C2

DISEÑO DE CIRCUITOS INTEGRADOS Y SEGURIDAD DE CIRCUITOS CRIPTOGRÁFICOS FRENTE A ATAQUES

Jiménez, C.J. (cjesus@us.es); Valencia, M.; Baena, C.; Parra, P.; Acosta, A.; Mora, J.M.l; Tena, E.; Potestad, E.
TIC180: Diseño de Circuitos Integrados Digitales y Mixtos

Instituto de Microelectrónica de Sevilla. CNM-CSIC/Universidad de Sevilla.

RESUMEN

Muchos sistemas electrónicos incorporan dispositivos criptográficos que implementan algoritmos que cifran la información almacenada. Pero aun cuando los algoritmos sean muy seguros, estos dispositivos pueden llegar a revelar cierta información debido a su implementación física, mediante el empleo de los llamados ataques laterales. Estos ataques hacen uso de información obtenida durante del funcionamiento del circuito para obtener información sobre la clave utilizada. Por lo tanto, hay que cuidar la implementación física de los dispositivos criptográficos, para minimizar la posibilidad de pérdida de información mediante estos ataques.

En nuestras líneas de investigación estamos trabajando en analizar la vulnerabilidad de implementaciones de circuitos criptográficos, fundamentalmente cifradores de clave privada, frente a ataques laterales pasivos y activos. Estos ataques obtienen información de la clave almacenada mediante la medida de magnitudes físicas como el consumo de potencia o la radiación electromagnética durante el funcionamiento del circuito o alterando las condiciones de funcionamiento para introducirles fallos y comparar las salidas sin y con fallos.

En esta comunicación presentamos un breve resumen del estado del arte en los ataques laterales sobre implementaciones hardware de cifradores, algunos de los temas en los que estamos trabajando y algunos resultados obtenidos por nuestro grupo de investigación.

Palabras clave: *Ataques laterales, cifrado de información, hardware criptográfico.*

ABSTRACT

Many electronic systems include devices that implement cryptographic algorithms that encrypt stored information. But even if the algorithms are very safe, these devices can reveal some information because of its physical implementation, through the use of so-called side channel attacks. These attacks make use of information obtained during the operation of the circuit to obtain information of the used key. Therefore, we must take care of the physical implementation of cryptographic devices to minimize the possibility of loss of information through these types of attacks.

In our research we are working on analyzing the vulnerability of implementations of cryptographic circuits, mainly private key ciphers, against side channel attacks, passive and active. These attacks obtain key information stored by measuring physical quantities such as power consumption or electromagnetic radiation during operation of the circuit, or altering the operating conditions to introduce faults and compare the output with and without faults.

In this paper we present a brief summary of the state of art of side channel attacks on ciphers hardware implementations, some of the topics we are working and some results obtained by our research group.

Keywords: *Side channel attacks, ciphered information, cryptographic hardware.*

SEGURIDAD, ALGORITMOS Y CIRCUITOS

Las cualidades de seguridad que se requieren hoy en día son las de (1) asegurar la confidencialidad de las transferencias y almacenamientos de los datos, (2) asegurar la integridad y autenticidad de los mismos, tanto cuando son recibidos a través de una transmisión, como cuando son recuperados de algún sistema de almacenamiento, y (3) la de no repudio, por la cual los agentes en juego no pueden desdecirse de haber realizado determinadas operaciones que se conocen como firmas digitales [1][2].

Para la protección de la confidencialidad hay que recurrir a los cifradores criptográficos. De entre todos ellos, los cifradores de flujo son los de menor complejidad y mayor velocidad de operación. Su operación consiste en generar una secuencia pseudo-aleatoria mediante un algoritmo criptográfico complejo bajo el control de una clave privada, que se guarda en secreto, y un valor de inicialización o semilla. El proceso de cifrado consiste en mezclar el mensaje, cuyo contenido se quiere proteger, con dicha secuencia pseudo-aleatoria mediante la operación XOR. El descifrado consiste en mezclar el mensaje cifrado con la misma secuencia pseudo-aleatoria, también con la operación XOR.

La implementación hardware en tecnologías VLSI de estos algoritmos plantea numerosos desafíos. Por una parte, la integración de sistemas VLSI ya no puede tener como único objetivo la consecución de sistemas funcionalmente correctos, sino que deben cumplir una serie de requerimientos como frecuencia de operación y consumo de potencia cuya consecución plantea los mayores problemas [3]. Para aplicaciones de sistemas portables, el consumo de potencia es crítico, pues limita su portabilidad (disminución de la vida efectiva de las baterías) y su fiabilidad (estrés térmico debido al aumento de temperatura). Pero además, las implementaciones hardware de sistemas criptográficos deben ser seguras frente al criptoanálisis, y en particular frente a ataques laterales [4]. Esto supone la necesidad de introducir en los diseños técnicas de control de los tiempos de respuesta y de los consumos.

Los ataques laterales se pueden clasificar en tres grandes grupos [5,6]. Los llamados “ataques laterales pasivos” explotan el hecho de que algunos valores físicos como el consumo de potencia o la radiación electromagnética dependen de los cálculos

internos realizados durante la operación normal del circuito. El segundo tipo, denominado “ataques laterales activos” o basados en inyección de fallos, modifican el comportamiento del circuito para obtener un funcionamiento diferente, es decir, se induce al circuito a producir salidas erróneas. Ambos tipos de ataques, no dejan huella, pues se usan los pines de acceso al circuito. Un tercer tipo, basado también en la inyección de fallos, se conoce como “ataques invasivos”, pues obtienen información del circuito accediendo físicamente a él. Dado que no existe la invulnerabilidad completa, existe una continua demanda de soluciones más seguras, para hacer frente a ataques cada vez más sofisticados.

De todos los mecanismos de cifrado, nuestro grupo de investigación se centra en los cifradores de flujo (RC4, Trivium, etc), que generan un mensaje encriptado a partir de un texto plano y una clave, bit a bit y que dan lugar a implementaciones que consumen pocos recursos y tienen numerosas aplicaciones (GSM, SSL/TLS, etc). Tradicionalmente se ha estudiado mucho la vulnerabilidad de los cifradores de bloque, reportándose cientos de implementaciones y ataques a los cifradores de bloque tipo AES, pero muchos menos a cifradores de flujo [5]. Las estrategias de ataques son comunes, aunque las implementaciones serán necesariamente distintas. A continuación se analizan las diferentes estrategias de ataques y contramedidas.

1. Ataques laterales pasivos basados en el consumo de potencia.

Los ataques laterales sobre dispositivos criptográficos emplean información física extraída del funcionamiento normal del mismo (consumo de potencia, tiempo de operación, radiación electromagnética, etc.) para encontrar la clave secreta [7,8]. De las distintas técnicas que se emplean, la técnica de análisis diferencial del consumo, Differential Power Analysis (DPA) [9,10] es una de las más potentes, por su simplicidad y efectividad. Un atacante puede obtener la clave secreta monitorizando el consumo de potencia y haciendo análisis estadístico de los datos obtenidos.

De todas las contramedidas propuestas, las soluciones a nivel de circuito son las más genéricas y aplicables, ya que no dependen del algoritmo específico. Se dividen en dos categorías, las de enmascaramiento (masking) y las de ocultación (hiding).

Otras soluciones que se muestran altamente efectivas son aquellas que emplean familias lógicas diferenciales CMOS que, si son cuidadosamente diseñadas ofrecen las mejores soluciones. Destacan DyCML, LSCML, SABL, TDPL y DDPL.

2. Ataques laterales activos

Los ataques laterales activos consisten en la inyección deliberada de fallos en un circuito criptográfico y la observación de las salidas erróneas [11]. Usando este tipo de ataques y analizando las salidas del circuito criptográfico, mediante el “análisis diferencial de fallos”, el número de experimentos que se necesitan para obtener la clave secreta puede reducirse enormemente. Las técnicas de inyección de fallos han sido objeto de una intensa investigación en los últimos años y han demostrado su

alta eficiencia, abarcando un amplio espectro de posibilidades: variaciones en los niveles de la tensión de alimentación, inyección de irregularidades en la señal de reloj, irradiación del circuito con señales electromagnéticas o luz visible, sobrecalentamiento del circuito, etc. [5].

Una técnica simple se basa en disminuir la tensión de alimentación hasta que se produzcan fallos. Aunque muy generalista, se ha mostrado efectiva en grandes circuitos [12] y en ASICs criptográficos más pequeños [13]. Una especialización de esta técnica consiste en la introducción de picos de tensión en la alimentación de forma controlada en el tiempo [14]. Otras opciones consisten en manipular la señal de reloj, por ejemplo acortando el tiempo de un ciclo de reloj hasta que el circuito funcione de forma incorrecta, induciendo fallos por modificaciones en el entorno (por calentamiento o por generación de radiaciones electromagnéticas en las proximidades del dispositivo), etc. [5].

Las técnicas invasivas de inserción de fallos requieren un equipamiento costoso y unos altos conocimientos y habilidades, además de un conocimiento preciso del layout del circuito pero son mucho más potentes. Un ejemplo de estas técnicas es la iluminación con un haz de luz preciso y fuerte de una o varias puertas lógicas de un circuito para alterar su comportamiento o cambiar el valor almacenado en una o varias celdas de memoria [15].

Las contramedidas para defenderse ataques laterales activos incluyen mecanismos de detección de los fallos o de tolerancia a los mismos. Una forma de hacer al circuito inmune a la inyección de fallos es dotarlo de detectores de frecuencias de reloj anómalas o de picos en la señal de reloj [16], de detectores de picos en la tensión de alimentación, sensores de temperatura, etc. Otras soluciones optan por incluir redundancia en el circuito criptográfico para detectar los fallos inyectados [17], duplicando el proceso que (des)cifra la información (utilizando redundancia de hardware o redundancia temporal) y comparar los resultados o incluyendo códigos de detección y corrección de errores.

Tradicionalmente los ataques por análisis de consumo se han considerado aparte de los ataques de inyección de fallos. Sin embargo se ha probado que los ataques por introducción de fallos pueden mejorar la eficiencia de los ataques de consumo. Ataques combinados han sido reportados tanto en circuitos con cifradores RSA [18] como con cifradores AES [19], pero no para cifradores de flujo.

3. Ataques y contramedidas para cifradores de flujo

Existen pocos ataques en cifradores de flujo, precisamente por la simplicidad de los mismos. El proyecto eSCARGOT [20] desarrolló un ASIC conteniendo un conjunto de cifradores de flujo, finalistas seleccionados del proyecto eSTREAM [21], reportándose ataques DPA a los mismos [22]. No existe, sin embargo, constancia explícita de otros tipos de ataques ni contramedidas específicas para este tipo de cifradores, empleándose las técnicas para cifradores de bloque, que pueden ser poco adecuadas a este tipo de circuitos tan simples.

También existen reportados pocos ataques laterales activos a cifradores de flujo. En [23] se presenta un ataque al Trivium en base a cambiar un bit del registro interno en ciclo de reloj dado. En [24] estiman que el número de fallos para obtener el valor completo del registro de estados es del orden de 380. En [25] han conseguido revelar el estado interno insertando 43 fallos en posiciones aleatorias. En [26] proponen una mejora de la técnica anterior, con un promedio de inyección de fallos para obtener la clave no superior a 16.

Para el cifrador Grain, en [27] se presenta un ataque mediante el cambio de cualquier bit del registro interno en un ciclo de reloj determinado. También hay reportadas técnicas de ataques para el cifrador SNOW 3G [28] induciendo un fallo en un bit preciso del registro interno del cifrador, en cualquier ciclo de reloj. Todos estos ataques han sido planteados de forma teórica, y en las referencias no aparecen pruebas de laboratorio ni propuestas de contramedidas concretas.

LÍNEAS DE TRABAJO DEL GRUPO DE INVESTIGACIÓN Y RESULTADOS OBTENIDOS

Los integrantes de este grupo de investigación comenzamos nuestra investigación en el diseño de circuitos criptográficos con nuestra participación en el proyecto Cripto-bio (Diseño Microelectrónico para Autenticación Cripto-Biométrica, Junta de Andalucía, P08-TIC-3674) y posteriormente en los proyectos CITIES (Circuitos Integrados Para Transmisión de Información Especialmente Segura, Ministerio de Ciencia y Tecnología, TEC2010-16870] y CESAR (Circuitos Microelectrónicos Seguros Frente a Ataques Laterales, Ministerio de Economía y Competitividad, TEC2013-45523-R).

En un primer paso, de entre los cifradores de flujo aprobados en eSTREAM [20], se escogió el Trivium, aunque también se trabajó con el cifrador Grain. Sobre el cifrador Trivium se le aplicó una técnica de reducción de consumo, consiguiéndose implementaciones con una reducción de más del 20% [29], obteniéndose la misma reducción de consumo en arquitecturas de Trivium que generan 2 bits en cada ciclo de reloj. También se ha desarrollado una metodología que permite el diseño y optimización de familias de puertas lógicas diferenciales de alta seguridad para aplicaciones de bajo consumo. Dicha metodología se ha aplicado al diseño óptimo de puertas y los resultados muestran mejoras en seguridad de varios órdenes de magnitud respecto a las puertas del mismo tipo más seguras que se han propuesto en la literatura [30, 31]. Paralelamente se ha avanzado en un montaje experimental con que poder medir la resistencia a ataques laterales de circuitos criptográficos. Este tipo de montajes es muy complejo y requiere numerosas fases. En una primera fase se ha desarrollado un montaje que mediante simulación lleva a cabo un ataque DPA del bloque Sbox9, usado en el algoritmo basado en cifradores de bloque de Kasumi [31]. En una segunda fase, se está realizando mediante simulación un ataque DPA al Trivium, con resultados preliminares altamente satisfactorios, tanto por la reducción del tiempo de ataque como por la efectividad del mismo [32]. De esta forma hemos ganado una valiosa experiencia en la realización de ataques laterales por simulación que estamos aplicando en los cifradores de flujo en el laboratorio. En

criptografía, se tiene experiencia también en generación de números aleatorios [33] y análisis de PUFs [34, 35], en el diseño de celdas lógicas diferenciales, además de trabajos en la automatización y gestión de obtención de datos en el laboratorio [36,37].

Como resultados de estos proyectos, se han diseñado y fabricado dos ASICs que incorporan distintas versiones del Trivium. El primero de ellos incluye Triviums, realizados con puertas estándar CMOS, con la técnica SABL y una propuesta de técnica mejorada con excelentes resultados. En el segundo, se incluyen propuestas de Trivium con técnicas de reducción de consumo, estando ahora en fase de test. Estos ASICs están sirviendo como primeros prototipos sobre los que estamos realizando ataques laterales.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente soportado por los proyectos CRIPTO-BIO (Diseño Microelectrónico para Autenticación Cripto-Biométrica, Junta de Andalucía, P08-TIC-3674), CITIES (Circuitos Integrados Para Transmisión de Información Especialmente Segura, Ministerio de Ciencia y Tecnología, TEC2010-16870] y CESAR (Circuitos Microelectrónicos Seguros Frente a Ataques Laterales, Ministerio de Economía y Competitividad, TEC2013-45523-R).

REFERENCIAS

[1] Francisco Rodríguez-Henríquez, N.A. Saqib, A. Dízan-Pèrez, Çetin Kaya Koç, “Cryptographic Algoritms on Reconfigurable Hardware”, Springer 2006.

[2] Serge Vaudenay. “A Classical Introduction to Cryptography: Applications for Communications Security”, Springer, 2006.

[3] International Technology Roadmap for Semiconductors, 2009, http://www.itrs.net/Links/2009ITRS/Home2009.htm

[4] Stefan Mangard, Elisabeth Oswald, Thomas Popp, “Power Analysis Attacks, Revealing the Secrets of Smart Cards”, Springer 2007.

[5] Barenghi, A.; Breveglieri, L.; Koren, I. ; Naccache, D., “Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures”, Proceedings of the IEEE, Vol.100, No. 11, Nov. 2012, pp. 3056 – 3076.

[6] Dutertre, J.-M. et. al, “Review of fault injection mechanisms and consequences on countermeasures design”, DTIS 2011.

[7] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, ”Examining smart-card security under the threat of power analysis attacks”, IEEE Trans. on Computers, vol. 51, no. 5, pp. 541-552, 2002

[8] Y-i. Hayashi, et al, ”Analysis of Electromagnetic Information Leakage From Cryptographic Devices With Different Physical Structures”, IEEE Trans. on Electromagnetic Compatibility, Vol. 55-3, pp. 571-580, June 2013.

[9] S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards, Springer, 2007.

[10] M. Alioto, M. Poli, and S. Rocchi, ”A General Power Model of Differential Power Analysis Attacks to Static Logic Circuits”, IEEE Trans. on VLSI Systems, vol.18, no.5, pp.711-724, May 2010.

[11] D. Boneh, R. DeMillo, and R. Lipton, “On the importance of eliminating errors in cryptographic computations,” Journal of Cryptology, vol. 14, no. 2, pp. 101–119, Nov. 2001

[12] A. Barenghi, et al, “Low Voltage Fault Attacks to AES,” HOST 2010, pp. 7–12.

[13] N. Selmane, S. Guilley, and J.-L. Danger, “Practical Setup Time Violation Attacks on AES,” EDCC 2008, pp. 91–96.

[14] M. Hutter, T. Plos, and J.-M. Schmidt, “Contact-Based Fault Injections and Power Analysis on RFID Tags,” ECCTD 2009, pp. 409–412.

[15] S. P. Skorobogatov and R. J. Anderson, “Optical Fault Induction Attacks,” CHES 2002, pp. 2–12.

[16] R. Jimenez, et al, "VLSI Implementation of digital frequency sensors as hardware countermeasure", ICECS 2012, pp. 384-387.

[17] R. Karri, K. Wu, P. Mishra, and Y. Kim, “Fault-based side-channel cryptanalysis tolerant Rijndael symmetric block cipher architecture,” in Proc. IEEE Int. Symp. on Defect and Fault Tolerance in VLSI Systems, pp. 427–435, 2001.

[18] F. Amiel, K. Villegas, B. Feix, and L. Marcel, “Passive and Active Combined Attacks: Combining Fault Attacks and Side Channel Analysis,” in Proc. Workshop on Fault Diagnosis and Tolerance in Cryptography, pp. 92–102, 2007.

[19] F. Regazzoni, et al, “Can knowledge regarding the presence of countermeasures against fault attacks simplify power attacks on cryptographic devices?” in Proc. IEEE Int. Symp. on Defect and Fault-Tolerance in VLSI Systems, pp. 202–210, 2008.

[20] eSTREAM: the ECRYPT Stream Cipher Project. http://www.ecrypt.eu.org/stream/

[21] http://www.sheffield.ac.uk/eee/escargot

[22] B. Gierlichs, et al, "Susceptibility of eSTREAM Candidates towards Side Channel Analysis," In ECRYPT Workshop, SASC - The State of the Art of Stream Ciphers, 2008

[23] A. Barenghi. "Fault Attacks on Stream Ciphers." In Fault Analysis in Cryptography. Springer, 2012.

[24] E. Biham, L. Granboulan, P.Q. Nguyen, "Impossible fault analysis of RC4 and differential fault analysis of RC4." FSE, pp. 359–367. Springer 2005.

[25] M. Hojsík, B. Rudolf. "Differential Fault Analysis of Trivium." 15th International Workshop, FSE 2008. 158-172.

[26] Y. Hu, J. Gao, Q. Liu, and Y. Zhang. "Fault analysis of Trivium." Journal Designs, Codes and Cryptography, Volume 62-3, March 2012: 289-311.

[27] A. Berzati, et al, "Fault analysis of GRAIN-128." HOST 2009. 7-14.

[28] B. Debraize, I.M. Corbella, "Fault Analysis of the Stream Cipher Snow 3G." FDTC 2009. 103-110.

[29] J.M. Mora, C.J. Jiménez, M. Valencia, "Low power implementation of Trivium stream cipher", PATMOS-2012, pp. 113-120.

[30] J. Castro, P. Parra, A. J. Acosta, "An improved differential pull-down network logic configuration for DPA resistant circuits," ICM'10, pp.311-314, Dec. 2010.

[31] E. Tena, J. Castro, A. J. Acosta, "A Methodology for Optimized Design of Secure Differential Logic Gates for DPA resistant Circuits," IEEE Transactions on Circuits and Systems-Part I. Under Revision, 2013.

[32] E. Tena, A.J. Acosta, "Efficient simulation-based DPA attack on TRIVIUM Stream Cipher", Submitted to Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE'14), 2014.

[33] M.J. Bellido, A.J. Acosta, M. Valencia, A. Barriga and J.L. Huertas, "Simple Binary Random Number Generator", Electronics Letters, Vol. 28, n. 7, pp. 617-618, April 1992.

[34] S. Eiroa, I. Baturone, A.J. Acosta, J. Dávila, "Using Physical Unclonable Functions for Hardware Authentication: A Survey, Desing of Circuits and Integrated Systems (DCIS'10), Nov. 2010.

[35] S. Eiroa, J. Castro, M. Martínez, E. Tena, P. Brox, I. Baturone, "Reducing bit flipping problems in SRAM physical unclonable functions for chip identification", ICECS'12, pp. 392-395, 2012

[36] E. Tena, J. Castro, A. J. Acosta, "Automatic and Systematic Test Toolset for Digital ASICs," DCIS'13, Nov. 27-29, 2013. Aceptado.

[37] E. Tena, J. Castro, A. J. Acosta, "Automatic and Systematic Control of Experimental Data Measurements on ASICs," IMEKO TC-4 Symposium Measurements of Electrical Quantities, pp. 114-119, 2013.