USO DE CÓDIGOS DE DECODIFICACIÓN ITERATIVA PARA MEJORAR LA TRANSMISIÓN DE MENSAJES CIFRADOS CON AES

Arnone[†] Leonardo, Castiñeira[††] Jorge, Liberatori[††] Mónica, Gayoso[†] Carlos y González[†] Claudio

[†] Facultad de Ingeniería. UNMDP. Argentina. Laboratorio de Componentes Electrónicos
[††] Facultad de Ingeniería. UNMDP. Argentina. Laboratorio de Comunicaciones

leoarn@fi.mdp.edu.ar

ABSTRACT

Se presenta un estudio de la mejora que se puede obtener en una transmisión de mensajes cifrados utilizando el algoritmo AES, al codificar mediante el uso de códigos LDPC y códigos Turbo.

Se muestran diferentes propuestas para su implementación, las cuales no sólo producen una mejora en la tasa de error del sistema, sino también un incremento en la capacidad de encriptamiento propia del algoritmo AES.

Por último se ilustra cómo es posible implementar fácilmente un sistema en lógica programable usando un decodificador LDPC que utiliza sólo sumas y restas realizadas en punto fijo y un encriptador-desencriptador AES de bloques de 128 bits y una llave de 128 bits.

.

1. INTRODUCCIÓN

El algoritmo de encriptamiento conocido como AES [1] genera un conjunto de operaciones no lineales sobre el mensaje original (típicamente un bloque de 128 bits de información) que le otorgan una fuerte capacidad de encriptamiento. Sin embargo, este mismo efecto no lineal ocasiona una fuerte propagación de errores, de manera que cuando se lo utiliza en una transmisión inalámbrica, por ejemplo, y frente a la acción del ruido, la performance de tasa de error (BER) se deteriora fuertemente, si lo comparamos con la transmisión sin codificar. Esta pérdida fluctúa entre los 2 y los $5dB$. Esto indica la necesidad de utilizar al algoritmo con eficientes técnicas para el control de errores, tales como los códigos LDPC [2] [3] o los códigos Turbo [4] [5].

En el presente trabajo se simula la performance de error en esquemas donde se combina el uso del algoritmo AES con códigos eficientes para el control de errores, como los códigos LDPC y Turbo.

El trabajo está dividido de la siguiente forma: la sección 2 muestra el efecto de propagación de errores que resulta de la utilización del algoritmo AES con $L = 128$ (longitud del bloque del algoritmo) en canales ruidosos. La sección 3 muestra la mejora obtenida con respecto al canal sin codificar al utilizar codificación LDPC con matices de paridad $\boldsymbol{H}$ de tamaño $128x256$ y $1280x2560$ combinado con el algoritmo AES.

En la sección 4 se realiza una comparación con el uso de códigos Turbo. Por último se muestra que es posible implementar prácticamente un sistema de bajo costo en lógica programable.

2. COMPARACIÓN ENTRE LA TRANSMISIÓN SIN CODIFICAR, Y LA TRANSMISIÓN UTILIZANDO EL ALGORITMO AES, EN UN CANAL CON RUIDO BLANCO Y GAUSSIANO.

En la Fig. 1 se observa la tasa de errores en una transmisión de información binaria en formato polar que no posee ningún tipo de codificación, en forma comparativa con la transmisión de esa misma información encriptada empleando el algoritmo AES.

Puede observarse que la utilización del algoritmo de encriptamiento trae aparejada una desmejora importante de la tasa de error con respecto a la transmisión no codificada. Esto sugiere que es necesario recurrir al uso de técnicas de control de error cuando se pretenda utilizar el algoritmo en esquemas de transmisión que enfrentan canales ruidosos.

Cuando se produce un error en los bits que forman algún elemento del campo $GF(256)$ sobre el que opera el algoritmo AES, y con cierta independencia respecto de la posición y de la cantidad de bits equivocados que se forman en la transmisión, el algoritmo AES produce una propagación de error que multiplica el número de bits errados respecto de la transmisión sin codificar por un factor que fluctúa entre $L/6$ y L. En una situación promediada este factor resulta ser aproximadamente igual a $T_{AES} \cong 74$. Esto significa que la tasa de error en bits se incrementa en un factor T_{AES}.

3. ESQUEMA COMBINADO DE UN CÓDIGO LDPC Y EL ALGORITMO AES.

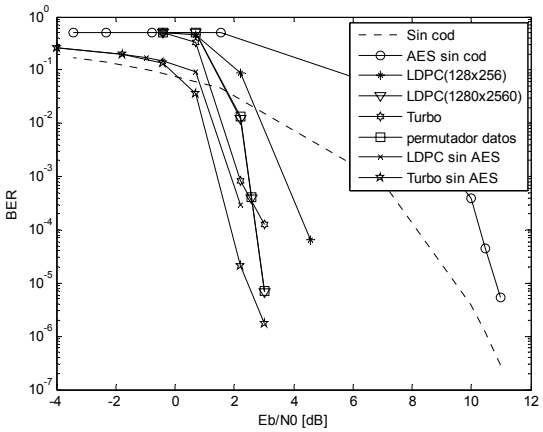

Fig. 1. Transmisión usando el algoritmo AES sin codificar y AES codificado.

El esquema combinado de codificación LDPC y encriptamiento AES que se propone se muestra en la Fig. 2. En este esquema se hace notar que el algoritmo de encriptamiento se aplica en el lado transmisor en primera instancia, para luego ser codificados para el control de error por un código LDPC. Esto es necesario dado que si se utilizaran en el sentido inverso, en el receptor, el algoritmo AES generaría como salida un bloque de 128 bits en formato de decisión rígida, produciendo la perdida de información suave obtenida del canal [2] [3]. De esta manera, se pierde la eficacia de la decodificación iterativa en este tipo de códigos, que esencialmente tienen una buena performance si operan sobre la base de entradas y salidas que sean estimaciones no rígidas. Además, el algoritmo AES opera sobre la base de información binaria y el decodificador LDPC le presenta la información en este formato, luego de haber decodificado iterativamente. Otra razón que justifica este orden, es que en el lado receptor, el decodificador LDPC reduce los errores producidos en el canal, aliviando así el efecto de propagación de error que el desencriptador del algoritmo AES produce. De esta manera el decodificador LDPC genera la entrada al desencriptador en formato binario explotando su capacidad de error y la información no rígida obtenida del canal.

En este primer esquema, el código utilizado es un código $C_{LDPC}(256,128)$, el cual tiene tasa de código $R_c = 1/2$, y se adapta al formato de bloques que entrega el encriptador de AES. De esta manera, el codificador LDPC genera un bloque de 256 bits. En este primer esquema, el código LDPC utiliza una matriz de paridad $\boldsymbol{H}$ cuyo tamaño es $128x256$.

El cifrador AES toma como entrada un bloque de 128 bits, y entrega un bloque de datos encriptados que también es de 128 bits.

Dado que como es sabido, los códigos LDPC son más eficientes cuanto más larga es la palabra del código, otro esquema propuesto consiste en utilizar a la salida del cifrador AES un registro que toma 10 bloques de 128 bits cada una, y genera una palabra de 1280 bits encriptados. Esta palabra de 1280 bits es aplicada a la

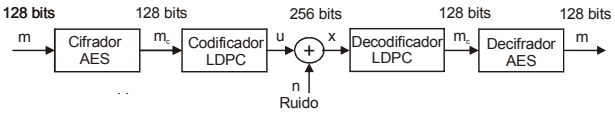

Fig. 2. Sistema de codificación para el control y encriptamiento combinado utilizando el algoritmo AES y un código LDPC.

entrada de un codificador $C_{LDPC}(2560,1280)$, que produce un bloque encriptado y codificado de 2560 bits.

Estos bits son transmitidos en el canal para ser primero decodificados, y luego desencriptados por los correspondientes decodificadores.

La performance de tasa de errores (BER) de este esquema puede verse en la Fig. 1. Se observa, tal como podía esperarse, que la tasa de error de este esquema que agrupa 10 bloques de mensaje para codificar, es mejor que la del que codifica bloques de sólo 128 bits. La mejora en la performance para una tasa de error de 10^{-4} es de aproximadamente $2dB$.

Dado que los esquemas propuestos pretenden ser utilizados con el doble propósito de controlar errores y encriptar la información, resulta conveniente adicionar algún tipo de encriptamiento en el esquema de codificación para el control de errores. Por tal motivo se efectúa una operación de permutación sobre la palabra codificada, una vez generada, y en el lado receptor se realiza la permutación inversa sobre la palabra recibida. Esta operación agrega al proceso una dificultad de desencriptamiento que puede medirse como $20L!$, Como se ve en la Fig. 1 el esquema presenta la misma tasa de error que el que no usa este procedimiento, pero ve incrementada su capacidad de encriptamiento en un factor sumamente elevado e igual a $20L!$, es decir $2.53x10^{7615}$

4. ESQUEMA COMBINADO DE UN CÓDIGO TURBO CON MEZCLADOR DE DATOS DE LONGITUD $L = 1280$ Y EL ALGORITMO AES.

En este esquema el cifrador AES toma como entrada un bloque de 128 bits, y genera un bloque encriptado de 128 bits. Agrupando 10 bloques de este tipo se forma un mensaje de 1280 bits que ingresan a un codificador Turbo cuyo mezclador de datos es de tipo aleatorio, y de longitud $L = 1280$.

La performance de tasa de error de este esquema puede verse en la Fig. 1. En la misma se observa que si bien es levemente mejor que la del esquema que utiliza el código LDPC $C_{LDPC}(2560,1280)$ en regiones de valor bajo de E_b / N_0, presenta también efecto de piso para valores más altos, donde el esquema que utiliza el código LDPC $C_{LDPC}(2560,1280)$ funciona mejor. En todos los casos, la utilización de un codificador para el control de errores eficiente produce una mejora sustancial en la performance del sistema, si se compara esta situación con la del uso del algoritmo AES sin

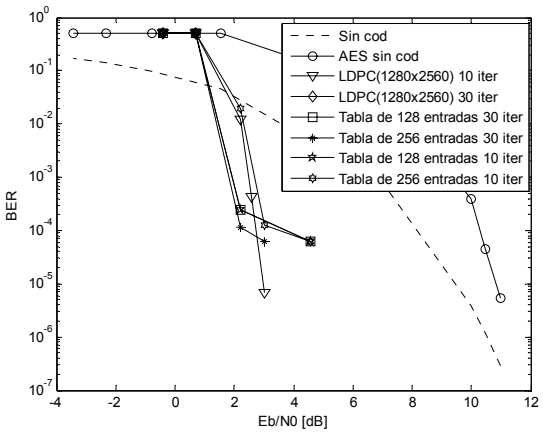

Fig. 3. BER del AES con código LDPC para diferentes tamaños de tabla de búsqueda.

codificación para el control de errores. Así, mientras la perdida de la transmisión encriptada con AES es de alrededor de 1 a $5dB$ respecto de la transmisión sin codificar, el empleo de codificación para controlar errores lleva al sistema a ganancias del orden de $8dB$, respecto de la transmisión encriptada.

Como se observa en la Fig. 1 para un E_b / N_0 de $3dB$ se obtiene mejor performance con el codificador LDPC de 10 iteraciones que con un codificador Turbo de 15 iteraciones. En el codificador LDPC con 30 iteraciones para $E_b / N_0 = 3dB$ la probabilidad de error se mantuvo por debajo de $1x10^{-7}$.

5. COMPARACIÓN DE LOS ESQUEMAS DE ENCRIPTAMIENTO Y CONTROL DE ERRORES PROPUESTOS CON ESQUEMAS SIMILARES SIN APLICACIÓN DEL ALGORITMO AES.

Los mismos esquemas propuestos en las secciones anteriores, donde el algoritmo AES se aplica a la información de mensaje para luego procesar su salida por medio de códigos de control de error, son simulados ahora sin la utilización del algoritmo de encriptamiento, con los fines de comparar las tasas de error en cada caso.

Como se observa en la Fig. 1, el efecto de propagación de errores que el algoritmo AES produce sobre la información, que como se dijo anteriormente puede medirse por un factor T_{AES} que incrementa la tasa de error en bits, permanece dentro de los órdenes medidos, aún cuando se utiliza codificación para el control de errores. Sin embargo, para la mayoría de los esquemas propuestos, utilizar el algoritmo de encriptamiento juntamente con el de codificación para el control de errores significa tener una diferencia en la tasa de error que puede considerarse una perdida de alrededor de aproximadamente $1dB$, mientras que en la comparación de las transmisiones sin codificación para el control de errores esta perdida fluctúa entre los 2 a $5dB$. En el caso del esquema que utiliza el código turbo, el uso del algoritmo AES acelera la aparición del efecto de piso en la performance de tasa de error.

El uso de códigos de decodificación iterativa junto con el algoritmo AES trae aparejada una mejora sustancial en la tasa de error total del esquema, de manera que si se transmite información encriptada sin codificar, para obtener una tasa de error en bits de $P_{be} = 10^{-5}$ se necesita una relación $E_b / N_0 \cong 11dB$, mientras que haciendo uso de codificadores de control de error eficientes como los LDPC o los Turbo junto con el AES, se tiene una tasa incluso levemente menor con $E_b / N_0 \cong 3dB$. Sin embargo, el efecto de propagación de errores no es totalmente contrarrestado en los esquemas propuestos.

El efecto de propagación de errores del algoritmo AES podría ser contrarrestado si la información fuera primeramente codificada para controlar errores, y luego de algún procedimiento de mezclado de datos, encriptada por este algoritmo. De esta forma las ráfagas de ruido ocasionadas por el AES en la decodificación, serían desparramadas en varias palabras de código por el proceso de mezclado de datos y luego mejor controladas por el decodificador correspondiente. Sin embargo, y como se explicó en la sección 3, este ordenamiento de los bloques ocasiona un endurecimiento de las decisiones en el decodificador, que le reduce fuertemente su poder de corrección de errores.

6. IMPLEMENTACIÓN PRÁCTICA. COMBINADO DE UN CÓDIGO LDPC $C_{LDPC}(2560,1280)$ Y EL ALGORITMO AES (128 BITS).

Es posible implementar un decodificador LDPC [9] [10] [11] [17] en forma muy sencilla en lógica programable utilizando un decodificador de sumas-restas en punto fijo. En este decodificador no se realizan productos ni cocientes, ni utiliza aritmética de punto flotante. El decodificador propuesto se describe en [11] [17] los resultado obtenidos no difieren en gran medida con los obtenidos en forma teórica cuando se utiliza un decodificador con una tabla de búsqueda de 256 entradas de 2 bytes y 30 iteraciones, tal como se observa en la Fig. 3.

En [12] [13] [14] se describe la forma de implementar en lógica programable un encriptador y desencriptador AES de 128 bits de bloques y una llave de 128 bits de bajo costo y área mínima [15] [16].

La combinación de las implementaciones mencionadas permite desarrollar un esquema de transmisión de datos en lógica programable con un alto nivel de privacidad y excelente performance en cuanto a la tasa de error (BER).

7. CONCLUSIONES

Como se observó en la sección 2, la transmisión de datos encriptados por medio del algoritmo AES en presencia

de ruido va acompañada de un efecto de propagación de errores proporcional al tamaño de bloque del encriptador. Esto sugiere el uso de este algoritmo conjuntamente con eficientes técnicas de codificación para el control de errores como los códigos LDPC y Turbo, debido a que el requisito de relación señal-ruido es considerablemente alto si se pretende lograr tasas de error aceptables en la mayoría de las aplicaciones prácticas.

En este trabajo se analizó como es posible mejorar la tasa de error (BER) en una transmisión de mensajes cifrados de un sistema que utilice AES mediante el uso de códigos LDPC y Turbo. El bloque de encriptamiento utilizado trae como consecuencia un efecto de propagación de error, que en el caso de la transmisión sin codificar, es equivalente a una perdida de relación señal ruido que fluctúa aproximadamente entre 2 y $5\,dB$. La utilización de códigos de decodificación iterativa, convierte este efecto en una pérdida menor, de aproximadamente $1\,dB$.

La utilización de técnicas de control de decodificación iterativa conjuntamente con el algoritmo AES permite lograr una tasa de error de aproximadamente $6x10^{-6}$ con una relación $E_b / N_0 \approx 3\,dB$, cuando para el caso sin codificar se necesita una relación $E_b / N_0 \approx 11\,dB$ para lograr la misma tasa de error.

También se muestra la mejora en la privacidad que se puede obtener en el sistema al permutar los elementos de la palabra codificada que se va a transmitir.

Por último se muestra como es posible implementar fácilmente este sistema en lógica programable usando un decodificador LDPC que utiliza sólo sumas y restas y un encriptador-desencriptador AES de 128 bits de bloques y una llave de 128 bits.

8. REFERENCIAS

[1] J. Daemen, V. Rijmen, ¨AES Proposal: Rijndael¨. Document version 2. NIST´s AES home page, http://www.nist.gov/aes, Sept. 1999

[2] R. G. Gallager. “Low Density Density Parity Check Codes”, IRE Trans. Information Theory, vol. IT-8, no 1, pp 21-28, January 1962.

[3] D.J.C.MacKay and R.M.Neal, “Near Shannon limit performance of low density parity check codes”. Electronics Letters, vol. 3, no6, pp. 457-458, March 1997.

[4] C. Berrou, A. Glavieux, P. and Thitimajshima. “Near Shannon limit error-correcting coding an decoding: Turbo codes”. Proc. 1993 IEEE Internacional Conference on Communications, Geneva, Switzerland, pp. 1064-1070. May 1993.

[5] L. Bahl, J. Cocke, F. Jelinek and J. Raviv. “Optimal decoding of linear codes for minimising symbol error rate”. IEEE Trans. Inf. Theory, vol. IT-20, pp. 284-287, March 1974.

[6] C. Heegard and S. Wicker. “Turbo Coding”. Kluver. Massachussets, 1999.

[7] L. Hanzo, T. H. Liew and B. L. Yeap. “Turbo Coding, Turbo Equalisation and Space-Time Coding, for Transmisión over Fading Channels”. IEEE/Wiley, New Cork. 2001.

[8] J. Castiñeira Moreira and P. G. Farrell. “Essential off Error-Control Coding”.Wiley, England, 2006.

[9] T. Bhatt, K. Narayanan and N. Kehtarnavaz, “Fixed Point DSP Implementation of Low-Density Parity Check Codes”, Proc IEEE DSP2000, Hunt, Tx, USA, Oct 2000.

[10] Li. Ping and W. K. Leung, “Decoding Low Density Parity Chek Codes with Finite Quantization Bits”, IEEE Communications Letters, vol. 4, no 2. February 2000.

[11] L. Arnone, C. Gayoso, C. González J. Castiñeira “Algoritmo de suma-resta para implementar códigos de paridad de baja densidad en lógica programable”, Anales XI Workshop Iberchip, pp. 127-129, Marzo 2005.

[12] J.C. Bonadero, M. Liberatori and H. Villagarcía Wanza, ¨Expansión de la Clave en Rijndael. Diseño y Optimización en VHDL¨. Anales XI RPIC XI Reunión de Trabajo en Procesamiento de la Información y Control, pp. 115-120, Sept. 2005.

[13] M. Liberatori and J.C. Bonadero, ¨Minimum Area, low cost FPGA implementation of AES¨. VIII International Symposium on Communications Theory and Applications, UK, pp. 461-466, Jul. 2005.

[14] M. Liberatori and J.C. Bonadero, ¨AES 128 cipher. Minimum Area, low cost FPGA implementation¨, SPL 06, II Southern Conference on Programmable Logic, pp. 51-58, March 2006.

[15] P. Mroczkowski, P, ¨Implementation of the block cipher Rijndael using Altera FPGA¨. http://csrc.nist.gov/encryption/aes/round2/comments /20000510-pmroczkowski.pdf , (2001).

[16] A. Elbirt, W. Yip,B. Chetwynd, and C. Paar, ¨An FPGA Implementation and Performance Evaluation of the AES block cipher candidates algorithm finalists¨. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, , pp. 545-557, August 2001.

[17] L. Arnone, C. Gayoso, C. González and J. Castiñeira Moreira, “Sum-Subtract Fixed Point LDPC Decoder”, SPL 06, II Southern Conference on Programmable Logic, pp. 155-161, March 2006.

Title Page