منهجية حقن الأخطاء الكهرومغناطيسية:

نموذج الأخطاء القائم على الشحنة

Haohao Liao
Department of Electrical and Computer Engineering University of Waterloo Waterloo, Canada N2L 3G1
haohao.liao@uwaterloo.ca

Catherine Gebotys
Department of Electrical and Computer Engineering University of Waterloo Waterloo, Canada N2L 3G1
cgebotys@uwaterloo.ca

ملخص الورقة البحثية

الملخص — في الآونة الأخيرة، وُجد أن تقنيات Electromagnetic Fault Injection (حقن الأخطاء الكهرومغناطيسية) أو EMFI لها آثار كبيرة على أمان embedded devices (الأجهزة المدمجة). لسوء الحظ، لا يزال هناك نقص في فهم EM fault models (نماذج الأخطاء الكهرومغناطيسية) countermeasuresg (التدابير المضادة) لـ embedded processors (المعالجات المدمجة). لأول مرة، تقترح هذه الورقة extended fault model (نموذج أخطاء موسع) يعتمد على مفهوم critical charge (الشحنة الحرجة) و EMFI backside methodology (منهجية حقن الأخطاء الكهرومغناطيسية عبر المسار غير المباشر) جديدة تعتمد على over-clocking (زيادة تردد التشغيل). تُظهر النتائج أن التوقيت الدقيق لـ EM pulses (النبضات الكهرومغناطيسية) يمكن أن يوفر instruction replacement faults (أخطاء استبدال التعليمات) موثوقة وقابلة للتكرار لبرامج محددة. تم إظهار هجوم على خوارزمية AES يوضح أن EMFI يتطلب في المتوسط أقل من 22^2 نبضة كهرومغناطيسية و5.3 plaintexts (نصوص عادية) لاسترجاع مفتاح AES الكامل. هذا البحث حاسم لضمان أن embedded processors instruction set architecturesg (نظام تعليمات المعالج) الخاصة بها آمنة ومقاومة لـ fault injection attacks (هجمات حقن الأخطاء).

الكلمات المفتاحية — القناة الجانبية (side channel)، حقن الأخطاء (fault injection)، كهرومغناطيسي (EM)، نموذج الأخطاء (fault model)، أمان المعالج المدمج (embedded processor security).

مقدمة

أصبح الأمان منتشراً بشكل متزايد في العديد من الأجهزة المدمجة (embedded devices). يجب على الأجهزة نفسها تخزين المفاتيح التشفيرية (cryptographic keys) وأن تكون مصممة لدعم الإقلاع الآمن (secure boots) والمعالجة الآمنة (secure processing) وما إلى ذلك. بالإضافة إلى التنفيذ الصحيح، يجب أن يكون الأمان مقاوماً للهجمات المادية (physical attacks). على سبيل المثال، يمكن تركيز الموجات الكهرومغناطيسية (electromagnetic waves) على الجهاز (باستخدام النبضات الكهرومغناطيسية - EM pulses) مما يسبب تغييراً في بعض العمليات الحسابية أو البيانات داخل الجهاز (يُشار إليه باسم هجوم حقن الأخطاء الكهرومغناطيسية - EM fault injection attack).

على الرغم من أن البحث قد فحص هجمات حقن الأخطاء (fault injection attacks) لعدة عقود، لا يزال هناك فهم محدود لـ نماذج الأخطاء (fault models) الخاصة بـ المعالجات المدمجة (embedded processors) وكيفية تصميم التدابير المضادة (countermeasures). لهجمات حقن الأخطاء عواقب مهمة على الأنظمة المدمجة (embedded systems) وبالتالي فإن قياس التهديد (quantization of the threat) أمر مهم.

بالنسبة لـ هجمات حقن الأخطاء الكهرومغناطيسية (EM fault injection attacks)، سيكون من المفيد أيضاً قياس عدد النبضات الكهرومغناطيسية المطلوبة لشن هجوم. من الناحية النظرية، إذا كان x من عمليات حقن الأخطاء قد تكشف المفتاح الكامل وفي المتوسط y نبضة كهرومغناطيسية مطلوبة قبل أن يكون حقن الخطأ ممكناً، فإن عمر المفتاح السري (secret key lifetime) يجب أن يدعم في المتوسط أقل من x×y استدعاء (invocations) للخوارزمية التشفيرية (cryptographic algorithm) لمنع هجوم ناجح. نظراً لأن عدداً متزايداً من الأجهزة مغلفة بتقنية flipchip، فإن قابلية تأثر EMFI من الجانب الخلفي (backside) مهمة أيضاً. "شرح إضافي من المترجم"

الأبحاث السابقة

تشمل هجمات حقن الأخطاء (fault injection attacks) إحداث خلل في الطاقة أو إشارة التوقيت (power or clock glitching)، حقن النبضات الكهرومغناطيسية (electromagnetic pulse injection)، حقن الليزر (laser injection)، وغيرها. بشكل عام، هجمات حقن الأخطاء الكهرومغناطيسية أقل تكلفة ولديها متطلبات أقل بخلاف الوصول إلى الشريحة (chip) أو القالب المفكك (decapsulated die).

تضمنت بعض تقنيات حقن الأخطاء المبكرة انخفاض الجهد المستمر [5] (constant under-voltaging) والذي أنتج أخطاء إعادة التعيين (reset faults) في تحميلات الذاكرة (memory loads) بشكل مستقل عن قيم العناوين (address values). كان هذا البحث على الأرجح الأول الذي اقترح أنواع أخطاء استبدال التعليمات (instruction replacement fault types).

اقترح الباحثون في [7,8] أن حقن الانحياز الأمامي للهيكل (forward body biasing injection - FBBI) سيكون له دقة مكانية (spatial resolution) أفضل من تلك التي تم تحقيقها باستخدام نبضة كهرومغناطيسية على الجانب الخلفي (backside) من الدائرة المتكاملة (IC)، ومع ذلك كان حوالي 2٪ فقط من الأخطاء قابلة للاستغلال (exploitable).

اقترح الباحثون في [1] نموذج خطأ التوقيت (timing fault model) حيث يقلل الاقتران (coupling) بين النبضة الكهرومغناطيسية وشبكة الطاقة (power-ground network) مؤقتاً من إمداد الطاقة (power supply)، يزيد من التأخير (delay)، وأخيراً يسبب انتهاك قيد وقت الإعداد (setup time constraint violation).

لاحقاً في [2] تم اقتراح نموذج خطأ أخذ العينات (sampling fault model) يشير إلى أن النبضة الكهرومغناطيسية تغير مؤقتاً الجهد (voltage) لعدة عقد (nodes) في الدائرة (circuit) خلال فترة زمنية معينة، وبعد هذه الفترة الزمنية، تستعيد الشريحة (chip) بسرعة حالتها الأصلية، مما يشير إلى أن الأخطاء يجب أن تُحقن بالقرب من حافة الساعة (clock edge) للتأثير على القيم المُثبتة (latched) في السجلات (registers) والذاكرة (memory).

لاحظ البحث في [3] أخطاء تعيين البت (bit set faults) واقترح عدم الاستقرار (metastability) كسبب أثناء تحميلات التعليمات (instruction loads) من ذاكرة الفلاش (flash). فحص باحثون آخرون تأثيرات حقن الأخطاء الكهرومغناطيسية على إحداث خلل في الساعة [15] (clock glitching)، شرائح [13] DRAM (DRAM chips)، أو استخدام حقن الأخطاء الكهرومغناطيسية التوافقية [16] (harmonic EM fault injection).

تم إظهار هجمات حقيقية باستخدام حقن الأخطاء الكهرومغناطيسية على وظيفة الإقلاع الآمن (secure boot functionality) مما يشير إلى أخطاء استبدال التعليمات [17] (instruction replacement faults).

تفترض معظم التدابير المضادة التشفيرية (cryptographic countermeasures) أن البيانات مُخطأة بأصفار أو قيم عشوائية [6] (zeros or random values) أو أخطاء تخطي التعليمات [10] (instruction skip faults) والتي تمثل فقط مجموعة محدودة من عمليات حقن الأخطاء [11].

لا يزال هناك تحليل متعمق محدود (limited in-depth analysis) للأخطاء القائمة على المعالج (processor)، بما في ذلك قياس محدود لصعوبة الهجوم (limited quantization of attack difficulty) من حيث عدد النبضات الكهرومغناطيسية المطلوبة. بالإضافة إلى ذلك، لا يزال هناك نقص في فهم نماذج الأخطاء (fault models) وأنواع الأخطاء (fault types).

في هذه الورقة، سيتم تعريف نموذج الخطأ (fault model) على أنه الآلية (mechanism) التي تشرح كيف قد يحدث الخطأ، بينما تشير أنواع الأخطاء (fault types) إلى تعليمات محددة (specific instructions) (استبدال التعليمات الخاطئة - faulty instruction replacement) التي تمثل السلوك الخاطئ (faulty behavior) لـ التعليمة المستهدفة بحقن الخطأ (targeted fault-injected instruction).

المنهجية التجريبية والنتائج

يتم وصف الإعداد التجريبي (experimental setup) والمنهجية (methodology) جنباً إلى جنب مع النتائج التجريبية (empirical results) على متحكم دقيق مدمج (embedded microcontroller) في هذا القسم. يتم تقديم نموذج الأخطاء القائم على الشحنة (charge-based fault model) المقترح المشتق تجريبياً (derived empirically) جنباً إلى جنب مع تحليل متعمق (in-depth analysis) وقياس (quantization) لـاستبدال التعليمات الخاطئة (faulty instruction replacement) وهجوم على AES Attack.

إعداد ومنهجية EMFI

كان الإعداد التجريبي (experimental setup) يعتمد على آلة CNC مكتبية (desktop CNC machine) منخفضة التكلفة (حوالي 2.5 ألف دولار أمريكي)، ومولد نبضات كهرومغناطيسية (EM pulse generator)، ومسبار كهرومغناطيسي (EM probe). تم تعديل آلة CNC لحمل المسبار الكهرومغناطيسي ومكّنت من الوضع الدقيق على محاور xyz بدقة 12.7 ميكرومتر (um). وفرت آلة CAN أيضاً فك التغليف الآلي من الجانب الخلفي (automated backside decapsulation) للمعالج.

كان نظام توليد النبضات الكهرومغناطيسية المستخدم هو 12] EMV Langer Burst power station 202] (النبضة الكهرومغناطيسية لها زمن صعود (rise time) يقارب 2 نانو ثانية). تم وضع طرف المسبار الكهرومغناطيسي (EM probe tip) (يقارب 0.5 ميكرومتر) على ارتفاع يقارب 0.8 ميليمتر فوق سطح القالب المكشوف من الجانب الخلفي (exposed backside die surface) للمعالج.

الجهاز قيد التحليل (device under analysis) هو PIC16F687 مفكك التغليف من الجانب الخلفي (تم اختياره بسبب أكواد العمليات (opcodes) البسيطة بطول 14 بت وحزمة DIP (DIP package) مع حجم القالب (die size) يقارب 2.3 ميليمتر × 2.6 ميليمتر). يستخدم PIC16F687 أربع دورات ساعة (Q clock cycles) Q لكل دورة تعليمة (instruction cycle). تستخدم دورات التعليمات خط أنابيب من مرحلتين (2-stage pipeline) (مراحل جلب (fetch) وتنفيذ (execute) التعليمة).

تم زيادة تردد تشغيل (over-clocking) الـPIC16F687 بساعة خارجية 52 ميجاهرتز (موردة بواسطة مولد دوال (function generator)) واستُخدمت لتوليد مشغل خارجي (external trigger) لنظام EM. كانت النبضات الكهرومغناطيسية المستخدمة لـحقن الأخطاء (fault injection) عبارة عن نبضات موجبة مفردة (single positive pulses) بجهد 500 فولت، ما لم يُذكر خلاف ذلك.

تمت كتابة جميع البرامج بـلغة التجميع (assembly language) لتمكين تحليل التوقيت التفصيلي (detailed timing analysis). بسبب نقص مصحح عالي السرعة (high speed debugger) للمعالج، تم إجراء التحليل التجريبي (empirical analysis) باستخدام تصميم كود لغة التجميع لتأكيد وجود وتفاصيل الأخطاء المحقونة (injected faults).

شملت الـ (parameters) المحللة لجميع التجارب توقيت النبضة الكهرومغناطيسية، والنسبة المئوية للجولات التي كان فيها خطأ محدد، وإحصائيات حول عدد النبضات الكهرومغناطيسية المطلوبة لحقن الخطأ الأول.

في البداية، تم مسح حقن النبضات الكهرومغناطيسية (EM pulse injection scanning) على تسلسل كود اختباري (test code sequence) بفواصل زمنية 10 نانو ثانية وأقصر من أجل إيجاد أوقات نبضات كهرومغناطيسية محددة حيث كانت الأخطاء ناجحة.

استخدمت تجارب حقن الأخطاء (fault injection experiments) سكريبت Python رئيسي (master python script) (للتحكم/المزامنة بين آلة CNC، ومولد الدوال، ومولد النبضات الكهرومغناطيسية، ومبرمج (PIC (PIC programmer) بالإضافة إلى برامج لغة التجميع التي نفذت عدداً محدداً من الجولات (rounds). في كل جولة، كانت حلقة من الكود (loop of code) مسؤولة عن توليد إشارة مشغل الإخراج (output trigger signal) وتنفيذ سلسلة من التعليمات (series of instructions)، واحدة منها كانت هدف حقن الخطأ (target of fault injection). تم تصميم التعليمات اللاحقة (subsequent instructions) في الحلقة بعد التعليمة المستهدفة (target instruction) للتعامل مع كشف وتحليل الأخطاء (fault detection and analysis).

تم الكشف عن الأخطاء في كل من البيانات والتحكم (faults in both data and control) في البرنامج في كل حلقة من خلال عدة تكرارات (iterations) لتصميم لغة التجميع حتى أصبحت جميع الأخطاء قابلة للحساب (accountable). بشكل عام، تم الكشف عن الأخطاء القائمة على البيانات (data-based faults) من قيم البيانات (data values) المكتوبة أو غير المكتوبة إلى sRAM، أو السجلات (registers)، أو بتات الحالة (status bits).

على سبيل المثال، إذا كانت التعليمة المستهدفة تخزن بيانات من سجل (register) (أو من خلال ALU) إلى الذاكرة (memory)، فإن البرنامج سيفحص في البداية قيم بيانات السجل والذاكرة (أو بتات الحالة). إذا تم العثور على قيمة بيانات غير متوقعة (unexpected data value)، فإن البرنامج سيقفز إلى روتين معالجة الأخطاء (fault handling routine). سيضع روتين معالجة الأخطاء قيمة بيانات علامة (flag data value) في الذاكرة ثم يعالج الخطأ.

تم استخدام بيانات العلامة (flag data) للتحقق من أخطاء التحكم (control faults). على سبيل المثال، إذا لم تُكتب البيانات كما هو متوقع ولم يتم تعيين بيانات العلامة، ومع ذلك نفذ البرنامج معالجة الأخطاء، فمن المحتمل أن يكون خطأ من نوع التحكم قد تم حقنه. في هذه الحالة، تم وضع علامات إضافية (further flags) في الكود للمساعدة في تتبع مسار التحكم (trace the control path) للتعليمة الخاطئة.

تم العثور على أفضل وضع للمسبار الكهرومغناطيسي (best placement of EM probe) بالنسبة للقالب باستخدام برنامج كتابة ذاكرة (memory writing program) متزامن مع آلة CNC. بعد كل 10 جولات، تم نقل المسبار إلى موقع

xy مختلف، مع المسح تدريجياً (gradually scanning) على المنطقة الكاملة للقالب (entire area of die). خلال كل جولة، تم تسجيل حقن الأخطاء ومعلمات أخرى.

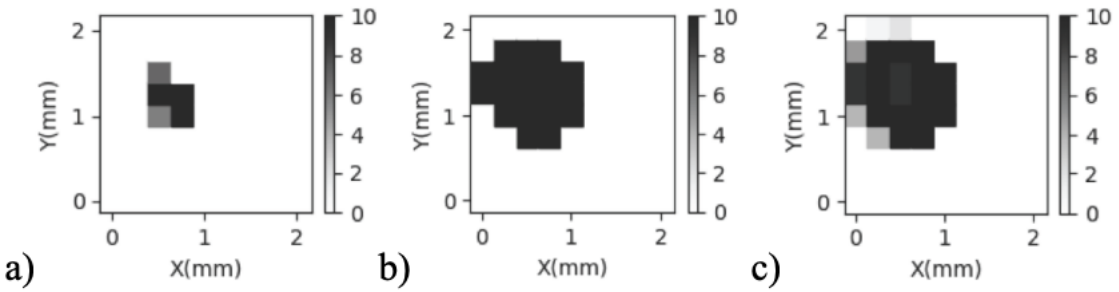
في البداية، تم وضع طرف المسبار تقريباً فوق زاوية من القالب (corner of die). ثم، للمسح الأول على القالب، تم استخدام دقة منخفضة (low resolution) لإيجاد منطقة حساسة (sensitive area) حيث من المرجح حقن الأخطاء. يوضح الشكل 1 هذا مخطط شمو الخشن (coarse grained shmoo plot) فوق منطقة القالب باستخدام مقادير مختلفة من جهود النبضات الكهرومغناطيسية (different magnitudes of EM pulse voltages).

بعد ذلك، تم إجراء مسح أكثر تفصيلاً بـدقة أعلى على المنطقة الحساسة المحددة في المسح الأول. تم استخدام أفضل موقع للمسبار (best probe location) (بناءً على عدد كبير من الأخطاء مع انحرافات معيارية منخفضة - low standard deviations) لجميع التجارب اللاحقة.

أشار التحليل الإضافي (further analysis) لـبرنامج كتابة الذاكرة إلى أن الخطأ (إعادة تعيين بت واحد - single bit reset) كان في الواقع مرتبطاً بـالجلب المسبق (prefetch) للتعليمة التي تلت كتابة الذاكرة، وتحديداً movlw، التي حملت قيمة بيانات فورية (immediate data value) في سجل عمل مؤقت (temporary working register)، وهو سجل w (w register).

تم تأكيد ذلك تجريبياً عن طريق إدراج عدة nops بين كتابة الذاكرة movlw (وتعديل إشارة المشغل وفقاً لذلك بحيث تحدث النبضة الكهرومغناطيسية أثناء الجلب المسبق لـ movlw). تم حقن الأخطاء إلى حد كبير بنجاح بالقرب من حافة دورة Q محددة (specific Q cycle edge) في مرحلة الجلب المسبق للتعليمة (instruction prefetch stage) (على الأرجح نهاية دورة Q4 بسبب تأخير نموذجي خارج الشريحة (typical off-chip delay) بمقدار 50 نانو ثانية [9]، مما يُفسد على الأرجح تحميل سجل التعليمات (instruction register load) أثناء بداية مرحلة التنفيذ التالية (start of following execution stage) [9]).

لسوء الحظ، لم يكن من الممكن التحقق من ذلك بما يتجاوز نتائجنا التجريبية حيث أنه من المعروف جيداً أن محتويات سجل التعليمات (contents of instruction register) غير متاحة.



صورة ا: مخططات المسح الأولي الواسع لعدد الجولات مع حقن أخطاء في تعليمة movlw 0x00 على سطح القالب باستخدام جهود نبضات كهرومغناطيسية 70 فولت (a)، 150 فولت (b)، و500 فولت (c).

نموذج قائم على الشحنة

لوحظ تجريبياً، على غرار [2]، أن حقن الأخطاء كان ممكناً فقط خلال نافذة توقيت محددة (specific timing window) بالقرب من حافة ساعة محددة (specific clock edge). ومع ذلك، على عكس [2]، عندما تم تقليل تردد الساعة (clock frequency)، لم يكن حقن الأخطاء ممكناً طوال دورة الس ضاعة (clock period). أشارت التجارب الإضافية إلى أن بعض ترددات الساعة المنخفضة يمكن أن تصبح عرضة لحقن الأخطاء فقط مع انخفاض مناسب في جهد التغذية Vdd، كما هو موضح في الجدول ا. لاحظ أن جميع التوليفات المستكشفة (explored combinations) من Vdd وتردد الساعة كانت تعمل بشكل كامل بدون حقن أخطاء.

تمثل التأخيرات (delays) في الأعمدة D1 إلى D4 من الجدول ا التأخير بين حافة الساعة المعنية (respective clock edge) والنبضة الكهرومغناطيسية. التأخير الموجب (positive delay) يعني أن النبضة الكهرومغناطيسية تحدث قبل حافة الساعة المحددة. على سبيل المثال، Dx هو التأخير بين النبضة الكهرومغناطيسية وحافة ساعة صاعدة أو هابطة x (rising or falling clock edge)، حيث x = 1,2,3,4 هي حواف هابطة، صاعدة، هابطة، صاعدة متتالية (consecutive) لساعة على التوالي (تمثل 1.5 دورة ساعة).

في الصف الأول من الجدول ا، النبضة الكهرومغناطيسية التي تحدث قبل 3.7 نانو ثانية من حافة الساعة الهابطة الأولى D1، تنتج خطأً عند 52 ميجاهرتز، 5 فولت (انظر العمود الأول). ومع ذلك، في الصف 2، عندما تحدث النبضة الكهرومغناطيسية مرة أخرى عند 3.7 نانو ثانية قبل نفس حافة الساعة الهابطة الأولى D1، لا يحدث خطأ عند 46.02 ميجاهرتز، 5 فولت. وبالمثل للصفوف الثلاثة التالية حيث النبضة الكهرومغناطيسية لها نفس مسافة التأخير (delay distance) من حواف الساعة الأخرى المسطرة (underlined)، مع ترددات الساعة الأبطأ لا يتم حقن خطأ عند 5 فولت.

بعد ذلك، لكل توقيت نبضة كهرومغناطيسية، تم تقليل جهد التغذية Vdd باستمرار بمقدار 0.1 فولت حتى يمكن حقن الخطأ، كما هو موضح في العمود الثاني من الجدول ا، مما يظهر تجريبياً أنه عند ترددات الساعة المنخفضة فقط مع جهد تغذية أقل يمكن حقن أخطاء كهرومغناطيسية.

يمكن الحصول على تفسير نظري محتمل (possible theoretical explanation) للسلوك المرصود من خلال فحص النموذج القائم على الشحنة (charge-based model). لنأخذ في الاعتبار عقدة دائرة (circuit node) والتي في ظروف التشغيل العادية (normal operating conditions) تشحن من '0' إلى '1'. عند 5 فولت مع ترددات ساعة أبطأ، يتم تراكم الحد الأقصى من الشحنة (maximum amount charge) على المكثف (capacitor) عند عقدة الدائرة.

على الرغم من أن النبضة الكهرومغناطيسية يمكنها تعديل الشحنة (عبر الضوضاء أو شبكة الطاقة-الخط الأرضي)، إلا أنها لا تستطيع تقليل قدر كافٍ من الشحنة من التراكم على العقدة للتسبب في حدوث '0' (عند التثبيت في قلاب - flipflop).

عند التشغيل بتردد ساعة عالٍ (مثل زيادة تردد التشغيل - overclocking) عند 5 فولت، يتم شحن المكثفات بنفس السرعة، ولكن لمدة دورة ساعة أقصر (shorter clock period duration)، وبالتالي يكون إجمالي الشحنة المتراكمة (total charge accumulated) على عقدة الدائرة أقل (وقد يكون فقط أعلى بقليل من العتبة للوصول إلى '1'، يُشار إليها أيضاً بإشارات التأرجح المنخفض - low swing signals).

عندما يتم تطبيق النبضات الكهرومغناطيسية على هذه العقدة، نظراً لأن المكثف غير مشحون بالكامل، فإن حقن النبضة الكهرومغناطيسية قادر على تعديل قدر كافٍ من الشحنة لتغيير قيمة البت، بحيث لا يتم الوصول إلى عتبة '1' وبالتالي يصبح البت '0'. مقدار إزاحة الشحنة (charge displacement) المطلوب لتغيير قيمة البت أقل بكثير من الحالة التي يتم فيها استخدام تردد ساعة أبطأ.

عندما يتم استخدام ترددات ساعة أبطأ مع انخفاض في Vdd، يتم شحن السعة (capacitance) بشكل أبطأ (بسبب انخفاض Vdd)، وبالتالي يكون لديها شحنة أقل في نهاية الدورة. وبالتالي عندما يتم تطبيق النبضة

الكهرومغناطيسية، مرة أخرى تحتاج شحنة أقل إلى التغيير من أجل منع البت من الوصول إلى '1' (عند التثبيت في flip-flop).

في الواقع، النموذج الموسع المقترح (proposed extended fault model) يعتمد على الحد الأدنى من الشحنة المطلوبة (minimum amount of charge required) لتغيير السلوك الطبيعي (normal behavior) للدائرة عند عقدة حساسة (sensitive node). غالباً ما يُشار إلى مقدار الشحنة هذا باسم الشحنة الحرجة (critical charge) في مجال الاضطرابات الناتجة عن حدث
واحد [4] (single event upsets).

عند ترددات الساعة المنخفضة مع انخفاض Vdd أو عند ترددات الساعة العالية، تكون الشحنة الحرجة أصغر وبالتالي تكون الدائرة أكثر عرضة لحقن الأخطاء الكهرومغناطيسية.

أخطاء استبدال التعليمات

يوضح الجدول II التعليمات الخاطئة المستبدلة (replaced faulty instructions) (العمود 2) التي استبدلت التعليمة المستهدفة (target instruction) (العمود 1) كنتيجة لحقن خطأ ناجح. تم استخدام إجمالي 340 جولة في تجارب الجدول II.

كان الوقت بين النبضة الكهرومغناطيسية ونهاية دورة Q المناسبة هو 15.23 نانو ثانية لجميع التعليمات باستثناء الصفين الأولين من الجدول اللذين استخدما تأخيرات 12.15 نانو ثانية و16 نانو ثانية.

على سبيل المثال، في الصف الأول، كانت التعليمة المستهدفة هي movlw 0x80 وكانت النبضة الكهرومغناطيسية على بُعد 12.15 نانو ثانية من نهاية دورة Q المناسبة. تسببت النبضة الكهرومغناطيسية في إعادة تعيين (reset) البت الأقل أهمية (least significant bit) من قيمة البيانات المشار إليها بواسطة سجل اختيار الملف (file select register) (العنوان غير المباشر - indirect address) (إلى 0).

التعليمة الوحيدة لتحقيق ذلك كانت bcf INDF,0. هذا غير مرتبط تماماً بوظيفة التعليمة المستهدفة (التي كانت تحميل القيمة 0x80 في سجل w)، وبالتالي يدعم بشكل أكبر فكرة أن الخطأ على الأرجح يؤثر على تحميل سجل التعليمات (load of instruction register).

بالنسبة لـتعليمة مستهدفة في تسلسل كود محدد (specific code sequence)، غالباً ما أدى تغيير طفيف (small variation) في توقيت النبضة الكهرومغناطيسية إلى تعليمات خاطئة مختلفة تماماً (quite different faulty instructions)، كما يظهر في الصفين 1 و2 من الجدول II.

TABLE I. FAULT INJECTION (FI) VS CLOCK FREQUENCY AND VDD

FI/5V	FI/Vdd	Clk.Freq (MHz)	Delay (ns)			
			D1	*D2*	*D3*	*D4*
Yes	Yes/5V	52	3.7	13.3	22.9	32.5
No	Yes/4.2V	46.02	3.7	14.6	25.4	36.3
No	Yes/4.2V	46.18	2.5	13.3	24.1	35
No	Yes/4.4V	46.33	1.3	12.1	22.9	33.7
No	Yes/4.4V	46.48	0.3	11	21.8	32.5

في الصفوف الأربعة الأخيرة حيث التعليمة المستهدفة هي xorwf 0x20, f، تم العثور على تعليمات خاطئة مختلفة مرة أخرى على الرغم من أن تأخير النبضة الكهرومغناطيسية بالنسبة لـ الجلب المسبق للتعليمة المستهدفة (prefetch of target instruction) كان نفسه.

في الحالتين a1 و a2، كانت التعليمة المستهدفة تقع في نفس العنوان (same address)، وتم استخدام نفس تسلسل الكود تماماً باستثناء التعليمات الثلاث الفورية (immediate 3 instructions) قبل التعليمة المستهدفة.

في الحالة a1، التعليمات الثلاث التي تسبق التعليمة المستهدفة هي 2 nop's و movf 0x30,w، بينما في الحالة a2 تسبق التعليمة المستهدفة تعليمات من نوع movf, xorwf,f و movf 0x30,w.

بالمثل، في الحالتين b1 و b2، تسبق التعليمة المستهدفة نفس التسلسلين كما في a1 و a2 على التوالي، ولكن هذا الكود مضمن (embedded) ضمن برنامج AES كامل (complete AES program)، وليس برنامج اختباري (test program).

في العمود الأخير من الجدول ١١، يمكن للمرء أن يرى أنه في جميع الحالات، باستثناء حالة واحدة، البتات أكثر احتمالاً لأن تُعاد تعيينها (reset) وليس تُعيّن (set). بعبارة أخرى، تأثير النبضة الكهرومغناطيسية على الأرجح هو التسبب في انتقال بتات كود العملية (opcode bits) من 1 إلى 0.

في جميع الحالات، بدا أن أكواد عمليات التعليمات الخاطئة (faulty instruction opcodes) غير مترابطة (uncorrelated) مع قيم أكواد العمليات من التعليمات السابقة (preceding instructions).

كشفت التجارب الإضافية أن الـ (address bits) ضمن كود العملية (عادةً b6..b0) أيضاً لم تكن عرضة لحقن الأخطاء (not susceptible to fault injection).

النبضات الكهرومغناطيسية السالبة (negative EM pulses) حقنت أخطاءً أيضاً ولكن فقط بعد زيادة التأخير إلى 25.23 نانو ثانية. تم أيضاً قياس تباين حقن الأخطاء (variance of fault injections)، مما يشير إلى أن الانحرافات المعيارية (standard deviations) كانت أقل من 2٪.

على سبيل المثال، في الصف 3 من الجدول ١١، حدثت تعليمة NOP المستبدلة (NOP replaced instruction) بنسبة 56.5٪ ± 2.8٪ (2 انحراف معياري). كان متوسط عدد النبضات الكهرومغناطيسية قبل حقن خطأ NOP الأول على الأقل نبضة كهرومغناطيسية واحدة وعلى الأكثر 11 نبضة كهرومغناطيسية.

هجوم على AES

تم استخدام كود AES الكامل (complete AES code) لشن هجوم حقن أخطاء (fault injection attack) لاسترجاع بايت مفتاح (AES key byte) AES. يفترض الهجوم أن النص المشفر الصحيح والخاطئ (correct and faulty ciphertext) متاح، لذا فإن المهاجم يعرف ما إذا كان قد تم حقن خطأ أم لا، ولكن النص العادي (plaintext) غير معروف (عشوائي).

تم استهداف التعليمة xorwf 0x20,f (w xor f=>f) من الجولة الأخيرة (last round)، والتي تحسب الـ OR الحصري (exclusive or) لـبايت المفتاح n (المخزن في سجل w) مع حالة AES (AES state) (المخزنة في البداية في الذاكرة عند العنوان f).

لاحظ أنه إذا حدثت التعليمة الخاطئة movwf 0x20 (w=>f)، فسيتم إخراج بايت المفتاح (k) n في بايت النص المشفر الخاطئ (faulty ciphertext byte). وإلا إذا حدثت التعليمة الخاطئة nop، فسيتم إخراج حالة AES (s) في بايت النص المشفر الخاطئ.

في هذه الحالة الأخيرة، ستكشف نتيجة الـ OR الحصري لهذا النص المشفر الخاطئ (s) مع النص المشفر الصحيح (= [s xor k]) عن بايت مفتاح ([s xor k] = s xor AES).

نظراً لأن أياً من التعليمتين الخاطئتين ستكشف عن بايت المفتاح، يحتفظ الهجوم بـقائمة من الأزواج (list of pairs)، واحد لكل حقن خطأ، حيث كل زوج هو [بايت-النص-المشفر-الخاطئ، OR-الحصري]. تنمو القائمة حتى يكون لدى زوجين إما نفس بايت النص المشفر الخاطئ أو نفس قيمة OR الحصري، وفي هذه الحالة يتم العثور على بايت المفتاح الصحيح المحتمل (potential correct key byte).

نشير إلى هذا على أنه بايت مفتاح صحيح محتمل نظراً لأنه لا يزال هناك احتمال صغير أن يتم العثور على مفتاح غير صحيح (حيث يوجد فقط 256 قيمة بايت ممكنة).

تم الحصول على نتائج تجريبية لـهجمات حقن الأخطاء على خوارزمية AES الكاملة التي تعمل على المعالج. باستخدام هذا الهجوم، من إجمالي 16 مفتاح AES مختلفاً، تم تحديد 11 مفتاحاً بشكل صحيح.

TABLE II. CODE SEQUENCE EFFECTS ON FAULT INJECTION AT 52MHZ

Target Instr	Statistics		
	Replaced faulty instruction	***Frequency Occurence***	***Opcode Bits reset[set]***
movlw 0x80 [d1]	*bcf INDF, 0*	98.4%	b13, b7
movlw 0x80 [d1]	*movwf INDF* *goto 0x80*	56.4% 42.3%	b13,b12 b12[b11]
xorwf 0x20,f [a1]	*iorwf 0x20,w* *NOP* *iorwf 0x20,f*	40.3% 57.9% 1.8%	b9,b7 b10,b9,b7 b9
xorwf 0x20,f [b1]	*subwf 0x20,f* *movwf 0x20*	65.8% 34.1%	b10 b10,b9
xorwf 0x20,f [a2]	*iorwf 0x20,w* *nop* *xorwf 0x20,w*	60% 35% 2.6%	b9,b7 b10,b9,b7 b7
xorwf 0x20,f [b2]	*iorwf 0x20,f*	98.7%	b9

[d1] Delay of 12.15ns and 16ns for 1st/2nd row. [a1,a2,b1,b2] Instruction embedded within diff. code seq.

تراوح عدد النبضات الكهرومغناطيسية المطلوبة للحصول على مفتاح AES واحد 128 بت صحيح من 134 إلى 453، بمتوسط 222 وانحراف معياري 81.

أشارت الإحصائيات الموضحة في الجدول II الصفين b1 و b2 إلى أنه ربما مع تطبيق مختلف لـ AES، قد تكون التعليمة الخاطئة للـ xorwf 0x20,f المستهدفة أيضاً iorwf 0x20,f بتردد 98.7٪.

في هذه الحالة، سيكون هجوم AES ممكناً أيضاً، من خلال مراقبة النص المشفر الخاطئ (monitoring faulty ciphertext) الناتج من تنفيذ نصوص عادية مختلفة (executing different plaintexts)، وتسجيل بتات (recording bits) بايت النص المشفر المستهدف التي تصبح '0'.

في كلتا حالتي الهجوم وعلى عكس الأبحاث السابقة، لا يفترض الهجوم أن نموذج الخطأ (fault model) هو قلب بت (bit flip)، أو بايت/كلمة عشوائية (random byte/word)، أو تخطي تعليمة (instruction skip).

النقاشات والاستنتاجات

من المعروف جيداً أنه مع تقدم التقنيات (technologies progress)، تنخفض أيضاً الشحنة الحرجة (critical charge). وبالتالي، من الممكن أن النبضة الكهرومغناطيسية لم تكن قوية بما يكفي لـإزاحة الشحنة الحرجة الأكبر عند ترددات الساعة الأبطأ (slower clock frequencies).

تبين أن تعليمة xorwf,f المبحوثة في هذه الورقة لها تأثير كبير (significant impact) على تطبيق أمان AES (AES security application). على الرغم من أن الأبحاث السابقة لاحظت ظهور بايت المفتاح في النص المشفر الخاطئ، إلا أن 2 فقط من أصل 16 بايت مفتاح كان لديهم هذا النوع من الخطأ [1]، وخوارزمية الهجوم المقترحة (suggested attack algorithm) لم تتضمن التعامل مع (handling) التعليمة الخاطئة nop.

في القسم III.D، تم تنفيذ هجوم كامل (complete attack) على بايت مفتاح AES في تطبيق حقيقي لـ AES (real implementation of AES). نظراً لأن عدد النصوص العادية المطلوبة (number of plaintexts required) كان منخفضاً للغاية (extremely low)، من المتوقع أنه مع جهد نبضة كهرومغناطيسية أعلى (higher EM pulse voltage) أو توقيت نبضة كهرومغناطيسية أكثر دقة (more accurate EM pulse timing)، قد يتم تقليل عدد النبضات الكهرومغناطيسية المستخدمة في الهجوم بشكل أكبر (further).

من المحتمل أيضاً استغلال (exploited) الهجمات باستخدام حقن أخطاء في تعليمات أخرى (other instructions)، مثل تعليمة movlw، في تطبيقات (applications) مثل الإقلاع الآمن (secure boot) حيث يمكن لـالتعليمة الخاطئة المقابلة goto (الصف الثاني من الجدول II) أن تتخطى فحوصات المصادقة (skip authentication checks) أثناء الإقلاع الآمن.

لأول مرة، يتم تقديم نموذج أخطاء موسع قائم على الشحنة (extended charge-based fault model) لـحقن الأخطاء الكهرومغناطيسية من الجانب الخلفي (backside EMFI) والتحقق منه تجريبياً (validated empirically). على عكس الأبحاث السابقة، يظهر أن الجانب الخلفي للدائرة المتكاملة (IC backside) عرضة للغاية (very susceptible) لـحقن الأخطاء الكهرومغناطيسية الموضعية والقابلة للتكرار (localized and repeatable EM fault injection).

لأول مرة، تم إظهار أنه يمكن مهاجمة تطبيق حقيقي لـ AES (real implementation of AES) بـطريقة بسيطة (simple manner). هذا البحث مهم (important) لـتحسين المرونة (improving resilience) والتدابير المضادة (countermeasures) لـهجمات حقن الأخطاء التي تعتبر حاسمة (critical) لـمنع هجمات حقن الأخطاء الكهرومغناطيسية المستقبلية (preventing future EM fault injection attacks).

يود المؤلفون شكر مصطفى فرج (Mustafa Faraj) على النقاشات المفيدة وتطوير بعض الأدوات (development of some tools) المستخدمة في هذه التجارب. يتم دعم البحث بتمويل جزئي (funding in part) من منح (grants) من NSERC XtremeEDAg.

المراجع

[1] A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria, "Electromagnetic transient faults injection on a hardware and a software implementations of AES," in Fault Diagnosis and Tolerance in Cryptography (FDTC), 2012 Workshop on, pp. 7-15, IEEE, 2012.

[2] S. Ordas, L. Guillaume-Sage, and P. Maurine, "Electromagnetic fault injection: the curse of flip-flops," Jnl of Crypt Eng, pp. 1-15, 2016.

[3] N. Moro, et al., "Electromagnetic fault injection: towards a fault model on a 32-bit microcontroller," in FDTC 2013, pp. 77-88, IEEE, 2013.

[4] P. Shivakumar, M. Kistler, S. W. Keckler, D. Burger and L. Alvisi, "Modeling the effect of technology trends on the soft error rate of combinational logic," Proc. Intl Conf on Dependable Sys and Networks, Washington, DC, USA, 2002, pp. 389-398.

[5] A. Barenghi et al., "Low Voltage Fault Attacks to AES and RSA on General Purpose Processors," eprint iacr 130/2010, 2010.

[6] P. Rauzy, S. Guilley, "A formal proof of countermeasures against fault injection attacks on CRT-RSA," eprint IACR 506/2013, 2013.

[7] K. Tobich, et al., "Voltage spikes on the substrate to obtain timing faults," Proc. of the 16th Euromicro Conf. on Dig. Sys. Des., 2013.

[8] P. Maurine, "Techniques for EM Fault Injection: Equipments and experimental results," in FDTC 2012, Belgium, 2012, pp. 3-4.

[9] Microchip, "PIC16F631/677/685/687/689/690 20-pin flash-based, 8-bit CMOS microcontrollers," DS40001262F Microchip, 2015.

[10] A. Barenghi et al., "Countermeasures against fault attacks on software implemented AES," Proc. of WESS 2010, ACM, 2010, pp. 1-10.

[11] N. Moro et al., "Experimental evaluation of two software countermeasures against fault attacks," IEEE Proc. of HOST 2014, 2014.

[12] EMV Langer Burst power station 202 and ICI HH500-15 LEFT pulse magnetic field source EM probe, http://www.langer-emv.de

[13] L. Riviere et al., "High precision fault injections on the instruction cache of ARMv7-M architectures," IEEE HOST 2015.

[14] A. Cui, R. Housley, "BADFET: Defeating modern secure boot using second-order pulsed electromagnetic fault injection," Usenix workshop on offensive technologies, WOOT, 2017.

[15] M. Ghodrati, "Thwarting electromagnetic fault injection attack utilizing timing attack countermeasure," MASc Thesis, Advisor P. Schaumont, Dec 2017.

[16] A. Boyer et al., "Evaluation of the Near-Field Injection Method at integrated circuit level," EMC Europe 2014, 2014, pp. 1-6.

[17] N. Timmers, A. Spruyt, M. Witteman, "Controlling PC on ARM using fault injection," in Fault Diagnosis and Tolerance in Cryptography (FDTC), 2016 Workshop on, IEEE, 2016.

إضافات المترجم

إضافة ١

اللي نفهمه من هنا محتاجين كام نبضة كهرومغناطيسية عشان نكسر التشفير؟ ودة يحدد مقياس صعوبة الهجوم نفسه. الفكرة الأساسية هنا هي إنه لو المفتاح تم استخدامه مرات كتير جداً، الهاكر هياخد فرص أكتر إنه يجمع بيانات كافية ويقدر يكسر المفتاح. خلينا ناخد مثال عملي عشان الموضوع يبقى أوضح. لو المفتاح استخدم 10,000 مرة والهاكر محتاج 5,000 نبضة عشان يكسره، يبقى المفتاح ده في خطر حقيقي لأن الهاكر عنده فرصة كبيرة إنه ينجح في الهجوم. الحل الأمني هنا هو إنك لازم تغيّر المفتاح قبل ما يوصل لعدد الاستخدامات اللي بتساوي x ضرب y، وبكده تحمي النظام من الاختراق.

عندنا متغيرين مهمين في الموضوع. المتغير الأول هو x واللي بيمثل عدد الأخطاء اللي محتاجها عشان أكشف المفتاح السري كامل. مثلاً لو عايز تكسر خوارزمية AES، ممكن تحتاج حوالي 5 أخطاء ناجحة عشان تطلع المفتاح الكامل. المتغير التاني هو y واللي بيمثل عدد النبضات الكهرومغناطيسية اللي بضربها قبل ما أنجح في حقن خطأ واحد مفيد. يعني مثلاً ممكن تضرب 1000 نبضة قبل ما تنجح في حقن خطأ واحد يفيدك في الهجوم. بناءً على كده، عدد النبضات الكلي اللي محتاجه عشان أكسر المفتاح هيكون x ضرب y. في المثال اللي قلناه، ده معناه 5 ضرب 1000 يساوي 5000 نبضة محتاجها عشان أكسر المفتاح بالكامل.

النبضة الكهرومغناطيسية هي موجة كهرومغناطيسية قوية جداً ومركزة بتنطلق لفترة زمنية قصيرة جداً، زي البرق بالظبط لكن أصغر بكتير ومتحكم فيه. الموجة دي بتحمل طاقة كهربائية ومغناطيسية في نفس الوقت.
الهاكر بيستخدم جهاز خاص اسمه EM Pulse Generator (مولد النبضات الكهرومغناطيسية). الجهاز ده شكله زي مسدس صغير أو عصاية فيها ملف نحاسي في الطرف. لما تشغله، بيطلق نبضة كهرومغناطيسية قوية جداً لمدة جزء من المليون من الثانية.

خاتمة الترجمة

ترجمة: محمد سيد من مكتبة قرطبة.

تم الترجمة بحمد الله في يناير ٢٠٢٦ - النسخة الاولى.

إذا استفدت من هذه الترجمة:

- شارك المعرفة مع الآخرين
- ساهم في تطوير المحتوى العربي
- استخدم المعلومات بمسؤولية وأخلاقية