Quantumzekere authenticatie

Authenticatie van personen of objecten kan met behulp van 'iets dat men weet' of door 'iets dat men heeft'. Nadeel van iets dat men weet, zoals een digitale code, is dat het geheim gehouden moet worden. Een traditionele sleutel, een bekend voorbeeld van iets dat men heeft, kan vaak makkelijk gekopieerd worden zonder dat het slachtoffer het opmerkt. Er bestaan fysieke onkloonbare sleutels die dit nadeel niet hebben. Een optisch voorbeeld is een stukje veelverstrooiend materiaal zoals wit keramiek, dat onder laserbelichting een uniek spikkelpatroon produceert. Emulatie van zo'n respons is echter nog steeds een gevaar als de optische eigenschappen van de sleutel bekend zijn. We introduceren een quantumfysische manier van uitlezen waardoor emulatie volledig uitgesloten kan worden. We noemen dit quantumzekere authenticatie. Boris Škorić en Pepijn Pinkse

Veel handelingen in onze moderne maatschappij vertrouwen op foutloze authenticatie. Denk maar aan de authenticatie van stemmers in een stembureau, de authenticatie van klanten van een bank bij financiële transacties of die van reizigers op een vliegveld. Traditionele vormen van authenticatie door middel van fysieke of digitale sleutels hebben beide een groot nadeel: zulke sleutels kunnen worden gekopieerd en de eigenaar zal in veel gevallen helemaal niet doorhebben dat zijn of haar sleutel gekopieerd is, tot het te laat is. Er is een moderne vorm van fysieke sleutels die dit nadeel niet kent: de zogenaamde 'fysieke onkloonbare sleutel' of in het Engels *physically unclonable function* (PUF) [1]. PUF's zijn zeer moeilijk te kopiëren, omdat de fabricage intrinsiek een groot aantal oncontroleerbare aspecten bevat. Verder kan je een PUF onderwerpen aan een fysieke prikkel (de vraag, in cryptografentaal), die leidt tot een ingewikkelde output (de respons). De vraag- en responsruimte van een PUF zijn beide groot. Na de fabricage van een PUF wordt er een database aangelegd van vraag-responsparen; daarna wordt de PUF afgegeven aan iemand die zich wil kunnen authenticeren (typisch Bob genoemd). Iemand, laten we zeggen Alice, kan Bob later authenticeren door zijn PUF aan vragen te onderwerpen en te kijken of de responsen kloppen met de database.

Boris Škorić studeerde theoretische natuurkunde aan de Universiteit van Amsterdam. In 1999 promoveerde hij daar op een proefschrift over het quantum-Hall-effect. Daarna werkte hij als onderzoeker bij Philips Research, eerst aan display-fysica en later aan codering en cryptografie. Sinds 2008 is hij universitair docent aan de faculteit Wiskunde en Informatica van de TU Eindhoven.

b.skoric@tue.nl

Spikkelpatroon

Wij gebruiken als PUF kleine stukjes sterk verstrooiend materiaal zoals droge witte verf of keramiek. Het spikkelpatroon (Engels: *speckle*) dat ontstaat als zulk materiaal met laserlicht wordt beschenen is uniek. Het spikkelpatroon (de respons) hangt, afgezien van de precieze belichting (de vraag), op een zeer gevoelige manier af van de positie, vorm en samenstelling van ontelbare verstrooiers op submicrometerschaal waaraan het licht veelvuldig verstrooit. Zelfs de fabrikant kan geen twee PUF's maken met identiek gedrag, want hij zou daarvoor miljoenen verstrooiers op de juiste manier in 3D moeten kunnen assembleren met een resolutie op nanometerschaal, en dat lukt zelfs de meest geavanceerde 3D-printer bij lange na niet. Het is tevens onbegonnen werk om een ander soort object te produceren dat het gedrag van een gegeven PUF nabootst. Met moderne technieken zoals beeldvormende chips, hologrammen of nanooptische circuits kunnen weliswaar

complexe transformaties gebouwd worden, maar zijn de lichtverliezen zo groot dat het meteen opvalt.

Emulatie

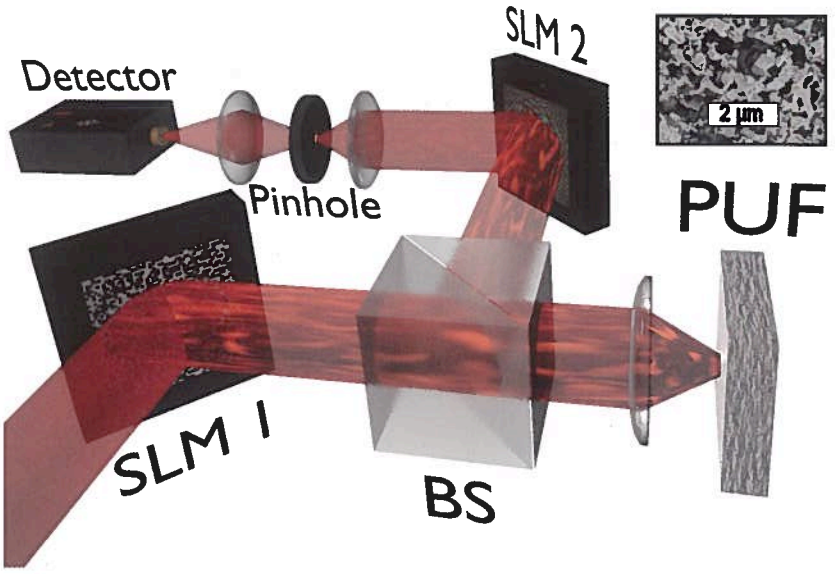
Alles dus in orde? Waarom hebben PUF's de wereld nog niet veroverd? Een van de redenen is de noodzaak om voor elke afzonderlijke PUF apart data op te slaan, wat voor logistieke overhead zorgt. Een andere reden is het probleem van emulatie. Het is niet uit te sluiten dat een aanvaller toegang verkrijgt tot Bobs PUF of zelfs tot de PUF-database. Als een aanvaller eenmaal kennis heeft van een groot aantal vraag-responsparen, dan is authenticatie problematisch geworden. De aanvaller kan zich dan namelijk voordoen als Bob: hij beantwoordt vragen door de respons op te zoeken in zijn persoonlijke database. Hier heeft hij de PUF niet voor nodig. Zo'n aanval noemen we PUF-emulatie.

Emulatie-aanvallen zijn te voorkomen door goede fysieke inspectie: je moet met zekerheid kunnen vaststellen dat je een fysiek object aan het bevragen bent en dat het object de juiste afmeting et cetera heeft. De aanvaller zou immers met zijn eigen apparatuur een fysieke respons kunnen genereren op grond van zijn database. Het bouwen versus om de tuin leiden van de inspectie is een wapenwedloop waarbij de kosten hoog oplopen en het nooit duidelijk is hoe veilig het systeem nou precies is.

Hier biedt quantumzekere authenticatie (QSA, *quantum-secure authentication*) [2] een uitkomst door quantumfysica in te zetten ter bescherming van de vragen. QSA is een uitleesmethode die emulatie onmogelijk maakt. Elke vraag bevat veel informatie die voor de aanvaller onvoorspelbaar is. De vraag wordt gesteld middels een klein aantal quanta (fotonen), of zelfs een enkel quantum. Vanwege de collaps van de golffunctie in geval van een meting, en vanwege het *no-cloning theorem* [3], bestaat er voor de aanvaller geen enkele betrouwbare manier om te leren welke informatie in de vraag verstopt zit. En als hij niet weet wat de vraag is, dan kan hij ook niet de respons opzoeken! Anderzijds is Alice wel in staat om de respons te checken, omdat zij de vraag volledig kent.

Experiment

Ons demonstratie-experiment van



Illustratie van het demonstratie-experiment voor quantumzekere authenticatie [2]. Een zwakke laserpuls wordt door SLM1 van een complex ruimtelijk patroon voorzien en wordt daarna afgebeeld op de PUF. De PUF bestaat uit pigmentpoeder op een glaasje. SLM2 is zo geprogrammeerd dat een correcte respons zal worden omgezet naar een vlakke golf (en een incorrect golffront naar een ingewikkeld spikkelpatroon). De vlakke golf wordt op een gaatje (*pinhole*) afgebeeld, en de detector telt hoeveel fotonen er door het diafragma passeren. Illustratie: T.J. Huisman.

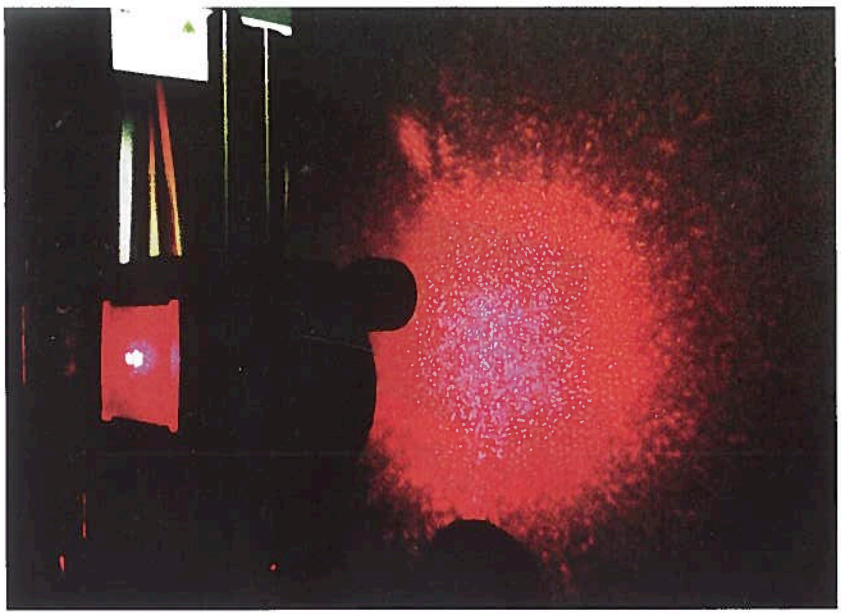
QSA is geïllustreerd in de figuur hierboven: we belichten de PUF met een zwakke laserpuls die bijvoorbeeld maar één enkel foton bevat. Om het ruimtelijke patroon van het licht te beschrijven is echter veel informatie nodig. Het ingewikkelde golffront (de vraag) wordt gemaakt door de puls te manipuleren met een *spatial light modulator* (SLM), een beeldvormende chip die op programmeerbare wijze in ieder van zijn vele pixels afzonderlijk de fase van het licht kan draaien. De respons van de PUF wordt afgebeeld op een klein gaatje met behulp van faseconjugatie: middels een tweede SLM compenseren we het ruimtelijke fasepatroon van de respons zodanig dat alleen het verwachte patroon netjes afgebeeld wordt op het gaatje. Een fotonenteller achter het gaatje kijkt of er voldoende fotonen passeren. Als de respons gelijk is aan de verwachte respons, dan passeren vrijwel alle fotonen het gaatje. Een verkeerde respons wordt door SLM2 getransformeerd naar een random spikkelpatroon, waardoor het grootste deel van het licht het gaatje mist.

We hebben bewezen dat QSA veilig is tegen alle aanvallen waarbij de aanvaller probeert de vraag te meten en op grond van die meting de bijbehorende respons opzoekt [4, 5]. QSA met optische PUF's is veilig zolang het aantal fotonen in de laserpuls kleiner is dan het aantal ruimtelijke 'kanalen', wat ongeveer het aantal spikkels is. Bij QSA wordt het hele vraag-responsproces een aantal keer herhaald, waarbij natuurlijk iedere keer een nieuwe random vraag wordt gebruikt. De totale kans van slagen van de aanvaller (zijn kans om geauthenticeerd te worden ook al heeft hij de PUF niet) daalt exponentieel met het aantal herhalingen.

In het demonstratie-experiment [2] hadden we al ruim duizend kanalen, zodat een emulatiecircuit al gauw meer dan een miljoen parameters zou moeten hebben en dat gecombineerd met zeer geringe lichtverliezen als de aanvaller het volledige gedrag van de

Pepijn Pinkse studeerde natuurkunde aan de Universiteit Leiden. Hij promoveerde aan de Universiteit van Amsterdam in 1997 op onderzoek aan atomair waterstof. Hierna werkte hij elf jaar in Duitsland, voornamelijk op het Max Planck Instituut voor Quantumoptica in Garching, waar hij resonator-QED en koude atoom- en molecuulgassen onderzocht. In 2009 werd hij programma directeur nano-optica aan het MESA+ Institute for Nanotechnology van de Universiteit Twente; sinds 2014 is hij adjunct hoogleraar.

Pepijn.Pinkse@utwente.nl



Spikkelpatroon in het lab. Op de voorgrond links staat een *physically unclonable function* (PUF) die – om het patroon op deze foto goed zichtbaar te maken – belicht wordt met een sterke rode laserbundel. Door veelvoudige verstrooiing in de PUF ontstaat het spikkelpatroon aan de achterkant. Dit illustreert hoe de response van de PUF in quantumzekere authenticatie er uit ziet. De paarse kleur is in werkelijkheid intens rood.

PUF wil klonen. Dat is op zich al een schier onmogelijke opgave. Het wordt nog moeilijker als we een laser gebruiken met een korte coherentielengte: dan mag het circuit ook nog eens niet veel groter zijn dan de PUF zelf. Ons is geen technologie bekend die dat ook maar bij benadering voor elkaar kan krijgen. Men kan denken aan andersoortige aanvallen, zoals het aanbieden van een overvloed aan licht zodat er altijd genoeg fotonen het diafragma passeren. Zulke aanvallen zijn op triviale wijze te herkennen, bijvoorbeeld door ook buiten het diafragma detectoren te plaatsen, of door op onvoorspelbare momenten nep-pulsen aan te bieden waarvan je juist helemaal niet verwacht dat ze tot fotondetectie leiden.

Veiligheid

QSA combineert quantumfysische aspecten met elementen uit random lichtverstrooiing en cryptografie. De veiligheid van de authenticatie berust op de combinatie daarvan:

- (het fysieke gedrag van) de sleutel is niet te kopiëren omdat daartoe de technologie ontbreekt,
- emulatie middels het opzoeken van responsen is fundamenteel onmogelijk vanwege de quantummechanische onzekerheid bij meting van de zwakke vraagpuls.

Interessant is dat QSA gewoon werkt met zwak laserlicht en het niet nodig is om dure quantumlichtbronnen te gebruiken die bijvoorbeeld precies één foton of verstrengelde fotonparen genereren. We denken daarom dan ook dat een commerciële implementatie niet duur hoeft te zijn. Bijna alle benodigde hardware is al te vinden in projector-smartphones.

Het is ook interessant om op te merken dat QSA geen geheimen nodig heeft: elke PUF kan geauthenticeerd worden op grond van publieke informatie. En als er geen geheimen zijn, kunnen die ook niet uitlekken; dat is wel zo veilig.

We verwachten dat QSA gecombineerd kan worden met quantumcryptografie om boodschappen te versturen. Voor veilige cryptografie zijn geheime digitale sleutels nodig. Er bestaan al commerciële systemen voor het uitwisselen van geheime digitale sleutels op een quantumveilige manier (*quantum key exchange*). Normaal gesproken is het daarbij vereist om naast een quantumkanaal ook een geauthenticeerd klassiek communicatiekanaal te hebben, bijvoorbeeld een telefoonlijn: Alice moet zeker weten dat ze met Bob communiceert en niet met iemand anders. De combinatie met QSA creëert een *geauthenticeerd quantumkanaal*, waardoor het klassieke kanaal niet langer geauthenticeerd hoeft te zijn. De praktische impact hiervan is dat het voor de partijen die samen quantumcryptografie doen niet meer nodig is om van tevoren een (korte) klassieke authenticatiesleutel af te spreken; in plaats daarvan kan publieke informatie over de PUF gebruikt worden.

Als de Snowden-affaire ons iets geleerd heeft, is dat het belang van echt goede informatiebeveiliging. Het zou fantastisch zijn als een fundamenteel fysisch principe als quantummechanische onzekerheid en meervoudige lichtverstrooiing daartoe kunnen bijdragen.

Dankwoord

We danken Jacopo Bertolotti, Klaus Boller, Geza Giedke, Jennifer Herek, Marcel Horstmann, Simon Huisman, Thomas Huisman, Bart Jacobs, Ad Lagendijk, Allard Mosk, Gerhard Rempe, Berry Schoenmakers, Willem Vos en Tom Wolterink.

Referenties

1 R. Pappu, B. Recht, J. Taylor en N. Gershenfeld, *Physical one-way functions*, *Science* **297** (2002) 2026.
2 B. Goorden, M. Horstmann, A.P. Mosk, B. Škoric en P.W.H. Pinkse, *Quantum-Secure Authentication of a Classical Key*, arxiv.org/1303.0142.
3 W.K. Wootters en W.H. Zurek, *A Single Quantum Cannot be Cloned*, *Nature* **299** (1982) 802.
4 B. Škoric, A.P. Mosk en P.W.H. Pinkse, *Security of quantum-readout PUFs against quadrature-based challenge-estimation attacks*, *Int. J. Quant. Inf.* **11**, 1350041–1 – 1350041–15 (2013).
5 B. Škoric, *Security analysis of Quantum-Readout PUFs in the case of challenge-estimation attacks*, http://eprint.iacr.org/2013/479.