

60 ÅR SØNDAG



BLÅ BOG

Ivan Bjerre Damgård

Opvokset i Klim og i Aulum.

1988: Ph.d, Institut for Matematik og Datalogi, Aarhus Universitet.

2005: Professor, Institut for Datalogi, AU.

2015: Modtager af "The RSA Conference Award for Excellence in Mathematics" og samme år modtager af ERC Advanced Grant, den mest prestigefyldte bevilling man kan opnå på europæisk plan.

To voksne sønner fra første ægteskab og fire bonusbørn i alderen 12-23 fra nyt forhold.

Ivan Damgaard er professor i datalogi og er i den europæiske elite blandt forskere i it-sikkerhed. Han er samtidig en fremragende og populær spillemand.
Foto: Rune Aarestrup Pedersen

Polkaer, protokolteorier og pauser

Datalogi med mere: Meget af Ivan Damgaards arbejde består i at tænke og tage sig tid til at få nye idéer. Han er en folkemusikspillende professor i datalogi, som hører til i den europæiske elite inden for sit felt.

KIRSTEN ELLEY
navneredaktør
kirsten.elley@jp.dk

Ivan Damgård hører til den sjældne kategori af jyske mænd, der aldrig har fået sig et kørekort.

Han er også noget så sjældent som en højt estimeret professor i datalogi, som samtidig er en af landets kun 16 officielle rigsspille-mænd.

Violinen er hans hovedinstrument, og folkemusikken er hans genre.

Men i særklasse er han dygtig til komponere og arrangere ny spillemandsmusik, hvis man spørger ham selv. Det er blevet til en del gennem årene, og allerede i 2007 modtog han en Danish Music Award i folk-kategorien som årets komponist.

Snart sagt al Ivan Damgaards fritid går med at spille i forskellige sammenhænge og med forskellige bands, og de læsere, der stadigvæk måtte have opfattelsen af, at folkemusik er langsom og kældedans udført af ældre borgere iklædt bidselsko, knæstrømper og nathuer, kan tro om igen.

Ny nordisk folkemusik

Nordisk folkemusik er blevet hip i mange nye sammenhænge i takt med, at de

gamle folkedansforeninger i Danmark svinder ind. Dansen trædes i dag elegant og gesvindt på festivaler, øleje og ved universiteternes fredags-barer og store folkemusikstævner med lige så mange unge som ældre, lige så mange udøvende spillere som dansere. Ivan kender man. Han vil som regel være der.

Den anden halvdel af Ivan Damgård, valgmenighedspræstens søn fra Aulum, er professor i datalogi ved Aarhus Universitet. Hans speciale er kryptering og protokolteori, og begge dele har med forskning i it-sikkerhed at gøre.

Europas bedste på området
Kryptering er kendt. Det er når computerens indhold oversættes til volapyk, så hackere ikke kan finde hoved og hale i materialet.

Problemet er bare, at når teksten eller indholdet er krypteret og sendt, og selv om det sker hurtigere end en Tesla kan accelerere, så kan det være for sent. Indholdet kan allerede være blevet stjålet inden krypteringen fandt sted.

Næste og nyeste skridt i forebyggelsen hedder protokoller.

Inden for det felt hører Ivan og hans kollegaer på Aarhus Universitet til blandt

Europas stærkeste og mest anerkendte.

»Man kender os da ude omkring,« som professoren underspillet udtrykker det. 152 videnskabelige publikationer i internationale tidsskrifter, plus medforfatter på en bog udgivet på Cambridge University Press sidste år, taler for sig selv.

Vi har at gøre med den absolutte elite indenfor et felt, som har stor bevågenhed og økonomisk potentiale. Bogens titel antyder kompleksiteten i forskningsfeltet: "Multiparty Computation and Secret Sharing".

Ivan Damgård var allerede for 30 år siden medstifter af datasikkerhedsselskabet Cryptomathic, og han er i dag medstifter og medejer af Partisia og Sepior, som begge er spin-off-firmaer med rod i Aarhus Universitet indenfor protokolteorien.

»Cryptomathic klarede sig godt, og jeg har solgt min andel, men selv om Sepior er tænkt mere ambitiøst kommercielt, så står vi ikke endnu med et firma i hånden, som kan sælges til Google for 100 mio. kr.,« ræsonnerer han.

Protokol hvad for noget?

Protokolteori er forskningen i, hvordan man får en flok computere i et netværk til at arbejde som én maskine i

forhold til hackerangreb. Fjenden kan stadigvæk bryde ind, men hvis han ikke rammer alle computere, kan han ikke få kun adgang til det ønskede materiale.

»Det er som kaptajn Flint på sørøverskibet, der river skattekortet i stykker og giver en flig til hver sømand. Sådan fungerer protokoller. Et hackerangreb vil ikke nytte noget, fordi det kun er en flig af netværket, man får fat i, og så ved man stadig ikke, hvor skatten er begravet,« fortæller Ivan Damgård.

Den musikalske åre

Som type er han en venuesæl og fremkommelig mand, der holder af fællesskaber. Måske er det træk så tydeligt, fordi han er enebarn.

Da han var ni år gav moderen ham valget mellem at spille klaver og violin.

»Jeg valgte violin, for klaver var for tøser. Sådan så jeg det dengang. Det er mit held, at jeg er begyndt så tidligt, for det giver jo en helt anden sikkerhed i spillet. En overgang havde jeg en ungarsk lærer på musikskolen i Holstebro, som mente, jeg burde gå videre ad den musiske vej, men idéen fadede, da han rejste. Jeg valgte så at læse matematik og datalogi, fordi det var de fag i gymnasiet, der

faldt mig lettest,« fortæller Ivan Damgård.

Han husker hverken at have haft ambitioner eller nogen større og overordnet livsplan på det tidspunkt i livet. Det var snarere den nemme udvej, han valgte, ved at satse på matematik.

»Jeg var dog den første på gymnasiet, der fik en lommeregner – en Sinclair. Hold op, det var stort, den havde alle fire regnemetoder, gange, dividere, plus og minus. Siden fik gymnasiet en datamaskine stillet til rådighed af Kommunedata – med hulbånd og APL, og det syntes jeg også var yderst interessant.«

Pauser i livet

Stik imod tidens orden, så er Ivan Damgård tilhænger af pauser i livet. Da han havde læst matematik på Aarhus Universitet i to år, fra 1977-78, holdt han pause og tog på Askov Højskole. Efter det år tog han for alvor fat i kraven på folkemusikken.

»Jeg mener, det er vigtigt at tage pauser og tænke over, hvad man egentlig vil. Meget af mit arbejde består jo også i at tænke og tage sig tid til at få nye idéer,« siger han. Da specialet i matematik var i hus, begyndte han at læse musik og tog bifag i det. Dog mener han ikke, at han som matematiker har

en fordel i forhold til at spille og komponere musik. Men mange matematikere spiller faktisk også musik, har han bemærket.

De spørgsmål, der bliver ved med at udfordre professoren i arbejdet, er følgende: Hvad kan en computer overhovedet? I netværk, hvad kan de så – og hvor mange fejl kan man tolerere?

Den slags kræver matematik og tanker. Det er det store, vi ikke forstår, der bliver ved med at pirre ham.

»Kryptering og sikkerhed er områder fyldt med problemer, som på overfladen ser ud til at være umulige at løse – men hvor vi så finder en løsning alligevel, når vi tænker os om. Det bliver ved med at fascinere mig,« siger Ivan Damgård, der kalder sit felt for et "våbenkapløb" med de lyssky elementer, der har til hensigt at bryde it-sikkerheden hos firmaer, regeringer, offentlige instanser og private.

Der er store interesser på spil og store penge involveret til dem, der vinder kapløbet.

Ivan Damgård er i spurt.

Ivan Bjerre Damgård,
professor,
Aabyhøj ved Aarhus