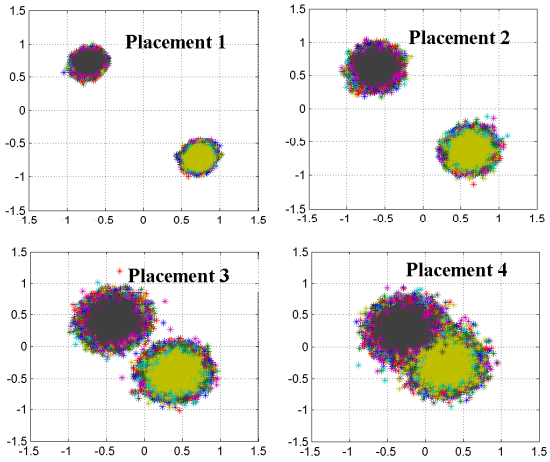

Fig. 6. The cloud of received points at different placements for conventional coding. The underlying constellation is $\{0, 1\}$.

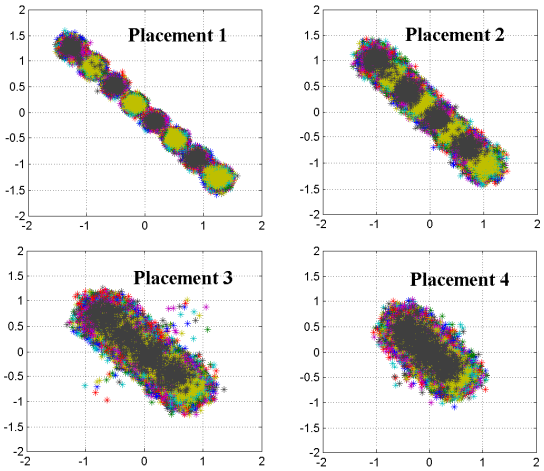

Fig. 8. The cloud of received points at different placements for coset encoding with 2 bits confusion. The underlying constellation is $\{0, 1, 2, \ldots, 7\}$.

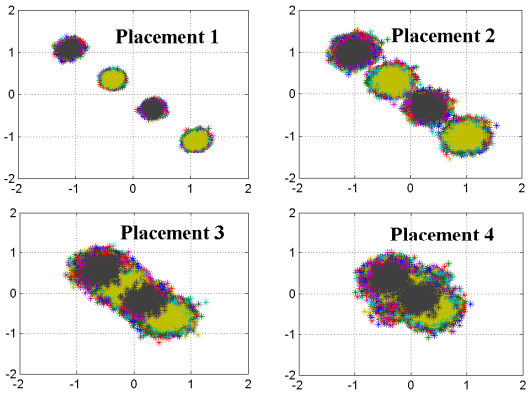

Fig. 7. The cloud of received points at different placements for coset encoding with 1 bit confusion. The underlying constellation is $\{0, 1, 2, 3\}$.

noise power. The measured SNR values at different frames are plotted in Fig. 9 (see first figure from top left clock-wise) which shows that the four placements correspond to the average SNR values of $20.6, 15, 9$ and 4.5 dB, respectively.

Before addressing the advantages of coset encoding for wiretap channels, we first present the experiment results on the error performance of conventional coding of lattice codes in $\mathbb{Z}, D_2, D_4$ and E_8. Since the lattice codes are over binary alphabet, the SNR values at Placement 1, 2, and 3 are too high to result in non-zero values of error probability. Hence, we repeat the experiments at two new locations for receiver USRP (with sufficiently low SNR) and then obtain the results. In Fig. 9 (see 2nd figure from top left clock-wise), we present the error performance of conventional encoding of lattice codes in different dimensions. The figure shows that the frames corresponding to lattices codes from E_8 are most resilient to channel errors since the underlying code is stronger than the other codes in smaller dimension.

We now present the error performance of lattice codes with coset encoding/decoding and compare them with that of conventional encoding/decoding. For conventional encoding, the transmitted symbols are binary values, whereas for coset encoding, the transmitted symbols take either 4 or 8 values depending on the number of bits for confusion, namely: (1) Dimension 1: we use the lattice $\mathbb{Z} = (2\mathbb{Z}) \cup (2\mathbb{Z} + 1)$, and either $2\{0, 1\} + \{0, 1\}$ or $2\{0, 1, 2, 3\} + \{0, 1\}$ for 1 bit of information, and 1 or 2 bits for confusion, respectively.

(2) Dimension 2: we use the checkerboard lattice D_2 constructed in (3), and either $2\{0, 1\}^2 + \{(0, 0), (1, 1)\}$ or $2\{0, 1, 2, 3\}^2 + \{(0, 0), (1, 1)\}$ for 1 bit of information, and 1 or 2 bits for confusion, respectively.

(3) Dimension 4: we use either $2\{0, 1\}^4 + (4, 3, 2)$ or $2\{0, 1, 2, 3\}^4 + (4, 3, 2)$, for 3 bits of information, corresponding to the Schäffli lattice D_4, given in (4), using a (4,3,2) single parity check code.

(4) Dimension 8: we use either $2\{0, 1\}^8 + (8, 4, 4)$ or $2\{0, 1, 2, 3\}^8 + (8, 4, 4)$, for 4 bits of information, for the lattice E_8 given in (5), using a (8,4,4) Reed-Muller code.

In Fig. 9 (see 3rd to 6th figure from top left clock-wise), we plot the frame error rate for both coset encoding and conventional encoding. The plots show that with 2 bits for confusion, coset encoding can degrade the performance at Placements 2, 3 and 4. However, the impact of coset encoding depends on the location of Eve (or the underlying SNR). For instance, at Placement 1, the SNR is too high for coset encoding with 1 bit to introduce confusion with all the three codes. In general, using more confusion bits (or larger constellations) can degrade the performance at Eve, however, the size of the expanded constellation must be chosen such that the SNR at Bob permits all the frames to be decoded without errors.

V. On-going and Future Work

This paper presented preliminary settings and results obtained from a USRP testbed meant to test wiretap lattice codes in wireless environments. There is a long list of on-going and future work to improve the current testbed, and in turn potentially improve the known wiretap lattice codes, including:

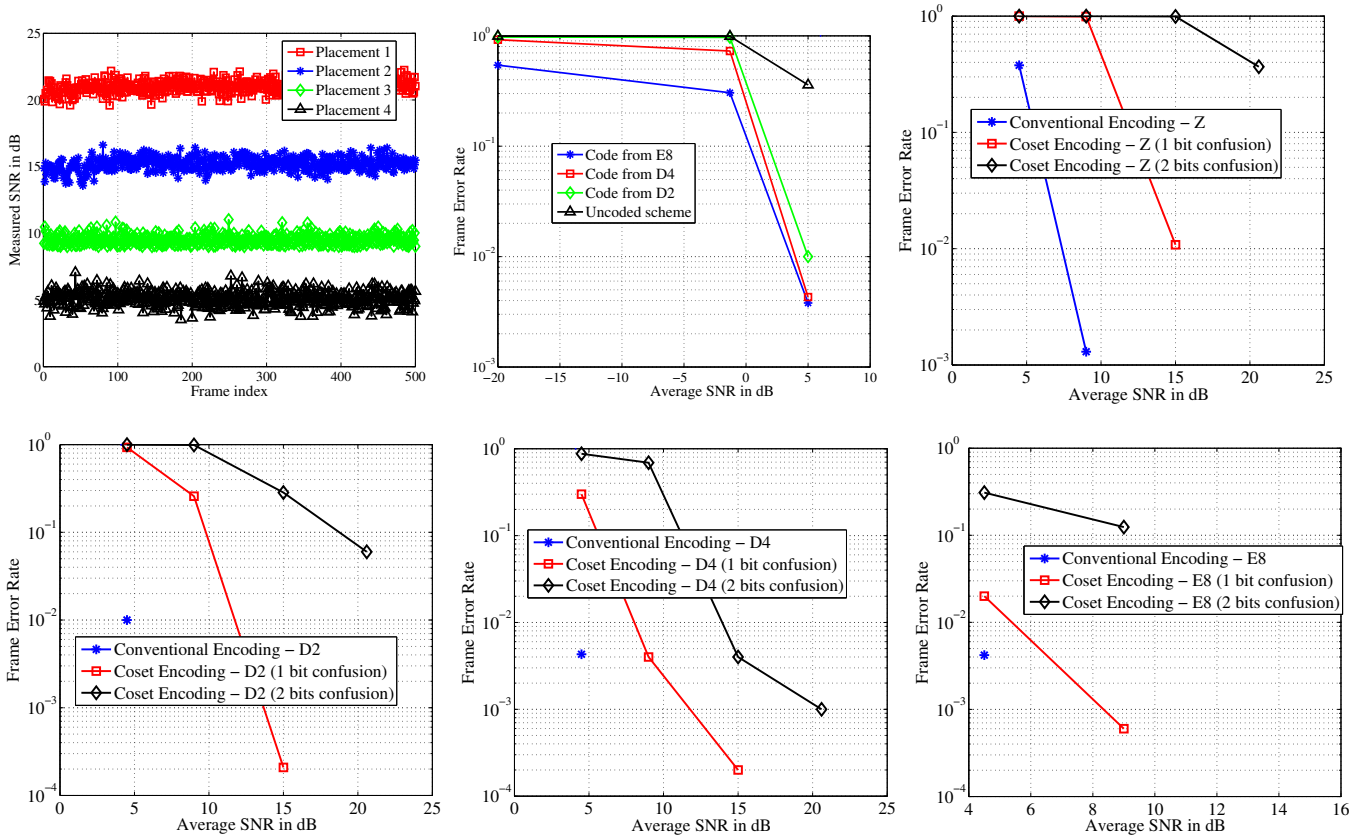

Fig. 9. From top left, clock-wise: (1) Measured basband SNR values on different frames at four different placements of the receiver USRP. (2) Error performance of various lattice codes on the USRP testbed. (3)-(6) Comparison between conventional and coset encoding for lattice codes with 1 bit and 2 bits for confusion. The average SNR values correspond to Placement 1, 2, 3 and 4. The frame error rates are marked only for non-zero values.

(1) Use lattices in higher dimensions, since the confidentiality is expected to increase with the dimension.

(2) Improve the lattice decoder algorithm to be able to handle higher dimensional lattices.

(3) Try experiments with and without knowledge of Eve's channel: (1) with knowledge of Eve's channel, better confidentiality is expected to be obtained, (2) without Eve's channel knowledge, experiment with a hierarchical labeling of the information bits as suggested theoretically.

ACKNOWLEDGMENT

The research of J. Lu and F. Oggier for this work is supported by the Singapore National Research Foundation under Research Grant NRF-RF2009-07. The research of J. Harshan is supported by the MoE Tier-2 grant eCODE: Erasure Codes for Datacenter Environments.

The authors would like to thank Prof. Matthieu Bloch for his advice on software defined radio, Prof. Guan Yong Liang and Prof. Ting See Ho for showing and explaining their own lab settings and experiments with software defined radio, and Liu Yun Xiang and Francois Quitin for their availability to answer questions.

REFERENCES

[1] A.D. Wyner, "The wire-tap channel," *Bell. Syst. Tech. Journal*, vol. 54, October 1975.

[2] C. Shannon, "Communication Theory of Secrecy Systems", *Bell System Technical Journal*, vol. 28(4), 1949.

[3] S.K. Leung, M.E. Hellman, "The Gaussian Wiretap", *IEEE Transactions on Information Theory*, vol 24, no 4, July 1978.

[4] Y. Liang, H.V. Poor and S. Shamai, "Information Theoretic Security," *Foundations and Trends in Communications and Information Theory*, Vol. 5, Issue 4-5, 2009, Now Publishers.

[5] F. Lin and F. Oggier, "Coding for wiretap channels", in Physical Layer Security in Wireless Communications, *Auerbach Publications*, CRC Press, Taylor & Francis Group.

[6] `http://www.cst.uwaterloo.ca/unconditionalSecurity.php`

[7] A. J. Pierrot, R. A. Chou, M. R. Bloch, "The Effect of Eavesdroppers Statistics in Experimental Wireless Secret Key Generation", `http://arxiv.org/abs/1312.3304`

[8] `http://www.whispercomm.com/`

[9] F. Oggier, P. Solé and J.-C. Belfiore, "Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis", `http://arxiv.org/pdf/1103.4086.pdf`

[10] S.S. Ong, F. Oggier, "Wiretap Lattice Codes from Number Fields with no Small Norm Elements, Designs, Codes and Cryptography", vol. 73, no. 2, 2014.

[11] J.H. Conway, N.J.A. Sloane,"Sphere packings, Lattices and Groups," Third edition, Springer-Verlag, New York, 1998.

[12] R. H. Barker "Group Synchronizing of Binary Digital Sequences," *Communication Theory*. London: Butterworth. pp. 273287, 1953.

[13] E. Viterbo and J. Boutros, "A Universal Lattice Code Decoder for Fading Channels", *IEEE Transactions on Information Theory*, vol. 45, n. 5, pp. 1639-1642, July 1999.

[14] `http://www.mathworks.com/help/shared_sdr_sdru/examples/`