O postranních kanálech, nové maskovací technice a jejím konkrétním využití proti Mangerovu útoku na PKCS#1

Vlastimil Klíma [1] a Tomáš Rosa [2]

[1]ICZ a.s., Praha, vlastimil.klima@i.cz

[2] ICZ a.s., Praha a ČVUT - FEL Praha, tomas.rosa@i.cz

Abstrakt

Tento příspěvek má tři hlavní cíle. Za prvé chceme upozornit na význam tvrzení o individuálních bitech RSA v souvislosti s postranními kanály. Za druhé navrhnout teoretickou konstrukci využívající zvláštní maskovací techniku ke snížení vyzařování informací z postranních kanálů a za třetí ukázat využití této maskovací techniky konkrétně při obraně proti Mangerově útoku na PKCS#1.

1 Úvod

Tři roky poté, co Daniel Bleichenbacher zveřejnil svůj útok ([BLEI98]) na formátovací metodu PKCS#1 verze 1.5, byl Jamesem Mangerem na konferenci Crypto´2001 popsán útok ([MANG01]) na opravenou verzi 2.1, konkrétně na formát, který se označuje jako EME-OAEP a je použit ve schématu RSAES-OAEP (některé zdroje používají označení RSA-OAEP). Dodejme, že tento útok nemá nic společného s kritikou odolnosti OAEP vůči útokům s voleným šifrovým textem, kterým tento formát čelí v obecné rovině, viz práce Victora Shoupa ([SHOU01]).

Tento stav ukazuje, že se v praxi začíná naplňovat důsledek často opomíjeného tvrzení o individuálních bitech RSA, které publikovali Johan Håstad a Mats Näslund na konferenci FOCS v roce 1998 ([HANA98]). Tvrzení o individuálních bitech RSA říká zhruba, že: *Pokud RSA není možné prolomit v náhodném polynomiálním čase, potom není možné předpovídat hodnotu libovolného zvoleného bitu otevřeného textu s pravděpodobností výrazněji odlišnou od hodnoty 1/2.* Prolomením RSA se zde rozumí získání hodnoty otevřeného textu, nikoliv získání hodnoty privátního klíče. V této formulaci se tvrzení o individuálních bitech využívá k ujištění, že jednotlivé bity otevřeného textu jsou chráněny stejně dobře jako celý otevřený text. Zároveň odtud ale plyne, že pokud umíme zvolený bit otevřeného textu predikovat s pravděpodobností výrazně odlišnou od hodnoty 1/2, potom existuje pravděpodobnostní polynomiální způsob vedoucí k luštění celého otevřeného textu!

V současné době se bouřlivě rozvíjí teorie postranních kanálů. Jedná se o studium metod založených na obecném modelu kryptografických modulů, které vedou k získání užitečných informací o výpočtech probíhajících v kryptografických modulech (ucelený přehled této problematiky viz [ROSA01], [MUIR01]). Například se může jednat právě o informaci o individuálních bitech otevřených textů vzniklých odšifrováním vstupních šifrových textů pomocí RSA. Jak se ukazuje, RSA je bez ohledu na použité kódovací schéma (například OAEP) při dostupnosti informace z postranních kanálů snadno náchylné k útokům s voleným šifrovým textem. Konkrétní metoda kódování použitá v napadeném šifrovacím schématu pochopitelně může tyto útoky více či méně ztížit. Jako příklad můžeme použít právě srovnání kódování EME-PKCS1-v1_5 dle PKCS#1 verze 1.5 a kódování EME-OAEP dle PKCS#1 verze 2.1. V prvním případě stačilo znát informaci o tom, zda byl otevřený text správně dekódován. Ve druhém případě již útočník potřebuje znát informaci, která se ze zařízení běžně neodesílá, ale i tak může být vyzářena některým z postranních kanálů.

Následující výklad má tři hlavní cíle. Za prvé chceme upozornit na význam tvrzení o individuálních bitech RSA v souvislosti s postranními kanály. Za druhé navrhnout teoretickou konstrukci využívající zvláštní maskovací techniku ke snížení vyzařování informací z postranních kanálů a za třetí ukázat

využití této maskovací techniky konkrétně při obraně proti Mangerově útoku, který využívá postranní informaci o nejvyšším bajtu otevřeného textu.

Předpokládáme, že všechny implementace PKCS#1 by měly projít revizemi, které zjistí použitelnost Mangerova útoku. Při těchto revizích je možné současně také provést některé úpravy, které vyplývají z navrhované maskovací techniky a jsou navrženy konkrétně jako změny v jednotlivých procedurách PKCS#1. V souladu s důsledky tvrzení o individuálních bitech zde poukazujeme i na další možné útoky na šifrovací schéma RSAES-OAEP, které jsou založeny na získaní postranních informací o jednotlivých bitech otevřeného textu RSA.

Navrhovaná maskovací technika je obecná a má relativně snadný teoretický popis. Obecnost zde znamená, že tato technika by při správném použití měla snižovat vyzařování na všech hrozících postranních kanálech bez ohledu na jejich konkrétní druh. Vlastní metoda vychází z toho, že do kritických operací je zaveden náhodně volený parametr, který neovlivní sémantický význam původní operace. Jeho přítomnost však vnáší do signálu šířeného po postranním kanálu náhodný šum, který snižuje efektivitu přenosu ostatních citlivých informací.

Pro odhad teoretických vlastností této konstrukce využijeme maticový model diskrétního kanálu, který se v teorii postranních kanálů zatím příliš nepoužívá, ačkoliv v teorii informace se jedná o naprosto základní konstrukci. Ukážeme, že navržená maskovací technika se dá chápat jako náhodná volba konkrétního druhu diskrétního kanálu.

Poslední část příspěvku se zabývá návrhem opatření proti Mangerově útoku na schéma RSAES-OAEP. Naším cílem bylo použít co možná nejuniverzálnější protiopatření, která jsou schopna účinně bránit využití několika různých postranních kanálů zároveň. Proto jsme navrhli využití maskovací techniky, jejíž vlastnosti jsme v tomto příspěvku teoreticky podložili. Naším cílem zde není předložit schéma, které prokazatelně odolá všem útokům založeným na postranních kanálech. S ohledem na rychlé tempo rozvoje této oblasti to patrně ani není možné. Naším záměrem je zde prezentovat základní aspekty, kterých by si taková protiopatření měla v obecné rovině všímat zejména. Je pravděpodobné, že při výskytu konkrétních druhů útoků cílených na konkrétní vlastnosti napadeného kryptografického modulu bude nutné doplnit také konkrétní a přesně cílená protiopatření. Námi prezentovaný příspěvek si klade za cíl jednak upozornit na to, že takové útoky mohou přijít (a uvést důvody pro tento předpoklad), jednak doporučit protiopatření obecného druhu, která mohou zpomalit dopad nově vzniklých útoků a tím poskytnout čas na doplnění zmíněných cílených protiopatření.

2 Poznámka o termínu „otevřený text“

V následujícím textu budeme často používat výraz otevřený text ve spojení s různými šifrovacími schématy na bázi RSA. Je důležité uvést, že pod tímto pojmem zde budeme rozumět přímo výsledek odšifrovací transformace RSA. Jedná se tedy o hodnotu m, pro kterou platí $m = c^d \bmod n$, kde c je příslušný šifrový text, d je privátní exponent a n je modul RSA. Většina současných šifrovacích schémat na bázi RSA tuto hodnotu m dále zpracovává operací dekódování (například EME-OAEP-Decode), čímž obdrží vlastní přenášenou zprávu M. I této zprávě se však někdy říká otevřený text, čímž by zde mohlo dojít k nedorozumění. Proto na tuto skutečnost raději ještě jednou upozorňujeme.

3 Vliv tvrzení o individuálních bitech

Tvrzení o individuálních bitech bylo poprvé publikováno v [HANA98]. Dodejme, že před tímto uveřejněním existovala řada tvrzení podobného druhu, která však byla poněkud slabší v tom smyslu, že se netýkala všech jednotlivých bitů (jejich přehled je v [HANA98] uveden). Tvrzení dokázané v [HANA98] již zahrnuje všechny bity otevřeného textu.

Z pohledu teorie postranních kanálů je důležité si uvědomit, že důkaz tvrzení o individuálních bitech obsahuje přímo popis luštícího algoritmu, který jako vstupní podmínku předpokládá přístup k orákulu,

které pro vstupní šifrový text poskytuje informaci o jednotlivých bitech otevřeného textu. V případě Mangerova útoku [MANG01] toto orákulum poskytovalo informaci o nulovosti, respektive nenulovosti nejvyššího bajtu otevřeného textu. Bylo ukázáno, že přístup k takovému orákulu umožňuje sestavení velmi efektivního luštícího procesu. Další způsoby využití informace o individuálních bitech najdeme například v [BLEI98] a [STIN95, str. 144-145]. V posledně jmenovaném odkazu se využívá orákulum poskytující informaci o nejvyšším či nejnižším bitu (je ukázáno, že tato dvě orákula jsou polynomiálně převoditelná). Ve srovnání s důkazem tvrzení v práci [HANA98] lze učinit odhad, že mezi jednotlivými bity otevřeného textu existují určité rozdíly v tom, k jak efektivnímu luštícímu algoritmu jejich znalost (přístup k orákulu, které tuto informaci poskytuje) vede. Toto pozorování je důležité zejména pro kryptoanalýzu, neboť dává návod k tomu, na jaké druhy orákul se má kryptoanalytik zaměřit v první řadě. Pro kryptografa je toto sice také podnětný závěr, neboť ví, na co si má dát určitě pozor, avšak v zásadě to velké ulehčení nepřináší. Z pohledu návrhu kryptoschémat totiž vzhledem k tvrzení [HANA98] musíme zabránit vyzáření jakékoliv informace vedoucí k možnosti úspěšného odhadu jednotlivých bitů otevřeného textu.

4 Odhad dalších možných útoků

V této části ukážeme další možný způsob napadení operace odšifrování ve schématu RSAES-OAEP. Vlastní popis útoku je založen na předpokladu, že existuje postranní kanál, vynášející jistou informaci o otevřeném textu. Konkrétně předpokládáme, že útočník má možnost zjistit Hammingovu váhu (budeme ji značit w(x)) určitého slova x. Náš předpoklad vychází z obecné vlastnosti napěťově-proudových postranních kanálů, které mají jasný sklon tuto informaci poměrně čitelným způsobem vyzařovat, viz [MDS99a]. Z citovaného zdroje jsme si sem dovolili pro ilustraci připojit obrázek 1, na kterém je vidět závislost průběhu signálu z napěťově-proudového postranního kanálu na Hammingově vzdálenosti jistých dvou datových položek (bližší komentář je uveden v odkazovaném článku). V uvedené práci je dále poznamenáno, že obdobně markantní závislost lze pozorovat i v případě Hammingovy váhy zpracovávaných dat. Na základě tohoto poznatku jsme navrhli dále popsaný postup útoku na schéma RSAES-OAEP. Poznamenáváme, že tento útok je možné s jistými obměnami provést i v případě, kdy máme přístup spíše k Hammingově vzdálenosti, než váze.

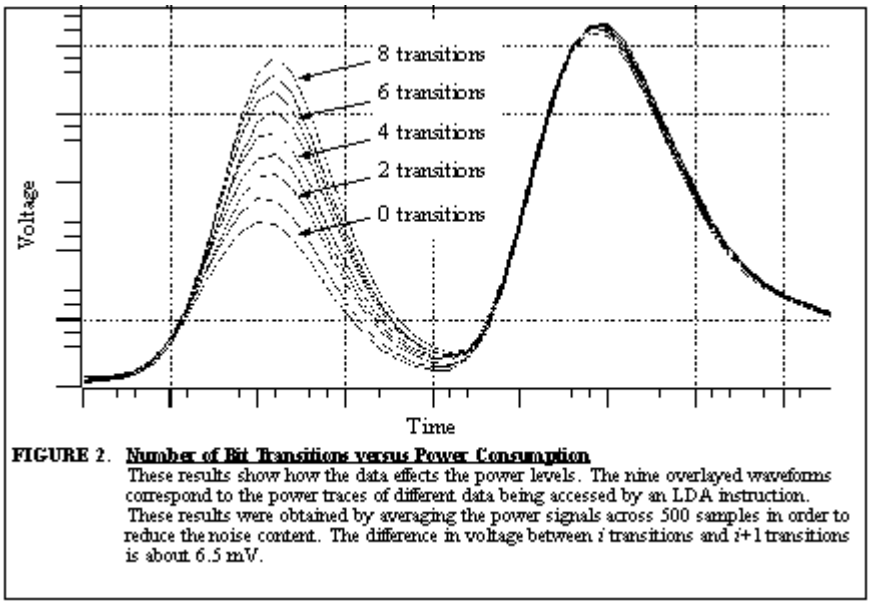


FIGURE 2. Number of Bit Transitions versus Power Consumption
These results show how the data effects the power levels. The nine overlayed waveforms correspond to the power traces of different data being accessed by an LDA instruction. These results were obtained by averaging the power signals across 500 samples in order to reduce the noise content. The difference in voltage between *i* transitions and *i*+1 transitions is about 6.5 mV.

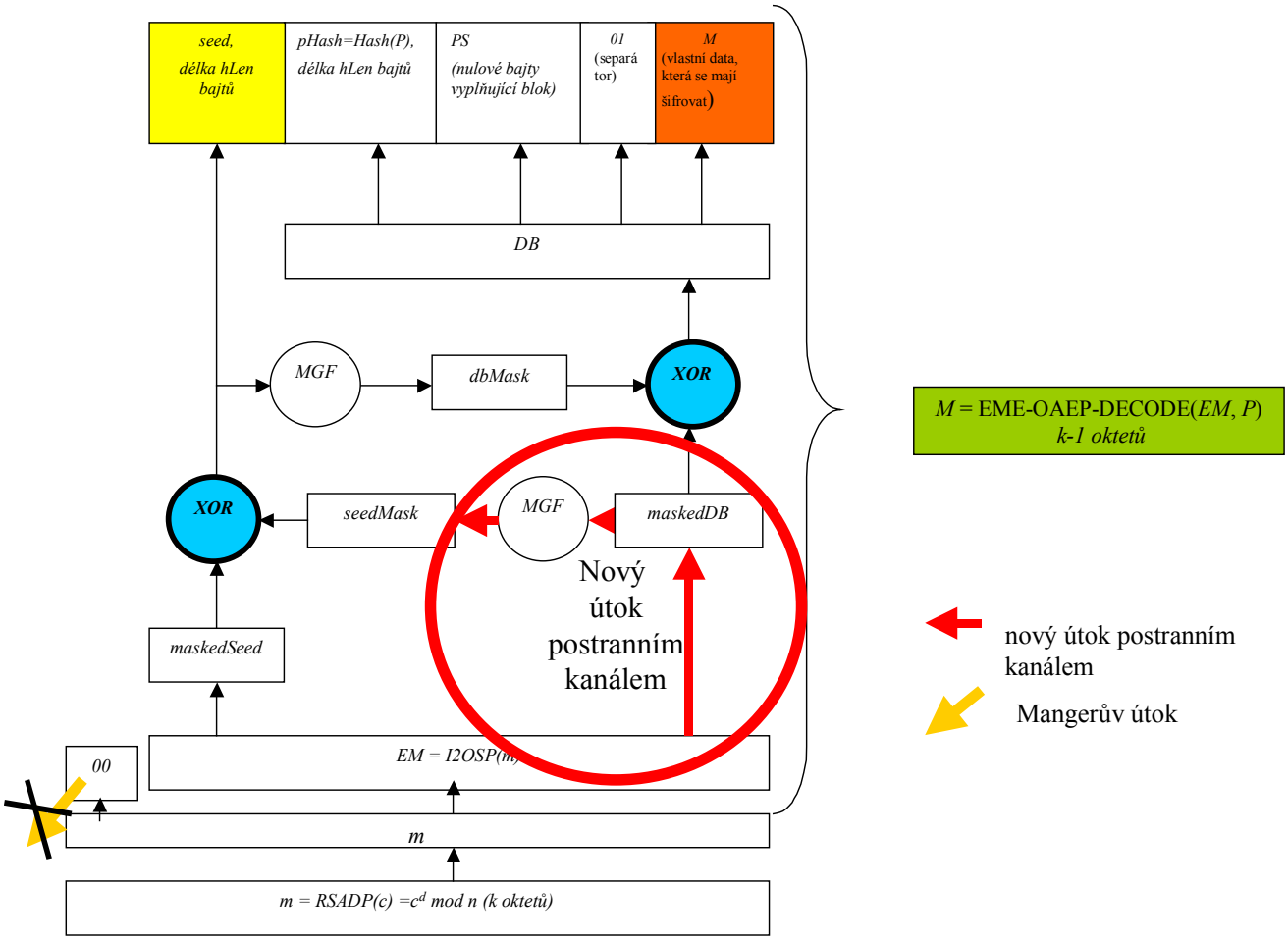
Obrázek 1: Vyzařování informace o Hammingově vzdálenosti (převzato z [MDS99a])

Hledáním konkrétního zařízení s touto vlastností jsme se nezabývali, neboť to nebylo hlavním cílem tohoto příspěvku. Naším cílem je spojit obecně známý poznatek o chování napěťově-proudových postranních kanálů s důsledky tvrzení o individuálních bitech a ukázat tak způsob konstrukce dalšího

možného útoku na schéma RSAES-OAEP. Touto konstrukcí chceme zejména podložit konstatování, že šifrovací schéma RSAES-OAEP je z pohledu postranních kanálů poměrně zranitelné. Přinejmenším více, než by se na první pohled zdálo.V tomto směru je třeba chápat Mangerův útok nikoliv jako ojedinělý exces, nýbrž jako první z řady dalších možných napadení tohoto druhu. Poznamenejme ještě jednou, že vliv postranních kanálů nevychází primárně z vlastností kódování EME-OAEP, ale ze základních vlastností RSA jako takového. Stejný dopad a stejné druhy útoků je tak možné očekávat ve všech šifrovacích schématech, která jsou na RSA založena.

4.1 Využití postranního kanálu k útoku na otevřený text, šifrovaný podle EME-OAEP PKCS#1 s využitím SHA-1

Uvažujme šifrování RSA s modulem n o délce N bitů. Protože nejčastěji používaná N jsou násobky 512 bitů, nechť N = 512*k, kde k je 1, 2, 3, ..., tj. vyšetřujeme mj. nejčastěji používané moduly o délkách 512, 1024, 2048 a 4096 bitů. Útok povedeme na schéma RSAES-OAEP ve fázi odšifrování přijatého šifrového textu. Předpokládáme, že jako funkce MGF1 je použita SHA-1 (bližší popis schématu viz [PKCS#1]). Bod, ve kterém útočíme, je znázorněn na obrázku 2.



Obrázek 2: Bod útoku novým způsobem

Při výpočtu seedMask je použita funkce MGF1 podle vzorce seedMask = MGF1(maskedDB, 20) = SHA-1(maskedDB || 00 00 00 00). Konkrétně tento tvar vyplývá z toho, že výsledek MGF1 má být 20 bajtů, tedy SHA-1 se použije jen jednou s nulovým counterem (counter = 00 00 00 00, viz definici MGF1 v [PKCS#1]). Protože používáme moduly n v délkách 512*k bitů (tj. k*64 bajtů), obsahuje maskedDB vždy 64*k - 1 - 20 bajtů a do zpracování SHA-1 jde tedy 64*k - 21 + 4 = 64*k -17 bajtů. Při výpočtu SHA-1(maskedDB || 00 00 00 00) tedy ve vlastní funkci SHA-1 dojde vždy k doplňování

vstupní zprávy o 17 bajtů na násobek 64 bajtů tak, aby kompresní funkce SHA-1 mohla pracovat s bloky o délkách 64 bajtů (512 bitů). Posledních 21 bajtů posledního bloku známe, neboť se jedná o 4bajtový counter (00 00 00 00) a 17bajtový doplněk. Abychom mohli konkrétně vyjádřit doplněk, uvažujme například 1024bitový modul. Potom do SHA-1 vstupuje (107 + 4 =) 111 bajtů, tj. 888 bitů. Máme 888 = 0x00 00 03 78. Doplněk je podle definice SHA-1 roven (bit jedna, nulové bity a posledních 64 bitů na vyjádření původní délky)

80 || 00 00 00 00 || 00 00 00 00 || 00 00 00 00 || 00 00 03 78. Posledních 21 bajtů je tedy rovno

00 || 00 00 00 80 || 00 00 00 00 || 00 00 00 00 || 00 00 00 00 || 00 00 03 78.

Pro potřeby zpracování funkcí SHA-1 je tento poslední blok naplněn do proměnných W_0,..., W_{15}, kde z W_{10} známe poslední bajt a W_{11} až W_{15} známe celé:

W_{10} = ?? ?? ?? 00

W_{11} = 00 00 00 80

W_{12} = 00 00 00 00

W_{13} = 00 00 00 00

W_{14} = 00 00 00 00

W_{15} = 00 00 03 78.

Při rozšiřování na slova W_{16} až W_{79} dále dostáváme

$W_{16} = S^1(W_{13} \text{ xor } \mathbf{W_8} \text{ xor } W_2 \text{ xor } W_{12})$

$W_{17} = S^1(W_{14} \text{ xor } \mathbf{W_9} \text{ xor } W_3 \text{ xor } W_{13})$

$W_{18} = S^1(W_{15} \text{ xor } \mathbf{W_{10}} \text{ xor } W_4 \text{ xor } W_{14})$

atd.

Při výpočtu W_{16} se provádí jako první operace W_{13} xor W_8, přičemž hodnota W_{13} je nám známa. Tento okamžik je právě příkladem obecné situace, kdy do N-ární operace vstupuje N-1 známých parametrů a jeden neznámý. Zde jsou často aplikovatelné různé postranní kanály, zejména napěťově-proudový a pod. Nyní uvedeme předpoklad útoku. Předpokládáme, že v roli útočníka jsme schopni určit bod, kdy dochází k operaci W_{13} xor W_8 a z jejího průběhu jsme schopni odvodit Hammingovu váhu $\mathbf{w(W_8)}$ neznámého operandu W_8. Obdobnou schopnost předpokládáme i u dalších dvou operací, takže jsme schopni zjistit váhy $\mathbf{w(W_9)}$ a $\mathbf{w(W_{10})}$.

Nyní ukážeme, že z tohoto předpokladu jsme schopni předpovídat hodnotu nejnižšího bitu otevřeného textu (odpovídá bitu $W_{10,8}$, kde $\mathbf{W_{10}} = W_{10,31}\ W_{10,30}\ W_{10,29}...\ W_{10,0}$) s pravděpodobností odlišnou od hodnoty 1/2. Odtud podle tvrzení o individuálních bitech lze očekávat možnost nalezení útoku na celý otevřený text. Vzhledem k tomu, že se zabýváme určením poměrně „citlivého“ bitu, můžeme použít i upravený postup uvedený v [STIN95]. Konkrétní rozbor tohoto postupu již přesahuje ilustrační záměr této části celého příspěvku.

Vlastní postup získání netriviální informace o hodnotě $W_{10,8}$ vypadá následovně: Označme si jako c šifrový text, na který útočíme, jako n modul RSA a jako e veřejný exponent RSA. Nejprve necháme napadené zařízení odšifrovat původní šifrový text c. Během této operace vznikne v zařízení otevřený text m a my získáme hodnoty Hammingových vah $A_1 = w(W_{10})$, $B_1 = w(W_9)$ a $C_1 = w(W_8)$. V následujícím kroku požádáme zařízení o odšifrování hodnoty $c' = c*2^{-e} \bmod n$. Přitom vznikne otevřený text m’ a my získáme Hammingovy váhy $A_2 = w(W_{10}')$, $B_2 = w(W_9')$ a $C_2 = w(W_8')$. Pokud byl bit $W_{10,8}$ nulový, potom po odšifrování vznikla hodnota $m' = m >> 1$. V opačném případě platí $m' = (m + n) >> 1$. Stanovíme-li si jako předpoklad, že $W_{10,8} = 0$, lze na základě uvedených vztahů pro otevřený text m’ odvodit následující tabulku popisující vzájemný vztah hodnot (A_1, B_1, C_1) a (A_2, B_2, C_2). Pokud $W_{10,8} = 0$, potom některý (právě jeden) z těchto řádků popisuje platný vztah mezi uvedenými hodnotami. Toho využijeme tím způsobem, že postupně pro naměřené hodnoty vah

zkoušíme, zda některému ze vztahů vyhoví. Pokud ne, potom hypotézu $W_{10,8} = 0$ zamítneme. V opačném případě ji s určitou chybou (jejíž rozbor přesahuje rámec tohoto příspěvku) přijmeme.

$A_2 = A_1$	$B_2 = B_1$	$C_2 = C_1$
$A_2 = A_1$	$B_2 = B_1$	$C_2 = C_1 + 1$
$A_2 = A_1$	$B_2 = B_1 + 1$	$C_2 = C_1$
$A_2 = A_1$	$B_2 = B_1 + 1$	$C_2 = C_1 - 1$
$A_2 = A_1 + 1$	$B_2 = B_1$	$C_2 = C_1$
$A_2 = A_1 + 1$	$B_2 = B_1$	$C_2 = C_1 - 1$
$A_2 = A_1 + 1$	$B_2 = B_1 - 1$	$C_2 = C_1$
$A_2 = A_1 + 1$	$B_2 = B_1 - 1$	$C_2 = C_1 + 1$

Tabulka 1: Možné vztahy mezi získanými hodnotami vah

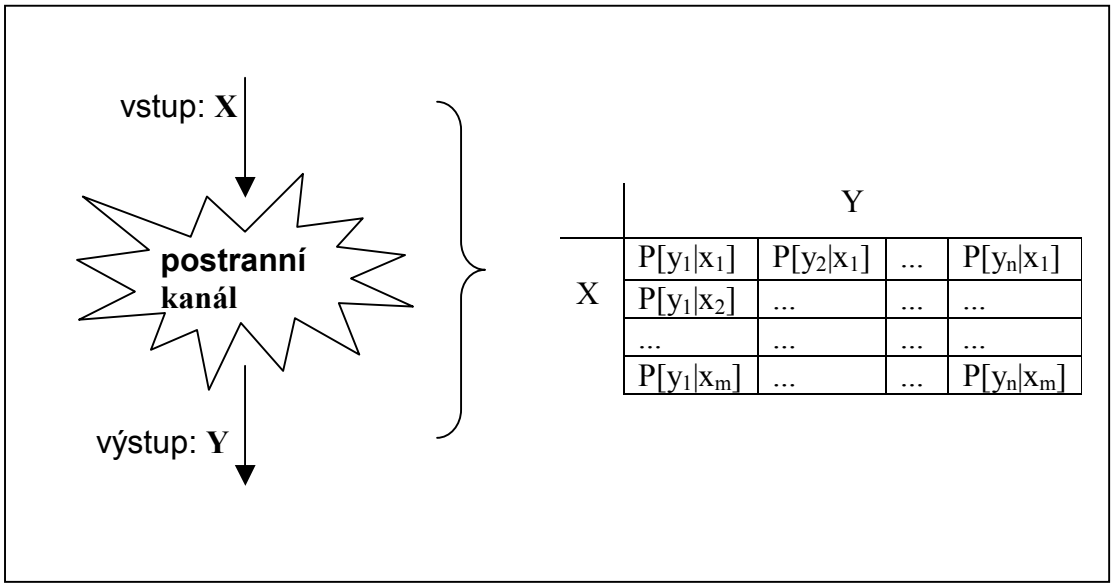
Určení chyby, s jakou s pomocí výše uvedeného postupu získáme hodnotu $W_{10,8}$ zde sice provádět nebudeme, nicméně ukážeme, že získaná informace je určitě netriviální a to v tom smyslu, že nám umožňuje odhadnout hodnotu $W_{10,8}$ s pravděpodobností lepší než 1/2. Označme si $H(W_{10,8} \mid \text{VÁŽENÍ})$ podmíněnou entropii bitu $W_{10,8}$ za předpokladu znalosti výsledku konfrontace získaných vah se vztahy v uvedené tabulce. Přitom VÁŽENÍ $\in$ {platí, neplatí}, kde VÁŽENÍ = platí iff některý z řádků tabulky popisuje platný vztah pro naměřené hodnoty vah. Z rozboru uvedeného postupu plyne, že $H(W_{10,8} \mid \text{VÁŽENÍ} = \text{neplatí}) = 0$, neboť za tohoto předpokladu máme výslednou hodnotu $W_{10,8}$ určenu jednoznačně. Protože $H(W_{10,8} \mid \text{VÁŽENÍ}) = H(W_{10,8} \mid \text{VÁŽENÍ} = \text{neplatí}) * P[\text{VÁŽENÍ} = \text{neplatí}] + H(W_{10,8} \mid \text{VÁŽENÍ} = \text{platí}) * P[\text{VÁŽENÍ} = \text{platí}]$ a $P[\text{VÁŽENÍ} = \text{platí}] < 1$, musí být $H(W_{10,8} \mid \text{VÁŽENÍ}) < 1$. Odtud přímo plyne, že jsme schopni odhadnout hodnotu bitu $W_{10,8}$ s pravděpodobností odlišnou od hodnoty 1/2. Lze tedy očekávat konstrukci úspěšného útoku na celé šifrovací schéma, který má s Mangerovým útokem společné právě jen to, že důsledně využívá zranitelnost RSA přes postranní kanály.

5 Obecná metoda obrany proti postranním kanálům (viz [KLRO01])

Nyní vysvětlíme námi navrhovanou obecnou metodu obrany proti obecným útokům, založeným na postranních kanálech. Poté ji zcela konkrétně aplikujeme na zodolnění formátování šifrovaných zpráv pomocí RSA-OAEP, použité v PKCS#1. Námi navrhovaná metoda je v řadě případů poměrně snadno prakticky implementovatelná, a přitom podle teoretického rozboru poskytuje užitečné obecné výsledky.

Definujme pojem postranního kanálu. *Postranním kanálem* nazýváme každý nežádoucí způsob výměny informací mezi kryptografickým modulem a jeho okolím (podrobněji viz [ROSA01] a série článků o postranních kanálech v [ARCH01]). Z této volné definice vidíme, o jak široké oblasti vlastně hovoříme. Její podání nám však už moc neříká o tom, co si máme pod tímto pojmem představit konkrétně. V kryptoanalýze nám to moc nevadí, neboť zde většinou pracujeme naráz jen s úzce specifickými druhy kanálů, kde se už s jejich přesným popisem nějak dokážeme vypořádat (mnohdy jej ani nepotřebujeme a těžiště leží v popisu metod *analýzy* a *útoku* – o pojmech podrobněji viz výše uvedené odkazy). Jiná situace je však v kryptografii. Zde s ohledem na to, že chceme vytvořit konstrukci odolnou vůči současným i budoucím druhům útoků, potřebujeme nějaký přesnější a zároveň dostatečně obecný model. Pro naše účely si zde představíme obecný model postranního kanálu, analogický k obecnému modelu diskrétního kanálu, který se již řadu let v teorii informace úspěšně používá (viz [HAMM80]).

V rámci našeho modelu si označíme jako X diskrétní náhodnou veličinu značící vstupující informaci a jako Y diskrétní náhodnou veličinu značící informaci vystupující z daného postranního kanálu. U obou veličin předpokládáme konečný obor hodnot, přičemž uvažujeme jen ty hodnoty, kterých tyto veličiny nabývají s nenulovou pravděpodobností. Tento předpoklad můžeme udělat s ohledem na to, že zdrojem veličiny X je v našem případě vždy nějaký počítač, který odpovídá konečnému automatu, a veličina Y je zase vyhodnocována nějakým konečným automatem útočníka. Předesíláme, že tímto modelem postranního kanálu nechceme v tuto chvíli pokrýt kanály založené na kvantové teorii informace.



	Y			
X	$P[y_1\|x_1]$	$P[y_2\|x_1]$	...	$P[y_n\|x_1]$
	$P[y_1\|x_2]$	...	...	...
	...	...	...	...
	$P[y_1\|x_m]$	...	...	$P[y_n\|x_m]$

Obrázek 3: Popis postranního kanálu kanálovou maticí

Vlastní kanál popíšeme maticí, kterou vidíme v pravé části obrázku 3. Tato matice má tvar **SC** = **(** $P_{i,j}$ **)**, kde $P_{i,j} = P[Y = y_j \mid X = x_i]$. Vidíme, že jednotlivé řádky této matice odpovídají příslušným vstupním hodnotám a jednotlivé sloupce zase korespondují s hodnotami výstupu. Konkrétní prvek matice SC (označení od výrazu *Side Channel*) pak odpovídá podmíněné pravděpodobnosti, že na výstupu se objeví hodnota y_j za předpokladu, že na vstupu je hodnota x_i. Matici SC budeme také nazývat *kanálovou maticí*.

Vzhledem k tomu, že pracujeme s pravděpodobnostmi, lze pro prvky kanálové matice poměrně snadno odvodit následující základní vztahy:

$$\Sigma_{(j)} P_{i,j} = \Sigma_{(j)} P[Y = y_j \mid X = x_i] = 1 \qquad (1)$$

$$\Sigma_{(i)} \Sigma_{(j)} P[X = x_i] * P_{i,j} = \Sigma_{(i)} \Sigma_{(j)} P[X = x_i] * P[Y = y_j \mid X = x_i] = 1 \qquad (2)$$

Dále se budeme zabývat určením přenosových vlastností postranního kanálu. K tomuto účelu použijeme konstrukci založenou na vyjádření množství informace o veličině X, která je obsažena ve veličině Y. V anglické literatuře se pro tento pojem používá výraz *vzájemné informace* (*mutual information*), my zde budeme ještě používat termín *informační přenos* (také přenos informace). Tento přenos budeme značit I(X; Y) a definovat jako:

$$I(X; Y) = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X) = I(Y; X) \qquad (3)$$

Výrazem H(X) zde rozumíme entropii veličiny X, H(X | Y) popisuje podmíněnou entropii veličiny X za předpokladu znalosti hodnoty veličiny Y. Stejně chápeme i výrazy H(Y) a H(Y | X).

5.1 O přenosu informace

Pro lepší přehled si výpočet přenosu I(X; Y) naznačíme v jeho významných krocích. Mějme dáno rozdělení vstupní veličiny X jako distribuční funkci $P[X = x_i]$ a matici postranního kanálu **SC** = **(** $P_{i,j}$ **)**

typu [m, n]. To znamená, že veličina X může nabývat (s nenulovou pravděpodobností) celkem m různých hodnot, kde každá z nich se může projevit jako n různých hodnot výstupní veličiny Y. Předpokládejme útočníka, který sleduje výstupní veličinu Y. Naším úkolem bude určit, jak velké množství informace o vstupní veličině X takový útočník může získat.

Nejprve si na základě matice SC určíme distribuční funkci veličiny Y jako $P[Y = y_j]$. Zde můžeme psát:

$$P[Y = y_j] = \sum_{(i)} P_{i,j} * P[X = x_i] \qquad (4)$$

Na základě získané distribuční funkce již snadno určíme entropii H(Y) jako:

$$H(Y) = \sum_{(j)} P[Y = y_j] * log_2(P[Y = y_j]^{-1}) \qquad (5)$$

Zde sčítáme přes všechny nenulové hodnoty distribuční funkce $P[Y = y_j]$. Dále pokračujeme ve výpočtu podmíněné entropie H(Y | X):

$$H(Y \mid X) = \sum_{(i)} P[X = x_i] * H(Y \mid X = x_i), \qquad (6)$$

$$kde\ H(Y \mid X = x_i) = \sum_{(j)} P_{i,j} * log_2(P_{i,j}^{-1}) \qquad (7)$$

Opět sčítáme přes všechny nenulové hodnoty $P_{i,j}$ a $H(Y \mid X = x_i)$. Pro snazší pochopení těchto vztahů připomeňme, že $P_{i,j} = P[Y = y_j \mid X = x_i]$. Nyní již zbývá jen dosadit do rovnice (3), kterou použijeme ve tvaru $I(X; Y) = H(Y) – H(Y \mid X)$.

Z uvedeného výpočtu vidíme, že výsledný informační přenos je závislý nejen na vlastnostech kanálu jako takového (ty zachycuje matice SC), ale i na rozdělení vstupní veličiny X. Konkrétně sem tato závislost vstupuje prostřednictvím rovnic (4) a (6).

$SC_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$SC_2 = \begin{bmatrix} 1/3 & 2/3 \\ 2/3 & 1/3 \end{bmatrix}$

$SC_3 = \begin{bmatrix} 1/3 & 2/3 \\ 1/3 & 2/3 \end{bmatrix}$

	SC_1	SC_2	SC_3
$P[x_1] = 1/2$ $P[x_2] = 1/2$ H(X) = 1b	I(X;Y) = 1 I(X;Y) / H(X) = 1	I(X;Y) = 0.0817 I(X;Y) / H(X) = 0.0817	I(X;Y) = 0 I(X;Y) / H(X) = 0
$P[x_1] = 1/3$ $P[x_2] = 2/3$ H(X) = 0.9183b	I(X;Y) = 0.9183 I(X;Y) / H(X) = 1	I(X;Y) = 0.0728 I(X;Y) / H(X) = 0.0793	I(X;Y) = 0 I(X;Y) / H(X) = 0
$P[x_1] = 1/10$ $P[x_2] = 9/10$ H(X) = 0.469b	I(X;Y) = 0.469 I(X;Y) / H(X) = 1	I(X;Y) = 0.0298 I(X;Y) / H(X) = 0.0635	I(X;Y) = 0 I(X;Y) / H(X) = 0

Obrázek 4: Příklady výpočtu informačního přenosu

Pro lepší názornost jsou na obrázku 4 uvedeny kanálové matice pro tři konkrétní postranní kanály. Všechny jsou typu [2, 2], takže předpokládáme vstupní a výstupní veličiny nabývající nejvýše dvou různých hodnot. Připojená tabulka uvádí informační přenosy jednotlivých kanálů v závislosti na rozdělení vstupních hodnot.

5.2 Nulový informační přenos

Při pohledu na obrázek 4 vidíme, že nejhoršího přenosu dosahuje kanál, v jehož matici si jsou vektory všech řádků rovny. Lze dokázat, že takový kanál má bez ohledu na rozdělení vstupu vždy nulový

informační přenos. Veličiny X a Y se za tohoto stavu chovají jako dvojice nezávislých náhodných veličin, takže $H(Y \mid X) = H(Y)$. Odtud pak přímo z rovnice (3) dostáváme, že $I(X; Y) = 0$.

5.3 Zajištění nulového přenosu

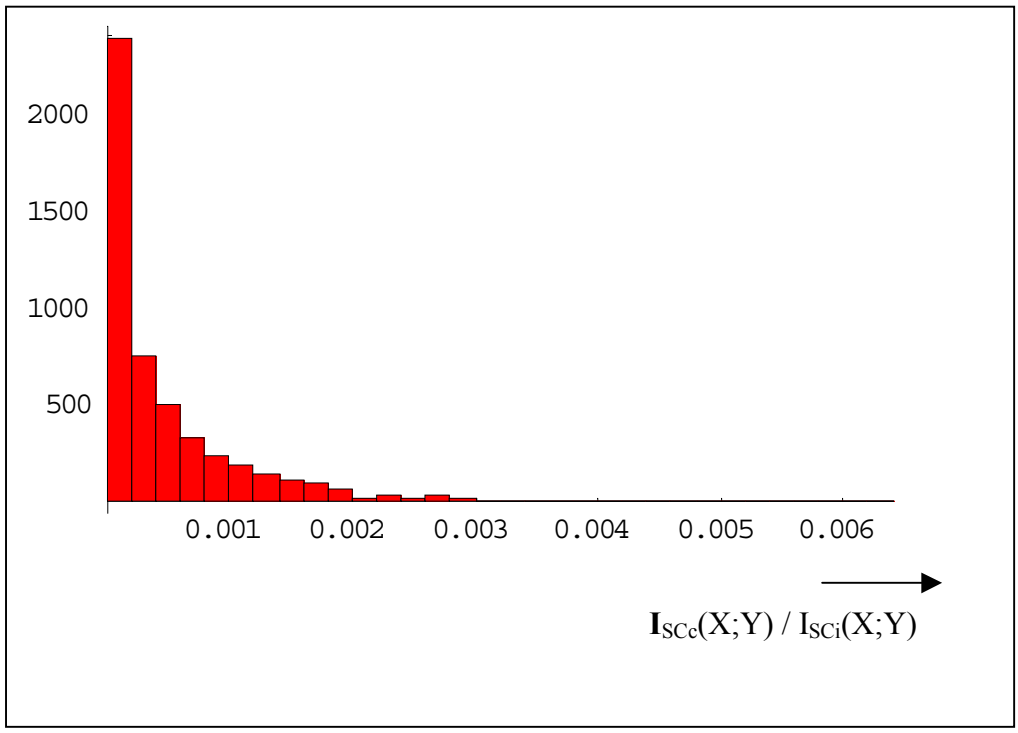
Z předchozího víme, jak by měla vypadat kanálová matice „neškodného" postranního kanálu. Otázkou však zůstává, jak takovou matici vytvořit. Cesta vedoucí přes přímé ovlivnění fyzikálních vlastností daného kanálu je s výjimkou použití dokonalého stínění technologicky téměř vyloučena. Alespoň tedy v obecném případě, a my se zde právě chceme na obecný případ zaměřit. Na první pohled by se mohlo zdát, že jsme zde v podobně svízelné situaci, v jaké jsou výzkumníci v oblasti teorie kódování – víme, jak by měla kanálová matice vypadat, ale nevíme, jak to schůdnou cestou zaručit. Zatímco v teorii kódování často nezbývá než tuto cestu zcela opustit a věnovat se toliko vhodnému přizpůsobení vysílače (vhodným kódem), my zde jistou šanci máme. Poznamenejme, že ji máme právě proto, že chceme dosáhnout minimálního a nikoliv maximálního přenosu.

Představme si, že sice nemáme možnost měnit fyzikální vlastnosti daného kanálu, ale že máme možnost nechat zařízení před každou vyzářenou informací náhodně zvolit jeden z r postranních kanálů. Předpokládejme, že tato volba probíhá s rovnoměrným rozdělením a že r je velké. Formálně tato situace znamená, že místo jedné matice SC máme množinu matic $\{ SC_1, SC_2, ..., SC_r \}$, z nichž se před každým odesláním informace do postranního kanálu náhodně vybere nějaká matice SC_i, podle které bude daný přenos probíhat. Před příštím přenosem se volba matice opět opakuje.

Položme si následující otázku: Jak bude vypadat výsledná kanálová matice takto řízeného kanálu z pohledu útočníka? Opět není příliš těžké dokázat, že situace se bude jevit, jako by byl použit postranní kanál popsaný maticí:

$$SCc = r^{-1} \sum_{i=1}^{r} SC_i \qquad (9)$$

V sumě je použit klasický maticový součet, násobení hodnotou r^{-1} představuje násobení matice skalárem. Zaměřme se nyní na chování hodnot v jednotlivých sloupcích výsledné matice SC_c (nazveme ji *maticí kanálové superpozice*). Zjednodušíme-li poněkud naše úvahy tím, že budeme odpovídající si hodnoty ve sloupcích matic SC_i považovat za hodnoty nezávislých náhodných veličin se stejným (po sloupcích) rozdělením, potom lze pro velká r podle zákona velkých čísel očekávat, že hodnoty ve sloupcích matice SC_c se budou blížit k určité střední hodnotě. Konkrétní číslo reprezentující tuto střední hodnotu zde pro nás není důležité. Důležité je, že vzdálenost mezi hodnotami ve sloupcových vektorech se bude s rostoucím r pravděpodobně zmenšovat, čímž se matice SC_c bude blížit tvaru, pro který dostáváme nulový informační přenos. Názorně tuto situaci ilustruje obrázek 5, na kterém je zachycena hustota distribuční funkce náhodné veličiny vyjadřující poměrnou změnu v informačním přenosu. Graf byl získán tak, že se 1000krát náhodně vygenerovala sada 256 (tj. r = 256) kanálových matic typu [2, 2]. Pro každou sadu se vypočítala výsledná matice SC_c a vyhodnotila se poměrná změna přenosu pro každou matici ze sady jako $I_{SCc}(X; Y)/I_{SCi}(X; Y)$. Každá sada tak poskytla 256 údajů o relativní změně, takže celkem se v grafu zpracovalo 256 000 takových změn. Vlastní graf byl vykreslen programem *Mathematica 4*. Pro tento ilustrační experiment bylo předpokládáno, že vstupní veličina X má rovnoměrné rozdělení. Nechceme zde tvrdit, že takto přesně bude vypadat chování všech možných superpozic. Chceme zde pouze prezentovat příklad popisující obecný trend relativní změny informačního přenosu, který plně podporuje námi odhadované chování celého systému. Tento trend říká, že ve většině případů dojde po superpozici k výraznému poklesu přenosu informace.



Obrázek 5: Rozdělení relativní změny informačního přenosu pro superponovaný kanál

5.4 Parazitní vyzařování operací

Zbývá ještě vyřešit otázku, jak do systému zanést náhodnou volbu kanálové matice. Pro tento účel se zaměříme na konkrétní operace, které probíhají v námi sledovaném a zabezpečovaném modulu. *Parazitním vyzařováním* zvolené operace nazveme postranní kanál, který přenáší informaci o vstupních hodnotách této operace. Mějme například operaci $f: A \rightarrow Im(f)$. Potom parazitní vyzařování této funkce bude popsáno kanálovou maticí, kde počet řádků bude odpovídat počtu prvků z množiny A, které s nenulovou pravděpodobností vstupují do funkce f. Počet sloupců pak bude korespondovat s počtem různých znaků, které je možné pozorovat na výstupu daného postranního kanálu. Pojem znak je v tomto kontextu třeba chápat velmi obecně.

Funkce, kterou jsme si představili, patří do kategorie unárních operací. Obecně si představme n-ární operaci vystupující jako zobrazení $f: A_1 \times A_2 \times ... \times A_n \rightarrow Im(f)$. Předpokládejme dále, že jeden z argumentů o dostatečně velkém rozsahu hodnot (m) není pro výsledek operace sémanticky důležitý, takže jej můžeme použít k libovolnému účelu (konkrétně nechť to je a_n, nabývající r hodnot). Navíc víme, že n-ární operaci $f(a_1, a_2, ..., a_n)$ můžeme pro vybraný argument a_n popsat jako r (n-1)-árních operací $\{ f_1(a_1, a_2, ..., a_{n-1}), f_2(a_1, a_2, ..., a_{n-1}), ..., f_m(a_1, a_2, ..., a_{n-1}) \}$, kde hodnotu a_n dosazujeme vždy implicitně. Přitom každá z těchto funkcí má vlastní charakter parazitního vyzařování, který je popsán maticemi $\{ SC_1, SC_2, ..., SC_r \}$. Volbou konkrétní hodnoty parametru a_n tak vlastně volíme konkrétní vyzařovací matici SC_i a to je právě ten „trik“, který jsme potřebovali.

5.5 Příklad použití

Ukázali jsme si, že ústřední myšlenkou popisované techniky je zanesení náhodné volby některého z parametrů zabezpečované operace. Tento parametr musí mít dostatečně velký rozsah hodnot, aby se začal projevovat zákon velkých čísel pro výslednou kanálovou matici parazitního vyzařování, a zároveň nesmí ovlivnit sémantiku této operace v daném kontextu. Představme si například, že potřebujeme ochránit součet dvou 16bitových (modulo 2^{16}) čísel a že máme k dispozici 32bitovou sčítačku. V takovém případě si můžeme za maskovací parametr zvolit obě horní (numericky významnější) poloviny vstupujících 32bitových slov, které naplníme náhodnými hodnotami. Do dolních polovin vstupních slov pak umístíme hodnoty, které chceme sečíst. Náhodné maskovací

hodnoty nám zde provádějí volbu jedné z 2^{32} kanálových matic, což by se mělo projevit výrazným poklesem nežádoucího informačního přenosu. Obdobně je možné maskovat operace násobení, logický součet, součin, nonekvivalenci a další.

5.6 Poznámka o účelu

Je třeba upozornit, že navrhovaná technika má sloužit zejména jako preventivní doplňková ochrana. Detailnímu rozboru jsme se zde věnovali proto, abychom ukázali, že její aplikace má svůj smysl, a že je tudíž vhodné věnovat jí během návrhu kryptografických modulů určitou pozornost. Nechceme však tvrdit, že tato technika je schopná nahradit ostatní protiopatření, která jsou konstruována přímo proti konkrétním druhům útoků (jejich popis je podán v připojených referencích). Na to je příliš obecná. V kombinaci s ostatními protiopatřeními však tato obecnost pomáhá čelit dosud neznámým druhům útoků, u kterých může výrazně zbrzdit jejich dopad. Protože útoky se většinou zdokonalují postupně, může toto zbrždění právě poskytnout konstruktérům čas na to, aby na nově vzniklé útoky reagovali vývojem cílených intenzivních protiopatření.

5.7 Shrnutí metody

Ukázali jsme si obecný model postranního kanálu a jeho souvislosti s parazitním vyzařováním operací, probíhajících v kryptografických modulech. Zavedli jsme si pojem informačního přenosu a odvodili jsme jeho závislost na matici postranního kanálu (SC). Na základě toho jsme prokázali kladný přínos techniky maskování citlivých operací náhodnou volbou sémanticky nedůležitých vstupních parametrů pro potlačení parazitního vyzařování těchto operací. Při odhadu síly konstruovaných mechanizmů jsme vyšli důsledně z teorie informace, což nám intuitivně říká, že výsledný návrh má dobré předpoklady pro to, aby v praxi obstál.

6 Některé návody pro obecná a praktická protiopatření proti postranním kanálům v implementacích PKCS#1

Klíčovou z hlediska Mangerova útoku na PKCS#1 byla procedura RSAES-OAEP-Decrypt, která je volána k odšifrování šifrového textu c. Tato procedura volá další dílčí procedury I2OSP a EME-OAEP-Decode. V následujícím mohou být všechny tyto procedury považovány za dílčí a mohou na ně být aplikována následující námi doporučovaná pravidla jako preventivní opatření proti útokům založeným na postranních kanálech. Uvažujme systém, který se skládá z posloupnosti několika částečných výpočtů (procedur) comp_1(...), comp_2(...), ..., comp_n(...).

6.1 Minimální obecná pravidla:

1. Nepoužívejme příkazy "stop" nebo "break". Zdá se to být zcela zřejmé, ale formálně jsou tyto příkazy v PKCS#1 použity a měly by být vyloučeny.
2. Pro různé datové vstupy udělejme výpočetní proces "spojitý" a "stejný", jak je to jen možné. Abychom se bránili časovému útoku, měla by být posloupnost výpočtů comp_1(...), comp_2(...), ... stejná a bez datově závislých větvení. Chování fyzikálního zařízení, které zajišťuje tyto výpočty, by mělo být co nejvíce nezávislé na datových vstupech. Pochopitelně, že je to teoreticky nemožné, ale v praxi bychom tento princip měli co nejvíce dodržovat, když píšeme program nebo používáme nějaké konkrétní zařízení.
3. Používejme standardní výstupy z dílčích výpočtů. Dílčí výsledky by měly vždy vracet nějaký chybový kód, nějaký pointer na výstupní data a délku těchto dat. Tyto proměnné by měly být počítány co možná nejvíce stejným procesem pro různé datové vstupy (i když někdy to není tak triviální, jak se na první pohled zdá). Dílčí procedury comp_X (X = 1, 2, ..., n) by měly vracet chybový kód error_X, pointer na výstupní data output_X a délku dat length_X. Poznamenejme, že ne všechny dílčí výpočty musí definovat všechny tři návratové hodnoty. Jakmile jsou ale definovány, musí být vždy počítány.

4. Dílčí návratové kódy by měly být nulové, jestliže vše proběhlo v pořádku, a náhodné nenulové, jestliže bylo něco špatně. Náhodné nenulové hodnoty (random nonzero, RNZ) by měly být k dispozici jako globální proměnné nebo by měly být vytvořeny na požádání jednou z dílčích procedur (například Get_RNZ(..)). Připomínáme zde, že se musí uplatnit pravidlo 2, což znamená, že volání a používání proměnné RNZ nesmí samo o sobě vytvářet větvení dílčí procedury. Poznámka: V některých případech může být těžké získat náhodnou hodnotu. Například v jednoduchých čipových kartách. V tomto případě ji můžeme odvodit přímo z nějakých částí dešifrované zprávy m. Musí to být uděláno velmi opatrně, jinak to může vytvářet nový postranní kanál.
5. V každém následujícím dílčím výpočtu comp_(X+1) kromě posledního můžeme využít datové výstupy z předchozích dílčích výpočtů (tj. output_X a length _X), ale nereagujeme na předchozí návratové chybové kódy error_X (pravděpodobně by to vytvořilo větvení v programu).
6. Po ukončení všech dílčích výpočtů vypočítáme závěrečný chybový kód jako OR všech dílčích chybových kódů: final_error = error_1 OR error_2 OR ... OR error_n. Podle této hodnoty se rozhoduje, zda výstupní data z celého výpočtu jsou platná nebo ne.
7. Nenulové náhodné návratové kódy by měly mít co největší rozsah, například to mohou být bajty nebo 32bitová slova. Čím delší, tím větší maskování se provádí. Tento princip je přímou aplikací techniky výběru náhodného kanálu, jak bylo popsáno výše. Konkrétně, pokud volíme bajtové hodnoty, používáme náhodný výběr jednoho z 255 náhodných kanálů.
8. Jako výsledek uvedených principů je možné z procedury I2OSP (klíčové pro Mangerův útok) vracet místo chybového hlášení "Integer too large" chybový kód rovný přímo nejvyššímu bajtu vstupního celého čísla, tj. error_ I2OSP = X, kde X je popsaný bajt, zatímco zbytek vstupního celého čísla se předává vždy k dalšímu zpracování (formou pointeru a délky). Návratový kód error_ EME-OAEP-Decode z procedury EME-OAEP-Decode je podle uvedených zásad buď nulový (dekódování a kontrola je v pořádku) nebo náhodný nenulový bajt. Výsledný chybový kód vznikne jako final_error = error_EME-OAEP-Decode OR error_ I2OSP , podle něhož se rozhoduje, zda výsledná data jsou platná, eventuelně se vydává závěrečné chybové hlášení z procedury RSAES-OAEP-Decrypt.
9. Předání chybových kódů z jednotlivých procedur musí být pokud možné prosté parazitního vyzařování. To se týká zejména bodu 8 a procedury I2OSP. Pro tyto hodnoty musí být použity paměťové oblasti s maximálně potlačeným parazitním vyzařováním (takové oblasti musí existovat, má-li dané zařízení vůbec obstát). Za určitých okolností mohou být stejně citlivé i návratové hodnoty lenght_X.

6.1.1 Příklad - Proč používat náhodné chybové kódy?

Ukážeme si to na příkladu PKCS#1, kdy použijeme jen hodnoty 0 a 1 pro chybové kódy error_I2OSP (zkráceně error_1) a error_EME-OAEP-Decode (error_2). Nechť X označuje nejvýznamnější bajt odšifrovaného celého čísla m ($m = c^d \bmod n$). Je-li X nenulové, šifrový text je špatný, takže nastavíme error_1 = 1. Je-li X nulové, nastavíme error_1 = 0. Výsledný chybový kód je defonován jako final_error = error_1 OR error_2. Útočník může volit šifrové texty a (například využitím napěťově-proudové analýzy) studovat chování systému v době, kdy je počítána final_error. Mohou nastat pouze tyto případy error_1 OR error_2:

(0 OR 0) - odpovídá správnému šifrovému textu

(1 OR 1) - odpovídá špatnému šifrovému textu, když nejlevější bajt není nula

(0 OR 1) - odpovídá špatnému šifrovému textu, když nejlevější bajt je náhodně nula

(1 OR 0) - skoro nemožná situace (při volbě šifrového textu za současné neznalosti textu otevřeného), když integritní kontrola na m je v pořádku, ale nejlevější bajt je špatně.

Jestliže útočník posílá správný šifrový text, učí se, jak se systém chová v prvním případě. Když posílá špatný šifrový text, učí se chování systému v druhém případě nebo ve třetím případě. Po fázi učení je útočník schopen rozlišit mezi případy, kdy error_final je počítána jako (0 OR 1) nebo jako (1 OR 1),

tedy zjistit error_1. Z error_1 však nyní dostává stejnou informaci jako z chybového hlášení "Integer too large" a máme zde zpět hrozbu v podobě Mangerova útoku.

Abychom předcházeli různým druhům postranních kanálů, musíme se obecně vyvarovat toho, aby (citlivá) proměnná X vstupovala do N-árních operací, kde zbývajících N-1 operandů je známých útočníkovi. Zejména to platí pro případ analýzy spotřeby energie. Například musíme vyloučit operace typu "X + const", "if (X != 0) then" atd. Z tohoto obecného principu a z výše uvedeného plyne, že pokud nastane chyba v proceduře EME-OAEP-Decode, jí vracená hodnota error_OAEP by měla být náhodná nenulová (pokud by byla konstantní, mohla by prozrazovat s ní zpracovávanou hodnotu error_1).

Abychom vyloučili jakýkoliv útok (zejména jeho učící fázi) využívající konstantní chybové kódy, je lepší používat náhodné nenulové hodnoty pro všechny chybové kódy v daném programu nebo aplikaci (teď už nehovoříme jen o PKCS#1). Tyto náhodné nenulové hodnoty by ale měly být připraveny před voláním odpovídajících procedur (comp_X) nebo voláním procedury "Get_RNZ" uvnitř nich na jejich počátku.

7 Závěr

V tomto příspěvku jsme připomněli některé zásadní důsledky, které má pro kryptosystém RSA tvrzení o individuálních bitech, které bylo formulováno a dokázáno v [HANA98]. Ačkoliv platnost tohoto tvrzení je obecně považována za dobrou vlastnost RSA, my jsme zde upozornili na možné negativní důsledky, které umožňují konstrukci útoků založených na postranních kanálech. Jak dokazují práce [BLEI98] a [MANG01], je schéma RSA náchylné k útokům založeným na postranních kanálech nejen teoreticky, ale i prakticky. V příspěvku [MANG01] byl původ této náchylnosti připisován vlastnostem použité kódovací metody označované jako OAEP. My však považujeme za důležité uvést, že skutečný původ této sensitivity jde daleko za rámec použitého kódování. Skutečný původ podle nás spočívá právě v tvrzení o individuálních bitech. Vlastní důkaz tohoto tvrzení je totiž zároveň sám o sobě návodem k tomu, jak z částečné znalosti otevřeného textu získat jeho znalost úplnou!

Použitý typ kódování může diskutovanou náchylnost snížit (což je vidět prakticky při srovnání formátů PKCS1-v1_5 a EME-OAEP, viz [PKCS#1], a příslušných útoků [BLEI98], [MANG01]), ale pro její úplné zamezení je patrně třeba provést specifické úpravy přímo konkrétních implementacích. Pro podložení tohoto názoru jsme v sekci 4 nastínili další z možných útoků na šifrovací schéma RSAES-OAEP, kde narozdíl od Mangerova přístupu útočíme na tu část otevřeného textu, která je pod „správou“ metody OAEP. Ukazujeme, že při dostupnosti určitého druhu postranního kanálu jsme schopni získat informaci o nejnižším bitu otevřeného textu. Na jejím základě je pak možné konstruovat další postupy vedoucí až k získání celého otevřeného textu. Pro zabránění tomuto útoku je třeba zamezit parazitnímu vyzařování jednotlivých operací v dílčích procedurách celého schématu, což už jde daleko za rámec obecného popisu kódovací metody OAEP.

Ve snaze přispět k obecným druhům opatření proti postranním kanálům jsme dále teoreticky prokázali přínos maskovací techniky založené na náhodné volbě sémanticky nevýznamných argumentů zabezpečovaných operací. Ve své podstatě se jedná o celkem jednoduchou myšlenku, avšak její teoretický rozbor ukazuje, že přes svoji jednoduchost může být tato metoda v praxi velmi přínosná. Její účel spatřujeme zejména v roli doplňkové ochrany, která má za úkol zpomalit dopad budoucích útoků a poskytnout tak čas na implementaci cílených protiopatření.

V šesté kapitole jsou pak uvedena obecná doporučení, která mají za úkol pomoci vytvořit implementaci schématu RSAES-OAEP, která je jednak odolná vůči aktuálnímu Mangerovu útoku [MANG01], jednak bere v úvahu další možné útoky založené na postranních kanálech. V tomto směru zejména doporučujeme sestavovat celé schéma ze základních funkčních bloků, u kterých byla provedena dostatečná ochrana proti parazitnímu vyzařování. To se zde v konkrétním případě týká nejen funkce SHA-1, ale i dalších operací, které pracují s citlivými informacemi. Ještě jednou připomínáme, že mezi citlivé informace patří všechny bity otevřeného textu. V roli doplňkové ochrany pak doporučujeme zvážit využití popsané maskovací techniky.

8 Reference

[ABDM00] Akkar, M.-L., Bevan, R., Dischamp, P. and Moyart, D.: *Power Analysis, What Is Now Possible...*, in Proc. of ASIACRYPT 2000, pp. 489-502, 2000.

[ANDE01] Anderson, R.: *Security Engineering*, John Wiley & Sons, Inc., 2001.

[ANKU96] Anderson, R. and Kuhn, M.: *Tamper Resistance – a Cautionary Note*, in Proc. of 2nd USENIX Workshop On Electronic Commerce, pp. 1-11, 1996.

[ANKU97] Anderson, R. and Kuhn, M.: *Low Cost Attacks on Tamper Resistant Devices*, in Proc. of *Security Protocols '97*, pp. 125-136, 1997.

[ANKU98] Anderson, R. and Kuhn, M.: *Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations*, in Proc. of Information Hiding '98, pp. 124-142, 1998.

[ARCH01] Archiv článků http://www.decros.cz/bezpecnost/_kryptografie.html.

[BDH+97] Bao, F., Deng, R.-H., Han, Y., Jeng, A., Narasimhalu, A.-D. and Ngair, T.: *Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient Faults*, in Proc. of Security Protocols '97, pp. 115-124, 1997.

[BISH97] Biham, E. and Shamir, A.: *Differential Fault Analysis of Secret Key Cryptosystems*, in Proc. of CRYPTO '97, pp. 513-525, 1997.

[BDL97] Boneh, D., DeMillo, R. A. and Lipton, R. J.: *On the Importance of Checking Cryptographic Protocols for Faults*, in Proc. of EUROCRYPT '97, pp. 37-51, 1997.

[BLEI98] Bleichenbacher, D.: *Chosen Ciphertexts Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1*, in Proc. of CRYPTO '98, pp. 1-12, 1998.

[BONE99] Boneh, D.: *Twenty Years of Attacks on the RSA Cryptosystems*, Notices of the American Mathematical Society, vol. 46, no. 2, pp. 203-213, 1999, available at http://crypto.stanford.edu/~dabo/pubs.html.

[CJRR99] Chari, S., Jutla, C.-S., Rao, J. and Rohatgi, P.: *Towards Sound Approaches to Counteract Power-Analysis Attacks*, in Proc. of CRYPTO '99, pp. 398-411, 1999.

[COGO00] Coron, J.-S. and Goubin, L.: *On Boolean and Arithmetic Masking against Differential Power Analysis*, in Proc. of CHES 2000, pp. 231-237, 2000.

[CSD00] Clavier, C., Coron, J.-S. and Dabbous, N.: *Differential Power Analysis in the Presence of Hardware Countermeasures*, in Proc. of CHES 2000, pp. 253-263, 2000.

[DKL+98] Dhem, J.-F., Koeune, F., Leroux, P.-A., Mestré, P. and Quisquater, J.-J. and Willems, J. - L.: *A Practical Implementation of the Timing Attack*, Technical Report CG-1998/1, 1998.

[FIPS-140] *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*, National Institute of Standards and Technology, Issued May 25 2001, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[GOOG01] the thread "*OAEP attack paper?*", 21st August 2001, sci.crypt, available at http://groups.google.com/groups?hl=cs&rnum=2&selm=3B822AED.2CCA0DD3%40zetnet.co.uk

[GOPA99] Goubin, L. and Patarin, J.: *DES and differential power analysis*, in Proc. of CHES '99, pp. 158-172, 1999.

[HAMM80] Hamming, R.-W.: *Coding and Information Theory*, Prentice Hall, 1980.

[HANA98] Håstad, J. and Näslund M.: *The Security of Individual RSA Bits*, in Proc. of FOCS '98, pp. 510-521, 1998.

[KSWH98] Kelsey, J., Schneier, B., Wagner, D. and Hall, C.: *Side Channel Cryptanalysis of Product Ciphers*, in Proc. of ESORICS '98, pp. 97-110, 1998.

[KJB99] Kocher, P., Jaffe, J. and Jun, B.: *Differential Power Analysis*, in Proc. of Crypto '99, pp. 388-397, 1999.

[KJJ98] Kocher, P., Jaffe, J. and Jun, B.: *Introduction to Differential Power Analysis and Related Attacks*, Technical Report, 1998, http://www.cryptography.com/dpa/technical.

[KJJ99] Kocher, P., Jaffe, J. and Jun, B.: *Differential Power Analysis: Leaking Secrets*, in Proc. of CRYPTO '99, pp. 388-397, 1999.

[KLRO01] Klíma V. a Rosa T.: *RSA v novém světle (3)*, Chip 01/2002, dostupné na [ARCH01].

[KOCH96] Kocher, P.: *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*, in Proc. of CRYPTO '96, pp. 104-113, 1996.

[KÖKU99] Kömmerling, O. and Kuhn, M.: *Design Principles for Tamper-Resistant Smartcard Processors*, in Proc. of USENIX Workshop on Smartcard Technology, pp. 9-20, 1999.

[MANG01] Manger, J.: *A Chosen Ciphertext Attack On RSA Optimal Asymmetric Encryption Padding (OAEP) as Standardized In PKCS #1*, in Proc. of CRYPTO 2001, August 2001.

[MASO00] Mayer-Sommer, R.: *Smartly Analyzing the Simplicity and the Power of Simple Power Analysis on Smartcards*, in Proc. of CHES 2000, pp. 78-92, 2000.

[MDS99a] Messegers, T.-S., Dabbish, E. A. and Sloan, R. H.: *Investigations of Power Analysis Attacks on Smartcards*, in Proc. of USENIX Workshop on Smartcard Technology, pp. 151-161, 1999.

[MDS99b] Messerges, T.-S., Dabbish, E. A. and Sloan, R. H.: *Power Analysis Attacks of Modular Exponentiation in Smartcards*, in Proc. of CHES '99, pp. 144-157, 1999.

[MESE00] Messerges, T.-S.: *Using Second-Order Power Analysis to Attack DPA Resistant Software*, in Proc. of CHES '00, pp. 238-251, 2000.

[MESE00b] Messerges, T.-S.: *Securing the AES Finalists Against Power Analysis Attacks*, in Proc. of FSE 2000, pp. 150-164, 2000.

[MOV96] Menezes, A. J., van Oorschot, P. C. and Vanstone, S. A.: *Handbook of Applied Cryptography*, CRC Press, 1996, online at http://www.cacr.math.uwaterloo.ca/hac/.

[MUIR01] Muir, J.-A.: *Techniques of Side Channel Cryptanalysis*, A thesis presented to the University of Waterloo, Canada, 2001, http://www.math.uwaterloo.ca/~jamuir/sidechannel.htm.

[PKCS#1] *PKCS#1 v2.1: RSA Cryptography Standard*, RSA Laboratories, DRAFT2 – January 5 2001, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/.

[RARO01] Rao, J.-R and Rohatgi, P.: *EMpowering Side-Channel Attacks*, preliminary technical report, May 11 2001.

[SCHI00] Schindler, W.: *A Timing Attack against RSA with the Chinese Remainder Theorem*, in Proc. of CHES 2000, pp. 109-124, 2000.

[SHOU01] Shoup, V.: *OAEP Reconsidered (Extended Abstract)*, in Proc. of CRYPTO 2001, August 2001.

[ROSA01] Rosa, T.: *Kryptoanalýza s využitím postranních kanálů*, Vojenská kryptografie IV, Sborník příspěvků, str. 113 – 156, 2001, dostupné v [ARCH01].

[STIN95] Stinson, D.-R.: *Cryptography – Theory and Practice*, CRC Press, 1995.

Informace o autorech

RNDr. Vlastimil Klima, kryptolog, ICZ a.s.

1997 - 2001 Decros - ICZ
1995 - 1996 Decros
1982 - 1992 FMV, FMO
1976 - 1981 MFF UK, obor matematická analýza

Podílel se například na těchto projektech:
SW šifrovací programy, autentizace a šifrování pro zařízení X.25, první český šifrovací čip, rodina algoritmů WinCros, první český systém na bázi eliptických křivek, první český i světový systém pro on-line šifrování souborů v OS Windows, první český Cryptographic Service Provider pro WindowsNT, projekty pro NBÚ.

Publikační činnost:
přes 100 článků, vystoupení na konferencích a přednášek, k dispozici na http://www.decros.cz/bezpecnost/_kryptografie.html, personální stránky na http://cryptography.hyperlink.cz

Ing. Tomáš Rosa

Ing. Tomáš Rosa studoval teoretickou informatiku na katedře počítačů ČVUT FEL (s vybranými partiemi z MFF UK), kde v současné době působí jako doktorand. V rámci vědecko výzkumné činnosti se zabývá teorií postranních kanálů a jejím využitím v kryptoanalýze. Má bohaté pedagogické, přednáškové a publikační zkušenosti z univerzitního i komerčního prostředí.

Ve společnosti ICZ a.s. pracuje jako vedoucí kryptolog. Vede kryptologické oddělení a pracuje na výzkumu a vývoji v oblasti aplikované kryptografie. Byl hlavním architektem prvního českého kryptografického modulu CSP (Cryptographic Service Provider), který je certifikován pro ochranu utajovaných skutečností dle zákona č. 148/1998 Sb. Rovněž se podílel a podílí na dalších projektech pro ochranu klasifikovaných informací dle zákona č. 148/1998 Sb., včetně stupně PŘÍSNĚ TAJNÉ.

Je členem mezinárodních organizací IACR a IEEE.

relevantní internetové odkazy:
http://www.decros.cz
http://www.i.cz
http://crypto.hyperlink.cz