Resumen de Tesis Doctoral

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola de Doctorat

DNI/NIE/Pasaporte	18024246-C
Nombre y apellidos	Rubén Lumbiarres López
Título de la tesis	Generación de falsas claves criptográficas como medida de protección frente a ataques por canal lateral.
Unidad estructural	Departament d'Electrònica
Programa	Doctorado en Enginyeria Electrònica
Códigos UNESCO	220300 / 120601 / 220307 /

(Mínimo 1 y màxim 4, podéis verlos en http://doctorat.upc.edu/gestion-academica/carpeta-impresos/tesis-matricula-y-deposito/codigos-unesco)

Resumen de la tesis de 4000 caracteres máximo (si se superan los 4000 se cortará automáticamente)

A finales de los 90 Paul C.Kocher introdujo por primera vez el concepto de ataque diferencial sobre el consumo de corriente de un dispositivo criptográfico. En este tipo de análisis, se conoce el texto plano que se envía al dispositivo y se plantean todas las posibles hipótesis de la clave para un punto concreto del algoritmo. Si el valor en ese punto del algoritmo depende únicamente de 1 byte de la clave, es posible calcular todos los valores que se producirán. Llegado a este punto, se compara, por métodos estadísticos, el consumo medido durante el procesado de cada texto plano y los valores intermedios relacionados con todas las hipótesis de la clave. Aquella que mayor nivel de similitud tenga corresponderá con la clave real.
Las contramedidas propuestas hasta la fecha, para evitar el éxito del ata-que, pueden separarse en dos grupos: enmascaramiento (Masking) y ocultación (Hiding). El enmascaramiento trata de desvincular el dato procesado del consumo eléctrico mediante la adición de una máscara aleatoria y desconocida por el atacante. En consecuencia, resulta imposible realizar una hipótesis que permita relacionar los consumos teórico y real del dispositivo. Si bien este es un método inicialmente válido, puede descubrirse la clave realizando un ataque de segundo orden que analiza varios puntos del consumo. La ocultación persigue que el consumo de un dispositivo sea el mismo en cada ciclo de reloj e independiente del dato procesado. Para ello, se procesa el dato en doble línea, por un lado el dato propiamente dicho y por el otro su complementario, de forma que siempre se produzcan la misma cantidad de transiciones en cada ciclo de reloj. La debilidad de este método radica en la práctica imposibilidad de construir celdas CMOS idénticas, esto provoca que siempre exista una diferencia de consumo entre las dos líneas y pueda usarse con éxito para descubrir la clave.
En esta tesis se propone una contramedida basada en una estrategia de protección claramente diferenciada con respecto a las propuestas realizadas en la bibliografía específica. Se pretende modificar el algoritmo con el objetivo de forzar una correlación muy alta en una hipótesis diferente a la de la clave (Faking). De este modo, la clave real se oculta tras la fuerte correlación aparecida, resulta imposible diferenciarla del resto de hipótesis falsas y queda protegida.
Para verificar su funcionamiento se ha montado un banco de pruebas para realizar ataques por análisis de consumo. Se ha implementado el algoritmo AES debido a su simplicidad y robustez. Se han realizado dos tipos de ataques: en el primero se han practicado análisis de correlación y diferencia de medias sin contramedida alguna; en el segundo, se ha añadido la contramedida y se han repetido los ataques para comprobar su eficacia.
Se han evaluado 3 escenarios diferentes, primeramente el algoritmo y la contramedida se resuelven mediante software en un procesador de 32 bits. En segundo lugar, el algoritmo se resuelve mediante software y la implementación de la contramedida se ha realizado en un coprocesador hardware específico. Fi-nalmente, se ha elegido una implementación totalmente hardware para resolver tanto el algoritmo como la contramedida. Todos ellos se han implementado sobre una FPGA Virtex5 de Xilinx.
Las conclusiones se obtienen de la comparación entre cada una de las im-plementaciones del AES sin contramedidas y su respectiva solución con la con-tramedida añadida. También se comparan los resultados obtenidos con otros que utilizan las técnicas “Masking” y “Hiding”
Los resultados demuestran que la propuesta es válida. En los tres casos, el sistema protegido se comporta igual que el sistema sin proteger, pero retornando la clave falsa ante los ataques realizados. Se ha de destacar que, la cantidad de recursos necesarios para llevar a cabo el “Faking” es menor que con el “Masking” o el “Hiding” y el tiempo necesario para procesar el texto plano no se ve particularmente afectado por su inclusión.

Lugar: Vilanova i la Geltrú Fecha: 19-Maig-2015

Firma

Rubén Lumbiarres López