Intelligent Poly Key
Zero Overhead Encode for Secure Communications

Gwain Bayley
IPK Technologies
San Diego, CA, USA
gwain.bayley@ipktek.com

William Spazante
IPK Technologies
San Diego, CA, USA
billy.spazante@ipktek.com

Brennan Eveland
TM Technologies
San Diego, CA, USA
beveland@tmtechnologies.com

***Abstract*—Intelligent Poly Key (IPK) Zero Overhead Encode (ZOE) is a novel and secure method of encoding the data transmission between nodes on wireless and wired networks. The throughput energy per bit needed for the link is decreased by the gain of the forward error correcting code while the physical layer data is secured by constantly changing codes. This provides physical layer security because the transmitted symbols cannot be decoded from the noise without knowing a priori the current chosen Quasi-Cyclic Low Density Parity Check prototype matrix. The method was used to improve security and communications reliability with a Transpositional Modulation (TM) enabled system providing obfuscated communications and greater than 50% increase in data throughput.**

Keywords—security; communications; encryption; encoding; modulation; reliability.

I. Introduction

Current state of the art communications uses Quasi-Cyclic Low Density Parity Check (QC-LDPC) codes using Proto Graph based code construction to create the Generator Matrix. The main reason for using these codes is the efficiency of encoding and the relative efficiency of decoding and the relative efficiency of a decoder implementation using belief-propagation-based decoding algorithms. The codes, however, are static for a particular data rate and Physical Layer modulation type. We propose generating codes using the same type of geometry but using a key schedule to drive the exact proto graph used and synchronizing the transmitter and receiver using the Intelligent Poly Key (IPK) protocol [1]. We can show that these methods produce codes that are as efficient as those in use by any system but with the added benefit of physical layer symbol security.

II. Background

Robert Gallager [2] first proposed Low Density Parity Check codes in the 1960s but the hardware to implement the iterative decoder was not practically implementable at that time. They are a class of linear block codes with sparse parity check matrices. The decoding algorithms work very well using iterative belief-propagation and inference algorithms like those used in AI.

To aid in the physical construction of these decoder inference networks in silicon, the structure of the sparse parity check matrix uses simple sub-matrices of row-column weight 1 based on pseudo-random cyclic variations of identity matrices. These are called non-overlapping permutation matrices. These codes are derived from finite geometry and combinatorial design and are called Quasi-Cyclic LDPC codes or QC-LDPC.

An example of the rate ¾ IEEE 802.11 standard QC-LDPC matrix prototype [3] is the following matrix made of 144 sub-matrices listed in the following proto graph:

16	17	22	24	9	3	14	-1	4	2	7	-1	26	-1	2	-1	21	-1	1	0	-1	-1	-1	-1
25	12	12	3	3	26	6	21	-1	15	22	-1	15	-1	4	-1	-1	16	-1	0	0	-1	-1	-1
25	18	26	16	22	23	9	-1	0	-1	4	-1	4	-1	8	23	11	-1	-1	-1	0	0	-1	-1
9	7	0	1	17	-1	-1	7	3	-1	3	23	-1	16	-1	-1	21	-1	0	-1	-1	0	0	-1
24	5	26	7	1	-1	-1	15	24	15	-1	8	-1	13	-1	13	-1	11	-1	-1	-1	-1	0	0
2	2	19	14	24	1	15	19	-1	21	-1	2	-1	24	-1	3	-1	2	1	-1	-1	-1	-1	0

Fig. 1. Matrix prototypes for codeword block length n=648 bits R=3/4

Each of the entries in the proto graph represents a 27x27 bit sub-matrix. The numerical entry indicates the amount of cyclical shift of the identity sub-matrix. The special case of sub-matrix value -1 is an all-zeroes sub-matrix and has no effect on the parity calculations.

III. IPK Operation

IPK generates a custom proto graph using a key schedule to drive the exact LDPC coding used and synchronizes the transmitter and receiver using the IPK protocol.

The codes are all constructed with the same geometry as standard 3GPP and IEEE LDPC prototype codes but with pseudo-randomized quasi-cyclic submatrices.

For the IEE802.11 proto graph above there are thus 27 possible variants of each active parity sub-matrix (of which there are 90) that contribute to parity and therefore 27^{90} possible Proto-Graphs using the same geometry. This is a search space of 6.6×10^{128} which is the equivalent of synchronous encryption with a 428-bit key.

IV. Test Methodology

The models used are implemented in MATLAB using standard models and custom encoders and decoders.

Further testing is done using Keysight Technologies WAVEJUDGE waveform generation and analysis tools.

Further testing is done using a custom FPGA implementation with a Software Defined Radio (SDR).

V. Architecture

The block diagram of the architecture of the IEEE802.11 test models is shown in the diagram below, showing standard Orthogonal Frequency Division Multiplexing (OFDM) with Quadrature Amplitude Modulation (QAM) of various orders from Quadrature Phase Shift Keying (QPSK) to QAM256.

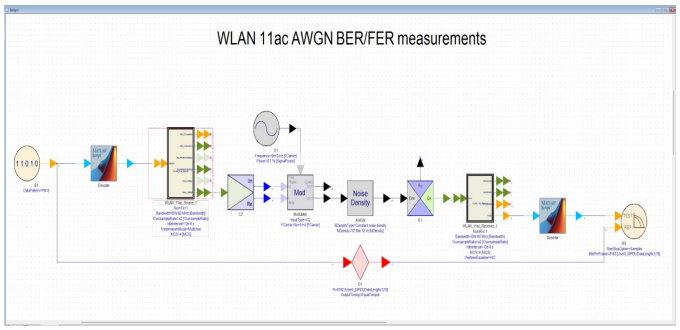


Fig. 2. Block diagram of the IEEE 802.11 test architecture.

The block diagram of the architecture of the 3GPP and TM test FPGA hardware architecture is shown in the diagram below, showing standard Orthogonal Frequency Division Multiplexing (OFDM) with Quadrature Amplitude Modulation (QAM) of various orders from Quadrature Phase Shift Keying (QPSK) to QAM256.

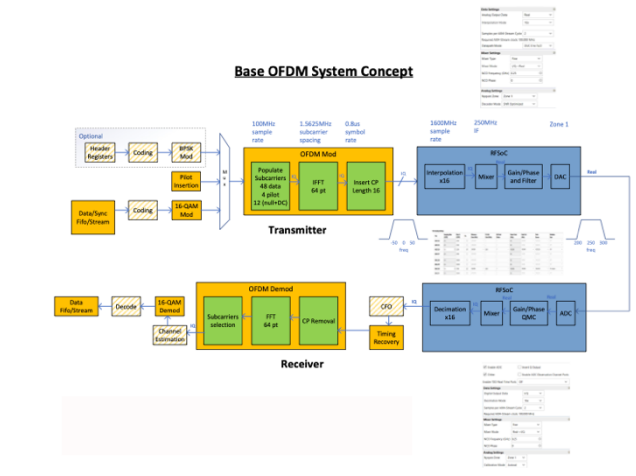


Fig. 3. Block diagram of the 3GPP OFDM test architecture.

VI. IPK Operation

IPK generates custom H (parity) and related G (generator) matrices in the Coding and Decoding blocks of the communications architecture above, using a key schedule to drive the exact LDPC coding used and synchronizing the transmitter and receiver using the IPK protocol.

Results are obtained in AWGN, Rayleigh, and Rician Fading channel models at different speeds and Doppler shifts.

VII. Further Testing

Proof-of-concept testing was recently performed with a Transpositional Modulation (TM) enabled hardware system. TM is a method for increasing the data rate of existing communications systems by transparently adding channels to underused areas of the RF spectrum [4]. For example, digital pre-distortion linearization techniques are used dynamically to make extra spectrum available by reducing intermodulation distortion. Also, self-interference cancellation techniques can be used to provide extra spectral headroom both in-band and in side channels. TM also relies on strong coding such as IPK Zero Overhead Encode to enhance the extra communications channels in congested RF environments and provide obfuscated communications:

1) *Waveform Configuration:*
   a) *50 MHz OFDM - 195.3125 kHz Subcarrier Spacing*
   b) *QPSK signal - 29.88 MHz Occupied Bandwidth*
   c) *16-QAM TM Signal - 10.16 MHz TM Bandwidth*
   d) *TM signal levels set 10 dB blow legacy signal*

2) *Hardware Testing Configuration:*
   a) *Xilinx Zynq UltraScale+*
   b) *RFSoC ZCU216*
   c) *Analog Devices AD9361 Transceiver*

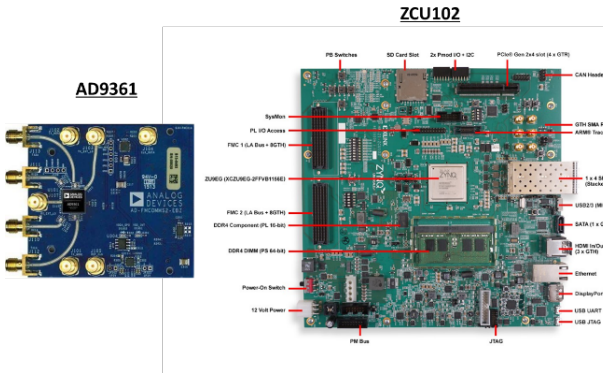


Fig. 4. Hardware testing configuration including Xilinx ZCU216 Kit.

VIII. Results

The performance of uncoded OFDM QAM at various rates is compared to a family of IPK Secure Codes as well as standard 802.11 LDPC Codes and standard 3GPP LDPC codes.

IX. IEEE 802.11 Codes

The first results are a MATLAB results plot of 802.11 LDPC standard codes vs. IPK secure codes and uncoded QAM256 OFDM performance.

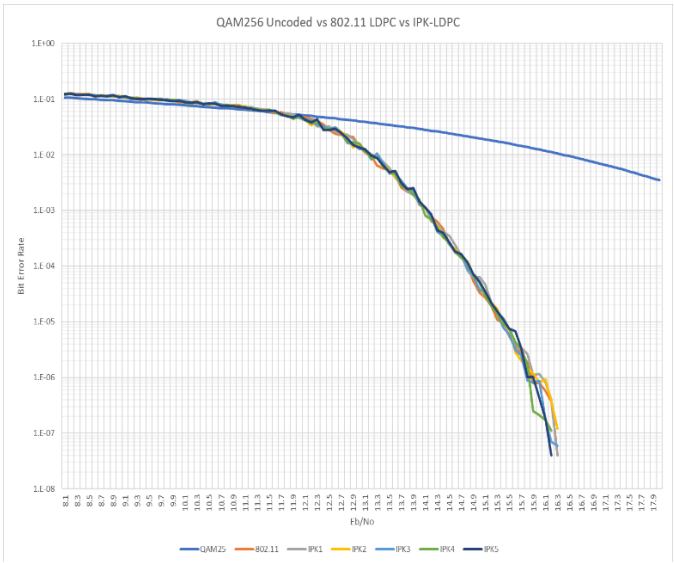


Fig. 5. 802.11 QAM256 performance vs. a family of IPK Secure Codes.

They family of curves show only fractions of a dB difference in performance across the family of 802.11 codes for a given bit error rate (BER). The performance is tested from +8 to +18 dB Signal to Noise Ratio (SNR).

X. 3GPP LDPC Codes

We show an Excel plot of the results from tests of 3GPP standard codes vs. IPK secure codes and uncoded QAM16 OFDM.

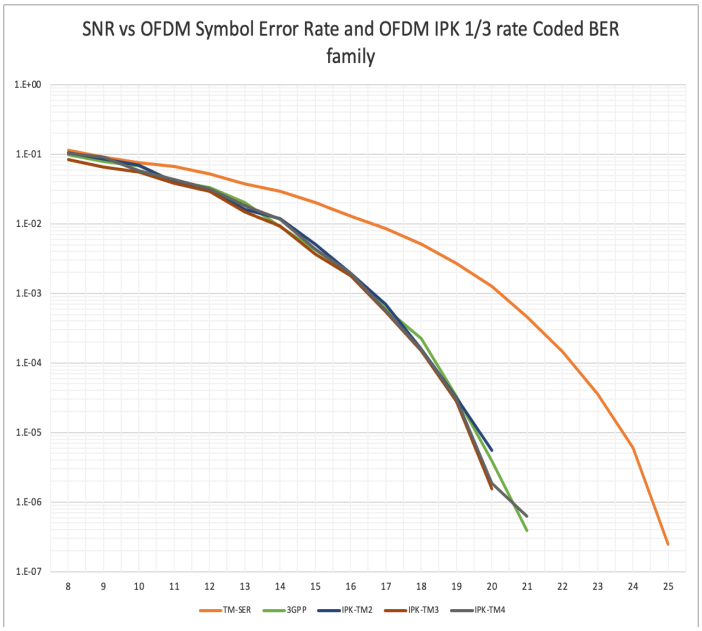


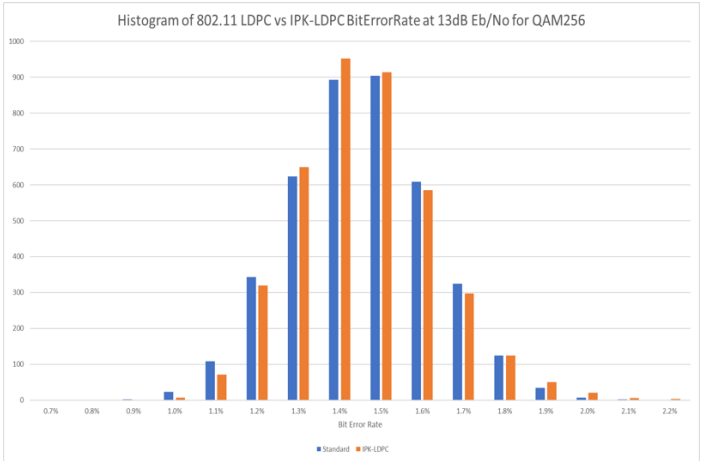
Fig. 6. 3GPP OFDM QAM16 performance and a family of IPK Secure Codes.

They family of curves show only fractions of a dB difference in performance across the family of 3GPP codes for a given bit error rate (BER). The performance is tested from +8 to +25 dB Signal to Noise Ratio (SNR).

XI. Histogram of Code Results

The target BER for a modern communication system is a balance between power and performance. These are expressed as the ratio of Energy per bit and Noise (Eb/No) and the resulting Bit Error Rate (BER).

A good target for this balance is between 1% and 2% BER. We thus compare the Histogram of the various simulated values of BER for a fixed Eb/No of 13dB for QAM256 modulation for the Standard vs. thousands of pseudo-random IPK-LDPC tables.



We see that the statistical spread of Bit Error Rate performance at a fixed SNR using thousands of pseudo-random IPK-LDPC codes is very similar to the statistical spread of performance of the standard IEEE 802.11 LDPC Codes.

XII. Transpositional Modulation

Test results on the TM enabled system are summarized below:

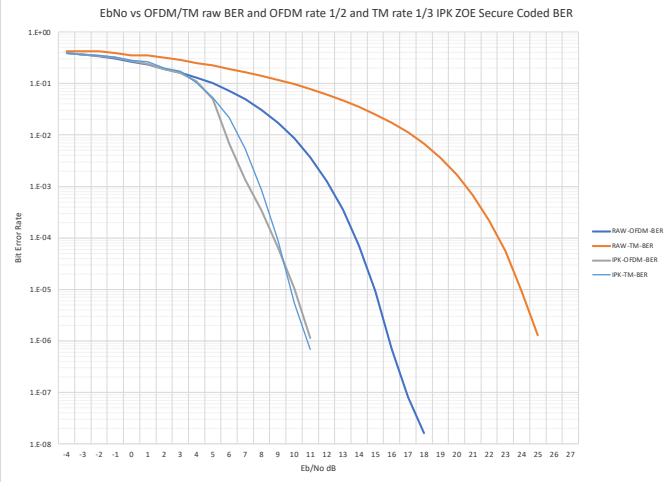


Fig. 7. The measured Eb/No vs uncoded Legacy OFDM and TM signals and the IPK-ZOE Secure Encoded signal Bit Error Rates.

The QPSK OFDM signal is a rate ½ code and the QAM16 TM signal is a rate 1/3 code.

The combined effect of the two codes on the two different modulation channels brings the combined targeted Eb/No to the same effective Energy per bit for both the OFDM base signal and the TM signal, saving 10dB of Signal Power for the TM signal and 5dB for the base OFDM signal.

XIII. Entropy

As seen below, we take a statistical analysis of encoded symbols of IPK LDPC coding vs the same number of symbols output from the Advanced Encryption Standard Galois Counter Mode (AESGCM).

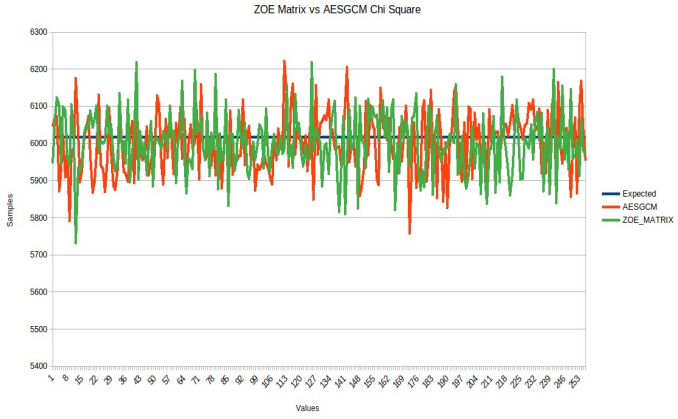


Fig. 7. The Chi Square test of IPK-LDPC and AESGCM

This result shows IPK-LDPC and AESGCM outputs are very similar in Chi-Square and Kolmogorov-Smirnov tests of randomness (entropy).

XIV. Conclusion

We have shown that these IPK secure LDPC code methods produce codes that are as efficient as those in use by any standard system but with the added benefit of physical layer symbol security.

Acknowledgment

Special thanks to Dr. Scott Velazquez for access to the Transpositional Modulation System development team, documentation, and papers.

References

[1] Gwain Bayley, William F. Van Duyne, William Spazante (2021). U.S. Patent No. 11,119,670, “Methods and systems for efficient encoding and decoding communications”.

[2] Robert G. Gallager, Low Density Parity Check Codes. Monograph, M.I.T. Press, 1963.

[3] IEEE 802.11 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification. IEEE, May 2021.

[4] S. R. Velazquez, D.H. McIntire, “Transpositional Modulation (TM) for Spectrum Efficiency and Obfuscated Communications” in Proceedings of GOMACTech Conference 2022, March 2022.