Effektanalysattacker
Del I: Effektanalysens principer

Anders

10 juni 2024 (21:01)

Sammanfattning

Häri beskrivs effektanalysens principer så som de teoretiskt beskrivs. Både simpla och differentiella effektanaylsattacker diskuteras. Artikeln tjänar som en förberedelse inför [Fur22a] och [Fur22b].

Innehåll

0 Inledning

Vid nyttjande av elektroniska beräkningsapparater kan effektförbrukningen avslöja information som man önskar hålla hemlig. Sådan information kan avslöja operander såväl som resultat av operationer. Informationen kan användas av en illvillig anfallare.

Vi ska här diskutera hur man anfaller apparater, i synnerhet kryptografisk utrustning, och hur man utnyttjar erhållen information.

Eftersom vissa tekniska termer är ovanliga i svensk översättning så anges ibland det engelska (*eng*: English) namnet.

1 Avgränsningar

Behövs det här kapitlet?

2 Skyddsvärd information och fördelar vid gissning

Vi definierar *skyddsvärd*, *hemlig* eller *känslig* information som data sådana att de inte får röjas till obehöriga. Ett typiskt exempel är hemliga uppgifter i *klartext*, vilket innebär att de inte är krypterade. Kryptografiska *nycklar* och *parametrar* är andra vanliga exempel.

Att skydda skyddsvärda data innebär att man inte avslöjar någon information som ger en anfallare någon fördel i gissandet av dem. Ekvivalent kan man sägga att ett skyddande har misslyckats om information har läckt sådan att en anfallare har lyckats bygga en sannolikhetsfördelning som ger honom en fördel i gissandet av den skyddsvärda informationen.

Som komplement kan vi ju definiera *hemlighållen* information som data sådana att en anfallare inte kan bygga någon sannolikhetsfördelning sådan att han har en fördel i gissandet av dessa data. I fallet kryptografiska nycklar så bör man (givet att man utgår från att de är dragna från slump) a priori anta en lådformad sannolikhetsfördelning. För en nyckel

$$\begin{aligned} k &\in \mathbb{B}^d \\ &= \underbrace{\mathbb{B} \times \ldots \times \mathbb{B}}_{d \text{ faktorer}} \end{aligned} \tag{0}$$

som alltså har d bitar *nyckelmassa*[†] bör alltså en sådan sannolikhetsfördelning se ut som

[†]Ibland skiljer man mellan termerna *nyckel* och *nyckelmassa* på så sätt att nyckeln ibland kan syfta på mer information än de som används som nyckel i de kryptografiska algoritmer den är ämnad för. För att ibland vara mycket tydlig med att man menar just de data som används som nyckel i kryptografiska algoritmer så används termen nyckelmassa.

$$\mathcal{P}[x] = \frac{1}{2^d} \tag{1}$$

vilket är en sannolikhetsfördelning som är konstant i den bemärkelsen att den är samma för varje nyckel $x \in \mathbb{B}^d$. Man vet alltså inte var man ska börja vid ett gissningsförfarande utan varje nyckel är lika sannolik. För ett stort värde på d, säg exempelvis 128, skulle det förmodligen krävas en enorm mängd gissningar innan man kommer fram till en korrekt nyckel (det antas här att anfallaren utan vidare kan testa nyckel efter nyckel). Förväntansvärdet för antalet gissningar som krävs för att hitta rätt nyckel blir 2^{127}. Det är så många gissningar att det kan vara svårt att begripa.

Om, å andra sidan, en anfallare har lyckats bygga en skev sannolikhetsfördelning, säg exempelvis att han vet att av 128 bitar så är minst 100 av dem satta till 1, då kommer förväntansvärdet att bli betydligt mindre än 2^{127}, kanske blir det så litet att det är görbart för anfallaren att utföra en uttömmande sökning.

Hädanefter kommer alla diskussioner angående skyddsvärda data avse kryptering och krypteringsapparater.

3 Sidokanaler

En sidokanal är en informationsväg sådan att en attackerare kan untyttja den för att förvärva kunskap om hemligheter. Information som läcker genom en krypteringsapparats sidokanaler kan avslöja, exempelvis, hur mycket effekt som förbrukas, hur lång tid en operation tar, värmeutvecklingen i enheten, i vilka skeden en delkomponent är aktiv, hur kraftfullt den EM-strålar, såväl som optiska och akustiska läckor. Med sådan information och antaganden om en fysikalisk modell kan statistiska transformer utföras sådana att en sannolikhetsfördelning erhålls. På så sätt kan en attackerare vinna fördel i utrönandet av hemliga data så som krypteringsnycklar.

4 Allmänt om effektanalysattacker

En särskilt intressant sidokanal är effektförbrukning. För en krypteringsapparat kan effektförbrukning avslöja de ingående operanderna för beräkningar under exekveringen av en algoritm, såväl som resultatet. Detta kommer sig av att hårdvaran som algoritmen är implementerad i inte förbrukar lika mycket effekt oavsett operandernas värden. Genom att mäta effektförbrukningen under loppet av en algoritms exekvering och sen jämföra med en fysikalisk modell (vanligen grundad på hammingvikt eller hammingavstånd) kan man få information som genom statistiska metoder (vanilgen flervariabelgaussiska korrelationsmodeller eller diskriminantmodeller) ger sannolikhetsfördelningar.

För att utföra en sådan attack krävs en mätuppställning. Vanligen mäter man strömförbrukning och antar att spänningen håller sig konstant. Man kan även, utan kontakt, mäta EM-fält runt enheten.

Vi skiljer mellan två huvudsakliga effektanalysattacker (*eng*: Power Analysis Attack, PAA): enkel effektanalysattack (*eng*: Simple Power Analysis, SPA) och differentiell effektanalysattack (*eng*: Differential Power Analysis, DPA).

Innan vi studerar dem närmare ska vi först fundera på effektförbrukningen hos digital elektronik.

5 Allmänt om Effektförbrukning

Digital elektronik förbrukar effekt (kanske litet slarvigt uttryckt, men effekt definieras som det momentana energiflödet) när de är igång. På den grövsta nivån kan vi dela upp effektförbrukningen i två delar, den *statiska förbrukningen* och den *dynamiska förbrukningen* av effekt. Alltjämt har vi $P = P_{\text{static}} + P_{\text{dynamic}}$

5.0 Statisk effektförbrukning

Statisk effektförbrukning, P_{static}, avser effektförbrukningen i en krets där ingenting ändrar tillstånd. Inga flip floppar, vippor eller kondensatorer byter tillstånd.

5.1 Dynamisk effektförbrukning

De dynamiska effekterna för effektförbrukningen, P_{dynamic}, får vi då tillstånd i logiken förändras. Vi föreställer oss en enkel modell där varje logikcell har två tillstånd, 0 och 1. Det ger upphov till fyra övergångar med fyra tillhörande effektförbrukningar:

$$\begin{array}{cccc} 0 \to 0 & 0 \to 1 & 1 \to 0 & 1 \to 1 \\ P_{0\to0} & P_{0\to1} & P_{1\to0} & P_{1\to1} \end{array} \tag{2}$$

Vi noterar att för fallen $0 \to 0$ och $1 \to 1$ har vi inget förändrat tillstånd så

$$\begin{aligned} P_{0\to0} &= P_{\text{static}} \\ P_{1\to1} &= P_{\text{static}} \end{aligned} \tag{3}$$

Dessa är alltså inte särskilt intressanta för sammanhanget eftersom deras dynamiska effektförbrukning är 0. Vi studerar de andra fallen i stället. Där har vi en dynamisk term som är differensen av dem och den statiska förbrukningen.

6 Effektförbrukning för CMOS-teknologi

CMOS[†] (*eng*: Complementary metal–oxide–semiconductor) är en särskilt viktig teknologi vars effektförbrukning kan beskrivas med de två termerna P_{static} och

[†]En mycket flitigt förekommande digital elektronikteknologi som används inom kretskort så som mikroprocessorer, microcontrollers, minneschips och många andra.

P_{dynamic}.

6.0 Högnivåbeskrivning av effektförbrukning för CMOS-teknologi

CMOS-celler är alltid i ett definierat tillstånd, i vilket de läcker mycket litet ström. Vanligen är läckaget i storleksordningen mikoampère, vilket för V_{dd} i storleksordningen volt ger pikowatt. Vi betecknar den $P_{\text{static}} = J_{\text{leak}} V_{\text{dd}}$, där J_{leak} betecknar strömläckaget.

Mer intressanta är de dynamiska effekterna. Denna dynamiska term kommer främst av två effekter. Först har vi att det, vid en övergång $0 \to 1$ eller $1 \to 1$, sker en kortslutning för en mycket kort stund i vilken ström läcker och sen har vi att en kondensator laddas upp, vilket kräver laddning och därför ström över en tid.

Vi delar upp den dynamiska effektförbrukningen och betecknar den enligt

$$
\begin{aligned}
P_{\text{dynamic}} &= P_{\text{short}} + P_{\text{switch}} \\
P_{\text{short}} &= J_{\text{short}} V_{\text{dd}} \\
P_{\text{switch}} &= \alpha C_L V_{\text{dd}}^2 \frac{\omega}{2\pi}
\end{aligned}
\tag{4}
$$

Där J_{short} är kortslutningsströmmen, $\alpha \in \mathbb{R}$ är en dimensionslös, skalär, koefficient som kallas aktivitetsfaktorn och beskriver sannolikheten för en övergång $0 \to 1$, C_L är lastkapacitansen för logikcellen och ω är vinkelfrekvensen för klockan.

6.0.0 Glitchar

I allmänhet är logikceller på en CMOS-krets kopplade sådana att en cells utgång kan vara en annan cells ingång. Detta har konsekvensen att om en logikcell har två olika ingångar som kommer från två olika håll kan de uppdateras vid olika tidpunkter även om de går på samma klocka på grund av det tar nollskild tid för signaler att gå igenom logik och ledare. Dessa mellantillstånd, som finns mellan att en cell varit i ett, av logiken som beskriver kretsen, väldefinierat tillstånd, till att det är i ett nytt väldefinierat tillstånd, kalls för en *glitch* (*eng*: glitch) eller *dynamisk fara* (*eng*: dynamic hazard).

Vid en glitch är det inte säkert att cellens utgång hinner nå värdet som definieras av glitchtillståndet utan den kan vara metastabil. Glitchar är uppenbart databeroende.

6.1 Lågnivåbeskrivning av läckage i MOS-transistorer

En MOS-transistor kan beskrivas som en elektronisk komponent med fyra olika potentialer:

0. ϕ_S, potentialen vid source-utgången
1. ϕ_D, potentialen vid drain-utgången
2. ϕ_G, potentialen vid gate-utgången
3. ϕ_B, potentialen för bulk-utgången

Vi väljer $\phi_b = 0$. Med det valet får vi spänningar för de andra utgångarna enligt

$$\begin{aligned} V_S &= \phi_S - \phi_B \\ V_d &= \phi_D - \phi_B \\ V_G &= \phi_G - \phi_B \end{aligned} \tag{5}$$

Utifrån dessa tre potentialer har vi åtta olika digitala tillstånd, men vi minns egenskaperna hos MOS-transistorer, nämligen att om V_G är hög så kan inte V_D och V_S var olika. Detta krymper rymden till sex olika tillstånd.

Vi kommer nu studera sex olika effekter som bidrar till den effektförbrukningen.

6.1.0 Undertröskelström

En statisk komponent kommer av *undertröskelström*, som är den ström som fortfarande går då spänningen är under tröskelspänningen. Denna effekt är aktiv vid de två tillstånd som definieras av $V_D \oplus V_S$, vilket betyder att vi har en potentialskillnad mellan source-utgången och drain-utgången. Eftersom transistorn, på låg nivå, inte är en perfekt brytare utan en komplicerad samling atomer, så kommer vi alltid, även om V_G är mycket låg, ha en ström i kanalen mellan source-utgången och drain-utgången.

Storleken av denna ström beror på konduktiviteten däremellan. Denna uttrycks i termer av teknologins parametrar, bredden W, längden L, spänningen mellan gate-utgång och source-utgång V_{GS}, spänningen mellan drain-utgång och source-utgång V_{DS}, temperaturen T, elementarladdningen q_e, den biaslösa rörligheten, μ_0, den effektiva kanaldopningen N_{ch}, ytpotentialen Φ_S, kapacitansen för oxidlagret och utarmningslagret C_{ox} respektive C_{dm}, permittiviteten hos kisel ϵ_{Si} och tröskelpotentialen V_{th}. Den läckta strömmen, J_{UTS}, blir i termer av dessa parametrar

$$\begin{aligned} J_{\mathrm{UTS}} &= K \left(\frac{k_B T}{q_e} \right)^2 \frac{W}{L} e^{(V_{GS} - V_{th})/(n q_e/[k_B T])} \\ &\text{med} \\ n &= 1 + \frac{C_{dm}}{C_{ox}} \\ K &= \mu_0 \sqrt{\frac{q_e \epsilon_{Si} N_{ch}}{2\Phi_S}} \end{aligned} \tag{6}$$

Temperaturberoendet är uppenbarligen mycket starkt. Likaså är beroendet av tröskelspänningen tydlig.

Innan vi lämnar denna effekt nämner vi några sätt som tröskelspänningen kan påverkas på utan att gå in på för mycket detaljer.

Tröskelspänningen kommer bero på kanalbredden och längden,

Tröskelspänningen kan bero av V_S. Denna effekt är mycket viktig. Vi kan alltså, genom att ändra spänningen mellan bulk-utgången och source-utgången och på så sätt förändra tröskelspänningen vilket förändrar J_{UTS}. Denna effekt kallas *stapeleffekten* (*eng*: stacking effect), och är den största faktorn till databeroende läckage i CMOS-teknologi.

Det finns också en effekt från spänningen mellan drain-utgången och source-utgången som också beror på den karakteristiska längden hos en MOS-transistor. Denna effekt är särskilt märkbar då transistorn inte är aktiv.

6.1.1 Gate läckage

Gate läckage består av två effekter, tunnling och HCI. Låt oss börja med tunnlingseffekterna som är de dominanta.

Det finns ett tunnt kiseldioxidlager som skiljer mellan gate-utgången och och kanalen. Om V_G är hög kommer två tunnlingsprocesser ske. I fallet $V_{ox} > \Phi_{ox}$ så har vi så kallad *Fowler-Nordheim-tunnling* i vilken laddningar inte tunnlar över hela lagret. Effekten är proportionell mot $\frac{E_{ox}^2}{\Phi_{ox}}$ och har i exponenten en faktor, proportionell mot, $-\frac{\Phi_{ox}^{3/2}}{E_{ox}}$, där E_{ox} är det elektriska fältet över kiseldioxidlagret. Denna effekt är försumbar för $V_{ox} < \Phi_{ox}$. I det andra fallet, som kallas *direkt tunnling*, har vi att laddningarna tunnlar hela vägen. Denna effekt är starkt beroende av värdet på V_{dd}.

HCI (*eng*: Hot Carrier Injection) är den mindre av effekterna. Den går ut på att laddningsbärare joniserar kiseldioxiden. Joniseringströskeln ligger på 1.3 elektronvolt, så laddningsbärare med mer kinetisk energi än så kan orsaka en hel del oreda. Barriären för elektroninjektion ligger vid 3.1 elektronvolt, så det är troligare än hålinjektion, vars barriäre ligger på 4.8 elektronvolt. Vidare har hålen mycket mindre rörlighet så elektroninjektion är den dominerande av effekterna.

6.1.2 Läckage i pn-övergång

Backspända dioder är välstuderade. I transistorfallet så har vi även diodverkan i drain-bulk-övergången.

Vi har en effekt av direkt tunnling från p-sidans valensband till n-sidans ledningsband. Mer än så går vi inte in på det här.

6.1.3 Gate-inducerad drain-läckage, GIDL

Denna effekt beskriver inverkan från gate-fältet på drain-utgångens utarmningslager. Ju högre V_G är desto tunnare kommer utarmningslagret att vara i den överlappande ytan mellan gate och drain. Detta ger upphov till tunnling mellan banden vars sannolikhet är proportionell mot V_{GS}.

6.1.4 Genomslag

Gemoetriska ojämnheter kan göra att strömmar går igenom där de inte borde gått igenom.

6.2 Produktionseffekter för CMOS

Eftersom många läckageparametrar är materialberoende så kommer tillverkningsprocessen vara central.

6.2.0 Interplättvariationer

Variationer från *plätt* (*eng*: die) till plätt kommer påverka läckage i och med variationer i dopning, etsning och strukturstoleksvariationer.

6.2.1 Intraplättvariationer

Variationer inom en plätt är främst av geometrisk karaktär. Detta har stora konsekvenser för undertröskelströmmar.

6.3 Databeroende i CMOS – stapeleffekten

Det finns databeroende för läckagemodeller i CMOS-designer. Den största av dessa är stapeleffekten. Föreställ dig en icke-ledande transistor mellan matningen och en andra transistor, vars läckage ska uppskattas. Den första transistorn kommer orsaka en liten backspänning mellan gate-utgången och source-utgången på den andra transistorn. Effekterna som beskrevs i avsnitt 6.1.0 kommer då orsaka en ökad tröskelspänning. Eftersom undertröskelströmmen är exponentiellt beroende av tröskelspänningen så kommer en märkbar skillnad uppstå.

7 Operandberoende effektmodeller

I allmänhet har en anfallare inte så detaljerad kunskap om kretsen att han kan utnyttja lågnivåbeskrivningar. Vad han då får göra är att låta lågnivåbeskrivningen gå mot en makroskopisk gräns och försöka formulera en högnivåbeskrivning för hur kretsens effektberoende påverkas av operationerna som processeras och operanderna som verkas på.

De vanligaste modellerna utgår från att en apparat läcker operanders hammingvikt eller hammingavstånd i något steg.

7.0 Hammingvikt och hammingavstånd

För en bitsträng, $v \in \mathbb{B}^d$, defineras hammingvikten som en funktion, HW:

$$HW : \mathbb{B}^d \to \{0, 1, ..., d\} \subset \mathbb{N} \tag{7}$$

sådan att v avbildas på antalet nollskilda tecken i bitsträngen, alltså med andra ord, antalet ettor i strängen. Ett exempel är strängen $(0, \mathbf{1}, \mathbf{1}, 0, \mathbf{1}, 0, 0, 0) \in \mathbb{B}^8$ som har hammingvikt enligt::

$$HW(0, \mathbf{1}, \mathbf{1}, 0, \mathbf{1}, 0, 0, 0) = 3 \tag{8}$$

eftersom det finns tre nollskilda tecken i bitsträngen $(0, \mathbf{1}, \mathbf{1}, 0, \mathbf{1}, 0, 0, 0) \in \mathbb{B}^8$ (de gjordes aningen tjockare än vanliga 1 för att belysa att de räknas). Hammingavstånd definieras för två bitsträngar, u och v, som en funktion, HD:

$$\begin{aligned} HD : \mathbb{B}^d \times \mathbb{B}^d &\to \{0, 1, ..., d\} \subset \mathbb{N} \\ (u, v) &\mapsto HW(u \oplus v) \end{aligned} \tag{9}$$

Några exempel är

(10)

$$\begin{aligned} HD((1,1,1,1,1),(1,0,1,0,1)) &= HW((1,1,1,1,1) \oplus (1,0,1,0,1)) \\ &= HW(0,1,0,1,0) \\ &= 2 \\ HD((0),(0)) &= HW(0 \oplus 0) \\ &= HW(0) \\ &= 0 \\ HD((1,0,1,0,0,1,0,1),(1,0,1,0,0,1,0,1)) &= HW((1,0,1,0,0,1,0,1) \oplus (1,0,1,0,0,1,0,1)) \\ &= HW(0,0,0,0,0,0,0,0) \\ &= 0 \end{aligned}$$

Vi kan notera att $HD(v, v) = 0, \quad \forall v$, eftersom bitsträngen $v \oplus v$ inte innehåller några nollskilda tecken alls.

7.1 Tecknat avstånd

För CMOS-logik hänger effektbeorendet på om kondensatorer laddas eller laddas ur. Därför bör man skilja mellan övergångarna $1 \to 0$ och $0 \to 1$.

Låt övergångarna $0 \rightarrow 0$ och $1 \rightarrow 1$ anses förbruka ingenting. Normalisera övergången $0 \rightarrow 1$. Då får övergången $1 \rightarrow 0$ effektförbrukningen $1 - \delta$ där δ typiskt är någonstans runt 0.15 till 0.20. Detta är alltså en justering av hammingavstånd där vi har viktat övergångarna olika.

7.2 Simulerade effektmodeller

En metod för att bygga en modell över effektförbrukning är att simulera en apparats beteende. Detta kan göras på flera olika nivåer, analog, logisk och beteendenivå. Det finns kraftfull mjukvara som är utvecklad i detta syfte och som med god noggrannhet kan förutsäga effektförbrukningen och dess operandberoende.

7.2.0 Analog nivå-simulering – differensekvationer

Simuleringar på analog nivå, som alltså tar hänsyn till vissa analoga effekter, är mycket resurskrävande och fordrar god kunskap om den simulerade kretsen.

För att utföra en simulering på analog nivå så använder man *nätlistan* som definierar transistorerna och hur de är kopplade. Vidare utnyttjar man kunskap om *parasitiska* element, i synnerhet parasitiska kapacitanser.

Parasitiska element kan vara svåra att beskriva så ofta klumpar man ihop dem. Noggrannheten för en simulering på analog nivå hänger mycket på hur exakt de parasitiska elementen beskrivs.

Effektmodellerna man använder utgår från differensekvationer och är den lägsta simuleringsnivån av de tre.

7.2.1 Logiknivå-simulering – HD-modeller

På logiknivå beskrivs inte kretsen lika precist som på analog nivå, men simuleringen är inte lika krävande. I stället för nätlista över transistorer används nätlista över logikceller. Ibland inkluderas även kunskap om ledningarna och fördröjningarna i dem, såväl som stig- och falltider för signalerna i kretsen.

Med en effektmodell för logikcellerna kan man simulera effektförbrukningen för apparaten. Utan tillgång till mer precisa effektmodeller kan HD-modeller användas.

I praktiken har en anfallare kanske inte tillgång till hela nätlistan, utan han måste gissa sig till hur han ska simulera den. Dessa gissningar grundar sig på antaganden. Om den studerade kretsen, till exempel, är en mikrocontroller så kommer den med stor sannolikhet ha minne, en aritmetisk enhet, en databuss, några gränssnitt och register. Vi kollar närmare på databussar och register.

En databuss består ofta av en klase långa ledare som är anslutna till flera komponenter. På så sätt bidrar en buss med stor kapacitiv last och kommer således påverka effektförbrukningen märkbart. De olika ledarna av en buss kommer påverka ungefär lika mycket. Därför är HD-modeller för bussar särskilt väl lämpade för att beskriva effektförbrukningen.

Register i en mikrocontroller håller små mängder data. De triggas av klocksignal och kan således bara byta värde en gång per klockcykel (jämför det med logikceller i en FPGA till exempel). HD-modeller lämpar sig väl för register eftersom effektförbrukningen av registret kommer vara proportionell mot hur många bitar i registret som ändras från en cykel till nästa.

7.2.2 Beteendenivå-simulering – HW-modeller

Beteendenivån är den högsta som simuleras. Fördelen är att det inte kräver så mycket kunskap om apparaten, men å andra sidan ger det de minst precisa resultaten av de tre simuleringsnivåerna. Man koncentrerar sig på att försöka utröna vad för operationer som sker och med vilka operander.

För simuleringar på beteendenivå så används både HW- och HD-modeller. HD-modeller används på ett liknande sätt som för simuleringar på logiknivå. HW-modellen är simplare och kräver ännu mindre kunskap om kretsen. Den är även praktisk om man bara känner till signalernas värden i en buss vid någon tid, men inte vad den var tidigare eller kommer att bli senare eftersom HD-modeller inte kan användas då.

HW-modeller grundar sig på antagandet att effektförbrukning är proportionell mot momentana värden för signaler i en krets. Detta är inte särskilt användbart för CMOS-teknologi eftersom det mesta av effektförbrukningen orsakas av övergångar, som inte beskrivs av HW-modeller. I allmänhet vill man undvika att tvingas använda HW-modeller så långt det går.

En situation där HW-modeller har en god använding är då vi redan vet, alla eller vissa, signalers värde vid ett tillstånd och mäter på nästa. I den situationen blir HW-modeller helt eller delvis till HD-modeller.

8 Mätning

För att få information ifrån apparaten som man vill anfalla krävs att man mäter på den. Vanligen sker mätningar med ett oscilloskop och en analog till digital konverterare (*eng*: Analog to Digital Converter, ADC). Dessa data, spår, sparas sedan till disk för analys.

8.0 Mätuppställning

Den vanligaste metoden att mäta effektförbrukning för effektanalysattacker är att placera ett litet motstånd mellan spänningsmatningen och apparaten man vill testa. Genom att mäta spänningen över det motståndet med sitt oscilloskop kan en anfallare få reda på strömförbrukningen och därmed effektförbrukningen. Motståndet väljs med omsorg, sådant att det är litet nog att inte störa spänningsmatningen, har jämnt energiupptag och inte medför onödiga parasitisa komponenter (vanliga kolmotstånd kan ha parasitisk induktivitet på hundratals mH).

Till spänningsmatningen kopplas, parallellt, kondensatorer för att filtrera höga frekvenser. Dessa väljs till olika värden, vanligen tre (3) med värden 1 μF, 100 nF och 1 nF.

Det går också att använda prober för EM-fältet, från vilka man exempelvis genom Lenz lag, kan mäta strömvariationer och därmed variationer i effektförbrukning.

8.1 Val av oscilloskop

Oscilloskop väljs efter tre viktiga egenskaper:

0. Bandbredd bestämmer hur höga frekvenser oscilloskopet kan mäta. Man kan alltså betrakta oscilloskopet som ett lågpassfilter. Bandbredden definieras vanligen som den högsta frekvens som kan mätas utan mer än -3 dB amplitudförlust.
1. Mätfrekvens bestämmer hur ofta mätningar sker. Nyqvistfrekvensen beaktas. Mätfrekvensen behöver alltså minst vara dubbelt så hög som frekvensen av det man önskar mäta.
2. Q-värde beskriver energiförlust per oscillering, alltså hur dämpat systemet är.

8.2 Störningar

Huvudsakligen kommer störningar i mätningen ifrån fyra (4) håll:

0. Störningar från omgivningen på den mätta apparaten.
1. Det passiva fördelningsnätverket (*eng*: Passive Distribution Network, PDN), som kan modelleras som små passiva komponenter, motstånd (0.1 - 10 Ω), induktanser (1 - 100 nH) och kapacitanser (10 pF - 100 nF).
2. Störningar från omgivningen på oscilloskopets prob.
3. Störningar från sampling och kvantisering.

8.3 ICEM-modellen

ICEM står för (*eng*) Integrated Circuit Electromagnetic Compatibility. Syftet med modellen är att förutsäga vilka strömmar som bidrar till den digitala logikens effektförbrukning genom att ta hänsyn till frånkopplingsimpedans mellan höga och låga ingångar till en krets. För att göra det krävs identifikation av de olika impedanserna i PDN. När en modell över PDN gjorts räknar man ut överföringsfunktionen mellan den mätta strömmen, alltså den som kommer utifrån in i apparaten, J_{ut}, och den som går inuti apparaten, J_{in}, från de höga spänningsingångarna till de låga parallellt med en frånkopplingsimpedans, Z_{decouple}.

Om vi klumpar ihop allt till en enkel modell har vi ett motstånd, R_{measure} som vi mäter spänningen, $V_{\text{oscilloscope}}$ över och således får strömmen, J_{ut}. Denna ström går igenom klumpimpedansen i PDN, Z_{klump}, och sen delar den sig parallelt mellan frånkopplingsimpedansen, Z_{decouple}, och den inre, sökta, strömmen, J_{in}, som är proportionell mot den digitala logikens effekt. Bevarande av energi (Kirchoffs spänningslag) i ett varv runt slingan som inte innefattar J_{in} ger ekvationen

$$
\begin{gathered}
(J_{\text{ut}} - J_{\text{in}})Z_{\text{decouple}} + J_{\text{ut}}(R_{\text{measure}} + Z_{\text{klump}}) = 0 \\
\text{Från vilket vi får } J_{\text{in}} \\
J_{\text{in}} = J_{\text{ut}} \frac{R_{\text{measure}} + Z_{\text{klump}} + Z_{\text{decouple}}}{Z_{\text{decouple}}}
\end{gathered} \tag{11}
$$

9 Statistika metoder

Sttatistisk behandling av mätvärden är en nödvändighet för att komma fram till den sannolikhetsfördelning som ger en attackerare fördel i att gissa hemliga data. Vanligen arbetar man inte direkt på spåren eftersom de innehåller för stora datamängder utan man väljer bort vissa data. Detta kan ske på olika vis men de vanligaste metoderna är:

0. Medelvärde över klockcykel, vilket innebär att man integrerar mätpunkterna över en klockcykel och sedan dividerar med klockperioden.
1. Högsta värde, vilket innebär att man sparar endast det högsta uppmätta värdet för varje klockcykel och låter det representera hela den perioden.

Att kasta bort data ger givetvis ingen teoretisk fördel utan det är helt enkelt en nödvändighet som orsakas av begränsningar i lagringsutrymme och beräkningskraft.

Genom att ansätta störningar med givna sannolikhetsfördelningar, typiskt normalfördelade, kan man få sannolikhetsfördelningar för olika spår som man jämför med simuleringar. Ifrån detta kan man göra nollhypotestest och sätta upp konfidensintervall. På så sätt kan en anfallare skaffa sig fördel i gissning av skyddsvärda data.

10 Vilostund

Vi har, vid det här laget, definierat vad vi menar med skyddsvärda data och fördelar vid gissning av dem. Vi har beskrivit effektförbrukning för digital elektronik, på hög och låg nivå. Vi har sammanfattat metoder för simulering av effektförbrukning och ställt upp naiva modeller för hur de relaterar till utförda operationer och vilka operander som ingår. Slutligen har vi beskrivit hur man mäter och, i ett första steg, behandlar mätdata.

Nu är vi mogna för att ta oss an artikelns huvudsyfte, effektanalysattacker. Dessa delas upp i två kategorier, SPA och DPA. Vi börjar med SPA.

11 Simpel effektanalysattack

SPA grundar sig på tanken att från ett eller ett fåtal spår (*eng*: Trace) gissa sig till hemligheter. Detta kräver detaljerad kunskap hur algoritmen som exekveras är implementerad.

Den vanligaste formen av SPA är mallattacker (*eng*: Template Attacks), där simulerad effekt, *mall*, jämförs med uppmätt, *spår*. Simuleringarna baseras på någon fysikalisk modell för effektförbrukning och för störningar. Mallattacker beskriver effektspåren i termer av flervariabelgaussisk fördelning (flervariabel definieras här som en kartesisk produkt mellan flera mängder av reella tal, $\mathbb{R}^d$).

En mall är ett par som består av ett medelvärde, en vektor $m \in V = \mathbb{R}^d$, och en kovarians, en (1,1)-tensor $C \in V^* \otimes V$. Dessa mallar byggs upp för varje tänkbar hemlighet, så att vi för varje par av operandtata och nyckel (d_μ, k_ν) får en mall, alltså ett par av medelvärde och kovarians, $(m, C)_{\mu,\nu}$. Mallar jämförs sedan med spåret, $t \in V$, så att en sannolikhetsfördelning, $\mathcal{P}$, erhålls enligt:

$$\mathcal{P}[t, (m, C)_{\mu,\nu}] = \frac{\exp[-\frac{1}{2}C^{-1}((t-m)^*, (t-m))]}{\sqrt{(2\pi)^d \det(C)}} \tag{12}$$

där C^{-1} är inversen av kovariansen och dualen av en vektor fås med avseende på den euklidiska metriken, g, på $\mathbb{R}^d$:

$$\begin{aligned} g &= \delta^\mu_\nu \frac{\partial}{\partial x^\mu} \otimes dx^\nu \\ &= \frac{\partial}{\partial x^\mu} \otimes dx^\mu \end{aligned} \tag{13}$$

(där δ^μ_ν är Koreneckers symbol) alltså transformen, för en vektor, $v \in V$,

$$v \to g(v, \cdot) = v^* \in V^* \tag{14}$$

vilken i en bas blir

$$v^\mu \frac{\partial}{\partial x^\mu} \to v_\mu dx^\mu \tag{15}$$

där $v_\mu = v^\mu$, vilket torde motsvara transponatet, $v \to v^t$ på komponentform.

Om a priori-antagandet består i att hemligheten är dragen ur en lådformad sannolikhetsfördelning, sådan att varje hemlighet ur mängden är lika sannolik som varje annan, så kommer det största elementet i $\mathcal{P}$ motsvara den mest sannolika nyckeln.

För att bygga en mall behöver man en fysikalisk modell för algoritmens implementering. Man kan koncentrera sig på en isolerad instruktion eller en längre sekvens av beräkningar. Till exempel kanske MOV-instruktionen på en mikroprocessor förbrukar mer effekt för operander med låg hammingvikt. Mallar kan byggas med avseende på exempelvis klartextdata eller kryptografiska nycklar.

11.0 Kollisionsattack

En annan form av SPA är *kollisionsattack* (*eng*: Collision Attack), vilken grundar sig på att i fallet att samma mellantillstånd, v, uppkommer i ett givet steg i algoritmen för två olika klartexter, d och d' med samma nyckel, k, alltså att

$$\begin{aligned} v &= f(d,k) \\ &= f(d',k) \end{aligned} \tag{16}$$

där f beskriver tillståndet i det givna algoritmsteget. Detta kan inte ske för vilka nycklar som helst utan minskar sökrymden som attackeraren behöver koncentrera sig på.

12 Differentiell effektanalysattack

DPA är betydligt mer populär. Den kräver inte lika mycket kunskap om hur algoritmen är implementerad som SPA, men kräver att man mäter fler spår. DPA har tolerans för lägre signal-brus-kvot (*eng*: Signal to Noise Ratio, SNR).

DPA utförs i allmänhet i fem (5) steg:

0) För att utföra DPA så riktar man först in sig på signalernas värden, v, i ett givet mellansteg som kan beskrivas som $v = f(d, k_\mu)$, för någon funktion, f, som beror av kända men variabla signaler, d, och en del av eller hela den kryptografiska nyckeln, k_μ. d är vanligtvis chiffertext eller klartext.

1) Nu är det dags att mäta krypteringsapparatens effektförbrukning. Låt oss kryptera D olika datablock av längd Δ,

$$d = (d_0, d_1, ..., d_{D-1}) \in (\mathbb{B}^\Delta)^D \tag{17}$$

Varje kryptering av sådant datablock ger upphov till ett spår som är T datapunkter långt

$$t_\mu = (t_{\mu,0}, t_{\mu,1}, ..., t_{\mu,T-1}) \in \mathbb{R}^T \tag{18}$$

Vi har alltså mätt D stycken krypteringar av vardera T datapunkter och har därmed $T \cdot D$ mätvärden. För att, på ett meningsfullt sätt, kunna jämföra de olika t_μ med varandra är det nödvändigt att de beskriver samma förlopp, alltså att för ett givet α ska $t_{\mu,\alpha} \in \mathbb{R}$ vara jämförbart, alltså beskriva samma steg i algoritmen, med $t_{\nu,\alpha} \in \mathbb{R}$. Med andra ord är det centralt att effektmätningen inte skiljer sig i tid för en exekvering som går på bestämd tid. Detta uppnås vanligen genom att synkroniera oscilloskopet med krypteringsapparatens klocka.

2) Man följer upp detta med att beräkna hypotetiska signalvärden, v, i mellansteg för varje möjligt val av k_μ. Låt oss nu skriva denna mängd som

$$k = (k_0, k_1, ..., k_{K-1}) \tag{19}$$

där K beskriver hur många kombinationer av k_μ som är möjliga. Det är, för en vanlig bitsträngsnyckel av längd λ, $K = 2^\lambda$, så att nyckellängden är $\lambda = log_2(K)$. Alltså har vi att $k \in (\mathbb{B}^\lambda)^K$. Nu när vi sorterat våra data kan vi räkna ut mellanstegsvärden för signalerna för varje datablock och nyckelgissning. Det ger oss alltså värdena

$$v_{\mu,\nu} = f(d_\mu, k_\nu), \quad \mu \in \{0, 1, ...D-1\}, \quad \nu \in \{0, 1, ..., K-1\} \tag{20}$$

Målet blir nu att hitta rätt ν för $v_{\mu,\nu}$, alltså vilket element, k_ν ur k som motsvarar den sökta nyckel, $k_\nu = k_{real} \in \mathbb{B}^\lambda$.

3) För att fortsätta härifrån måste vi ju ha något att jämföra våra mätningar med. Detta kräver en fysikalisk modell och alltså information om

- ⋆ Algoritmen som exekveras
- ⋆ Hårdvaran den exekveras på
- ⋆ Operationernas effektberoende med avseende på operanderna

De vanligaste modellerna grundar sig på hammingvikt, hammingavstånd, nollvärde (alltså att fallet att operanden 0 i vissa fall ger lägst eller högst effektförbrukning) eller beroende av enskilda bitar, men det finns också andra modeller. På samma sätt som vi, med mätningar, byggde upp $v_{\mu,\nu}$ bygger vi nu, genom simuleringar, upp motsvarande $h_{\mu,\nu}$.

4) Nu blir det dags för att gissa hemligheter. Detta görs med statistiska metoder som jämför våra spår, $t_{\mu,\nu}$ med våra simuleringar, $h_{\mu,\nu}$. För att sätta upp ett linjärt förhållande mellan dem räknar vi ut korrelationskoefficienter, $r_{\alpha,\beta} \in \mathbb{R}$, (med avseende på de olika k_ν) som alltså beskriver korrelationen mellan simulering för nyckeln k_α och spår för nyckeln k_β. Genom att beteckna medelvärdet med avseende på datablocken som $\overline{h_\alpha}$ och $\overline{t_\beta}$ för simulering med nyckel k_α respektive spår med nyckel k_β kan vi skriva korrelationskoefficienterna som:

$$r_{\alpha,\beta} = \frac{\sum_{\rho=0}^{D-1}(h_{\rho,\alpha} - \overline{h_\alpha}) \cdot (t_{\rho,\beta} - \overline{t_\beta})}{\sqrt{\sum_{\rho=0}^{D-1}(h_{\rho,\alpha} - \overline{h_\alpha})^2 \cdot \sum_{\rho=0}^{D-1}(t_{\rho,\beta} - \overline{t_\beta})^2}} \tag{21}$$

där större värde för $r_{\alpha,\beta}$ innebär mer korrelation. Detta ger sannolikhetsfördelningen på vilken en attackerare grundar sina hemlighetsgissningar.

Det finns andra statistiska metoder än korrelationskoefficientjämförelse. Bland annat medelvärdesdifferens, medelvärdesavstånd, generaliserad maximal sannoliketsuppskattning.

DPA kan generaliseras till högre ordningar genom att ta hänsyn till effektförbrukningens beroende av fler än ett mellanstegsvärde.

12.0 Högre ordningens DPA

skriva denna lmao

13 Utblick

Nu bör vi ställa oss frågan hur vi försvarar oss mot effektanalysattacker. Detta ulöser givetvis en lek mellan dem som vill hålla information hemlig och dem som vill skaffa sig fördel i att gissa den. För varje skyddsåtgärd kommer en ny attack. För varje attack kommer en ny skyddsåtgärd.

Försvar mot effektanalysattacker delas vanligen upp i två huvudsakliga kategorier, döljning och maskering. Döljning går ut på att försöka få så små variationer i effektförbrukningen att de blir svåra att mäta. På så sätt får en anfallare inte lika lätt information om effekförbrukningsvariatoner. Maskering går ut på att, på algoritmnivå eller implementationsnivå, konstruera apparaten sådan att effektförbrukningen är operandoberoende. På så sätt kan en anfallare inte lära sig något av sina mätningar.

A Notation och definitioner

Notationen som används skiljer sig en del från standardnotation inom ingenjörsvärlden och drar mer åt det hållet som används inom teoretisk såväl som matetmatisk fysik. Notationen följer [Fur22c] som läsaren bör konsumerat vid det här laget.

$\mathbb{B}$ används för att beteckna mängden $\{0, 1\}$ som är mycket vanlig inom digital elektronik.

$\oplus$ används för den exklusiva eller-operatorn, som definieras bitvis enligt

$$\begin{aligned} \oplus : \mathbb{B} \times \mathbb{B} &\to \mathbb{B} \\ (\alpha, \beta) &\mapsto \alpha \oplus \beta \\ &= |\alpha - \beta| \end{aligned} \tag{22}$$

Och från den definitionen för längre bitsträngar

$$\begin{aligned} \oplus : \mathbb{B}^d \times \mathbb{B}^d &\to \mathbb{B}^d \\ (\alpha_\mu, \beta_\mu) &\mapsto \alpha_\mu \oplus \beta_\mu \\ &= |\alpha_\mu - \beta_\mu|_\mu \end{aligned} \tag{23}$$

Resultatet blir alltså en bitsträng i vilken varje komponent är resultaten av en $\oplus$ mellan motsvarande komponenter i operanderna.

B Förkunskaper

B.0 Naturfilosofi

Läsaren bör vara bekant med

- ⋆ Kretselektronik, se exempelvis [Wes14]
- ⋆ Digital elektronik, se exempelvis [Wes14]
- ⋆ Elektrodynamik, se exempelvis [Fur22d], [Nor] och [Jac62]
- ⋆ För delarna om lågnivåbeskrivning av CMOS fordras även kunskap inom
  - ℘ Kvantmekanik, se exempelvis [Dir82], [Sha13] och [Wol94]
  - ℘ Fasta tillståndets fysik, se exempelvis [Kra87] och [McK93]

B.1 Matematik

Läsaren bör, förutom att ha konsumerat [Fur22c], vara ha kunskaper inom

- ⋆ Reell analys, se exempelvis [Lar05a], [Lar05b], [Kol75], [Spi67] och [Rud66]
- ⋆ Linjär algebra, se exempelvis [Gus13]
- ⋆ Multilinjär algebra, se exempelvis [Gre78]
- ⋆ Sannolikhetslära, se exempelvis [Jay79] och [Kol56]

C Vidare läsning

Läsaren uppmanas gå vidare till [Fur22a] och sen [Fur22b].

En nyfiken läsare kan fördjupa sig med de böcker som har använts vid skrivandet av denna artikel. För effektanalysdelarna framförallt [Eff10], [MO07], [Wes14], [Ros97], [al99], [al09], [Sch04] och [Pee13].

För fördjupning om en fysikalisk lågnivåbeskrivning av strömläckage i CMOS-teknologi hänvisas läsaren till [Nor], [Jac62], [Gri99], [Che89], [Hec15], [Sha13], [Gri18], [Fur22d], [Dir82], [Hen15], [Wol94], [Neu32], [Mag05], [Sch95], [Sch00], [Fol08], [Wei05], [Dre65], [Bae92], [Kra87], [Fur22e] och [McK93].

Referenser

[Fur22a] Anders Furufors. *Effektanalys, Del II: Döljning*. 2022.

[Fur22b] Anders Furufors. *Effektanalys, Del III: Maskering*. 2022.

[Fur22c] Anders Furufors. *Matematisk introduktion*. 2022.

[Wes14] Westcott och Westcott. *Basic Electronics: Theory and Practice*. Mercury Learning & Information, 2014.

[Fur22d] Anders Furufors. *Elektromagnetiska fält, vågledare och antenner, Del I: Elektrodynamikens principer*. 2022.

[Nor] Martin Norgren. *Kompendium i elektromagnetisk fältteori, 2H1250*. Avdelningen för teoretisk elektroteknik, Alfvénlaboratoriet, KTH.

[Jac62] David Jackson. *Classical Electrodynamics*. Wiley, 1962.

[Dir82] Paul Dirac. *The Principles of Quantum Mechanics*. Clarendon Press, 1982.

[Sha13] Ramamurti Shankar. *Principles of Quantum Mechanics*. Springer Verlag, 2013.

[Wol94] Haken och Wolf. *The Physics of Atoms and Quanta*. Springer Verlag, 1994.

[Kra87] Kenneth Krane. *Introductory Nuclear Physics*. Third. Wiley, 1987.

[McK93] John McKelvey. *Solid State Physics for Engineering and Materials Science*. Krieger Pub Co, 1993.

[Lar05a] Arne Persson och Lars-Christer Böiers. *Analys i en variabel*. Studentlitteratur AB, 2005.

[Lar05b] Arne Persson och Lars-Christer Böiers. *Analys i flera variabel*. Studentlitteratur AB, 2005.

[Kol75] Andrej Kolmogorov. *Introductory Real Analysis*. Dover Publications, 1975.

[Spi67] Michel Spivak. *Calculus*. Publish or Perish, 1967.

[Rud66] Walter Rudin. *Real and Complex Analysis*. McGraw-Hill, 1966.

[Gus13] Ivar Gustafsson. *Linjär algebra och numerisk analys*. Institutionen för matematik, Chalmers, 2013.

[Gre78] Werner Greub. *Multilinear Algebra*. Springer Verlag, 1978.

[Jay79] Edwin Thompson Jaynes. *Probability Theory: The Logic of Science*. Cambridge University Press, 1979.

[Kol56] Andrej Kolmogorov. *Foundations of the Theory of Probability*. Martino Fine Books, 1956.

[Eff10] Rankl och Effing. *Smart Card Handbook*. Fourth. Wiley, 2010.

[MO07] Mangard och Oswald. *Power Analysis Attacks*. Springer Verlag, 2007.

[Ros97] Markus Kuhn och Ross Anderson. "Low Cost Attacks on Tamper Resistant Devices". I: *Springer LNCS* (1997).

[al99] Kocher & al. "Differential Power Analysis". I: *Cryptography Research, Inc* (1999).

[al09] Danger & al. "Overview of Dual Rail with Precharge Logic Styles to Thwart Implementation-Level Attacks on Hardware Cryptoprocessors". I: *HAL* (2009).

[Sch04] Helms och Schmidt och Nebel. "Leakage in CMOS Circuits – An Introduction". I: *Springer Verlag* (2004).

[Pee13] Eric Peeters. *Advanced DPA Theory and Practice*. Fourth. Springer Verlag, 2013.

[Gri99] David Griffith. *Introduction to Electrodynamics*. Cambridge University Press, 1999.

[Che89] David Cheng. *Field and Wave Electromagnetics*. Addison-Wesley, 1989.

[Hec15] Eugene Hecht. *Optics*. Pearson, 2015.

[Gri18] David Griffiths. *Introduction to Quantum Mechanics*. Cambridge University Press, 2018.

[Hen15] Måns Henningson. *Börja med kvantfysik*. Institutionen för fundamental fysik, Chalmers, 2015.

[Neu32] John Neumann. *Mathematische Grundlagen der Quantenmechanik*. Springer Verlag, 1932.

[Mag05] Michele Maggiore. *A Modern Introduction to Quantum Field Theory*. Oxford University Press, 2005.

[Sch95] Peskin och Schroeder. *An Introduction to Quantum Field Theory*. CRC Press, 1995.

[Sch00] Franz Schwabl. *Advanced Quantum Mechanics*. Springer Verlag, 2000.

[Fol08] Gerald Folland. *Quantum Field Theory: A Tourist Guide for Mathematicians*. American Mathematical Society, 2008.

[Wei05] Steven Weinberg. *The Quantum Theory of Fields*. Cambridge University Press, 2005.

[Dre65] Bjorken och Drell. *Relativistic Quantum Fields*. McGraw-Hill, 1965.

[Bae92] John Baez. *Introduction to Algebraic and Constructive Quantum Field Theory*. Princeton University Press, 1992.

[Fur22e] Anders Furufors. *Kvantinformatik, Del I: Kvantfysikens principer*. 2022.