Estudio exploratorio de la técnicaTimming Attack en el criptosistema RSA
Exploratory study of Timing Attack on RSA cryptosystem

Francisco Bolaños Burgos, Luis García Tenesaca y Antonio Cevallos Gamboa

***Resumen*— El presente trabajo realiza un análisis bibliográfico exploratorio del tipo de ataque *Timing Attack (TA)* de *On The Side Channel Attack (SCA) en RSA*. Para lo cual, se analizaron los activos de información, los modos de operación y las contramedidas efectuadas de 22 artículos. Los resultados evidencian que el activo de información que más ataques tuvo son las tarjetas inteligentes (32%), la contramedida mayormente aplicada es el cegamiento (33%) y los modos de operación más utilizados son el Chinese Remainder Theorem (CRT) o Montgomery Multiplication (MM) con CRT (41%). Adicionalmente se evidencia que sólo un ataque fue realizado a los sistemas de telecomunicaciones, lo cual permite plantear trabajos futuros en el análisis de la misma técnica con base en las tecnologías WiMAX y el protocolo SIP de VoIP.**

***Palabras Claves*— Side Channel Attacks; Timing Attack; RSA;activos de información; modos de operación; contramedidas**

***Abstract*— This paper makes an exploratory bibliographic analysis of the Timing Attack (TA) technique on the Side Channel Attacks (SCA) in RSA. The information assets, operation modes and countermeasures of 22 papers were analyzed. Findings show that smartcards are the most attacked information assets (32%), blinding is the most applied countermeasure (33%) and the Chinese Remainder Theorem (CRT) or Montgomery Multiplication (MM) with CRT are the most frequent operation modes(41%). Furthermore, just one attack was executed in telecomunication systems, this opens the possibilty for future work, analyzing the same technique using the tecnologies WiMAX and the SIP VoIP protocol.**

***Index Terms*— Side; Channel; attacks; Timing; systems; countermeasures.**

I. Introducción

El SCA se considera una clase de ataque físico, en el cual un adversario trata de explotar la filtración de información que el dispositivo emite en la ejecución del algoritmo criptográfico basado en: la medición de tiempo, el consumo de potencia o las radiaciones electromagnéticas [1]. El ataque TA mide el tiempo que se demora una unidad en realizar una operación. Por medio de la medición precisa de la cantidad de tiempo requerida para generar operaciones de clave secretas, el atacante puede encontrar exponentes de Diffie-Hellman, factores de una clave RSA, y quebrar otros sistemas criptográficos [2]. Las implementaciones de algoritmos criptográficos por lo general ejecutan cómputos en tiempos no constantes debido a las optimizaciones de rendimiento. Si estas operaciones incluyen parámetros secretos, dichas variaciones en el tiempo pueden filtrar información, y con el conocimiento adecuado del criptosistema se puede llevar a cabo un análisis estadístico que desencadena en la recuperación de estos parámetros secretos [3]. Además, un TA es esencialmente una forma de obtener información privada de algún usuario a través de la medición dependiente del tiempo que el usuario necesita para llevar a cabo operaciones criptográficas. Una vez que se dispone de información suficiente, el criptosistema podría ser roto [4].

El ataque Power Analysis Attack (PA), es un ataque enfocado en el análisis del consumo de energía o potencia de una unidad mientras realiza una operación de cifrado [1]. Un equipo criptográfico, por medio de su consumo de energía puede proveer información relacionada con las operaciones que se está realizando y los parámetros involucrados en las mismas [3]. Este ataque puede ser divido en dos clases que son Simple Power Analysis (SPA) y Differential Power Analysis (DPA). En los ataques SPA, el enfoque apunta a interpretar el consumo de energía del equipo y deducir información acerca de las operaciones ejecutadas. En el caso de los ataques DPA, tienen como objetivo tomar ventaja de la dependencia de datos en los patrones de consumo de energía [1].

El ataque Electromagnetic Attack (EMA) se enfoca en las radiaciones electromagnéticas generadas por los componentes de una computadora o equipos electrónicos como parte de su funcionamiento. Un atacante puede observar estas emisiones y entender e inferir una gran cantidad de información acerca de los cálculos y datos que están siendo ejecutados. Similar a los ataques de consumo de energía, los ataques EMA pueden dividirse en dos tipos que son Simple ElectroMagnetic Analysis (SEMA) y Differential ElectroMagnetic Analysis (DEMA) [3].

El presente estudio tiene como objetivo analizar las implementaciones de los SCA con base en la técnica de TA

Francisco Bolaños Burgos es investigador de la Universidad de Especialidades Espíritu Santo de Guayaquil, e-mail: fcobolanos@uees.edu.ec
Luis García Tenesaca es investigador de la Universidad de Especialidades Espíritu Santo de Guayaquil, e-mail: lfgarcia@uees.edu.ec
Antonio Cevallos Gamboa, es investigador de la Universidad de Especialidades Espíritu Santo de Guayaquil, e-mail: acevallos@uees.edu.ec

tomando los 22 estudios seleccionados por juicio de expertos. Con la finalidad de conocer si existen relaciones entre los modos de operación, activos de información atacados y las contramedidas. En el capítulo II se describen las principales características de los 22 artículos seleccionados. En el capítulo III se analizan los estudios previo en términos delos activos de información más atacados, las contramedidas y los modos de operación utilizados. Finalmente en el capítulo IV se concluye en función del objetivo planteado y se plantean trabajos futuros.

II. Estudios Representativos

La selección de los artículos científicos se dio mediante juicio de expertos. Se realizó un focus group de seis expertos. Dos de ellos son peritos en criptografía, uno en matemáticas y los dos restantes en algoritmia. Los expertos efectuaron dos rondas de selección para decidir la inclusión de los artículos en este estudio.

El origen del SCA se da en el año 1965, la agencia británica de inteligencia (MI5), trató de penetrar el algoritmo de cifrado usado por la embajada egipcia en Londres. Pero sus esfuerzos fueron obstaculizados por los límites de su poder computacional en aquel tiempo. Se colocó un micrófono cerca del rotor de la máquina de cifrado, usado por los egipcios, para espiar el sonido de los clics que la máquina realizaba. MI5 dedujo correctamente la posición central de 2 o 3 rotores de la máquina. Esta información adicional redujo el esfuerzo de cálculo que se necesitaba para romper el cifrado y MI5 pudo espiar la comunicación de la embajada durante años [3].

En [5] mencionó que, por medio de la medición cuidadosa de la cantidad de tiempo requerida para realizar operaciones de claves secretas, los atacantes pueden ser capaces de encontrar exponentes Diffie-Hellman, factores RSA y quebrar otros criptosistemas. El ataque propuesto en [6] presenta mejoras al ataque presentado en [5], realizando una implementación, en tarjetas inteligentes, capaz de romper una clave de 512 bits en pocos minutos. En [7] se introduce un nuevo tipo de TA que permite la factorización de un módulo RSA si la exponenciación matemática con el exponente secreto usa CRT y el algoritmo de MM. En [8] el ataque *Divide and Conquer* trató de recuperar pequeñas porciones de claves criptográficas, dividiendo las claves en pequeñas partes que permitan realizar búsquedas exhaustivas y puedan ser manejadas por separado. En [9] un nuevo ataque es expuesto por medio del análisis de las variaciones de tiempo en una implementación de multiplicación modular, si un algoritmo de exponenciación binaria es utilizado, sólo un pequeño número de observaciones es necesario para realizar un ataque exitoso. En [10] se presentó un ataque mejorado eficientemente por medio de la observación de los factores básicos hacia el uso racional de potentes herramientas estadísticas. En [11] se enseñó una mejora al ataque [9] usando métodos estocásticos adecuados, la eficiencia del ataque se mejora por un factor de 5 en tablas de 2 bits.

En [12] se exhibió un ataque que aplica la teoría de decisión estadística y optimizó dos variantes relacionadas a los TA introducidos en [5; 6]. En [13] se mostró un ataque que apunta a las implementaciones del algoritmo MM y adoptado la metodología descrita en [9], ha sido demostrado en algunos algoritmos de exponenciación estándar, como MM, se realizan restas condicionales produciendo suficiente información para deducir el valor del exponente secreto. En [14] se expuso que una vez que las claves fueran lo suficientemente largas, aumentar la longitud de las mismas puede tender a la disminución de su seguridad y aumento en la fuga de información por canales laterales. En [15] se señaló un TA en la librería *Open-SSL*, en el cual mediante experimentos se expuso que las claves pueden ser extraídas de un servidor web. En [16] se exteriorizó un ataque en implementaciones desprotegidas de *Open-SSL* mejorando la eficiencia por un factor mayor a 10 al ataque previo demostrado en [15], en este nuevo ataque se explotó el comportamiento de MM en la fase de inicialización incrementando el número de multiplicaciones que proveen información útil para revelar información secreta. En [17] se propuso un método general para optimizar la eficiencia de los SCA por medio de métodos estocásticos avanzados, específicamente se aplicó el cálculo de procesos estocásticos y teorías de decisiones estadísticas. En [18] una extensión de [7] se dio en implementaciones RSA con CRT y MM, el ataque requirió el tiempo de procesamiento durante la exponenciación. En [19] se estudió el potencial de realizar TA remotos, como en una red de área local LAN o en Internet, ambos ataques requieren múltiples mediciones de tiempo de un evento en un servidor remoto y el filtrado de dichas mediciones para eliminar el ruido que puede ser causado por la red o hosts finales.

En [20] un esquema de TA avanzado en algoritmos criptográficos fue exhibido, donde el atacante puede usar el algoritmo enseñado para romper un sistema criptográfico por medio de la reconstrucción de la clave secreta. En [21] la idea principal fue explotar los mecanismos de certificado de caché soportados en las infraestructuras SIP VoIP, este ataque puede ser usado para revelar efectivamente el historial de llamadas de un grupo de usuarios de VoIP. En [22] se expuso un TA avanzado en RSA con CRT con una política de corrección de error, por medio de la corrección de errores una clave RSA de 1024 bits puede ser recuperada. En [4] para incrementar la factibilidad de un ataque de medición de tiempo, los autores propusieron un esquema mejorado de un ataque en la implementación RSA con CRT, el algoritmo proporciona un mecanismo de detección de error y corrección de estrategia que puede detectar y corregir decisiones erróneas realizadas por los atacantes. En [23] se presentó un TA en contra del algoritmo RSA con CRT usado en la librería *Polar-SSL*, la implementación de este ataque hace uso de una contramedida clásica para evitar los dos previos ataques propuestos en [7,15]. En [24] se demostró que la suposición de cegamiento del exponente prevendría los TA, no es generalmente cierta, aunque reduce enormemente el ataque. En [25] se expone que exclusivamente cegar el exponente ha sido asumido como una prevención para los ataques de medición de tiempo, aunque reduce significativamente en impacto de los mismos, no es generalmente verdadera y la eficiencia de este ataque es mayor en comparación con [24].

III. Análisis de los Estudios

En el Apéndice se muestra de una manera holística y resumida todos los papers analizados. Exponiendo de manera cronológica los ataques ejecutados, los autores de los mismos, el país de origen de los estudios, los modos de operación empleados, los equipos atacados y las contramedidas desarrolladas por los autores.

Las columnas Autores y Años, demuestran la cantidad de ataques ejecutados a las implementaciones en RSA de acuerdo a los diferentes autores, también se evidencia el orden cronológico de los mismos. Con base en la cantidad de ataques por autor se observa que el autor con más ataques es Schindler, con un 45.5%. La cantidad de ataques realizados por año es notorio que el pico más alto es el 2005 con 18.2% de ataques ejecutados. La tendencia de los autores es desarrollar ataques más efectivos y precisos para poder recuperar claves RSA en tiempos menores y con la menor cantidad de mediciones de tiempo necesarios. El ataque desarrollado por Kocher [5], es un punto de partida para los diferentes ataques, los siguientes ataques tratan de mejorar los rendimientos de los ataques anteriores como Dhem y otros [6], trató de mejorar la efectividad del ataque Kocher. Otros ejemplos son los de: Schindler [11], Schindler y Walter [13], Chen, Wang y Tiang [22,4].

Adicionalmente, en la columna Modos de Operación, se observa los modos que los atacantes utilizaron con una paridad del 41% entre los que utilizaron sólo MM o MM con CRT. En los primeros TA realizados por Kocher [5], y Dhem y otros [6], se apuntaba a las implementaciones RSA que sólo utilizaban el algoritmo de multiplicación modular Montgomery. Esto era debido a la suposición que si estas implementaciones realizaban las reducciones con CRT eran impenetrables a este tipo de ataques. Sin embargo, Schindler [7], demuestra en su TA que dicha teoría era falsa, las implementaciones que usaban MM o MM con CRT son vulnerables a estos ataques de medición de tiempo. A partir de estas primicias los autores desarrollan diferentes tipos de ataques que apuntan a los diferentes modos de operación que utilizan las implementaciones RSA, en los cuales ambas son vulnerables a los TA.

En la columna Contramedidas, la principal defensa empleada por los autores es el cegamiento con 33%, introducida por Kocher [5], se utiliza como prevención para que los atacantes no puedan conocer los valores de entrada de las exponenciaciones modulares. La mayoría de los autores hacen uso del cegamiento del exponente como prevención de los TA. No obstante, Schindler [25], expone que sólo el cegamiento del exponente no es una defensa suficiente para estos ataques, aunque la eficiencia del ataque es reducida significativamente igual pueden ser vulnerados. Se recomienda que el cegamiento deba ser combinado tanto como la base y el exponente. Además, se observa con un 11% la segunda contramedida más empleada es la Reducción Adicional, pero también Schindler [25], recomienda que esta reducción debe ser evitada debido a que la fuga de información es mayor. Las contramedidas, se emplean dependiendo del ataque.

En la columna Equipos Atacados, se puede observar los diferentes tipos de equipos implementados. Siendo las primeras víctimas las tarjetas inteligentes con un 32% debido a que en estos equipos la facilidad de implementación de ataques era mayor como los demuestran Dhem y otros [6], Schindler [7,12], Schindler, Kouene y Quisquater [8], Walter [14], entre otros. Hasta el ataque presentado por Brumley y Boneh [15], existía la hipótesis que los servidores de uso general como los servidores web no podían ser víctimas. Sin embargo, esto fue desafiado y un TA fue ejecutado en servidores de código abierto *Open-SSL*. A partir de este ataque el enfoque a los servidores *Open-SSL*, con un 23%, fue implementado por varios autores como Aciiçmez, Schindler y Koç [16] o Chen, Wang y Tiang [22,4].

IV. Conclusiones y Trabajos Futuros

Tanto los sistemas computacionales como los de telecomunicaciones pueden ser víctimas de los TA, inclusive cuando estos sistemas emplean sistemas de cifrado, como RSA. Los resultados alcanzados demostraron que el enfoque de los autores es la creación de mejores ataques aprovechando la información de los anteriores y lo que en un principio se pensaba impenetrable se pudo demostrar que no es así. Se puede comprobar que la información relacionada a los sistemas de telecomunicaciones no es tan extensa como la presentada en los sistemas computacionales.

Una limitación al presente trabajo, es por ser un estudio exploratorio no hay acceso a toda la información y solo se pudo analizar 22 casos de los TA en RSA. También, al ser un tema nuevo en los sistemas de telecomunicaciones no hay suficiente información publicada en revistas científicas o de libre acceso. Además, no se poseen los equipos necesarios para realizar una simulación de una implementación de ataque en estos sistemas.

Por esta razón, como trabajo futuro se recomienda realizar investigaciones aplicando técnicas de meta análisis en estos sistemas para conocer otros tipos de defensas que puedan ser empleadas y también ataques adicionales. Además, enfocarse en otros tipos de SCA, en los sistemas de telecomunicaciones, para poder realizar una simulación de estos ataques en las tecnologías WiMAX, protocolo SIP de VoIP o en otros sistemas de telecomunicaciones. Por medio de estos nuevos ataques se podrá conocer si las contramedidas existentes son suficientes en los sistemas de telecomunicaciones. Adicionalmente se puede realizar una comparativa de los ataques estudiados en un mismo equipo.

Referencias

[1] F.-X. Standaert, «Introduction to Side-Channel Attacks,» de Secure Integrated Circuits and Systems, Boston, MA, USA, Springer US, 2010, pp. 27-42.

[2] R. Oppliger, Contemporary Cryptography (2nd Edition), Norwood, MA: Artech House, 2011.

[3] Y. Zhou y D. Feng, «Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing,» 2006. [En línea]. Available: https://www.eprint.iacr.org.

[4] C. Chen, T. Wang y J. Tian, «Improving timing attack on RSA-CRT via error detection and correction strategy,» Information Sciences, vol. 232, pp. 464-474, 2013.

[5] P. C. Kocher, «Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems.,» de Andvances in Cryptology - CRYPTO'96: 16th Annual International Cryptology Conference, 1996.

[6] J.-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestré, J.-J. Quisquater y J.-L. Willems, «A practical implementation of the timing attack,» de Smart Card Research and Applications: Third International Conference, CARDIS'98, 2000.

[7] W. Schindler, «A timing attack against RSA with the chinese remainder theorem,» de Cryptographic Hardware and Embedded Systems — CHES 2000: Second International Workshop, 2000.

[8] W. Schindler, F. Koeune y J.-J. Quisquater, «Improving divide and conquer attacks against cryptosystems by better error deteecction / correction strategies,» de Cryptography and Coding: 8th IMA International Conference, 2001.

[9] C. D. Walter y S. Thompson, «Distinguishing exponent digits by observing modular substractions,» de Topics in Cryptology - CT-RSA 2001: The Cryptographers' Track at RSA Conference 2001, 2001.

[10] W. Schindler, F. Koeune y J.-J. Quisquater, «Unleashing the full power of timing attack,» Catholic University of Louvain - Crypto Group, 2001, 2001.

[11] W. Schindler, «A combined timing and power attack,» Public Key Cryptography: 5th International Workshop on Practice and Theory in Public Key Cryptosystems, pp. 263-279, Febrero 2002a.

[12] W. Schindler, «Optimized timing attacks against public key cryptosystems,» Statistics & Risk Modeling, vol. 20, nº 1-4, pp. 191-210, 2002b.

[13] W. Schindler y C. D. Walter, «More detail for a combined timing and power attack against implementations of RSA,» Cryptography and Coding: 9th IMA International Conference, vol. 2898, pp. 245-263, 2003.

[14] C. D. Walter, «Longer keys may facilitate side channel attacks,» Selected Areas in Cryptography: 10th Annual International Workshop, SAC 2003, vol. 3006, pp. 42-57, 2004.

[15] D. Brumley y D. Boneh, «Remote timing attacks are practical,» Computer Networks, vol. 48, nº 5, pp. 701-716, 2005.

[16] O. Aciiçmez, W. Schindler y Ç. K. Koç, «Improving Brumley and Boneh timing attack on unprotected SSL implementations,» de Proceedings of the 12th ACM Conference on Computer and Communications Security, 2005.

[17] W. Schindler, «On the optimization of side-channel attacks by advanced stochastic methods,» Public Key Cryptography - PKC 2005: 8th International Workshop on Theory and Practice in Public Key Cryptography, vol. 3386, pp. 85-103, 2005.

[18] Y. Tomoeda, H. Miyake, A. Shimbo y S. Kawamura, «An SPA-based extension of Schindler's timing attack against RSA using CRT,» de IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2005.

[19] S. A. Crosby, D. S. Wallach y R. H. Riedi, «Opportunities and limits of remote timing attacks,» ACM Transactions on Information and System Security (TISSEC), vol. 12, nº 3, 2009.

[20] R. Tóth, Z. Faigl, M. Szalay y S. Imre, «An advanced timing attack scheme on RSA,» de Telecommunications Network Strategy and Planning Symposium, 2008. Networks 2008. The 13th International, 2008.

[21] Z. Ge, F.-H. Simone, L. A. Martucci y S. Ehlert, «Revealing the calling history of SIP VoIP systems by timing attacks,» de 2009 International Conference on Availability, Reliability and Security, 2009.

[22] C. Chen, T. Wang y J. Tiang, «An improved timing attack with error detection on RSA-CRT,» 2010. [En línea]. Available: https://eprint.iacr.org/2010/054.

[23] C. Arnaud y P. Fouque, «Timing attack against protected RSA-CRT implementation used in PolarSSL,» de Topics in Cryptology – CT-RSA 2013: The Cryptographers' Track at the RSA Conference 2013 , 2013.

[24] W. Schindler, «Exponent blinding may not prevent timing attacks on RSA,» 2014. [En línea]. Available: https://www.eprint.iacr.org/.

[25] W. Schindler, «Exclusive exponent blinding may not suffice to prevent timing attacks on RSA,» de Cryptographic Hardware and Embedded Systems – CHES 2015: 17th International Workshop, 2015.

Francisco Bolaños Burgos es ingeniero en Computación y magíster en seguridad informática aplicada de la Escuela Superior Politécnica del Litoral (ESPOL) en Guayaquil, Ecuador. Se desempeña como director de la Maestría en Auditoría de Tecnologías de la Información (MATI). Enseña criptografía, hackeo ético y seguridad de la información en la Facultad de Postgrados en UEES. Sus líneas de investigación son: seguridad de la información y herramientas de evaluación (rubrics y scripts).

Luis García Tenesaca es ingeniero en Telecomunicaciones de la UEES. Se desempeña como Account Manager de Huawei Technologies CO., LTD. Sus líneas de investigación son: protocolos y estándares de comunicación.

Antonio Cevallos Gamboa es ingeniero en sistemas, magíster en Sistemas de Información Gerencial y Administración de Empresas, PhD candidate de la Universidad Del Rosario en Bogotá, Colombia. Es decano de la Facultad de Ingeniería en Sistemas Telecomunicaciones y Electrónica (FISTE). Enseña escritura académica, metodología de la investigación y sistemas de información en la Facultad de Postgrado en UEES. Sus líneas de investigación son: sistemas de información, Tics, innovación y liderazgo tecnológico.

APÉNDICE

Tabla 1: Resumen de los diferentes tipos de ataques ejecutados en implementaciones RSA.

#	Título	Autores	País	Año	Modos de Operación	Equipos Atacados	Contramedidas
1	Timing Attacks en implementaciones de Diffie-Hellman, RSA, DSS y otros sistemas	Kocher, P.	EEUU	1996	MM	Computadora	Enmascaramiento. Mediciones Imprecisas. Cegamiento.
2	Una implementación práctica de un Timing Attack	Dhem, J-F., Koeune, F., Leroux, P-A., Mestré, P., Quisquater, J-J., Willems, J.	Bélgica	2000	MM	Tarjeta Inteligente	Reducción Adicional. Cegamiento.
3	Un Timing Attack en contra de RSA con CRT	Schindler, W.	Alemania EEUU	2000	MM CRT	Tarjeta Inteligente	Reducción Adicional. Cegamiento.
4	Mejora de ataque Divide and Conquer en contra de criptosistemas por mejor detección de error / estrategias de corrección	Schindler, W., Koeune, F., Quisquater, J-J.	Alemania Bélgica	2001	MM y MM CRT	Tarjeta Inteligente	No especifica
5	Distinción de dígitos de exponentes por observación de sustracciones modulares	Walter, C.D., Thompson, S.	Inglaterra	2001	MM	Computadora	Modificación del Exponente.
6	Desencadenamiento de todo el poder de un Timing Attack	Schindler, W., Koeune, F., Quisquater, J-J.	Alemania Bélgica	2001	MM	Tarjeta Inteligente	No especifica
7	Un Timing and Power Attacks combinados	Schindler, W.	Alemania	2002a	MM	Computadora	Modificación del Exponente.
8	Timing Attacks optimizados en contra de sistemas criptográficos de clave pública	Schindler, W.	Alemania	2002b	MM	Tarjeta Inteligente	No especifica
9	Mayor detalle para un ataque combinado de Timing y Power Attacks contra implementaciones de RSA	Schindler, W., Walter, C.D.	Alemania Inglaterra	2003	MM	Computadora	Cegamiento. Modificación del Exponente.
10	Las claves largas pueden facilitar los Side Channel Attacks	Walter, C.D.	Inglaterra	2004	MM	Tarjeta Inteligente	Cegamiento. Reducción Adicional.
11	Los Timing Attacks Remotos son prácticos	Brumley, D., Boneh, D.	EEUU	2005	MM CRT	Open-SSL	Cegamiento. Descifrado Independiente. Descifrado Cuantificado.
12	Mejora al ataque de Brumley y Boneh en implementaciones desprotegidas de SSL	Aciiçmez, O., Schindler, W., Koç, Ç. K.	EEUU Alemania	2005	MM CRT	Open-SSL	Cegamiento.
13	Optimización de Side Channel Attacks por métodos estocásticos avanzados	Schindler, W.	Alemania	2005	MM y MM CRT	Tarjeta Inteligente	Cegamiento. Tiempos de procesamiento constantes.
14	Una extensión SPA del TA de Schindler en contra de RSA usando CRT	Tomoeda, Y., Miyake, H., Shimbo, A., Kawamura, S.	Japón	2005	MM CRT	No especifica	Reducción Adicional. Cegamiento.
15	Oportunidades y límites de Timing Attacks remotos	Crosby, S.A., Wallach, D.S., Riedi, R.H.	EEUU	2007	No especifica	Open-SSL	No especifica
16	Un esquema avanzado de Timing Attack en RSA	Tóth, R., Faigl, Z., Szalay, M. Imre, S.	Hungría	2008	MM	No especifica	No especifica
17	Desvelamiento del historial de llamadas de SIP en los sistemas de VoIP por medio de Timing Attacks	Zhang, G., Fischer-Huebner, S., Martucci, L. A., Ehlert, S.	Varios	2009	No especifica	SIP-VoIP	Evitar Certificado Cache. Tiempo de Proxy Uniforme.
18	Un Timing Attacks mejorado con detección de error en RSA-CRT	Chen, C.,Wang, T., Tiang, J.	China	2010	MM CRT	Open-SSL	Cegamiento.
19	Mejora de los Timing Attacks en RSA con CRT por medio de la detección de errores y la estrategia de corrección	Chen, C., Wang, T., Tiang, J.	China	2013	MM CRT	Open-SSL	Cegamiento.
20	Timing Attacks en contra de implementaciones protegidas de RSA con CRT usados en Polar-SSL	Arnaud, C., Fouque, P.-A.	Francia	2013	MM CRT	Polar-SSL	Cegamiento. Modificación del Módulo. Modificación generación de clave.
21	Cegamiento del exponente puede que no prevenga Timing Attacks en RSA	Schindler, W.	Alemania	2014	MM CRT	No especifica	Evitar Reducción Adicional. Cegamiento combinado.
22	Exclusivamente cegamiento del exponente puede no ser suficiente para prevenir Timing Attacks en RSA	Schindler, W.	Alemania	2015	MM CRT	No especifica	Evitar Reducción Adicional. Cegamiento combinado.