Christine van Vredendaal
Faculteit Wiskunde en Informatica
Technische Universiteit Eindhoven
c.v.vredendaal@tue.nl

Column Masterscriptie

Zekere veiligheid door kangoeroes

Elk jaar reikt de Technische Universiteit Eindhoven prijzen uit voor de beste afstudeerwerken van het afgelopen kalenderjaar. Dit jaar mocht Christine van Vredendaal de prijs voor de beste masterscriptie van het jaar 2014 in ontvangst nemen. In dit artikel zet zij uiteen wat haar afstudeerwerk inhield.

Tegenwoordig is een wereld zonder elektromagnetische cryptografie niet meer voor te stellen. Cryptografie wordt gebruikt voor het versleutelen van je telefoonverkeer, bankinformatie, e-mails en nog veel meer. Versleuteling werkt als volgt (zie Figuur 1). Als Alice een bericht naar haar vriend Bob wil versturen, versleutelt ze dit eerst met een *sleutel*. Als ze het versleutelde bericht dan verzendt, kan niemand het lezen, behalve Bob die het met een sleutel weer kan ontcijferen. In dit artikel zullen we het hebben over asymmetrische cryptografie. Hier heeft iedereen een privésleutel $k \in \mathbb{N}$ en een publieke sleutel $p_k = f(k) \in \mathbb{N}$ voor een bepaalde functie f.

Alice versleutelt haar bericht met Bobs publieke sleutel, waarna alleen Bob met zijn privésleutel het bericht kan lezen. De veiligheid zit in het feit dat f^{-1} zeer moeilijk te evalueren is en dus uit de publieke sleutel de privésleutel niet gevonden kan worden én dat er in principe zoveel mogelijkheden voor de sleutel zijn dat hij niet zomaar te raden valt. Voor elliptische-kromme-cryptosystemen is een veilige sleutel minstens een 256-bits getal. Voor RSA moet men eerder aan een 2048-bits getal denken.

Aanvallen van het nevenkanaal

Een aanvaller Eve probeert toch de sleutel van een cryptosysteem te vinden in de hoop deze te gebruiken om geheimen te achterhalen. Een van de manieren waarop ze dit kan doen is door naar de wiskunde van de versleuteling te kijken, maar we zullen ervan uitgaan dat deze veilig is. Een andere manier om meer informatie over de sleutel te vinden is door het doen van *nevenkanaal-aanvallen* (Engels: side-channel attacks). Van machines die het versleutelen uitvoeren, kan het stroomverbruik, het geluidsniveau of soms zelfs straling gemeten worden. Deze gemeten waarden zijn gecorreleerd aan de operaties die de machine uitvoert en dus ook aan de bits van de waarde van de sleutel. Eén klasse van dergelijke metingen resulteert in informatie die er zo uitziet:

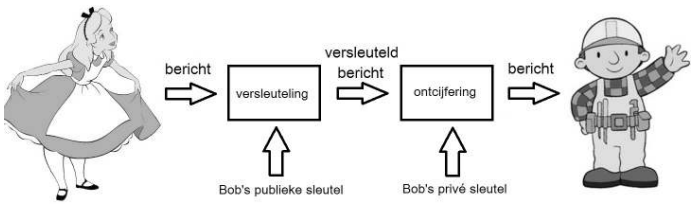
$$k = \underbrace{k_1|\cdots|k_{o-1}}_{\text{groen}}\,|\,\underbrace{k_o|\cdots|k_{r-1}}_{\text{oranje}}\,|\,\underbrace{k_r|\cdots|k_n}_{\text{rood}}.$$

Van de privésleutel k kunnen de meest significante bits (groen) precies achterhaald worden (dit kunnen er ook 0 zijn). Dit betekent dat het interval in $\mathbb{N}$ van 2^n mogelijke sleutels tot een interval van grootte 2^{n-o+1} gereduceerd wordt. Over de volgende bits (oranje) kan men *partiële* informatie vinden. Dit betekent dat er een kansverdeling is die aangeeft wat de kans is dat de sleutel in elk van 2^{r-o} intervallen van grootte $2^{n-r+1} := \ell$ zit. Over de minst significante bits (rood) kan geen informatie gevonden worden. De hoeveelheid groene, oranje en rode bits is afhankelijk van hoe goed het systeem tegen dergelijke aanvallen beschermd is.

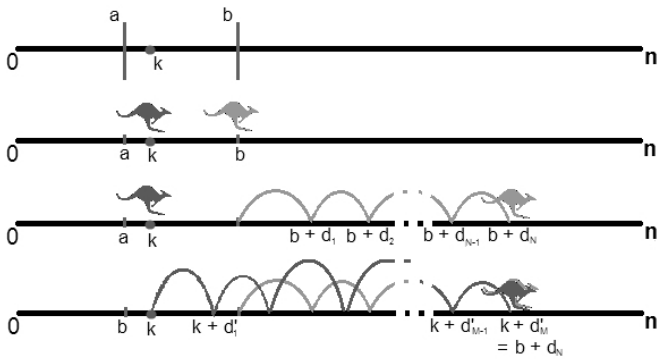
Het ordenen van sleutels

Nadat Eve een nevenkanaal-aanval heeft gebruikt, kan ze de resultaten gebruiken om de sleutel slimmer te zoeken. Wat ze zou doen is begin-

Christine van Vredendaal



Figuur 1



Figuur 2

nen met het interval dat de grootste kans krijgt van de aanval, deze ℓ sleutels doorzoeken en als ze de goede sleutel niet vindt, doorgaan naar het volgende interval met de grootste kans. De zoektijd die Eve op deze manier nodig heeft om de sleutel te vinden, heet de *rang* van een sleutel [3]. Voor Eve zelf is dit concept niet nuttig, omdat ze de sleutel en dus de rang niet weet. Bedrijven die hun creditkaarten, laptops of telefoons met encryptie willen verkopen, weten de sleutel echter wel en kunnen via metingen bepalen welke rang hij heeft. Als de rang van een sleutel laag is dan is de cryptografie niet veilig en kunnen de spullen niet verkocht worden. Als de rang van een sleutel hoger is dan de computerkracht die we veronderstellen dat een aanvaller heeft, dan is de cryptografie veilig genoeg om te gebruiken. Zo kan een gemiddelde laptop in een week 2^{40} sleutels proberen, een computercluster van een universiteit 2^{50} sleutels en misschien dat bepaalde overheidsinstanties wel 2^{80} sleutels kunnen testen. Een rang geeft dus aan hoe veilig een sleutel is, maar dit is alleen relevant als die berekend wordt op basis van de best mogelijke aanvallen. Als men de rang zou berekenen door met brute force alle mogelijkheden te proberen en zou concluderen dat een bepaald systeem veilig is, kan men bedrogen uitkomen als er een slimmere manier bestaat om de sleutels te doorzoeken.

Kruskals kaarttruc

Voor de beschreven nevenkanaal-aanvallen bestaat er een slimmere manier. Voor we bij de methode komen om sneller een interval te doorzoeken, beschouwen we eerst de volgende kaarttruc [1]. Neem een standaard stok kaarten en leg ze open gedraaid in een lange rij op de tafel. Ga denkbeeldig met je vinger op de eerste kaart staan en loop als volgt naar rechts:

- Als je op een getal staat, ga evenveel stappen naar rechts.
- Als je op een Aas staat, ga een stap naar rechts.
- Als je op een plaatje (Boer, Vrouw, Heer) staat, ga vijf stappen naar rechts.

Herhaal dit totdat je van de rij af zou vallen met de volgende stap en onthoud de kaart waar je eindigt. Vertel je slachtoffer dat hij een van de eerste tien kaarten van de rij mag kiezen en op dezelfde manier naar rechts moet lopen als hierboven beschreven. Als jij kan gokken waar hij terechtkomt (voordat hij zijn keuze bekend maakt), win jij de weddenschap. Wijs vervolgens de kaart aan die jij vanaf de eerste kaart had gevonden. In $5/6$ van de keren zal je slachtoffer op dezelfde plaats terechtkomen. Bij dezelfde truc met twee stokken kaarten is dit zelfs in meer dan 95 procent van de gevallen.

Pollards kangoeroe-algoritme

Het concept van Kruskals kaarttruc legt goed uit hoe je een sleutel in een interval vindt met Pollards kangoeroe-algoritme [2]. We plaatsen twee kangoeroes in het interval van mogelijke sleutels, zie Figuur 2. Van de donkergrijze kangoeroe weten we niet wat de sleutel k is (het slachtoffer in de kaarttruc). Van de lichtgrijze kangoeroe weten we de sleutel b wel (de eerste kaart van Kruskal). Vervolgens laten we beide volgens vaste regels naar rechts springen.

Hoe langer ze springen, hoe groter de kans dat ze botsen en op dezelfde waarden terechtkomen. Zo'n botsing kunnen we detecteren met behulp van de functie f en er is dan een methode om te bepalen wat de oorsprong van de donkergrijze kangoeroe was zonder dat we f^{-1} nodig hebben.

Het schatten van de rang

Pollards kangoeroe-algoritme is het best bekende algoritme om een sleutel in een interval te vinden. Als de lengte van het interval ℓ was en allebei de kangoeroes in het interval begonnen, verwachten we dat ze in $O(\sqrt{\ell})$ stappen botsen. Sterker, we kunnen gegeven X stappen van de kangoeroes de kans uitrekenen dat k in het interval zat, maar nog niet gevonden is. Deze kans is voor $X = c \cdot \sqrt{\ell}$ (constante c) zo dicht bij 0 dat we beter het volgende interval kunnen gaan doorzoeken dan alle ℓ sleutels controleren. Daarom weten we dat een aanvaller in elk interval maar $O(\sqrt{\ell})$ berekeningen hoeft te doen om de sleutel te vinden (of niet) en kunnen we nu ook de rang van een sleutel bepalen. We tellen stappen in elk van de intervallen waar de sleutel niet inzit, maar die volgens de nevenkanaal-aanval wel een grotere kans hebben, op en dit is de rang van de sleutel. Deze rang is vele malen realistischer dan simpelweg alle sleutels te tellen in de intervallen. Stel immers dat $\ell = 2^{40}$ en de gebruikte sleutel zit in het 1025ste interval. Als in elk interval alle sleutels getest moeten worden, dan is de rang $1024 * 2^{40} = 2^{50}$. Echter met Pollards kangoeroe-algoritme is een rang van $1024 \cdot c \cdot 2^{20} \approx 2^{30}$ veel realistischer.

Ten slotte

Om de veiligheid van onze cryptografische systemen te garanderen is onderzoek naar de rang erg belangrijk. Mijn bijdrage hierin was het modelleren van nevenkanaal-aanvallen waarin Pollards kangoeroe-algoritme gebruikt kan worden en vervolgens de theorieën ontwikkelen die nodig zijn om de rang van een sleutel te schatten in dit model. Dit zorgt ervoor dat we zekerder kunnen zijn over de veiligheid van onze laptops, creditkaarten en telefoons.

Referenties

1 M. Gardner, Mathematical games, *Scientific American*, februari 1978.

2 J.M. Pollard, Kangaroos, monopoly and discrete logarithms, *Journal of Cryptology*, Volume 13, 2000.

3 C. van Vredendaal, *Rank Estimation Methods in Side-Channel Attacks*, masterscriptie, 2014.