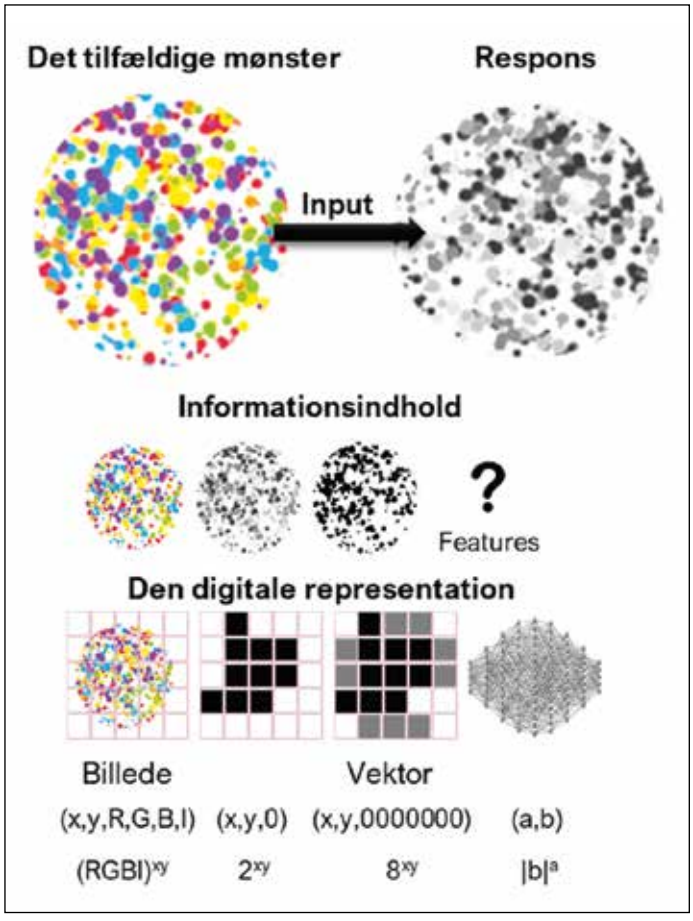
Physical Unclonable Functions

Fremtidens sikkerhedsløsninger baserer sig på tilfældige mønstre.

Af Thomas Just Sørensen, Nano-Science Center og Kemisk Institut, Københavns Universitet

Sikker identifikation af fysiske objekter er ved at blive en nødvendighed for virksomheder. Det gælder på tværs af produktkategorier og i flere regioner verden over. Den eneste praktiske løsning er at mærke de fysiske produkter og knytte hvert enkelt mærke til en digital identitet. De eksisterende teknologier har alle den indbyggede svaghed, at de fysiske mærker kan kopieres, genskabes eller klones af kopister med en tilstrækkelig motivation. Den form for snyd bliver umuligt, hvis produkterne forsynes med PUF-mærker baseret på pigmenter i tilfældige mønstre.



Figur 1. Et eksempel på en Physical Unclonable Function eller PUF (øverst til venstre), og et input-respons par i form af et gråtonebillede (øverst til højre). Informationsindholdet (i midten) er forskelligt, alt efter hvordan mønsteret aflæses. Det kan aflæses i farver, gråtoner, sort/hvid eller som features. Det sidste er sådan, O-KEYs læses. Den digitale repræsentation (nederst) er det unikke ID, der knyttes til hver PUF. Det kan være et billede, en simpel 2D stregkode, en mere kompleks vektor eller outputtet fra et neuralt netværk.

I 2001 beskrev forskeren Pappu som den første en ny type mærkning: en fysisk envejsfunktion; et mærke der ikke kan kopieres eller reproduceres [1]. Året efter blev begrebet udviklet til det, vi i dag kender som en Physical Unclonable Function (en PUF). Konceptet er i dag etableret i elektronikbranchen, hvor PUF-teknologi bruges til at sikre blandt andet IoT-enheder. Her er sikkerheden imidlertid kun garanteret, så længe PUF'en forbliver en integreret del af selve enheden. Optiske PUF'er fungerer anderledes. De aflæses med lys, og deres unikke, komplekse respons gør det muligt at bruge dem i åbne systemer – eksempelvis via scanning med en smartphone. Alligevel findes der stadig kun få eksempler på produktmærkning med optiske PUF-mærker.

Elementerne i en PUF

Et PUFmærke består af fire lige vigtige elementer. Selve PUF'en er et tilfældigt mønster, der i princippet kan skabes af næsten hvad som helst [2], men et PUFmærke skal opfylde strenge designkrav, som afhænger af den måde, det bruges på:

Det fysiske PUF-mærke skal enten være en integreret del af produktet eller fungere som en forsegling af varen eller emballagen. Et indbygget mærke må ikke kunne fjernes uden at ødelægge produktet, og et PUF-segl skal destrueres, hvis nogen forsøger at pille det af.

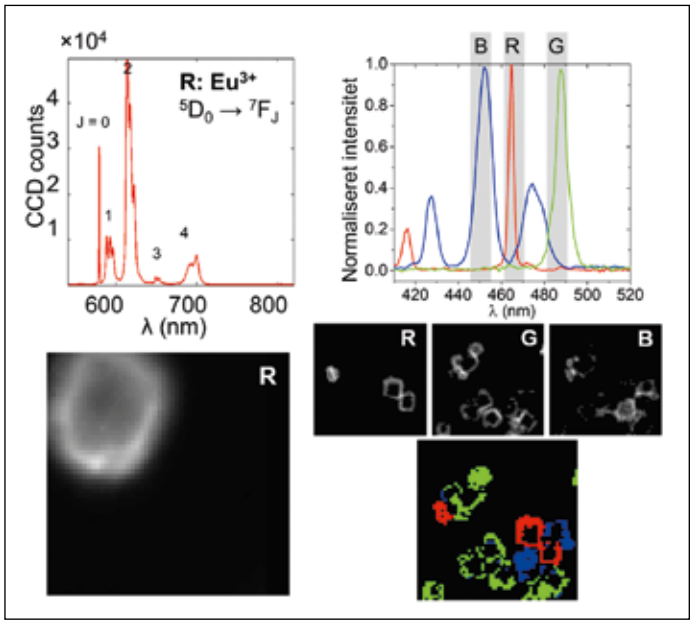
Registreringen af PUF-mærket udgør systemets juridiske kontrakt. Her kobles PUF'en til en digital registrering via et bestemt inputrespons par. For optiske PUF'er består både input og respons af lys, typisk i form af et referencebillede, der lagres sikkert og med langt højere kvalitet end en normal aflæsning. Det er denne registrering, der etablerer den unikke ID.

Når PUF'en læses, gentages input og det respons, der fremkommer ved læsningen, sammenlignes med det registrerede respons. Nye AI-baserede metoder er på vej til at blive et standardværktøj for denne sammenligning [3]. Et neuralt netværk oversætter respons fra både registrering og aflæsning til vektorer, og systemet afgør identiteten ved at måle afstanden mellem dem. Ligger afstanden under en fast tærskelværdi, leveres PUF'ens unikke ID.

Samlet udgør elementerne et kryptografisk system, der automatisk sikrer, at det PUF-mærkede produkt er ægte [4].

Kemien bag PUF-mærkerne

I figur 1 er der tegnet et tilfældigt mønster i flere farver. Det illustrerer den fysiske PUF, der i dette eksempel aflæses i et



Figur 2. Emissionsspektrum og billede optaget i et mikroskop fra et europium(III)-pigment (til venstre). Excitationsspektra af dysprosium(III)-pigment (B), europium(III)-pigment (R) og terbium(III)-pigment (G) samt billeder af et PUF mønster bestående af de tre pigmenter (øverst til højre). De tre individuelle billeder er PUF'ens respons til tre forskellige laserlinjer, som samles til en digital repræsentation, et farvebillede (nederst til højre).

gråtonebillede (respons). Informationsindholdet i responset er naturligt mindre i gråtoner end i farve, men er større end i et rent sort/hvidt billede. Informationsindholdet kan blive yderligere reduceret i den digitale repræsentation, alt efter hvilken type der bruges. Både den fysiske PUF og aflæsningen kan være kompleks. Vi kan for eksempel lave et tilfældigt mønster af pigmenter, der indeholder de sjældne jordarter europium(III), terbium(III) og dysprosium(III). De udsender henholdsvis rødt, grønt og blåt lys. Derved kan det tilfældige mønster både aflæses som et sort/hvidt billede, men vi kan også bruge de unikke egenskaber af lanthanidernes luminescens, som vist i figur 2 [5].

Her kan vi både lave et respons i sort/hvid, i farve, og vi kan lave billeder afhængigt af, om vi giver et input specifik møntet på en enkelt farve. De data, der er vist i figur 2, er alene pigmenter på en glasoverflade; en PUF, men ikke et PUF-mærke.

Physical Unclonable Function

Physical Unclonable Function, PUF: Et mønster, der er så småt og så kompliceret, at det ikke kan genskabes.
Input: Den metode, der bruges til at læse en PUF. Det kan være lys, elektriske felter, strøm m.m.
Respons: Det signal en PUF giver efter et input. Det kan være et simpelt billede, strøm, et trådløst signal m.m.
Input-respons par: Kryptologisk koncept, hvor et bestemt input kun har et korrekt svar, der skaber en sikker forbindelse mellem afsender og modtager.
Digital repræsentation: Det dataformat som et PUF-respons gemmes i.
Digital ID: Det unikke ID, der er knyttet til en PUF.
PUF-mærke: En registreret PUF i et veldefineret område, der har en digital ID, og som kan læses med det rette udstyr.

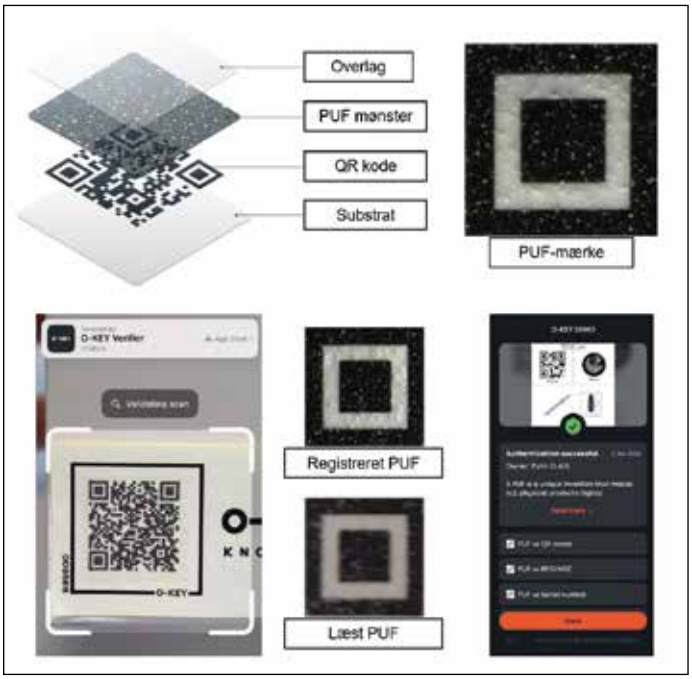
For at kunne bruge det som et PUF-mærke, skal pigmenterne i en lim/lak, der ikke forstyrrer signalet, og vi kan ikke printe på papir, da papir faktisk har en kraftig egenluminescens, hvilket gør, at vi ikke får et klart respons fra PUF-mønsteret. Derfor kan den PUF, der fungerer fint i forskningslaboratoriet, ikke bruges i praksis.

Figur 3 viser det PUF-mærke, som er kommercialiseret under varemærket O-KEY. Det er et tilfældigt mønster af mikroskopiske hvide partikler printet på papir. Kompleksiteten er mere end rigelig til at sikre, at systemet er sikkert, men som en videnskabelig udfordring kan der laves meget mere komplicerede PUF-mærker [6].

Et eksempel på et PUF-mærke

For at kunne bruge en PUF i et PUF-mærke, skal det område, det tilfældige mønster findes i, defineres. Det har vi valgt at gøre i hjørnerne af en QR-kode. Fordelen er, at QR-koder både er veldefinerede og er noget, som de fleste allerede er vant til at scanne. PUF-mærkerne fremstilles på et almindeligt trykkeri, ved at trykke med et klart blæk, der indeholder PUF-partikler i titaniumdioxid, oven på den sorte farve, som vist i figur 3. Derved skabes der helt unikke mønstre af hvide partikler oven på det sorte tryk. Mønstre, der er umulige at kopiere, hvilket er definitionen på en PUF. Da trykket foregår på en label, har vi automatisk lavet et PUF-mærke, og figur 3 viser tydeligt, at PUF-mønsteret kan læses på et billede. Hvis PUF-mærket skal holde længe, kan der lægges en klar film, et overlag, på.

PUF-mærkerne kommer på ruller, som vi registrerer med højopløste billeder, og læser med hjælp af computervisionalgoritmer i en mobilapp [7]. I figur 3 vises brugergrænsefladen i appen, samt et billede der er taget med appen. Kvalitetsforskellen til det registreringsbillede, læsningen er matchet med, er tydelig. I dette eksempel er der knyttet både billeder og link til PUF-mærkets ID. Disse vises direkte i appen, når PUF-mærket er læst.



Figur 3. Sammensætningen af et PUF-mærke: papirlabel, printet QR-kode, printet PUF-lag og øverst et beskyttende lag (øverst til venstre). Et registreringsbillede af et PUF-mærke, det tilfældige PUF-mønster er de små hvide partikler (øverst til højre). Appen, der kan læse de tilfældige mønstre, et brugerbillede fra appen matchet til det korrekte registreringsbillede, og den info der vises i appen (nederst).

Sammenlignes dette eksempel med den generelle PUF i figur 1, så består PUF'en af det tilfældige mønster, de hvide partikler danner. Husk, at PUF-mærket er mønster, QR-kode samt label. Registrering og læsning af mønsteret foregår med et input, der er helt almindeligt lys og et respons, der er et digitalt farvebillede i varierende kvalitet. Kvalitetskravet er stort ved registrering, mens selv meget dårlige billeder kan matches til det rigtige unikke ID ved hjælp af kunstig intelligens. Det er vigtigt at nævne, at der aldrig matches til et forkert ID, mens der vil være billeder, der er så dårlige, at de ikke kan matches til et ID.

Konklusion

Ved at skabe mikroskopiske, unikke PUF-mønstre på eksisterende labels og emballager, kan disse linkes til et unikt digitalt ID. Billeder taget med dedikerede kameraer, laver en digital repræsentation af PUF'en og der linkes til det unikke ID. Når nye billeder tages af PUF'en, kan disse matches til én digital repræsentation, og derved kan man nemt læse de unikke mønstre og finde de tilhørende unikke ID'er. Hele dette koncept kaldes for Physical Unclonable Functions, der i en udformning, som kan printes på almindelige trykkerier og læses med mobiltelefoner, er opfundet på Københavns Universitet og udviklet til et produkt i virksomheden PUFIN-ID.

E-mail:
Thomas Just Sørensen: tjs@chem.ku.dk

Referencer

1. Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. Physical One-Way Functions. *Science* **2002**, *297* (5589), 2026-2030. DOI: doi:10.1126/science.1074376.
2. Arppe, R.; Sørensen, T.J. Physical unclonable functions generated through chemical methods for anti-counterfeiting. *Nature Reviews Chemistry* **2017**, *1* (4), 31. DOI: UNSP 0031 10.1038/s41570-017-0031.
3. a) Arppe-Tabbara, R.; Tabbara, M.; Sørensen, T.J. Versatile and Validated Optical Authentication System Based on Physical Unclonable Functions. *ACS Applied Materials & Interfaces* **2019**, *11* (6), 6475-6482. DOI: 10.1021/acsami.8b17403. b) Fernández-Benito, A.; Hoyos, M.; López-Manchado, M.A.; Sørensen, T.J.A Physical Unclonable Function Based on Recyclable Polymer Nanoparticles to Enable the Circular Economy. *ACS Applied Nano Materials* **2022**, Review. DOI: 10.1021/acsanm.2c00808.
4. Landrock, Peter: kryptologi i Lex på lex.dk. Hentet 6. februar 2026 fra https://lex.dk/kryptologi.
5. Carro-Temboury, M.R.; Arppe, R.; Vosch, T.; Sørensen, T.J. An optical authentication system based on imaging of excitation-selected lanthanide luminescence. *Science Advances* **2018**, *4* (1), e1701384. DOI: 10.1126/sciadv.1701384.
6. Klausen, M.; Zhang, J.; Stevens, M.M. Designing Physical Unclonable Functions From Optically Active Materials. *Adv Mater* **2025**, e2502059. DOI: 10.1002/adma.202502059.
7. I kan selv hente O-KEY verifier appen i jeres foretrukne app store. I skal dog bruge nogle O-KEYs for at se, hvordan den faktisk virker.