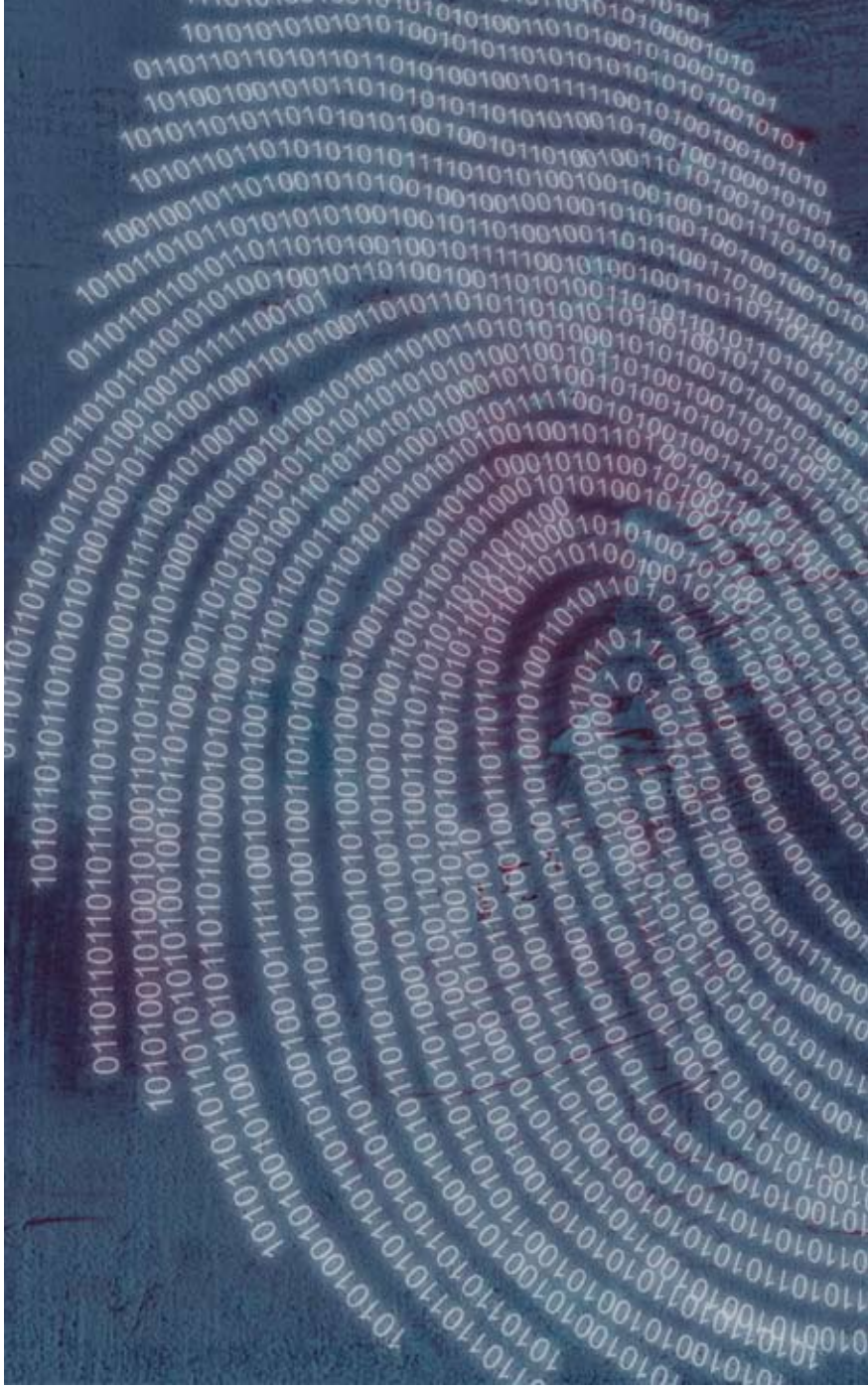


Biometrische eigenschappen van personen, zoals vingerafdrukken, worden reeds enige tijd gebruikt voor identificatie. Recentelijk is aangetoond dat ook microchips een vorm van unieke vingerafdruk bezitten en werden constructies beschreven om deze op een efficiënte manier op te meten. Het gebruik van deze chipbiometrie laat toe om apparaten eenduidig te identificeren. Bovendien zijn de opgemeten vingerafdrukken fysisch onkloonbaar, wat interessante voordelen oplevert, onder meer in de strijd tegen namaak.

Roel Maes

Veiligheid uit de “biometrie

Namaak is een probleem van alle tijden, maar het afgelopen decennium vormt de georganiseerde en verreikende namaakindustrie een grote bedreiging voor veel innoverende ondernemingen. Producenten van waardevolle zaken zoals elektronica, uurwerken, kledij, geneesmiddelen, multimedia, enz..., lijden enorm onder piraterij en namaak van hun producten. Veel bedrijven investeren grote bedragen in de ontwikkeling van vernieuwende producten, in de hoop een sterke marktpositie te realiseren. Vaak echter zien ze deze markt onder hun neus ingepalmd worden door namakers die er onmiddellijk profijt uit halen. Zij hebben namelijk geen ontwikkelingskosten gemaakt, maar het originele product simpelweg gekopieerd. Dit leidt mogelijk tot grote financiële verliezen voor de oorspronkelijke ontwikkelaar en is bijgevolg nefast voor innovatie. Bovendien profiteren namakers vaak van de naambekendheid van de originele fabrikant, waardoor deze laatste zelfs risico loopt op imagobeschadiging. De nagemaakte producten zijn meestal immers van inferieure kwaliteit, maar worden door de klant toch met de originele producent geassocieerd. In sommige gevallen, bijvoorbeeld als het gaat over medicijnen of vliegtuigonderdelen, kan de ondermaatse kwaliteit van de nagemaakte producten zelfs tot regelrechte catastrofes leiden.

Figuur 1

Figuur 2

” van chips

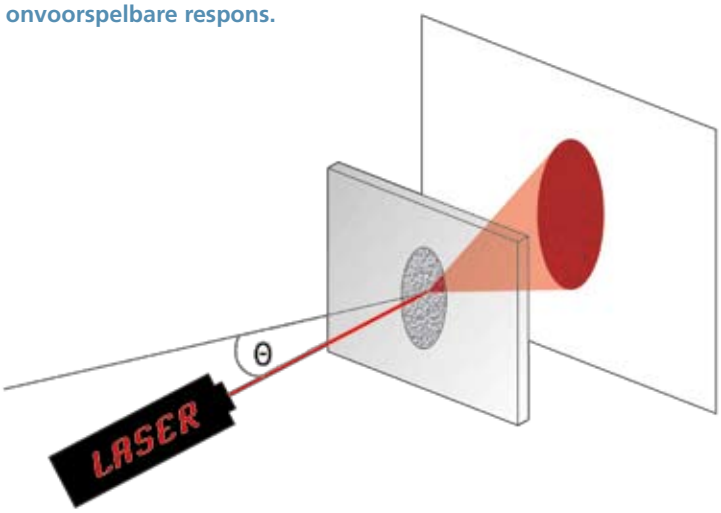
Cryptografie als oplossing?

In het geval van digitale data, zoals multimedia-inhoud, kan cryptografie een oplossing bieden tegen namaak. Door de gegevens te vercijferen met een geheime sleutel kunnen ze publiek verspreid worden. Een namaker kan in dat geval nog steeds een kopie maken, maar omdat de gegevens vercijferd zijn met een sleutel die hij niet kent, is die kopie voor hem van weinig waarde. Dit vereist echter dat elke legitieme toepassing een geheime cryptografische sleutel bezit om de vercijferde informatie terug leesbaar te maken. In vele huidige toepassingen houdt dit in dat een unieke sleutel, in de vorm van een bitvector, wordt voorgeprogrammeerd in een permanent digitaal geheugen op een chip.

Voor niet-digitale goederen berust de beveiliging tegen namaak nog vaak op allerhande zegels, logo's en hologrammen die onlosmakelijk met het product verbonden worden. Een voorbeeld van een hologram op een bankbiljet is te zien in figuur 1. Het probleem hier is, dat zelfs de meest vernuftige hologrammen met enige moeite nagemaakt kunnen worden. Bovendien zien vervalste hologrammen er voor een onwetende klant vaak echt genoeg uit om misleid te worden. Om deze redenen begint men voor niet-digitale producten ook steeds meer over te schakelen op digitale beveiliging. In de plaats van een zegel of hologram wordt een goedkope en kleine microchip, zoals te zien in figuur 2, onlosmakelijk aan het product of zijn verpakking bevestigd. Deze microchip bevat een unieke geheime code die door een legitieme

Optische PUF en Challenge-Respons-Paren

De werking van een PUF, kort voor Physical Unclonable Function, wordt onmiddellijk duidelijk in de beschrijving van een typerend voorbeeld, de zogenaamde optische PUF [3,5], voorgesteld in figuur 3. In een doorzichtig plaatje worden op een ongecontroleerde manier onzuiverheden aangebracht. Een laserstraal die het plaatje beschijnt wordt door de onzuiverheden verstrooid en er vormt zich een willekeurig en onvoorspelbaar spikkelpatroon. Het gevormde patroon is sterk afhankelijk van de exacte posities en afmetingen van de onzuiverheden in het plaatje. Het plaatje met de onzuiverheden zo exact namaken dat zich hetzelfde patroon vormt is praktisch ondoenbaar, zelfs voor de fabrikant van de PUF. De fysische structuur van de PUF is dus in praktijk onkloonbaar. Het spikkelpatroon, en dus ook de sleutel die ervan afgeleid wordt, is uniek, willekeurig en onvoorspelbaar voor een bepaald glasplaatje en bepaalde instellingen van de laserstraal. De gemeten waarde van de fysische parameter, in dit geval de unieke structuur van het bekomen spikkel-patroon, wordt de respons van de PUF genoemd. De fysische stimulus die tot de respons leidt, in dit geval de laserstraal, noemt men de challenge. Door de laserstraal op een andere manier in te stellen, bijvoorbeeld onder een andere invalshoek, of met een andere golflengte, kunnen verschillende challenges aangelegd worden aan de optische PUF, elk met hun eigen unieke en onvoorspelbare respons.



Figuur 3: Constructie van een optische PUF met een laser en een doorzichtig plaatje met onzuiverheden. Het gevormde spikkelpatroon is uniek voor elk plaatje en voor elke invalshoek θ van de laserstraal [3,5].

lezer draadloos gecontroleerd kan worden. Als de code correct is dan betreft het een authentiek product. Een aanvaller die het product wil namaken en voor echt wil laten doorgaan, zal in dat geval ook de microchip met de geheime code moeten klonen!

Naast tegenmaatregelen voor namaak, zijn er nog allerhande andere toepassingen waarbij chips gevoelige geheime data bevatten, bijvoorbeeld in systemen waar een gebruiker zich moet authentiseren om een bepaalde actie uit te voeren. Deze chips komen vaak voor in de vorm van smartcards zoals bankkaarten, creditcards, elektronische identiteitskaarten, SIM-kaarten,... Ook hier is het voor een aanvaller interessant om deze chipkaarten te klonen, maar daarvoor moet hij eerst de geheime sleutel die op de kaart is voorgeprogrammeerd achterhalen. In vroegere systemen, waar de gegevens nog werden bewaard op een magneetstrip, kwam dit soort kloonaanvallen geregeld voor, voornamelijk bij creditcards, en stond bekend onder de naam skimming. De overschakeling van magneetkaarten naar chipkaarten maakt het klonen een stuk moeilijker, maar zoals zal blijken, niet onmogelijk!

Sterke cryptografie is niet voldoende!

Cryptografen hebben de afgelopen decennia ook goed werk geleverd en momenteel beschikken we over een aantal sterke cryptografische algoritmes en protocols voor de meeste toepassingen. Dit wil zeggen dat er na jaren van doorgedreven cryptanalyse, zeg maar codebreken, geen substantiële theoretische aanvallen gevonden zijn tegen deze algoritmes, en dat niet verwacht wordt dat die er in de nabije toekomst wel gaan komen. In praktijk richten vele aanvallen zich echter niet meer op de theoretische onderbouw van de algoritmes, maar wel op de implementatie ervan in cryptografische toepassingen. Zo blijkt dat naïeve implementaties van veel algoritmes ongewenst informatie over de sleutel lekken langs zogenaamde nevenkanalen. Voorbeelden van zulke nevenkanalen zijn het verbruikte vermogen of de uitgezonden elektromagnetische straling van een digitale implementatie. Dit type van aanvallen wordt nevenkanaalaanvallen genoemd en momenteel gebeurt veel onderzoek naar de ontwikkeling van tegenmaatregelen die deze aanvallen onmogelijk moeten maken.

In dit artikel wordt echter een tegenmaatregel besproken voor aanvalsmethodes die cryptografische implementaties op een meer drastische manier te lijf gaan. Het bewaren van geheime data in een permanente digitale vorm op een chip, zoals in de overgrote meerderheid van de hedendaagse toepassingen gebeurt, houdt immers een belangrijk veiligheidsrisico in wanneer de aanvaller fysieke toegang heeft tot het apparaat. Hij heeft dan immers de mogelijkheid om de chip fysisch open te breken en de bewaarde geheimen te achterhalen. Technieken en apparaten die typisch gebruikt worden voor de inspectie van chips staan hiervoor ter zijner beschikking. Enkele voorbeelden hiervan zijn [2]:

- Het chemisch oplossen of wegetsen van (afschermende) lagen van een chip om onderliggende lagen zichtbaar te maken. Met bepaalde geavanceerde etstechnieken kan zelfs het verschil tussen een opgeslagen nul en één in een ROM-geheugen waargenomen worden.
- Met (elektronen)microscopen kunnen minuscule structuren op een chip in detail bestudeerd worden, onder andere voor reverse-engineering. Bepaalde elektronenmicroscopen bezitten zelfs een spanningscontrastfunctie waarmee spanningen in een elektronisch circuit in reële tijd waargenomen kunnen worden!
- Minuscule naaldprobes kunnen op metaalbaantjes van een chip geplaatst worden om de overgebrachte spanningssignalen af te luisteren, of zelfs om foutieve signalen te injecteren.

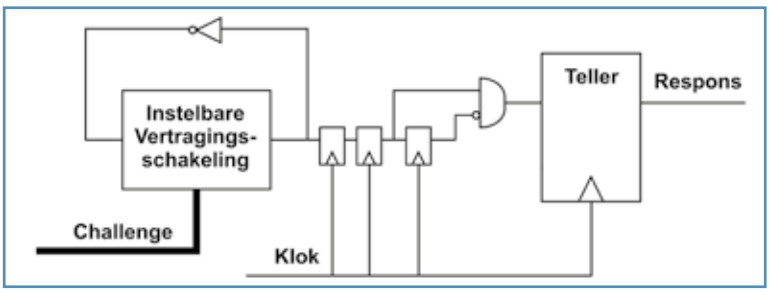
- Een gefocusseerde ionenstraal of FIB is een geavanceerd apparaat waarmee niet enkel detailbeelden van de minuscule structuren op een chip gemaakt kunnen worden, maar zelfs op zeer kleine schaal veranderingen aangebracht kunnen worden aan het bestudeerde circuit. Dit soort aanvallen wordt fysieke aanvallen genoemd en in het geval de aanvaller de chip fysisch verandert, door bijvoorbeeld te etsen of gaatjes te boren, spreekt men zelfs van invasieve aanvallen. Het spreekt voor zich dat het zeer moeilijk is om de digitale bits van een sleutel op een chip geheim te houden voor een aanvaller die in staat is fysieke aanvallen uit te voeren. Hieruit kan besloten worden dat het gebruik van een sterk cryptografisch algoritme op zich niet voldoende is om veiligheid te waarborgen. Er is eveneens nood aan een fysische infrastructuur die gegevens op een chip waarlijk geheim kan houden, zelfs voor een aanvaller die fysieke aanvallen kan uitvoeren! In het vervolg van dit artikel zal besproken worden hoe een dergelijke infrastructuur op een kost-efficiënte manier op een chip geconstrueerd kan worden.

Fysisch onkloonbare functie: PUF

Een fysisch onkloonbare functie, kortweg PUF is een recentelijk voorgestelde cryptografische primitieve die het potentieel bezit om de behoefte aan eenvoudig en fysisch veilig geheugen in te vullen. Een PUF is gedefinieerd als een functie die vervat zit in een fysisch systeem, die gemakkelijk geëvalueerd kan worden, maar moeilijk te karakteriseren is. De eigenlijke constructie van een PUF kan op verschillende manieren gebeuren, maar het werkingsprincipe is steeds hetzelfde. Een evaluatie van de PUF houdt een meting van een fysische parameter in die een zekere graad van willekeurigheid bevat. Deze willekeurigheid ontstaat door een natuurlijk en ongecontroleerd proces dat inherent is aan de productie van het fysisch systeem of daar expliciet in geïntroduceerd wordt. Uit deze fysisch willekeurige meting kan een unieke en onvoorspelbare cryptografische sleutel afgeleid worden. Op een later tijdstip kan dezelfde sleutel gereconstrueerd worden door dezelfde fysische parameter op te meten. Dit houdt in dat geheime sleutels niet meer in permanente digitale vorm op een chip aanwezig moeten zijn, wat reeds een groot aantal fysieke aanvallen uitsluit! In plaats daarvan zit de sleutel vervat in de exacte analoge waarden van bepaalde onvoorspelbare fysische parameters van de PUF, die niet met fysieke aanvallen bepaald kunnen worden. Meer nog, door het uitvoeren van fysieke aanvallen is de kans groot dat de fysische parameters die de sleutel bepalen gewijzigd worden, waardoor ook de sleutel verandert en dus verloren gaat! PUF's bezitten dus als het ware een zelfvernietigingsfunctie.

Procesvariaties als vingerafdruk van een chip

Microchips die met een identiek proces gefabriceerd worden zullen toch niet helemaal identiek zijn. Productieparameters en omgevingsfactoren die een invloed hebben op de fabricatie kunnen slechts binnen bepaalde grenzen gecontroleerd worden en willekeurige fluctuaties binnen deze grenzen worden procesvariaties genoemd. Fabrikanten van chips moeten uitgebreide voorzorgsmaatregelen nemen om de procesvariaties zo klein mogelijk te houden en circuitontwerpers moeten de aanwezige procesvariaties in rekening nemen zodat hun digitale schakelingen correct en eenduidig blijven functioneren. Vanuit het standpunt van dit artikel blijkt het echter interessant om digitale schakelingen te ontwikkelen die géén eenduidige uitkomst voortbrengen, maar een waarde die afhankelijk is van de procesvariaties die aanwezig zijn op de specifieke chip waarop de schakeling geïmplementeerd is. Een dergelijke schakeling kan namelijk gebruikt worden als digitale PUF. De bron van willekeurigheid, namelijk het optreden van procesvariaties, is in dit geval inherent aanwezig in het productieproces van de chip en het meetcircuit kan rechtstreeks op de chip geïmplementeerd worden. Dit leidt tot een PUF-constructie die handiger en goedkoper in gebruik is dan bijvoorbeeld de optische PUF uit figuur 3, waarbij een aantal uitwendige apparaten nodig zijn. De afgeleide sleutel hangt rechtstreeks af van de unieke fysische eigenschappen van de chip en de analogie met een unieke vingerafdruk van een persoon of andere biometrische eigenschappen is dus snel gemaakt. Om de willekeurigheid uit de procesvariaties te benutten in een PUF, moet een fysische parameter van de chip opgemeten worden die onderhevig is aan deze procesvariaties. Eén van dergelijke parameters is de vertraging die een schakeling nodig heeft voor de propagatie van een signaal van zijn ingang naar zijn uitgang. De uitdaging bestaat er nu nog in om een digitaal circuit te ontwerpen dat de vertraging van een vertragingsschakeling zo nauwkeurig kan opmeten, dat de invloed van procesvariaties zichtbaar wordt. Door de uitgang van een vertragingsschakeling geïnverteerd terug te koppelen naar de ingang ontstaat een oscillerende lus waarvan de oscillatiefrequentie het inverse is van de vertraging van de oorspronkelijke schakeling. Deze frequentie kan bovendien redelijk nauwkeurig bepaald worden met behulp van enkele bemonsteringsflipflops en een digitale teller. De telleruitgang is recht evenredig met de exacte frequentie en kan dus gebruikt worden als respons van deze vertragingsgebaseerde PUF. Deze constructie is te zien in figuur 4 en wordt ook wel silicon-PUF genoemd, omdat het de eerste beschreven PUF was die volledig op een silicium chip geïmplementeerd kon worden [4]. Het exacte pad dat een signaal doorheen de vertragingsschakeling volgt, kan bovendien digitaal ingesteld worden, wat een andere unieke vertraging tot gevolg heeft. Net als bij de optische PUF kunnen hier dus ook verschillende challenge-respons-paren bekomen worden.



Figuur 4: Constructie van het meetcircuit voor de vertragingsmeting [4]. Door het aantal oscillaties in een bepaald tijdsinterval te tellen kan een maat voor de frequentie en dus de vertraging bekomen worden

FPGA's: Herconfigureerbare chips

Een Field Programmable Gate Array of FPGA, afgebeeld in figuur 5, is een silicium microchip waarvan de functionaliteit niet vastligt, maar die geprogrammeerd kan worden om een bepaalde digitale operatie uit te voeren. Deze herconfigureerbaarheid is mogelijk doordat de verbindingen tussen de kleine digitale primitieven op een FPGA niet vastliggen. De wijze waarop de elementen juist verbonden worden, zit bevat in een bitstroom die ingeladen wordt als de FPGA wordt ingeschakeld en bepaalt de functionaliteit die de chip zal uitvoeren. De mogelijkheid om de geïmplementeerde schakeling snel en zonder extra kost te kunnen aanpassen, zorgt ervoor dat FPGA's onder andere interessant zijn voor het maken van testopstellingen.

Figuur 5: Een Field Programmable Gate Array of FPGA van het merk Xilinx®. Met dit type van FPGA (Spartan3®) werden de testen in het onderzoek verricht.

Van vertragingsmeting tot sleutel

We hebben de voorgestelde schakeling voor een silicon-PUF geïmplementeerd op een FPGA en de resultaten uit [4] bevestigd. Zoals verwacht bekomen we een verschillende respons bij metingen met dezelfde, identiek ingestelde schakeling, maar geïmplementeerd op verschillende FPGA-chips. De respons van een silicon-PUF kan dus gebruikt worden om de gebruikte FPGA-chip te identificeren en er is mogelijkheid om er een cryptografische sleutel van af te leiden. Deze sleutelextractie vereist echter een grondige analyse van de responsstatistieken en het gebruik van daaraan aangepaste naverwerkings-algoritmes. Het gebruik van een PUF voor veilige sleutel-opslag gebeurt typisch in twee afzonderlijke fasen. In de eerste fase of registratiefase wordt een willekeurige challenge gekozen en van de bekomen fysische respons-meting worden een aantal sleutelbits afgeleid. Deze registratie gebeurt typisch door de fabrikant of de verdeler en de afgeleide sleutelbits worden op een vertrouwelijke manier bewaard. In de tweede fase of verificatiefase wordt dezelfde challenge opnieuw aangelegd en zal de PUF zijn identiteit proberen te bewijzen, door met zijn unieke respons dezelfde sleutelbits te genereren als in de registratiefase. Een belangrijke vraag die hierbij gesteld kan worden, is hoeveel sleutelbits gemiddeld op een veilige manier van een responsmeting afgeleid kunnen worden. Het blijkt dat twee factoren hier een rol spelen, namelijk:

1. De onzekerheid die een buitenstaander heeft over het voorkomen van een bepaalde respons op een bepaalde FPGA. Als gevolg van procesvariaties tijdens de productie van de FPGA's zal éénzelfde vertragingsmeting op twee FPGA's steeds een willekeurige hoeveelheid verschillen. Een goede maat voor deze onzekerheid is de spreiding van de responsmetingen, bij een identieke challenge, over alle FPGA's en deze spreiding noemen we de inter-FPGA-variatie.
2. De onzekerheid die we zelf hebben over de correctheid van de gemeten respons. Door ruis zal de vertragingsmeting in de verificatiefase immers steeds een willekeurige hoeveelheid afwijken van die in de registratiefase. Een goede maat voor deze onzekerheid is de spreiding van herhaaldelijke responsmetingen op één en dezelfde FPGA. Deze spreiding wordt de intra-FPGA-variatie genoemd.

Het is duidelijk dat de eerste factor, veroorzaakt door willekeurige procesvariaties, een positieve invloed heeft op het aantal veilig afleidbare sleutelbits en de tweede factor, veroorzaakt door ruis, een negatieve. Zoals opgemerkt in [4] is een vertraging op een microchip sterk afhankelijk van omgevingsparameters zoals temperatuur en dit kan mogelijk een grote ruisafwijking tussen herhaalde responsmetingen geven, indien bijvoorbeeld de temperatuur fel veranderd is tussen de metingen. Door te werken met verhoudingen van vertragingen in plaats van met de absolute meetwaarden, kan een groot deel van deze omgevingsinvloed gecompenseerd worden.

Door herhaaldelijke metingen uit te voeren op verschillende FPGA's van hetzelfde type en bij verschillende challenges hebben we de statistieken van de responses geschat. Het resultaat is te zien in figuur 6. Hieruit blijkt dat voor de gecompenseerde responsmetingen de inter-FPGA-variatie gemiddeld zo'n 150 maal groter is dan de intra-FPGA-variatie. Eigenschappen uit de informatietheorie vertellen ons dat het gemiddeld aantal veilig afleidbare bits per respons, ook wel de veiligheidscapaciteit genoemd, in dat geval ruim 7 bits bedraagt [5]. Een gelijkaardig resultaat werd aangetoond in [4].

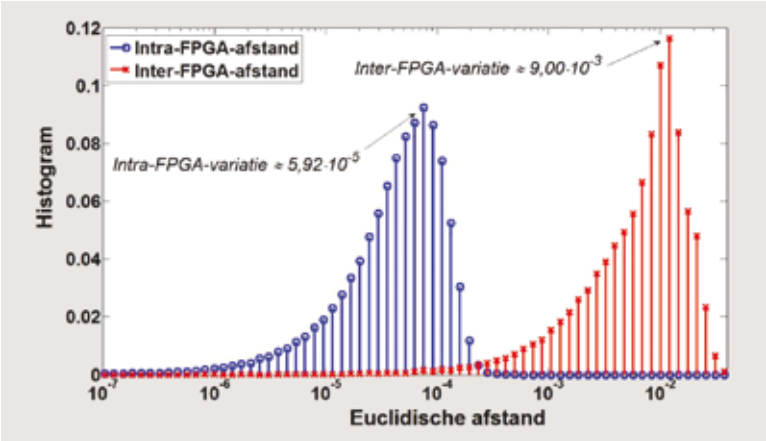
Voorzichtigheid is echter geboden bij het trekken van conclusies omtrent de veiligheidscapaciteit. De gebruikte formules uit de informatietheorie veronderstellen immers onafhankelijkheid tussen responses op verschillende FPGA's en bij verschillende challenges. We merken echter dat er in beide gevallen een sterke lineaire afhankelijkheid bestaat tussen de responsmetingen. Dit wordt duidelijk uit de hoge gemiddelde correlatiecoëfficiënten tussen de gecompenseerde responsmetingen bekeken over verschillende FPGA's en over verschillende challenges. Een groot deel van een responsmeting bestaat dus uit een deterministische waarde die we hebben getracht te verwijderen in een proces dat we normalisatie noemen. De gemiddelde correlatiecoëfficiënten voor en na normalisatie zijn te zien in tabel 1.

Tabel 1: Effect van de normalisatiestap

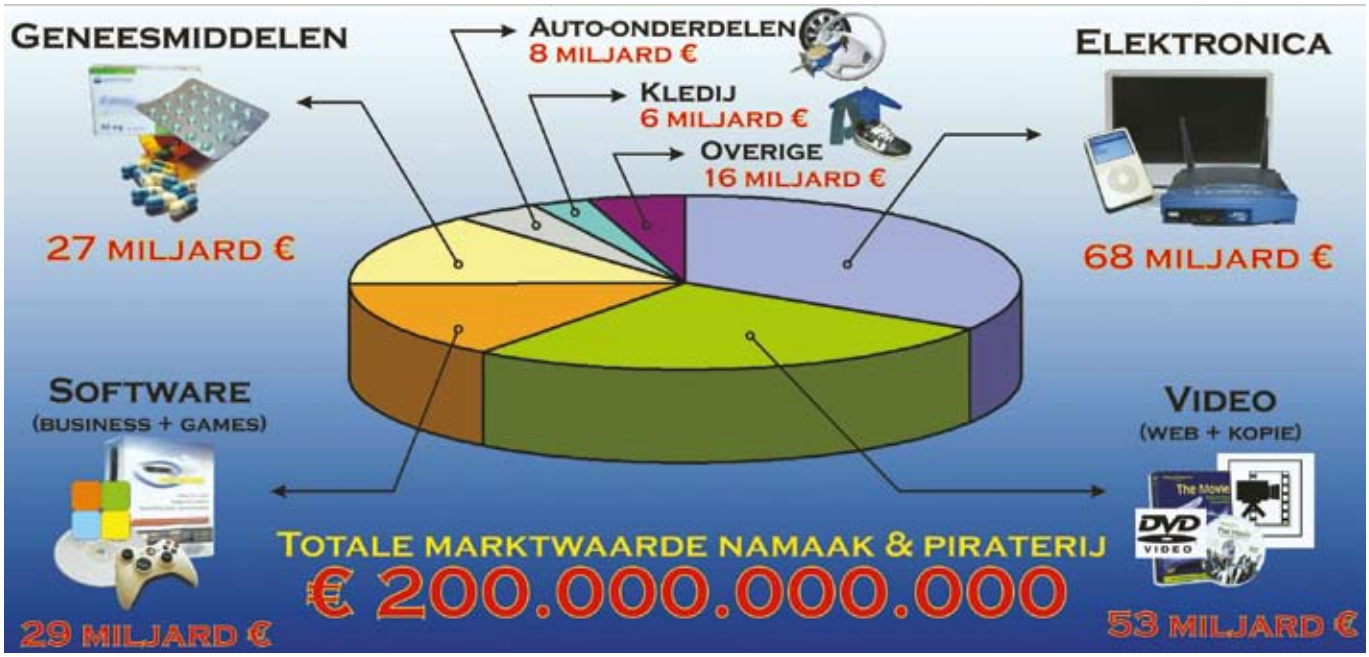
	Voor normalisatie	Na normalisatie
Correlatie van responses over verschillende FPGA's	64,6 %	2,94 %
Correlatie van responses over verschillende challenges	96,8 %	-4,99 %
Verhouding inter/intra-FPGA-variatie	±150	±20

Uitbesteding en IP-bescherming

Veel producenten van elektronische apparaten proberen hun productiekosten te drukken door de eigenlijke productie van microchips niet meer binnenshuis te doen, maar uit te besteden aan gespecialiseerde bedrijven, vaak in lagelonenlanden. De producent ontwikkelt dus enkel nog de plannen van de chip en de waarde van het product zit voor hem dan ook vervat in de *intellectuele eigendom (IP)* van deze plannen. Het bedrijf waaraan de eigenlijke productie wordt uitbesteed heeft echter noodzakelijkerwijs ook beschikking over deze plannen en produceert vaak meer dan de bestelde hoeveelheid. Deze overschot kan dan als namaak verkocht worden en bovendien ver onder de eigenlijke kostprijs doordat er geen ontwikkelingskosten gedragen moeten worden. Om deze malafide praktijken te verhinderen zijn een aantal internationale wetten opgesteld ter bescherming van de intellectuele eigendom, maar onder andere in lagelonenlanden is hier zelden controle op waardoor namaak en piraterij vrij spel krijgen. Naast legale beperkingen zijn technische beschermingsmaatregelen in dit geval noodzakelijk!



Figuur 6: Histogrammen van opgemeten intra- en inter-FPGA-afstanden. Een intra-FPGA-afstand (ruis) is het verschil tussen responses van twee identieke metingen op dezelfde FPGA, een inter-FPGA-afstand (procesvariatie) tussen responses van twee identieke metingen op verschillende FPGA-chips.



Figuur 7: Bedrijven verloren afgelopen jaar wereldwijd naar schatting 200 miljard euro door namaak en piraterij. De namaak-producten met de grootste marktwaarde zijn gegeven. De resterende 16 miljard € bestaat onder meer uit nagemaakte muziek (3 miljard €), sigaretten (2,7 miljard €), cosmetica (2 miljard €), vliegtuigonderdelen (1,4 miljard €) en handwapens (1,2 miljard €) [1].

We zien dat de normalisatiestap de lineaire afhankelijkheid nagenoeg verwijdert. Het zorgt er echter ook voor dat de verhouding tussen inter- en intra-FPGA-variatie daalt tot ongeveer 20, wat de effectieve veiligheidscapaciteit terugbrengt tot ruim 4 bits. Praktische uitvoeringen van een sleutelbitextractor [6], zoals degene die we in functie van dit onderzoek implementeerden, zullen steeds onder dit theoretisch maximum blijven. In onze uitvoering waren ongeveer een 50-tal verschillende challenge-respons-paren nodig om tot een bruikbare 128-bit cryptografische sleutel te komen.

Meer veiligheid door onkloonbaarheid

In het begin van dit artikel werd namaak aangehaald als een pijnpunt voor veel innoverende ondernemingen. Cryptografie kon een oplossing bieden, maar enkel wanneer het gecombineerd werd met een waarlijk veilige opslag van de geheime sleutels en daar spande het schoentje. Het gebruik van een PUF voor veilige sleutelopslag biedt hiervoor echter een passende oplossing.

Veel hoogtechnologische bedrijven gebruiken momenteel FPGA's in hun nieuwste producten om wille van de flexibiliteit die geboden wordt door de herprogrammeerbaarheid van deze chips. Veel tijd en geld wordt gestoken in de ontwikkeling van een optimaal digitaal ontwerp en de uiteindelijke implementatie ervan zit bevat in de bitstroom, die automatisch op de FPGA wordt ingeladen bij het inschakelen. Deze bitstroom is op die manier echter bijzonder kwetsbaar doordat een aanvaller hem met een minimum aan middelen kan afluisteren. Éénmaal hij de bitstroom kent, kan hij de implementatie onbeperkt inladen op andere FPGA's en heeft op die manier het oorspronkelijke ontwerp simpelweg gekopieerd. De bitstroom kan beschermd worden door hem te vercijferen, maar dit vereist het veilig opslaan van een unieke geheime sleutel op elke FPGA. Tot op heden was dit een omslachtige en soms onmogelijke opdracht, toch zeker indien de aanvaller in staat was om fysieke aanvallen uit te voeren. Door hiervoor een PUF te gebruiken, zoals degene beschreven in dit artikel, kan dit probleem op een eenvoudige en kost-efficiënte manier overwonnen worden!

Waardevolle goederen die beschermd worden met een microchip kunnen enkel nog nagemaakt worden als de microchip en de daarin bevatte geheime sleutel gekloond worden. Door de microchip te voorzien van een PUF voor het bewaren van een sleutel, wordt deze onkloonbaar en is het onmogelijk om een nagemaakt product nog voor echt te laten doorgaan. Zelfs fysieke aanvallen kunnen de sleutel in dat geval niet achterhalen. Door zijn zelfvernietigingseigenschap kan de PUF er immers voor zorgen dat dergelijke aanvallen de sleutel vernietigen.

PUF's kunnen hun nut bewijzen in nog vele andere toepassingen. Door processoren te voorzien van een PUF kan de identiteit van een computersysteem onweerlegbaar aangetoond worden, omdat elke PUF een unieke en onkloonbare respons voortbrengt. Door PUF's te gebruiken voor de opslag van geheime sleutels in bijvoorbeeld bankkaarten worden skimming-aanvallen onmogelijk, zelfs als de aanvaller over heel vernuftige apparatuur beschikt.

Besluit

Veilige sleutelopslag is een nadrukkelijke voorwaarde voor veilige cryptografische toepassingen. In veel gevallen wordt hier echter weinig aandacht aan besteed en door de ontwikkeling van steeds meer geavanceerde fysieke aanvallen vormt dit vaak een groot probleem. Het gebruik van recentelijk ontwikkelde fysisch onkloonbare functies of PUF's biedt hiervoor een kost-efficiënte oplossing.

Referenties

[1] HAVOCSCOPE - Global Index of Illicit Markets™. [Online]. Beschikbaar: http://www.havocscope.com/.

[2] M. Witteman, "Advances in Smartcard Security.", Information Security Bulletin, juli 2002, pagina's 11-22.

[3] S. R. Pappu, "Physical one-way functions.", Ph.D. dissertatie, Massachusetts Institute of Technology, 2001.

[4] B. Gassend, D. Clarke, M. van Dijk and S. Devadas, "Silicon physical random functions.", In Proceedings of the 9th ACM Conference on Computer and Communications Security, november 2002.

[5] P. Tuyls, B. Škorić, S. Stallinga, A.H.M. Akkermans, W. Ophey, "Information-Theoretic Security Analysis of Physical Uncloneable Functions", Proc. 9th Conf. on Financial Cryptography and Data Security, LNCS 3570, pagina's 141-155 , maart 2005.

[6] Y. Dodis, R. Ostrovsky, L. Reyzin and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data", In EUROCRYPT, pagina's 523-540, 2004.

De auteur

Roel MAES behaalde in 2007 het diploma van Burgerlijk Elektrotechnisch Ingenieur aan de Katholieke Universiteit Leuven met als eindverhandeling "Sleutelextractie van een silicon-PUF op FPGA". Op dit moment is Roel als doctoraalstudent verbonden aan de onderzoeksgroep Computer Security and Industrial Cryptography (COSIC) in het departement Elektrotechniek van de K.U.Leuven. Zijn onderzoek richt zich voornamelijk op de constructie van efficiënte fysisch onkloonbare functies gebaseerd op procesvariaties aanwezig in microchips.

Dankwoord

De auteur wil zijn promotor, Prof. Dr. Ir. Ingrid Verbauwhede (SCD/COSIC, K.U.Leuven), en zijn copromotor, Dr. Pim Tuyls (Philips Research, Eindhoven; SCD/COSIC, K.U.Leuven) danken voor de dagelijkse begeleiding bij dit eindwerk.