تحليل اختلافات القدرة الكهربائية

Paul Kocher, Joshua Jae, and Benjamin Jun
Cryptography Research, Inc.
607 Market Street, 5th Floor
San Francisco, CA 94105, USA.
http://www.cryptography.com
E-mail: {fpaul,josh,beng}@cryptography.com.

ملخص الورقة البحثية

غالباً ما يفترض مصممو الأنظمة التشفيرية أن الأسرار سيتم التعامل معها في بيئات حوسبة مغلقة وموثوقة. لسوء الحظ، أجهزة الكمبيوتر والشرائح الدقيقة الفعلية تسرب معلومات حول العمليات التي تعالجها. تفحص هذه الورقة طرقاً محددة لتحليل قياسات استهلاك الطاقة للعثور على مفاتيح سرية من الأجهزة المقاومة للعبث. نناقش أيضاً أساليب لبناء أنظمة تشفيرية يمكنها العمل بشكل آمن في المكونات المادية الموجودة التي تسرب المعلومات.

الكلمات المفتاحية: تحليل الطاقة التفاضلي (differential power analysis)، DPA، SPA، تحليل التشفير (cryptanalysis)، DES

الخلفية

الهجمات التي تشمل أجزاء متعددة من نظام الأمان يصعب التنبؤ بها ونمذجتها. إذا لم يفهم مصممو الشفرات ومطورو البرمجيات ومهندسو المكونات المادية أو يراجعوا عمل بعضهم البعض، فقد تكون الافتراضات الأمنية المتخذة على كل مستوى من مستويات تصميم النظام غير مكتملة أو غير واقعية. ونتيجة لذلك، غالباً ما تتضمن أخطاء الأمان تفاعلات غير متوقعة بين المكونات المصممة من قبل أشخاص مختلفين.

تم تصميم العديد من التقنيات لاختبار الخوارزميات التشفيرية بشكل منعزل. على سبيل المثال، يمكن لتحليل التشفير التفاضلي [3] (differential cryptanalysis) وتحليل التشفير الخطي [8] (linear cryptanalysis) استغلال خصائص إحصائية صغيرة للغاية في مدخلات ومخرجات الشفرة (cipher's inputs and outputs). تمت دراسة هذه الأساليب جيداً لأنها يمكن تطبيقها بتحليل جزء واحد فقط من بنية النظام (system's architecture) - البنية الرياضية للخوارزمية.

التنفيذ الصحيح لبروتوكول قوي ليس آمناً بالضرورة. على سبيل المثال، يمكن أن يحدث فشل بسبب العمليات الحسابية المعيبة [5, 4] (defective computations) والمعلومات المسربة أثناء عمليات المفتاح السري.

تم إثبات الهجمات باستخدام معلومات التوقيت [7, 11] بالإضافة إلى البيانات المجمعة باستخدام تقنيات القياس الاختراقية[2,1] . استثمرت حكومة الولايات المتحدة موارد كبيرة في برنامج TEMPEST السري لمنع تسرب المعلومات الحساسة من خلال الانبعاثات الكهرومغناطيسية.

مقدمة في تحليل الطاقة

يتم تنفيذ معظم الأجهزة التشفيرية الحديثة باستخدام بوابات منطقية من أشباه الموصلات، والتي يتم بناؤها من الترانزستورات. تتدفق الإلكترونات عبر الركيزة السيليكونية عندما يتم تطبيق شحنة على (أو إزالتها من) بوابة الترانزستور، مما يستهلك طاقة وينتج إشعاعاً كهرومغناطيسياً.

لقياس استهلاك الطاقة للدائرة، يتم إدراج مقاوم صغير (مثل 50 أوم) على التوالي مع مدخل الطاقة أو الأرضي. فرق الجهد عبر المقاوم مقسوماً على المقاومة يعطي التيار.

المختبرات الإلكترونية المجهزة جيداً لديها معدات يمكنها أخذ عينات رقمية من فروق الجهد بمعدلات عالية بشكل استثنائي (أكثر من 1 جيجاهرتز) بدقة ممتازة (أقل من 1٪ خطأ). يمكن شراء أجهزة قادرة على أخذ العينات بسرعة 20 ميجاهرتز أو أسرع ونقل البيانات إلى الكمبيوتر مقابل أقل من 400 دولار [6].

تحليل الطاقة البسيط (Simple Power Analysis - SPA) هو تقنية تتضمن تفسير قياسات استهلاك الطاقة مباشرة التي يتم جمعها أثناء العمليات التشفيرية. يمكن لـ SPA أن يعطي معلومات عن تشغيل الجهاز بالإضافة إلى مادة المفتاح.

ملاحظة من المترجم: تحليل الطاقة البسيط (SPA) يعتمد على قياس الكهرباء التي يستهلكها الجهاز أثناء التشفير، حيث إن العمليات المختلفة تستهلك كميات مختلفة من الطاقة، مما يكشف عن المفاتيح السرية. (انتهى)

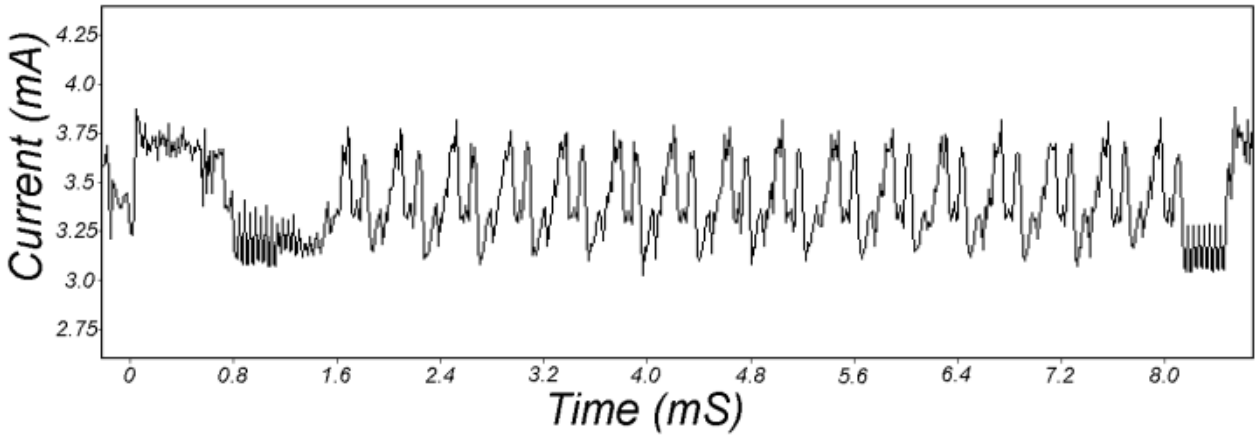

Figure 1: SPA trace showing an entire DES operation.

يشير القياس (trace) إلى مجموعة من قياسات استهلاك الطاقة المأخوذة عبر عملية تشفيرية. على سبيل المثال، عملية مدتها 1 ميلي ثانية بمعدل أخذ عينات 5 ميجاهرتز تعطي قياساً يحتوي على 5000 نقطة. يظهر الشكل 1 قياس SPA من بطاقة ذكية نموذجية (typical smart card) أثناء تنفيذ عملية DES. لاحظ أن جولات DES الـ 16 (16 DES rounds) واضحة جداً.

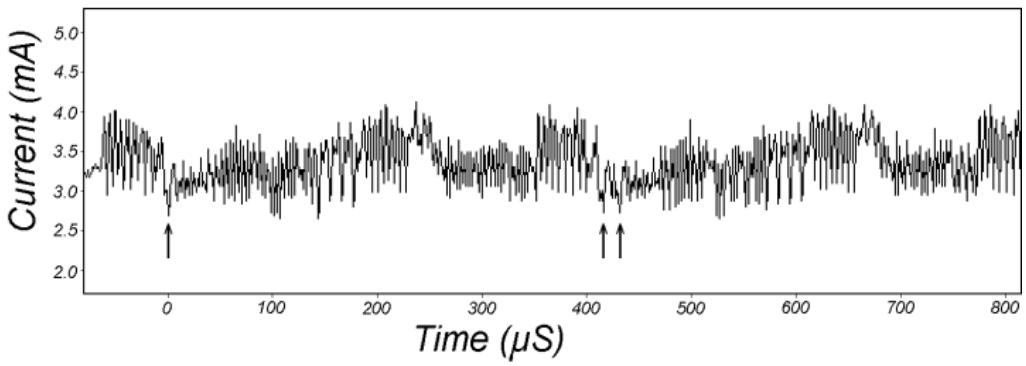

Figure 2: SPA trace showing DES rounds 2 and 3.

الشكل 2 هو عرض أكثر تفصيلاً لنفس القياس يوضح الجولة الثانية والثالثة من عملية تشفير DES. العديد من تفاصيل عملية DES مرئية الآن. على سبيل المثال، يتم تدوير سجلات مفتاح DES بـ 28 بت C وD مرة واحدة في الجولة 2 (السهم الأيسر) ومرتين في الجولة 3 (الأسهم اليمنى).

في الشكل 2، يمكن إدراك اختلافات صغيرة بين الجولات. العديد من هذه الميزات المميزة هي نقاط ضعف SPA (SPA weaknesses) ناتجة عن قفزات شرطية (conditional jumps) بناءً على خانات المفتاح (key bits) والنتائج الحسابية الوسيطة (computational intermediates).

يوضح الشكل 3 عروضاً بدقة أعلى للقياس توضح استهلاك الطاقة عبر منطقتين، كل منهما من سبع دورات (seven clock cycles) عند 3.5714 ميجاهرتز. تنتج الاختلافات المرئية بين دورات الساعة بشكل أساسي من اختلافات في استهلاك الطاقة لتعليمات المعالج الدقيق المختلفة.

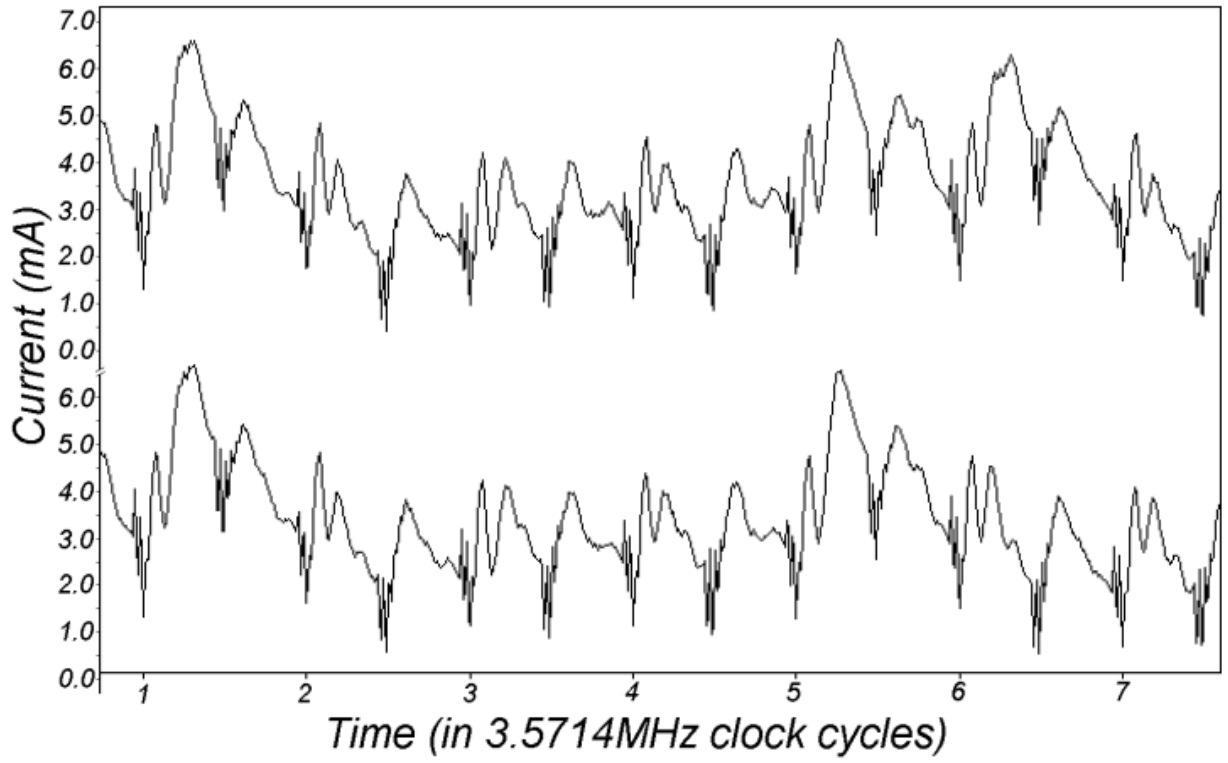

Figure 3: SPA trace showing individual clock cycles.

يُظهر القياس العلوي في الشكل 3 مسار التنفيذ عبر ميزة SPA حيث يتم تنفيذ تعليمة قفز (jump instruction)، ويظهر القياس السفلي حالة لا يتم فيها القفز. نقطة الاختلاف عند دورة الساعة 6 وواضحة جداً.

نظراً لأن SPA يمكنه الكشف عن تسلسل التعليمات المنفذة، يمكن استخدامه لكسر التطبيقات التشفيرية التي يعتمد فيها مسار التنفيذ على البيانات التي يتم معالجتها. على سبيل المثال:

جدولة مفتاح (DES (DES key schedule: تتضمن عملية حساب جدولة مفتاح DES تدوير سجلات المفتاح بـ28 بت. عادةً ما يُستخدم فرع شرطي (conditional branch) للتحقق من الـ bit المُزاح (shifted off) من النهاية بحيث يمكن لف الـ bits "1". ستحتوي قياسات استهلاك الطاقة الناتجة لـ bit "1" و bit "0" على ميزات SPA مختلفة إذا اتخذت مسارات التنفيذ فروعاً مختلفة لكل منهما.

تبديلات (DES (DES permutations: تُنفذ تطبيقات DES مجموعة متنوعة من تبديلات الـbits (bit permutations). يمكن أن يتسبب التفريع الشرطي (conditional branching) في البرمجيات أو الكود الدقيق (software or microcode) في اختلافات كبيرة في استهلاك الطاقة لبتات (bits) "0" و"1".

المقارنات (Comparisons): عادةً ما تنفذ عمليات مقارنة السلاسل أو الذاكرة فرعاً شرطياً عند العثور على عدم تطابق (mismatch). يتسبب هذا التفريع الشرطي في خصائص SPA كبيرة (وأحياناً توقيت).

المضاعفات (Multipliers): تميل دوائر الضرب المعياري (modular multiplication circuits) إلى تسريب قدر كبير من المعلومات حول البيانات التي تعالجها. تعتمد دوالّ التسريب على تصميم المضاعف (multiplier)، ولكنها غالباً ما ترتبط بشدة بقيم المعاملات (operand values) وأوزان هامينغ (Hamming weights).

الـ (**Exponentiators**): تقوم دالة الأُس المعياري البسيطة (modular exponentiation) بالمسح عبر الأس، وتنفذ عملية تربيع في كل تكرار مع عملية ضرب إضافية لكل bit من الأُس يساوي "1". يمكن اختراق الأس إذا كانت عمليات التربيع والضرب لها خصائص استهلاك طاقة مختلفة، أو تستغرق أوقاتاً مختلفة، أو مفصولة بكود مختلف. قد يكون لدوالّ الأس النمطي التي تعمل على بتين (2 bits) أو أكثر من الأس في وقت واحد دوالّ تسريب أكثر تعقيداً.

منع الـ SPA

بشكل عام، تقنيات منع تحليل الطاقة البسيط بسيطة إلى حد ما في التنفيذ. تجنب الإجراءات التي تستخدم نتائج وسيطة سرية أو مفاتيح في عمليات التفريع الشرطي سيخفي العديد من خصائص SPA.

في حالات مثل الخوارزميات التي تفترض التفريع (branching) بطبيعتها، قد يتطلب هذا برمجة إبداعية (creative coding) ويؤدي إلى انخفاض كبير في الأداء.

أيضاً، الكود الدقيق (microcode) في بعض المعالجات الدقيقة (microprocessors) يتسبب في ميزات استهلاك طاقة كبيرة تعتمد على المعاملات. بالنسبة لهذه الأنظمة، حتى كود مسار التنفيذ الثابت يمكن أن يكون له نقاط ضعف SPA خطيرة.

معظم (ولكن ليس كل) التطبيقات المادية السلكية الثابتة (hard-wired hardware implementations) لخوارزميات التشفير المتماثل (symmetric cryptographic algorithms) لديها اختلافات استهلاك طاقة صغيرة بما فيه الكفاية بحيث لا يعطي SPA الـ (key material).

تحليل الطاقة التفاضلي لتطبيقات DES

بالإضافة إلى الاختلافات الكبيرة في الطاقة بسبب تسلسل التعليمات (instruction)، هناك تأثيرات مرتبطة بقيم البيانات التي يتم التعامل معها. تميل هذه الاختلافات إلى أن تكون أصغر وأحياناً تُطغى عليها أخطاء القياس والضوضاء الأخرى (noise). في مثل هذه الحالات، لا يزال من الممكن في كثير من الأحيان كسر النظام باستخدام دوال إحصائية مُصممة خصيصاً للخوارزمية المستهدفة.

ملاحظة من المترجم: تحليل الطاقة التفاضلي (DPA) يعتمد على تحليل آلاف القياسات لاستهلاك الكهرباء. الفكرة إن المهاجم بيقارن متوسط الطاقة لما بت معين يكون "0" مع متوسط الطاقة لما نفس البت يكون "1"، والفرق بين الاتنين بيكشف المفتاح السري. (انتهى)

نظراً لاستخدامه الواسع النطاق، سيتم فحص معيار تشفير البيانات (Data Encryption Standard - DES) بالتفصيل.

في كل من الجولات الـ16 (16 rounds)، تنفذ خوارزمية تشفير DES ثماني عمليات بحث في صندوق الاستبدال S. تأخذ صناديق S الثمانية (8 S boxes) كمدخل مفتاح ستة بتات مع عملية XOR مع ستة بتات من السجل (register) R وتنتج أربعة بتات. يتم إعادة ترتيب بتات الخارجة الـ32 من S وإجراء XOR معها على L. ثم يتم تبديل النصفين L و R. (للحصول على وصف تفصيلي لخوارزمية DES، انظر [9].)

يتم تعريف دالة اختيار DPA (DPA selection function) D(C, b, Ks) على أنها حساب قيمة البت 32 > b => 0 من النتيجة الوسيطة L في DES (DES intermediate L) في بداية الجولة 16 للنص المشفر C (ciphertext C)، حيث يتم تمثيل بتات المفتاح الستة (6 key bits) الداخلة إلى صندوق S المقابل للبت b بواسطة 2^6 > Ks => 0. لاحظ أنه إذا كان Ks غير صحيح، فإن تقييم D(C, b, Ks) سيعطي القيمة الصحيحة للبت b باحتمال 1/2 ≈ P لكل نص مشفر.

لتنفيذ هجوم DPA، يراقب المهاجم أولاً m عملية تشفير ويلتقط قياسات طاقة T1 m[1...k] تحتوي على k عينة لكل منها. بالإضافة إلى ذلك، يسجل المهاجم النصوص المشفرة C1..m. لا حاجة لمعرفة النص غير المشفر.

يستخدم تحليل DPA قياسات استهلاك الطاقة لتحديد ما إذا كان تخمين كتلة المفتاح Ks صحيحاً. يحسب المهاجم منحنى الفرق بعينة k Δ[1..k] عن طريق إيجاد الفرق بين متوسط القياسات التي يكون فيها D(C, b, Ks) يساوي واحد ومتوسط القياسات التي يكون فيها D(C, b, Ks) يساوي صفر.

وبالتالي، Δ[j] هو المتوسط على C1..m للتأثير بسبب القيمة الممثلة بدالة الاختيار D على قياسات استهلاك الطاقة عند النقطة j، على وجه الخصوص

$$\begin{aligned}\Delta_D[j] &= \frac{\sum_{i=1}^{m} D(C_i, b, K_s)\mathbf{T}_i[j]}{\sum_{i=1}^{m} D(C_i, b, K_s)} - \frac{\sum_{i=1}^{m} (1 - D(C_i, b, K_s))\,\mathbf{T}_i[j]}{\sum_{i=1}^{m} (1 - D(C_i, b, K_s))} \\ &\approx 2\left(\frac{\sum_{i=1}^{m} D(C_i, b, K_s)\mathbf{T}_i[j]}{\sum_{i=1}^{m} D(C_i, b, K_s)} - \frac{\sum_{i=1}^{m} \mathbf{T}_i[j]}{m}\right).\end{aligned}$$

إذا كان Ks غير صحيح، فإن البت المحسوب باستخدام D سيختلف عن البت المستهدف الفعلي لحوالي نصف النصوص المشفرة Ci. وبالتالي فإن دالة الاختيار D(Ci, b, Ks) غير مرتبطة فعلياً بما تم حسابه فعلياً بواسطة الجهاز المستهدف.

إذا تم استخدام دالة عشوائية لتقسيم مجموعة إلى مجموعتين فرعيتين، فإن الفرق في متوسطات المجموعات الفرعية يجب أن يقترب من الصفر مع اقتراب أحجام المجموعات الفرعية من اللانهاية. وبالتالي، إذا كان Ks غير صحيح،

$$\lim_{m \to \infty} \Delta_D[j] \approx 0$$

لأن مكونات القياس غير المرتبطة بـ D ستتضاءل مع √(m/1)، مما يتسبب في أن يصبح القياس التفاضلي مسطحاً. (قد لا يكون القياس الفعلي مسطحاً تماماً، لأن دالة الاختيار D عند استخدام Ks خاطئ قد يكون لها ارتباط ضعيف مع دالة الاختيار D عند استخدام Ks الصحيح، مما يُظهر بعض التذبذبات الطفيفة في المنحنى.)

ومع ذلك، إذا كان Ks صحيحاً، فإن القيمة المحسوبة لـ D(Ci, b, Ks) ستساوي القيمة الفعلية للبت المستهدف b باحتمال 1. وبالتالي فإن دالة الاختيار مرتبطة بقيمة البت الذي يتم التعامل معه في الجولة 16.

ونتيجة لذلك، يقترب Δ[j] من تأثير البت المستهدف على استهلاك الطاقة مع m → ∞. قيم البيانات الأخرى وأخطاء القياس وما إلى ذلك التي لا ترتبط بـ D تقترب من الصفر. نظراً لأن استهلاك الطاقة مرتبط بقيم بتات البيانات، فإن رسم Δ سيكون مسطحاً مع قمم (spikes) في المناطق التي يرتبط فيها D بالقيم التي يتم معالجتها.

وبالتالي يمكن تحديد القيمة الصحيحة لـ Ks من القمم (spikes) في قياسها التفاضلي. تتوافق أربع قيم من b مع كل صندوق S، مما يوفر تأكيداً لتخمينات المفتاح. العثور على جميع Ks الثمانية يعطي المفتاح الفرعي للجولة الكامل 48 بت (entire 48-bit round subkey). يمكن العثور على بتات المفتاح الثمانية المتبقية بسهولة باستخدام البحث الشامل أو بتحليل جولة إضافية واحدة.

يمكن العثور على مفاتيح Triple DES بتحليل عملية DES الخارجية أولاً، واستخدام المفتاح الناتج لفك تشفير النصوص المشفرة، ومهاجمة مفتاح DES التالي. يمكن لـ DPA استخدام نص عادي (plaintext) معروف أو نص مشفر معروف ويمكنه العثور على مفاتيح التشفير أو فك التشفير.

يوضح الشكل 4 أربع قياسات تم إعدادها باستخدام نصوص عادية معروفة تدخل دالة تشفير DES على بطاقة ذكية أخرى. في الأعلى يوجد قياس الطاقة المرجعي الذي يوضح متوسط استهلاك الطاقة أثناء عمليات DES.

في الأسفل توجد ثلاث قياسات تفاضلية، حيث تم إنتاج الأول باستخدام تخمين صحيح لـ Ks. تم إنتاج القياسين السفليين باستخدام قيم غير صحيحة لـ Ks. تم إعداد هذه القياسات باستخدام 1000 عينة (m = 10^3). على الرغم من أن الإشارة واضحة جداً في القياس التفاضلي، إلا أن هناك قدراً متواضعاً من الضوضاء (noise).

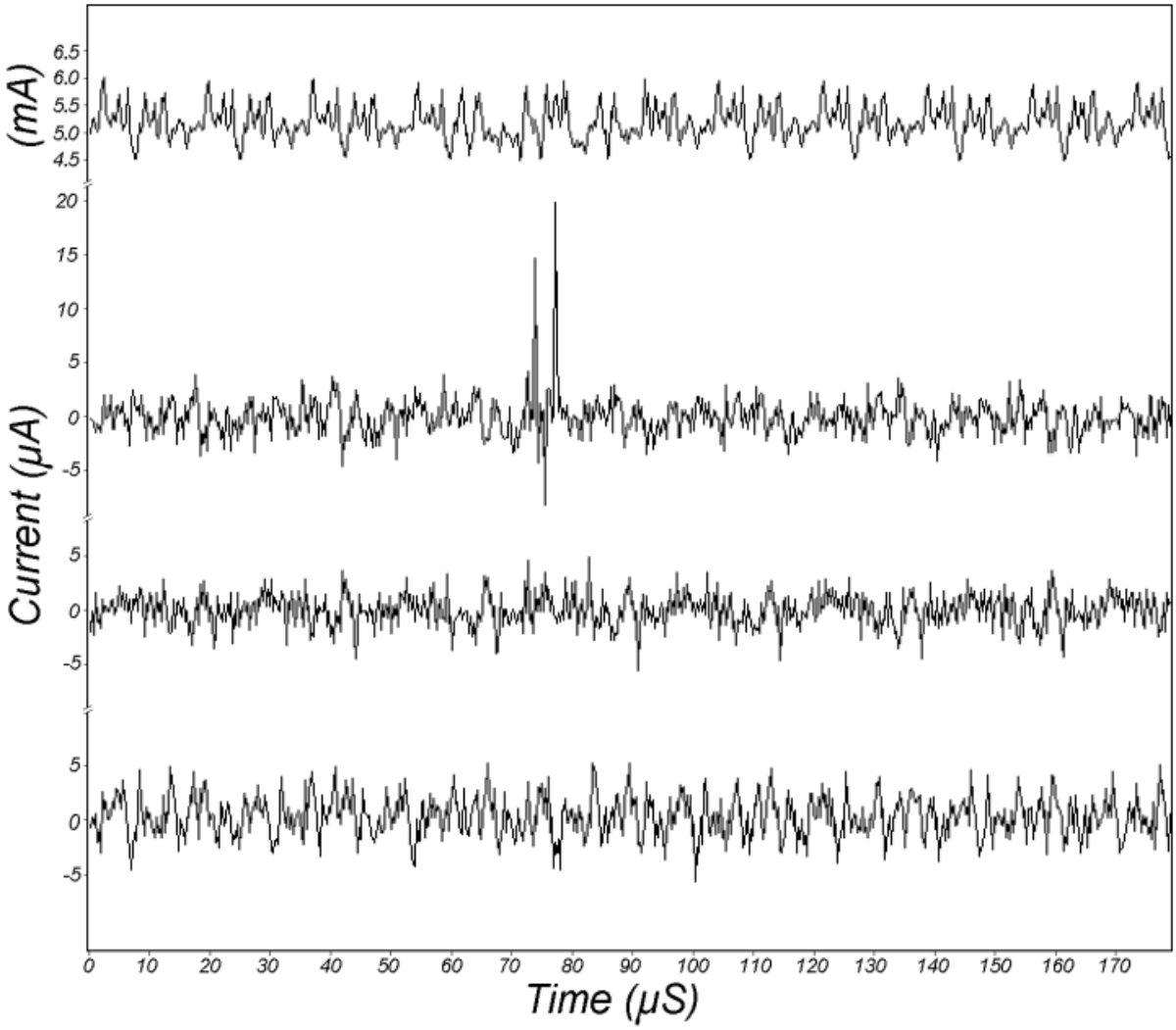

Figure 4: DPA traces, one correct and two incorrect, with power reference.

يوضح الشكل 5 متوسط تأثير بت واحد على قياسات استهلاك الطاقة التفصيلية. في الأعلى يوجد قياس استهلاك الطاقة المرجعي. يُظهر القياس الأوسط الانحراف المعياري في قياسات استهلاك الطاقة. أخيراً، يُظهر القياس السفلي قياساً تفاضلياً تم إعداده بـ m = 10^4. لاحظ أن المناطق غير المرتبطة بالبت أقرب إلى الصفر بأكثر من رتبة من حيث الحجم، مما يشير إلى بقاء القليل من الضوضاء أو الخطأ.

حجم خاصية (characteristic) الـ DPA حوالي 40 ميكروأمبير، وهو أقل عدة مرات من الانحراف المعياري الملاحظ عند تلك النقطة. الارتفاع في الانحراف المعياري عند دورة الساعة 6 (clock cycle 6) الذي يتزامن مع خاصية قوية يشير

إلى أن قيمة المعامل لها تأثير كبير على استهلاك طاقة التعليمة وأن هناك تبايناً كبيراً في قيم المعاملات التي يتم التعامل معها.

نظراً لأن التعليمات منخفضة المستوى غالباً ما تتعامل مع عدة خانات (bits)، يمكن لدالة الاختيار أن تختار في وقت واحد قيم خانات متعددة (multiple bits). تميل خصائص DPA الناتجة إلى أن يكون لها قمم أكبر (larger peaks)، ولكن ليس بالضرورة أن يكون لها نسب إشارة إلى ضوضاء أفضل لأن عدداً أقل من العينات يتم تضمينها في حساب المتوسط.

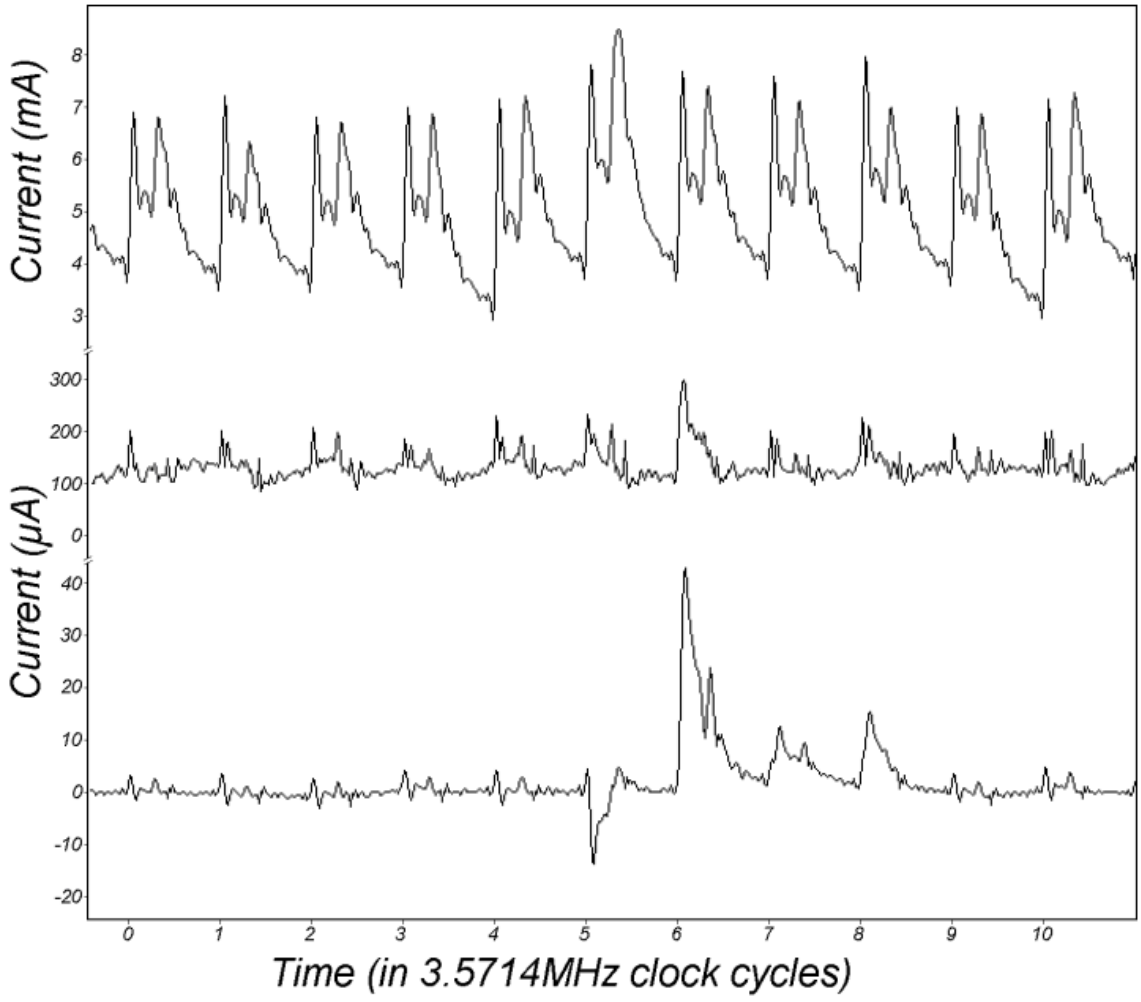

Figure 5: Quantitative DPA measurements

تُدخل عدة مصادر ضوضاء في قياسات DPA، بما في ذلك الإشعاع الكهرومغناطيسي والضوضاء الحرارية. يمكن أن تتسبب أخطاء التكميم (quantization errors) بسبب عدم تطابق ساعات الجهاز وساعات العينات في أخطاء إضافية. أخيراً، يمكن أن يُدخل عدم التوافق الزمني غير المصحح للقياسات قدراً كبيراً من الضوضاء في القياسات.

يمكن تطبيق العديد من التحسينات على عمليات جمع البيانات وتحليل الـ DPA لتقليل عدد العينات المطلوبة أو للتحايل على التدابير المضادة.

على سبيل المثال، من المفيد تصحيح تباين القياس، مما يعطي أهمية الاختلافات بدلاً من حجمها. أحد الأشكال المختلفة لهذا النهج، DPA النموذجي الآلي، يمكنه العثور على مفاتيح DES باستخدام أقل من 15 قياساً من معظم البطاقات الذكية. يمكن أيضاً استخدام دوال اختيار أكثر تطوراً. ذات أهمية خاصة هي دوال DPA من رتبة أعلى التي تجمع عينات متعددة من داخل القياس.

يمكن أيضاً لدوال الاختيار تعيين أوزان مختلفة لقياسات مختلفة أو تقسيم القياسات إلى أكثر من فئتين. يمكن لمثل هذه الدوال التغلب علي العديد من التدابير المضادة، أو مهاجمة الأنظمة حيث تتوفر معلومات جزئية أو لا تتوفر معلومات عن النصوص العادية أو النصوص المشفرة. يكون تحليل البيانات باستخدام دوال غير حساب المتوسط العادي (ordinary averaging) مفيداً مع مجموعات البيانات التي لها توزيعات إحصائية غير عادية.

تحليل الطاقة التفاضلي لخوارزميات أخرى

يمكن مهاجمة خوارزميات المفتاح العام باستخدام DPA من خلال تخمين قيم وسيطة في العمليات الحسابية ومقارنتها بقياسات استهلاك الطاقة. بالنسبة لعمليات الأس المعياري (سيجما)، من الممكن اختبار تخمينات خانات الأس عن طريق اختبار ما إذا كانت القيم الوسيطة المتوقعة مرتبطة بالعملية الحسابية الفعلية.

يمكن أيضاً تحليل تطبيقات RSA باستخدام نظرية الباقي الصيني (Chinese Remainder Theorem)، على سبيل المثال من خلال تعريف دوال اختيار على عمليات الاختزال أو إعادة التجميع في نظرية الباقي الصيني.

بشكل عام، تميل الإشارات المتسربة أثناء العمليات غير المتماثلة إلى أن تكون أقوى بكثير من تلك الناتجة عن العديد من الخوارزميات المتماثلة، على سبيل المثال بسبب التعقيد الحسابي المرتفع نسبياً لعمليات الضرب. ونتيجة لذلك، يمكن أن يكون تطبيق التدابير المضادة الفعالة لـ SPA و DPA أمراً صعباً.

يمكن استخدام DPA لكسر تطبيقات أي خوارزمية متماثلة أو غير متماثلة تقريباً. لقد استخدمنا حتى هذه التقنية للهندسة العكسية لخوارزميات وبروتوكولات غير معروفة عن طريق استخدام بيانات DPA لاختبار الفرضيات حول العمليات الحسابية للجهاز. (قد يكون من الممكن حتى أتمتة عملية الهندسة العكسية هذه.)

منع الـ DPA

تقع التقنيات الخاصة بمنع DPA والهجمات ذات الصلة تقريباً ضمن ثلاث فئات.

النهج الأول هو تقليل أحجام الإشارات، مثل استخدام كود بمسار تنفيذ ثابت، واختيار عمليات تسرب معلومات أقل في استهلاكها للطاقة، وموازنة أوزان هامينغ (Hamming Weight) وانتقالات الحالة، والحماية المادية للجهاز. لسوء الحظ، بشكل عام لا يمكن لتقليل حجم الإشارة تقليل حجم الإشارة إلى الصفر، حيث أن المهاجم الذي لديه عدد لا نهائي من العينات سيظل قادراً على تنفيذ DPA على الإشارة (المتدهورة بشدة). عملياً، يمكن للحماية القوية أن تجعل الهجمات غير ممكنة عملياً، ولكنها تضيف بشكل كبير إلى تكلفة الجهاز وحجمه.

النهج الثاني يتضمن إدخال ضوضاء في قياسات استهلاك الطاقة. مثل تقليل حجم الإشارة، تزيد إضافة الضوضاء من عدد العينات المطلوبة للهجوم، ربما إلى عدد كبير بشكل غير عملي. بالإضافة إلى ذلك، يمكن جعل توقيت وترتيب التنفيذ عشوائياً. يجب على المصممين والمراجعين التعامل مع التشويش الزمني بحذر شديد، حيث يمكن استخدام العديد من التقنيات لتجاوز أو تعويض هذه التأثيرات. لقد اجتازت العديد من المنتجات الضعيفة المراجعات التي استخدمت طرق معالجة بيانات ساذجة. من أجل السلامة، يجب أن يكون من الممكن تعطيل طرق التشويش الزمني أثناء المراجعة واختبار الاعتماد.

النهج الأخير يتضمن تصميم أنظمة تشفيرية مع افتراضات واقعية حول المكونات المادية الأساسية. يمكن استخدام إجراءات تحديث مفتاح غير خطية لضمان عدم إمكانية ربط قياسات الطاقة بين المعاملات. كمثال بسيط، يجب أن يؤدي تجزئة مفتاح 160 خانة باستخدام SHA[10] إلى تدمير المعلومات الجزئية التي قد يكون المهاجم قد جمعها عن المفتاح بشكل فعال. بالمثل، يمكن استخدام الاستخدام القوي لعمليات تعديل الأس والمعامل في أنظمة المفتاح العام لمنع المهاجمين من تجميع البيانات عبر أعداد كبيرة من العمليات. يمكن لعدادات استخدام المفتاح منع المهاجمين من جمع أعداد كبيرة من العينات.

باستخدام منهجية تصميم متسامحة مع التسريب، يجب على مصمم النظام التشفيري تحديد معدلات ودوال التسريب التي يمكن للتشفير أن يتحملها. يمكن تحليل دوال التسريب على أنها موجهات توفر معلومات حول العمليات الحسابية والبيانات، حيث يكون معدل التسريب هو الحد الأعلى لكمية المعلومات المقدمة من دالة التسريب. يمكن للمطورين بعد ذلك استخدام تقنيات تقليل التسريب وإخفاء التسريب حسب الحاجة لتلبية المعايير المحددة. أخيراً، يجب على المراجعين التحقق من أن افتراضات التصميم مناسبة وتتوافق مع الخصائص المادية للجهاز المكتمل.

الهجمات ذات الصلة

يُعد الإشعاع الكهرومغناطيسي مشكلة خطيرة بشكل خاص للأجهزة التي تمرر مفاتيح أو نتائج وسيطة سرية عبر ناقل البيانات. حتى راديو AM بسيط يمكنه اكتشاف إشارات قوية من العديد من الأجهزة التشفيرية. تُظهر أيضاً مجموعة واسعة من تقنيات قياس الإشارات الأخرى (مثل أجهزة التصوير البصري الكمي فائقة التوصيل) إمكانيات واعدة. يمكن استخدام الأساليب الإحصائية المتعلقة بـ SPA و DPA للعثور على إشارات في البيانات الصاخبة.

الخلاصة

تُعد تقنيات تحليل الطاقة مصدر قلق كبير لأن عدداً كبيراً جداً من المنتجات الضعيفة منتشرة. الهجمات سهلة التنفيذ، ولها تكلفة منخفضة جداً لكل جهاز، وهي غير اختراقية، مما يجعل من الصعب اكتشافها.

نظراً لأن DPA يحدد تلقائياً المناطق المرتبطة في استهلاك طاقة الجهاز، يمكن أتمتة الهجوم ولا يُطلب سوى القليل من المعلومات أو لا يُطلب أي معلومات عن التطبيق المستهدف. أخيراً، هذه الهجمات ليست نظرية أو مقتصرة على البطاقات الذكية؛ في مختبرنا، استخدمنا تقنيات تحليل الطاقة لاستخراج مفاتيح من حوالي 50 منتجاً مختلفاً في مجموعة متنوعة من الأشكال المادية.

الحل الموثوق الوحيد لـ DPA يتضمن تصميم أنظمة تشفيرية مع افتراضات واقعية حول المكونات المادية الأساسية. يسلط DPA الضوء على الحاجة إلى أن يعمل الأشخاص الذين يصممون الخوارزميات والبروتوكولات والبرمجيات والمكونات المادية معاً بشكل وثيق عند إنتاج منتجات الأمان.

المراجع

[1] R. Anderson, M. Kuhn, "Low Cost Attacks on Tamper Resistant Devices," Security Protocol Workshop, April 1997, http://www.cl.cam.ac.uk/ftp/users/rja14/tamper2.ps.gz.

[2] R. Anderson and M. Kuhn, "Tamper Resistance – a Cautionary Note," The Second USENIX Workshop on Electronic Commerce Proceedings, November 1996, pp. 1-11.

[3] E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.

[4] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," Advances in Cryptology: Proceedings of CRYPTO '97, Springer-Verlag, August 1997, pp. 513-525.

[5] D. Boneh, R. DeMillo, and R. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults," Advances in Cryptology: Proceedings of EUROCRYPT '97, Springer-Verlag, May 1997, pp. 37-51.

[6] Jameco Electronics, "PC-MultiScope (part #142834)," February 1999 Catalog, p. 103.

[7] P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," Advances in Cryptology: Proceedings of CRYPTO '96, Springer-Verlag, August 1996, pp. 104-113.

[8] M. Matsui, "The First Experimental Cryptanalysis of the Data Encryption Standard," Advances in Cryptology: Proceedings of CRYPTO '94, Springer-Verlag, August 1994, pp. 1-11.

[9] National Bureau of Standards, "Data Encryption Standard," Federal Information Processing Standards Publication 46, January 1977.

[10] National Institute of Standards and Technology, "Secure Hash Standard," Federal Information Processing Standards Publication 180-1, April 1995.

[11] J. Dhem, F. Koeune, P. Leroux, P. Mestre, J. Quisquater, and J. Willems, "A practical implementation of the timing attack," UCL Crypto Group Technical Report Series: CG-1998/1, 1998.

[12] R.L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, 21, 1978, pp. 120-126.

خاتمة الترجمة

ترجمة: محمد سيد من مكتبة قرطبة.

تم الترجمة بحمد الله في يناير ٢٠٢٦ - النسخة الاولى.

إذا استفدت من هذه الترجمة:

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