PROTOKOLL

Datum
2025-11-10

Diarienummer
PA-2025-0013

Fakultetsnämnden vid skolan för elektroteknik och datavetenskap

Protokoll nummer: 9/2025

Datum och plats för mötet:
Henrik Eriksson kl. 09.00-12.00, lindstedtsvägen 3 plan 4

Närvarande lärarledamöter:
Ann Lantz, *ordförande*
Joakim Jaldén, vice ordförande
Ivy Bo Peng
Cyrille Artho
Hedvig Kjellström
Ingo Sander
Kristina Höök

Närvarande studentledamöter:
Jura Miniota, doktorandrepresentant

Närvarande externa ledamöter:
Ambra Sannino, Vattenfall

Företrädare för arbetstagarorganisationer:
Monica Åkerström, ST

Frånvarande ledamöter:
Hanifeh Khayyeri, RISE
Alexander Baltatzis, SACO

Övriga närvarande:
Joakim Palestro, kanslichef
Elina Bjurbäck, sekreterare
Karl Meinke, prefekt §3
Sofia Norlander, Utbildningsadministrativt ansvarig §6
Markus Hidell, grundutbildningsansvarig §7, §8, §9
Viktoria Fodor vice grundutbildningsansvarig §12

---

§ 1 Mötet öppnas

a) Val av justerare

Nämnden beslutar att till justerare utse Kristina Höök

b) Dagordning

Nämnden beslutade at lägga till punkten kvalitetsrapport till övriga frågor och sedan godkänna föreslagen dagordning

c) Fråga om jäv

Ingen ledamot anmäler jäv

d) Föregående möte

Ordförande följer upp doktorandernas punkt (§11) från föregående möte. Ordförande har lyft frågan vidare till forskarutbildningsansvarig för fortsatt hantering. Doktorandrepresentanten arbetar vidare med att ta fram ett konkret förslag.

§ 2 Skolans reformagenda

Ordförande Ann Lantz informerar om reformagendans nuvarande innehåll och redogör för pågående samt avslutade projekt. Skolan har möjlighet att revidera och vidareutveckla reformagendan, och ledamöterna uppmuntras att inkomma med synpunkter och förslag på förbättringar. Fakultetsnämnden för en diskussion om nämndens roll i beredningen av frågor kopplade till reformagendan, liksom hur nämnden aktivt kan bidra till genomförandet av planerade aktiviteter. Det lyfts även att en förbättrad överhörning och informationsdelning mellan ledningsrådet och fakultetsnämnden skulle kunna stärka samspelet och skapa bättre förankring i skolans verksamhet i de frågor som tillhör nämndens ansvarsområden.

§ 3 Ansökan om utnämning till affilierad fakultet i kryptologi

PA-2025-3360

Prefekt Karl Meinke föredrar ärendet.

Fakultetsnämnden beslutar att:

Utnämna Martin Ekerå till affilierad fakultet i kryptologi från och med den 1 januari 2026 och tills vidare, dock längst till och med den 31 december 2028 med en omfattning om 30 % av heltid, under förutsättning att avtal enligt KTH:s riktlinjer sluts med Martin Ekerås huvudarbetsgivare MUST, Försvarsmakten. Utnämningen kan förlängas efter ansökan. Den sammanlagda utnämningstiden får dock omfatta högst 12 år. Om Martin Ekerås anställning vid MUST inom FM avslutas, upphör med omedelbar verkan även utnämningen till affilierad fakultet vid EECS-skolan, KTH. Ekerås lön bekostas till 100% av MUST.

§ 4 Förhållningssätt i vår kommunikation från fakultetsnämnden

Vice ordförande Joakim Jaldén föredrar ärendet och betonar vikten av ett professionellt och respektfullt bemötande vid fakultetsnämndens sammanträden. Han understryker att ledamöternas ton och sätt att framföra kommentarer och återkoppling har stor betydelse, särskilt när externa eller inbjudna gäster deltar. Ledamöterna uppmanas därför att

säkerställa att synpunkter uttrycks konstruktivt, tydligt och med respekt för mötets syfte och för de personer som presenterar eller deltar.

§ 5 Remiss JML-styrdokument

Vice ordförande Joakim Jaldén föredrar ärendet. Fakultetsnämnden har möjlighet att lämna ett gemensamt remissvar. Kanslichef Joakim Palestro utses att sammanställa remissvaret och skicka det till Equality Office senast den 1 december.

Nämnden för ett resonemang kring dokumentets ambitionsnivå och målsättningar. Nämnden lyfter bland annat att målen bör formuleras som att KTH bör uppnå dem, och inte endast verka för att uppnå dem.

PAUS 10.05-10.20

§ 6 Tentaadministration

Katarina Jonsson Berglund och Petra Krödel är föredragande

De föredragande framför ett stort tack till fakultetsnämnden för det samlade inspel och den konstruktiva feedback som tidigare lämnats gällande tentaadministrationen. Föredraganden deltar vid dagens sammanträde för att bemöta synpunkterna och föra dialog kring möjliga förbättringsåtgärder. De föredragande redogör för de förbättringsförslag som tagits vidare utifrån nämndens inspel. Förslagen diskuteras i helgrupp, bland annat tydligare och mer tillgänglig information på hemsidan avseende rutiner och administrativa processer. Nämnden lämnar ytterligare inspel för fortsatt utveckling av området och ser positivt på det fortsatta samarbetet.

§ 7 Tilläggsbeslut gällande kurslista och utbildningens genomförande kull HT26 för CDATE, CMETE, TIVNM, spår HCI

(HS-2025-2537)

Föredragande: grundutbildningsansvarig Markus Hidell

Fakultetsnämnden beslutar att:

Fastställa beslut om tillägg till beslutet HS-2025-1370 fastställande av kurslistor och text för studenter som antas höstterminen 2026 enligt bilagor §7a, §7b för följande program inom grundutbildningen: Civilingenjörsutbildning i datateknik (CDATE), civilingenjörsutbildning i medieteknik (CMETE).

Fakultetsnämnden beslutar att bordlägga:

Förslaget om tilläggsbeslut till Masterprogram, ICT Innovation (TIVNM) enligt bilaga §7c och remitterar frågan tillbaka till grundutbildningsansvarig för vidare åtgärd.

§ 8 Beslut om ändring av CMETEs utbildningsplaner kull HT23, HT24, HT24

(HS-2025-2538)

Fakultetsnämnden beslutar att:

Fastställa beslut om tillägg av mappningarna för civilingenjörsutbildningen i medieteknik (CMETE) retroaktivt för kullarna HT23, HT24 och HT25, enligt bilaga §8.

§ 9 Beslut om ändringar av kursadminislista i utbildningsplan för TIELA, kull HT24, HT25, HT26

(HS-2025-2628)

Fakultetsnämnden beslutar att:

Fastställa förslag till beslut att revidera utbildningsplan gällande kurslistor för studenter som antas höstterminen 2024, 2025 och 2026 för följande program inom grundutbildningen: Högskoleingenjörsutbildning i elektroteknik, Flemingsberg (TIELA) enligt bilaga §9.

§ 10 Lärares undervisningsmaterial

Föredragande Cyrille Artho informerar om ett möte med Wanda Manninger och Hans Wolfart avseende planerad nedstängning av personliga hemsidor på KTH:s webbplattformar. I mötet lyftes bland annat frågor kring juridiska rättigheter kopplade till material som skapats av anställda men som finns kvar efter att personer lämnat KTH. Det råder i nuläget osäkerhet kring i vilken utsträckning KTH har rätt att fortsätta använda eller publicera sådant material utan uttryckligt samtycke. Det framhålls att det kan behövas en överenskommelse i samband med anställning där medarbetare godkänner att innehåll producerat på KTH:s plattformar får användas av KTH även efter att anställningen har upphört. Frågan beskrivs som komplex och gemensam för flera svenska universitet, och bedöms även vara juridiskt svår att lösa.

Mot bakgrund av omfattande protester från fakulteten förs frågan vidare av ordförande Ann Lantz, som avser ta upp den med universitetsledningen och rektor under veckan. Fakultetsnämnden uttrycker sitt stöd för att frågan drivs vidare. Nämnden lyfter också att eventuell implementeringen behöver genomföras på ett sätt som säkerställer kvalitet och rimlig tidsplanering.

§ 11 Breddad rekrytering och breddat deltagande

Föredragande Viktoria Fodor presenterar uppdraget samt den arbetsgrupp som arbetar med skolans målsättning kopplad till breddad rekrytering och breddat deltagande. Hon redogör för nulägesbilden inklusive aktuella mål och pågående initiativ för att öka breddad rekrytering och genomströmning. Nämnden diskuterar vidare möjliga samarbeten och riktade insatser för att öka intresset hos underrepresenterade grupper.

§ 12 Studenternas punkt

Doktorandrepresentant Jura Miniota

Doktorandrepresentant Jura Miniota informerar om att val till student council kommer att hållas den 8 december kl. 17.00 i Fantum. Ledamöterna uppmanas att sprida informationen så att studenter ges möjlighet att delta.
Det framkommer att den tilltänkta ersättaren för Jura eventuellt inte kommer talar svenska. Detta kan försvåra studenternas möjlighet att delta och bidra i ledningsmöten där svenska är arbetsspråk. Frågan behöver hanteras för att säkerställa att studentinflytandet inte begränsas av språkliga hinder.

§ 13 Övriga frågor

Återkoppling ges från verksamhetsdialogen, med fokus på kvalitetsrapporten. Skolan lyfte behovet av mer verksamhetsnära och decentraliserat stöd under dialogen. Rektor efterfrågade tydligare reflektioner kring forskningskvalitet från avdelningarna, inklusive att även lyfta problemområden.

Vid protokollet

Elina Bjurbäck

Elina Bjurbäck
Sekreterare

Ann Lantz

Ann Lantz
Ordförande
Justeringsdatum: 2025-11-13

Kristina Höök

Justerare

Justeringsdatum: 2025-11-13

Fakultetsnämnden vid EECS-skolan

§ X Ansökan om utnämning till affilierad fakultet i kryptologi (PA-2025-3360)

Ärendet

Institutionen för Datavetenskap vid Skolan för elektroteknik och datavetenskap (EECS) ansöker om att påbörja ett förfarande om att utnämna Martin Ekerå till affilierad fakultet inom ämnesområdet kryptologi (*eng*. cryptography) från och med 1 januari 2026 och tills vidare dock längst till och med 31 december 2028. Martin Ekerås arbetsgivare MUST, Försvarsmakten, har godkänt dennes engagemang i KTH:s verksamhet. I ansökan ingår önskemål om att utnämningen ska kunna förlängas vid behov.

Fakultetsnämnden har att besluta om utnämning till affilierad fakultet för en viss period och omfattning i enlighet med KTH:s *riktlinje om affilieringar*.

Bifogade handlingar

- Institutionens anhållan om utnämning till affilierad fakultet i kryptologi.
- Kandidatens viljeyttring, CV och publikationslista.
- Utkast till avtal i ärendet med bilaga.

Förslag till beslut:

Fakultetsnämnden vid EECS-skolan, KTH, beslutar att utnämna Martin Ekerå till affilierad fakultet i kryptologi från och med den 1 januari 2026 och tills vidare, dock längst till och med den 31 december 2028 med en omfattning om 30 % av heltid, under förutsättning att avtal enligt KTH:s riktlinjer sluts med Martin Ekerås huvudarbetsgivare MUST, Försvarsmakten.

Utnämningen kan förlängas efter ansökan. Den sammanlagda utnämningstiden får dock omfatta högst 12 år.

Om Martin Ekerås anställning vid MUST inom FM avslutas, upphör med omedelbar verkan även utnämningen till affilierad fakultet vid EECS-skolan, KTH.

Datum: 2025-10-20 Dnr: PA-2025-3360

Institutionen för Datavetenskap vid Skolan för elektroteknik och datavetenskap (EECS) ansöker om att påbörja ett förfarande om att utnämna Martin Ekerå till affilierad fakultet inom ämnesområdet kryptologi (*eng*. cryptography).

Ansökan är utarbetat i enlighet med aktuell riktlinje för affilierade.

Prefekt har avstämt ansökan med Fakultetsförnyelseansvarig ☒ Datum: 2024-11-26

Bilagor som bifogas till ansökan:

- Utkast till avtal om anknytning som affilierad fakultet. Om utkast inte finns räcker i detta skede en skriftlig viljeyttring från samverkansparten att under angiven period låta den föreslagna personen avsätta del av sin arbetstid hos samverkansparten för verksamhet vid KTH.

- CV samt publikationslista för den föreslagna personen.

Ansökan om att utnämna en person till affilierad fakultet

Innan en ansökan om att utnämna en person till affilierad fakultet lämnas in ska en inledande diskussion föras mellan prefekt och fakultetsförnyelseansvarig.

Prefekt ansöker till fakultetsnämnden om att utnämna en person till affilierad fakultet. Efter föredragning av prefekt beslutar fakultetsnämnden om utnämning till affilierad fakultet för viss period och omfattning.

Ansökan ska ha följande innehåll:

	Beskrivning av förväntad nytta för KTH och samverkansparten inkluderande koppling till skolans identifierade behov av önskad tillförd kompetens i ämnesområdet. Huvudsakliga uppgifter inom ramen för affilieringen samt en beskrivning av hur kandidaten kompletterar befintlig fakultet i verksamheten och på skolnivå ska anges. Ämnesområde, planerade uppgifter inom forskning och utbildning, samt jämställdhet kan beaktas avseende förväntad nytta för KTH.
	Cybersäkerhet (där kryptografi anses som ett kritiskt men specialiserat område) är ett brett ämne med snabbt ökande nationell och geopolitisk betydelse, och har varit ett område där KTH under många år systematiskt har etablerat en kritisk massa av forskare med både nationell och internationell påverkan. Idag är KTH:s cybersäkerhetsforskning fokuserad kring systemsäkerhet (SCS-avdelningen), nätverkssäkerhet (NSE-avdelningen) samt mjukvaru- och hårdvarusäkerhet och integritet (TCS-avdelningen). Vi bör också notera etableringen av KTH CDIS forskningscentrum inom cybersäkerhet och mer nyligen det nationella Cybercampus, där KTH-forskare spelar en ledande roll. När det gäller utbildning har KTH nyligen etablerat ett nytt masterprogram i cybersäkerhet och deltar i utbildningen av cybersoldater för Försvarsmakten. Forskning inom kryptografi vid KTH har länge bedrivits vid TCS-avdelningen (docent Douglas Wikström – nyligen avgick för industrin) och Matematiska institutionen (professor Johan Håstad – närmar sig pensionering). Håstads gemensamma forskning med hans tidigare doktorand Dr Martin Ekerå har varit avgörande för att sätta KTH på den internationella kartan för forskning inom kvantkryptanalys. Ekerå är en ledande expert inom detta område, i en känslig tid då framväxande kvantberäkningsteknik står på gränsen till att äventyra nationell säkerhetsinfrastruktur genom effektiv kodknäckning. Ekerå har cirka 18 års både teoretisk och praktisk erfarenhet av att arbeta som kryptograf på NCSA vid den militära underrättelse- och säkerhetstjänsten (Must), som i sin tur är en del av Försvarsmakten (FM). Ekerå tjänstgör för närvarande som chefskryptograf för NCSA. NCSA styr och samordnar all statlig verksamhet relaterad till kommunikationssäkerhet (COMSEC) inom det svenska totalförsvaret. För att skydda sekretessen för sekretessbelagd information när den ska kommuniceras till ett informationssystem som ligger utanför operatörens kontroll, föreskriver svensk lag att ett så kallat COMSEC-system som är godkänt av NCSA ska användas. NCSA skriver kraven för, utvecklar, granskar och godkänner COMSEC-system i samarbete med FMV och den svenska kryptografiska industrin. Följaktligen utför NCSA ett betydande arbete inom kryptografiområdet – från arbete med algoritmer och protokoll till arbete med säker implementering i programvara och hårdvara. Eftersom information kan vara sekretessbelagd under mycket långa tidsperioder (50 år eller mer) planerar NCSA mycket långt framåt i sin hotbildsanalys och i hur man bygger COMSEC-system. NCSA ligger därför idag i framkant när det gäller att hantera kvantum – något som i sin tur har möjliggjort att den offentliga forskning som hittills har bedrivits vid KTH i samarbete med NCSA snabbt har kommit igång och levererat resultat som har placerat Sverige, NCSA och KTH på kartan internationellt.

Ur NCSA:s perspektiv är det viktigt att en livskraftig kryptografigrupp finns kvar på KTH även i framtiden, med förbehållet att åtminstone en del av den inre kärnan i en sådan grupp bör bestå av svenska medborgare som kan genomgå en säkerhetsprövning för att kunna skapa en länk mellan KTH och NCSA, och hantera sekretessbelagd information. Inte minst kan en sådan grupp bidra till att säkerställa kvaliteten på grundutbildningen i kryptografi på KTH, och den stadiga tillgången på lämpligt utbildade kryptografer i Stockholmsregionen.

Slutligen noterar vi att KTH nyligen har etablerat ett kvantteknologiskt nav (KTH QTH). Dessutom förbereder KTH, Chalmers och Lunds universitet för närvarande ett förslag för kvantteknologin VR SFO som gemensamt kommer att täcka alla tre områdena kvantberäkning, kommunikation och sensorteknik.

Information om huvudsakliga uppgifter inom forskning och utbildning.

Ekerå kommer att fortsätta bedriva egen forskning, samt agera bihandledare till en FM-finansierad doktorand vid CDIS förutsatt att en sådan kan rekryteras. (Härutöver är det tänkbart att Ekerå även kan komma att handleda arbeten på masternivå om de ligger inom ett relevant ämnesområde och tid finns tillgänglig.)

1. Handledning av FM-finansierad doktorand

- *Forskningsämne:* Doktoranden kommer att bedriva forskning inom kryptologiområdet, med tänkt tonvikt på kvantdatorsäker kryptologi och kvantdatorassisterad kryptoanalys (där Ekerå redan har en upparbetad forskningslinje).

- *Handledning:* Avsikten är att via CDIS rekrytera in en doktorand, för vilken Ekerå är tänkt att fungera som bihandledare och Johan Håstad är tänkt att fungera som huvudhandledare.

  Doktoranden kommer att placeras 20% på Must och resterande 80% på KTH i likhet med det upplägg som tidigare användes för Joel Gärtner som nyligen disputerade.

  Ekerå kommer regelbundet delta i handledningsmöten (cirka 1 timme varannan vecka) med kryptogruppen, främst för att stödja den nya doktoranden och för att diskutera forskning.

  Det är på sikt möjligt att fler FM-finansierade doktorander kan tillkomma, samt att kryptologer från Must kan komma att medverka i arbetet vid KTH på olika sätt. Målet är att bygga en livskraftig forskningsgrupp då Johan Håstad närmar sig pensionsåldern.

2. Egen forskning

- Ekerå kommer för egen del att fortsätta bedriva egen forskning inom kvantdatorassisterad kryptoanalys och kvantdatorsäker kryptologi, samt kryptologi i bredare bemärkelse när det är relevant inom ramen för hans roll som chefskryptolog vid Must, samtidigt som han följer utvecklingen av kryptoanalytiskt relevanta storskaliga feltoleranta kvantdatorer.

  (Ovanstående kommer även att bidra till att stärka KTH:s ställning inom kvantberäkning, samtidigt som vi respekterar begränsningen att Must primärt är intresserat av kryptologi.)

2. Bidrag till grundutbildningen

- DD2520 Applied cryptography: Ekerå med stöd av kollegor vid Must kommer fortsatt att bidra med gästföreläsningar om signalskyddet i Sverige.
- DD2440 Avancerade algoritmer: Ekerå kan även bidra med gästföreläsningar om kvantberäkningar och kvantdatoralgoritmer för kryptoanalys, t.ex. om Shors algoritm.

Förslag på utnämningens längd och omfattning i procent av en heltid.

Vi föreslår en utnämningslängd om tre år med start 2026-01-01 och en omfattning av 30% av en heltidstjänst (omfattningen anger ett medelvärde, då Ekerå har många åtaganden inom ramen för sin roll som chefskryptolog vid Must). Vi önskar även att utnämningen ska kunna förlängas vid behov.

Martin Ekerå
Kungsklippan 14, 3 tr
112 25 Stockholm

22 oktober 2025

Kungliga Tekniska Högkolan
106 91 Stockholm

Till den det berör,

Jag har arbetat i olika positioner inom kryptologiområdet i omkring 18 år vid avdelningen för krypto och IT-säkerhet vid Must, och tjänstgör idag som chefskryptolog vid avdelningen. Härutöver har jag doktorerat inom kvantdatorassisterad kryptoanalys och kvantdatorsäker kryptologi vid KTH med Johan Håstad som handledare. Jag är idag en internationellt erkänd expert inom kvantdatorassisterad kryptoanalys.

I syfte att framgent bibehålla en stark koppling mellan Must och KTH inom kryptologiområdet, samt en livskraftig kryptogrupp vid KTH, ansöker jag härmed om att bli affilierad fakultet i kryptologi vid KTH.

Min förhoppning är vidare att jag genom min affiliering ska kunna bidra till att fortsatt sätta KTH på kartan inom kvantområdet, särskilt vad avser kvantdatoralgoritmer med kryptoanalytiska tillämpningar, samt till grundutbildningen.

Med förhoppning om ett positivt utfall,

Martin Ekerå

Curriculum vitae

1. Personal data

1.1. Name: Martin Ekerå

Personal number: (19)831113-1919

Citizenship(s): Swedish

1.2. Date of birth: 1983-11-13

1.3. Sex: Male

1.4. Home address, telephone, email

- **Postal address:**

  Kungsklippan 14, 3 tr
  SE-112 25 Stockholm
  SWEDEN
- **Telephone:** +46-(0)709-64 89 60
- **E-mail:** ekera@kth.se, martin@ekera.se

1.5. Work address, telephone, email

- **Postal address:**

  Swedish Armed Forces
  MUST SÄKK SÄKT
  SE-107 85 Stockholm
  SWEDEN
- **Telephone:** +46-(0)8-788 79 08
- **E-mail:** martin.ekera@mil.se

1.6. Present employment: Chief cryptographer (*swe.* Chefskryptolog), Swedish NCSA, Swedish Armed Forces (from 2024-01-01)

The Swedish National Communications Security Authority (NCSA) is a function within the Military Intelligence and Security Directorate (*swe.* Militära Underrättelse- och Säkerhetstjänsten (Must)) which is in turn a part of the Swedish Armed Forces (*swe.* Försvarsmakten).

The Swedish NCSA directs and coordinates government activities related to communications security (COMSEC), including activities related to so-called "secure cryptographic functions" — ranging from cryptographic algorithm and protocol development to the development, evaluation and approval of complete COMSEC systems. By Swedish law, if classified information (*swe.* säkerhetsskyddsklassificerade uppgifter) is to be communicated to an information system that is beyond the operator's control, the information must be encrypted with COMSEC systems approved by the Swedish NCSA.

The Swedish NCSA advises the government offices (*swe.* Regeringskansliet) on cryptography, and acts as a CCA/NCSA and NDA in the EU/NATO.

For instance, the Swedish NCSA evaluates and approves COMSEC system for EU classified information up to C-UE/EU-C, and is one of five appropriate qualified authorities (AQUAs) within the EU that provide policy guidance on cryptography and are responsible for carrying out second-party evaluations for EU approvals of COMSEC systems us to TS-UE/EU-TS. The Swedish NCSA furthermore approves COMSEC systems for NATO classified information up to NC, and interfaces with SECAN for obtaining approvals up to CTS. As an NDA, the Swedish NCSA produces and distributes cryptographic keys.

I currently serve as the chief cryptographer of the Swedish NCSA, overseeing the area of cryptography as a whole (we have several groups of cryptographers).

I have served in various roles as a cryptographer within the Swedish NCSA since 2007, and have thus accumulated approximately 18 years of experience.

During this time, I have been extensively involved in classified research and development work. Unfortunately, I cannot provide much details on this work (and therefore I have had to leave quite a lot of material out of this CV).

1.7. Previous employments: All of the below roles are within the Swedish NCSA, Swedish Armed Forces, without interruption from 2008 to the present:

- Cryptographer (*swe.* Kryptolog) (2008 – 2012)
- Expert in cryptography (*swe.* Expert i kryptologi) (2012 – 2015)
- Chief cryptographer (*swe.* Huvudansvarig kryptolog) (2015 – 2023)

(I have also run my own businesses, and I have been employed as a developer at Saab back when I studied for my high school and engineering degrees, etc.)

2. Degrees:

2.1. Academic degrees including year of graduation:

- MSc in engineering physics at KTH (full time 2003–2008, with exchange studies 2005–2006 at the EPFL in Lausanne, degree issued 2008-11-27) with a specialization in computer science and discrete mathematics.

  I did my master thesis at the Swedish NCSA on differential cryptanalysis of MD5 and then started working at the NCSA whilst finalizing my degree.
- PhD in computer science at KTH (part time 2016–2025 at approximately 50% whilst retaining my role at the Swedish NCSA, defended 2024-10-25, degree issued 2025-02-25) focused primarily on quantum cryptanalysis.

  My doctoral thesis is on factoring integers and computing orders and discrete logarithms quantumly with a particular focus on cryptographically relevant problem instances. It significantly advances the state of the art. To my best knowledge, at the time it was published it featured the best high-level algorithms for breaking widely used schemes such as RSA, DSA and Diffie–Hellman (and it still does, at the time of writing this CV).

(I do of course also hold high school and pre-high school degrees, etc.)

3. Research expertise

I have been active in the field of cryptology since 2008. Consequently, I have a fairly extensive network of contacts, both in academia, government and industry.

Since I started doing public research in 2015, I have established myself as a leading figure in the field of quantum cryptanalysis. As previously noted, to my best knowledge, the best high-level quantum algorithms for breaking widely used schemes such as RSA, DSA and Diffie–Hellman stem from my research.

3.1. Development of, participation and collaboration in international networks, particularly in the last five years

I do public research alone or in some cases with leading international experts. The work is not formalized in the way that the subject heading indicates.

3.2. Leadership within research and development that you would like to bring to our attention, such as leading international/national research projects, particularly in the last five years

I do public research alone or in some cases with leading international experts. The work is not formalized in the way that the subject heading indicates.

3.3. Patents

I have not applied for any patents. (Patents on cryptographic algorithms (or software) do not have a positive societal impact in my opinion so even if I have developed several algorithms I have never considered patenting them.)

3.4 Participation in national and international conferences and seminars, particularly the last five years. Indicate types of activity, such as plenary speaker, special invitation speaker, poster, chairmanship etc.

Selected talks related to my research:

- "Quantum Algorithms for Computing Short Discrete Logarithms and Factoring RSA Integers", presentation of my joint paper with Johan Håstad at PQCrypto 2017, Utrecht, the Netherlands, 2017-06-27.
- "On factoring RSA integers and computing discrete logarithms on quantum computers", invited lecture at the Nordic Institute for Theoretical Physics (NORDITA) Seminar in Stockholm, Sweden, 2019-03-04.
- "Quantum computing and its impact on the field of cryptology", talk at SEC-T, Stockholm, Sweden, 2019-09-19.
- "On completely factoring any integer efficiently in a single run of an order-finding algorithm", presentation of my pre-print at a seminar with the CryptoSec Group of researchers at LTH, Lund, Sweden, 2022-06-10.
- "Advice on mitigating the quantum threat to cryptography", talk at ESA, Noordwijk, the Netherlands, 2022-07-27. (I also served on a panel the same day to discuss Quantum Key Distribution (QKD).)
- "The quantum threat to cryptography, our mitigation strategy, and our stance on quantum key distribution", keynote at a NATO symposium in Amsterdam, the Netherlands, 2023-10-03–04.

- "On the state of the art of factoring integers and computing discrete logarithms quantumly", invited lecture for the researchers at WACQT at Chalmers, Göteborg, Sweden, 2023-12-14.
- "On the quantum threat to cryptography, our mitigation strategy, and our stance on quantum key distribution", talk at "Temadag om kvantteknologier inom försvar och säkerhet" organized by the Swedish Defence Research Agency (FOI), Kista, Sweden, 2024-11-08.
- "On the quantum threat to cryptography", talk at the CDIS Spring Conference 2025, Stockholm, Sweden, 2025-05-22.

I have also spoken in a number of context that I am unable to list in this CV.

Dagstuhl seminars: I have been personally invited four times in a row to the bi-annual Schloss Dagstuhl seminar on quantum cryptanalysis. Specifically, I have attended (or will shortly attend) the following seminars:

- Dagstuhl seminar 19421 on Quantum Cryptanalysis, 2019-10-14–18.

  I gave an extended presentation entitled "On factoring RSA integers and computing discrete logarithms on quantum computers" where I surveyed the current state of the literature on quantumly breaking cryptosystems based on the hardness of factoring RSA integers and computing discrete logarithms. In particular, I gave a detailed overview of my own works as they constituted a considerable part of the state of the art at the time.

- Dagstuhl seminar 21421 on Quantum Cryptanalysis, 2021-10-17–22.

  I gave a presentation entitled "On completely factoring any integer efficiently in a single run of an order-finding algorithm" in which I gave an overview of my then recent pre-print with the same title.

- Dagstuhl seminar 23421 on Quantum Cryptanalysis, 2023-10-15–20.

  I gave an informal presentation on ongoing research work of myself and Joel Gärtner on extending Regev's then recently introduced quantum factoring algorithm to algorithms for computing discrete logarithms and orders quantumly, and to algorithms for factoring completely via order finding. Said work was later made publicly available as a pre-print.

  The work at this seminar was divided into working groups. I co-chaired the discussions in the working group devoted to Regev's algorithm.

- Dagstuhl seminar 25431 on Quantum Cryptanalysis, 2025-10-19–24.

  This seminar has yet to take place. I foresee that it will focus to a large extent on recent full-stack cost estimates and efficient implementation techniques for the high-level quantum algorithms developed by myself, by myself and Johan Håstad, and by myself and Joel Gärtner.

Selected events at the Simons Institute: I have been personally invited to participate at various events at the Simons Institute at UC Berkeley:

- Panelist at the so-called "Quantum Colloquium" on "The Jacobi Factor-

ing Circuit: Classically Hard Factoring in Sublinear Quantum Space and Depth", 2025-03-25.

Seyoon Ragavan gave an approximately one-hour-long presentation of the pre-print referenced in the title, which is a joint work between Seyoon Ragavan (MIT), Gregory D. Kahanamoku-Meyer (MIT), Vinod Vaikuntanathan (MIT) and Katherine Van Kirk (Harvard).

A panel discussion of approximately one hour then ensued. I was invited by Umesh Vazirani (UC Berkeley) to sit on the panel alongside Zvika Brakerski (Weizmann Institute of Technology) and Antoine Joux (Sorbonne Université). Umesh chaired the panel himself.

- Participant in the "Quantum Cryptanalysis of Post-Quantum Cryptography" (2020-02-22–24) and "Quantum Algorithms" (2020-02-25–28) seminars held at the Simons Institute, UC Berkeley.

Other panels: Amongst other unclassified panels, I should perhaps mention:

- Panelist on "Public Sector Views On Quantum Computers And Threats To Governments" at the ETSI / IQC Quantum Safe Workshop 2018 in Beijing, China, 2018-11-06.

  The other panelists were Lily Chen (NIST), Manfred Lochter (BSI), Shiho Moriai (NICT), David Sabourin (CCCS) and Michael Groves (NCSC which is a part of the GCHQ). Michael chaired the panel himself.

  "Governments around the world are the most at risk and are concerned about the threats posed by Quantum Computing. Learn more about their views and some of the early mitigation plans."

Program committees: PQCrypto 2024 (Oxford, UK), PQCrypto 2025 (Taipei, Taiwan), PQCrypto 2026 (Saint Malo, France, ongoing).

Reviewer for conferences (and journals): CRYPTO, EuroCrypt, PQCrypto, FOCS, STOC, SODA, J. Cryptol., Math. Comp., Quantum Inf. Comput., Quantum Inf. Proc., Des. Codes Cryptogr., etc.

Selected standardization-related activities: Swedish expert on cryptography in ISO, participation in various NIST processes and meetings (SHA-3, ECC, PQC), participation in various ETSI and IETF/CFRG meetings, etc.

Summarized conference/workshop/seminar participation:

FSE 2008 (Lausanne, Switzerland), ECC 2008 (Utrecht, The Netherlands), AsiaCrypt 2009 (Tokyo, Japan), CRYPTO 2010 (Santa Barbara, USA), CHES 2010 (Santa Barbara, USA), FDTC 2010 (Santa Barbara, USA), the 2nd NIST SHA-3 Candidate Conference 2010 (Santa Barbara, USA), AsiaCrypt 2011 (Seoul, South Korea), DIAC 2012 (Stockholm, Sweden), SHARCS 2012 (Washington DC, USA), FSE 2012 (Washington DC, USA), the 3rd NIST SHA-3 Candidate 2013 Conference (Washington DC, USA), Workshop on Lattice-Based Cryptography 2013 (Bangalore, India), AsiaCrypt 2013 (Bangalore, India), CRYPTO 2014 (Santa Barbara, USA), DIAC 2014 (Santa Barbara, USA), NIST Workshop on Elliptic Curve Cryptography Standards 2015 (Gaithersburg,

USA), AsiaCrypt 2015 (Auckland, New Zealand), Post-Quantum Cryptography Winter School 2016 (Fukuoka, Japan), PQCrypto 2016 (Fukuoka, Japan), the 4th ETSI/IQC Quantum-Safe Cryptography Workshop 2016 (Toronto, Canada), PQCrypto 2017 (Utrecht, the Netherlands), the 5th ETSI/IQC Quantum-Safe Cryptography Workshop 2017 (London, UK), CBC 2018 (Davie, USA), PQCrypto 2018 (Fort Lauderdale, USA), the 1st NIST PQC Standardization Conference 2018 (Fort Lauderdale, USA), KTH S^3CS Summer School 2018 on "Quantum Computing" and "Lattices and Cryptography" (Stockholm, Sweden), the 6th ETSI/IQC Quantum-safe Cryptography Workshop 2018 (Beijing, China), CRYPTO 2019 (Santa Barbara, USA), the 2nd NIST PQC Standardization Conference 2019 (Santa Barbara, USA), SEC-T 2019 (Stockholm, Sweden), Schloss Dagstuhl seminar 19421 on "Quantum Cryptanalysis" 2019 (Wadern, Germany), the "Quantum Cryptanalysis of Post-Quantum Cryptography" and "Quantum Algorithms" seminars at the Simons Institute 2020 (Berkeley, USA), the 3rd NIST PQC Standardization Conference 2021 (Virtual), Schloss Dagstuhl seminar 21421 on "Quantum Cryptanalysis" 2021 (Wadern, Germany), CRYPTO 2022 (Santa Barbara, USA), the 4th NIST PQC Standardization Conference 2022 (Virtual), PQCrypto 2023 (College Park, Maryland, USA), Crypto meets AI — GHTC, MathCrypt and CFAIL affiliated events to CRYPTO 2023 (Santa Barbara, USA), CRYPTO 2023 (Santa Barbara, USA), Schloss Dagstuhl seminar 23421 on "Quantum Cryptanalysis" 2023 (Wadern, Germany), PQCrypto 2024 (Oxford, UK), MathCrypt affiliated event to CRYPTO 2025 (Santa Barbara, USA), CRYPTO 2025 (Santa Barbara, USA).

3.5 Miscellaneous — in this section you could provide numbered lists of publications (if there are less than ten co-authors, state all named in the order published) if you wish to bring such to our attention.

Metrics: (public research, according to Google Scholar as of 2025-09-30)

- Citations: 1463 (1394 since 2020)
- h-index: 10 (9 since 2020)
- i-index: 10 (9 since 2020)

Erdős number: ≤ 3 (M. Ekerå $\rightarrow$ J. Håstad $\rightarrow$ N. Alon $\rightarrow$ P. Erdős)

Selected publications:

- M. Ekerå and J. Håstad. Quantum algorithms for computing short discrete logarithms and factoring RSA integers. In: PQCrypto 2017. Lecture Notes in Computer Science (LNCS) 10346, 347–363 (2017).
- M. Ekerå. On post-processing in the quantum algorithm for computing short discrete logarithms. Des. Codes Cryptogr. 88(11), 2313–2335 (2020).
- C. Gidney and M. Ekerå. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum 5, 433 (2021)..
- M. Ekerå. Quantum algorithms for computing general discrete logarithms and orders with tradeoffs. J. Math. Cryptol. 15(1), 359–407 (2021).
- M. Ekerå. On completely factoring any integer efficiently in a single run of an order-finding algorithm. Quantum Inf. Proc. 20(6):205 (2021).

- M. Ekerå. On the success probability of quantum order finding. ACM Trans. Quantum Comput. 5(2):11 (2024).
- M. Ekerå and J. Gärtner. Extending Regev's factoring algorithm to compute discrete logarithms. In: PQCrypto 2024. Lecture Notes in Computer Science (LNCS) 14772, 211–242 (2024).
- M. Ekerå. On factoring integers, and computing discrete logarithms and orders, quantumly. PhD thesis, KTH (2024).
- M. Ekerå. Revisiting Shor's quantum algorithm for computing general discrete logarithms. ArXiv pre-print 1905.09084v4 (2024).
- M. Ekerå and J. Gärtner. A high-level comparison of state-of-the-art quantum algorithms for breaking asymmetric cryptography. IACR Commun. Cryptol. 2(1):30 (2025).
- M. Ekerå. On the success probability of the quantum algorithm for the short DLP. ArXiv 2309.01754v2 (2025).

Selected software: (public research) I have developed an extensive framework of software to support my research. Most of it is available on my GitHub (ekera).

- The Quaspy library for Python (available via Pip3)
- The Qunundrum suite of MPI programs
- The Factoritall collection of Sage scripts
- Simulators for Regev's quantum factoring algorithm and Ekerå–Gärtner's extensions to discrete logarithm finding, order finding and factoring via order finding

Selected surveys: (public research) I am of 14 respondents in all incarnations of the Quantum Threat Timeline Report up to and including the year 2024:

- Quantum Threat Timeline Report 2019
- Quantum Threat Timeline Report 2020
- Quantum Threat Timeline Report 2021
- Quantum Threat Timeline Report 2022
- Quantum Threat Timeline Report 2023
- Quantum Threat Timeline Report 2024
- Quantum Threat Timeline Report 2025 (ongoing; not yet published)

The other 13 respondents are Dorit Aharonov (Hebrew University of Jerusalem), Alexandre Blais (Université de Sherbrooke), Ignacio Cirac (Max Planck Institute of Quantum Optics), Bill Coish (McGill University), David DiVincenzo (Jülich Research Center), Artur Ekert (University of Oxford), Daniel Gottesman (UMD), Andrea Morello (UNSW Sydney), Tracy Northup (University of Innsbruck), Stephanie Simmons (Simon Fraser University), Peter Shor (MIT), Frank Wilhelm-Mauch (Forschungszentrum Jülich) and Shengyu Zhang (Tencent Quantum Lab). The 2024 version of the survey had 32 respondents in total. Amongst the newer respondents are Sergio Boixo (Google), Andrew Childs (UMD), Jay

Gambetta (IBM), Aram Harrow (MIT), David J. Wineland (University of Oregon) and several other well-known scientists.

My work is also extensively referenced in the BSI survey "The status of quantum computer development" (*ger.* Entwicklungsstand Quantencomputer).

The 20 million qubits physical cost estimate of myself and Craig Gidney is referenced extensively, for instance in the report "Defense Primer: Quantum Technology" by the US Congressional Research Service.

4. Pedagogical skills

4.1. In this section you should focus on individual guidance, such as mentoring and supervising degree projects, licentiate or doctorate degrees.

I participated in the bi-weekly supervisory meetings for the PhD student Joel Gärtner (that the Swedish NCSA and the Swedish Armed Forces funded) to provide feedback, suggest topics, and keep up to date on the research progress.

I also took an active part in the recruitment of Joel, and I have recently been taking an active part in attempting to recruit a new PhD student.

I have some limited experience with providing help and individual guidance to BSc and MSc student projects. Typically because students reach out directly to me and ask for my help, or to interview me, or similar. On multiple occasions students have also contacted to me to ask for career advice.

4.2. Pedagogic merits/experience in the industry, within authorities or university environments, such as experience in developing and leading internal training programs at the company/organization, as well as publications in popular science.

Selected training programs: I have setup and run an introductory program for recently recruited cryptographers at the Swedish NCSA. (I have worked to build up the area of cryptography during my approximately 18 years at the NCSA. I recruited many of the people who are now seniors, and trained them so that they can in turn train newly recruited cryptographers, recursively.)

Within my role at the Swedish NCSA I have also created a technical document collection, called TDITS, that specifies the policy, standards and processes of the authority for the development of COMSEC systems. It is extensively used by our cryptographic industry, by FMV and by the staff at the Swedish NCSA. It serves not only as a technical reference but also as a training tool — not least for newly recruited employees, and for the industry.

Selected contributions to popular science: People have written about me and my (research) work in popular science, and I have been interviewed in popular-science contexts. Selected examples are given below:

- Interviewed for the article "Intervju med Martin som är kryptolog på Must" published by Kryptera.se, 2017-04-27. (I also provided textual material and photographs for this article.)
- Interviewed for the special episode "Specialavsnitt — Kvantdatorer och

kvantkrypto" of the podcast "Säkerhetssnack", 2019-05-21.

- My joint pre-print with Craig Gidney (ArXiv 1905.09749) is featured in the popular-science article "How a quantum computer could break 2048-bit RSA encryption in 8 hours" published by the MIT Technology Review, 2019-05-30. (Neither Craig nor I were interviewed for this article.)
- Interviewed for "Kvantdatorer väntas kunna avslöja hemligheter på nätet" published by SVT Vetenskap, 2022-12-07. Broadcast in the SVT evening news "Aktuellt". Unfortunately the video is no longer available.
- Interviewed for the article "Kvantdatorn kan bli ett hot" in the "Tema: Kvant" special issue of the magazine "Teknisk prognos" by FMV, no. 1, 2023. I also contributed by reviewing other articles and illustrations in this issue and providing critical feedback. Several of the figures in the issue are taken from my works (as stated in the footnotes).
- Interviewed for "Thirty Years Later, a Speed Boost for Quantum Factoring" by Ben Brubaker, published in Quanta Magazine, 2023-10-17.
- Interviewed for the story "'Surprising and super cool.' Quantum algorithm offers faster way to hack internet encryption" by Anna Kramer, published in Science 381(6664), p. 1270, 2023-11-22.
- Interviewed for the article "Forskar om att framtidssäkra Internet" that was published by KTH, 2024-10-30.

Selected invited lectures at courses: I have been an invited lecturer at a number of MSc and PhD courses. Selected examples are given below:

- "On Shor's algorithms, the various derivatives, their implementation and their applications", invited lecture at the course "Advanced quantum algorithms" at WACQT at Chalmers, Göteborg, Sweden, 2019-11-15.
  (I also provided proposed exercises for the following exercise session.)
- "An introduction to communications security in Sweden", invited lecture at the course "DD2520 Applied cryptography" (*swe.* "Tillämpad kryptografi") at KTH, Stockholm, Sweden, 2020-02-12.
- "Quantum computing and its impact on the field of cryptology", invited lecture at the course "DD2520 Applied cryptography" (*swe.* "Tillämpad kryptografi") at KTH, Stockholm, Sweden, 2020-02-12.
- "On Shor's algorithms, the various derivatives, their implementation and their applications", invited lecture at the course "Advanced quantum algorithms" at WACQT at Chalmers, Göteborg, Sweden, 2020-11-13.
  (I also provided proposed exercises for the following exercise session.)
- "An introduction to communications security in Sweden", invited lecture at the course "DD2520 Applied cryptography" (*swe.* "Tillämpad kryptografi") at KTH, Stockholm, Sweden, 2021-03-03.
- 'On Shor's algorithms, the various derivatives, their implementation and their applications", invited lecture at the course "Advanced quantum algorithms" at WACQT at Chalmers, Göteborg, Sweden, 2021-11-15.
  (I also provided proposed exercises for the following exercise session.)
- "An introduction to quantum computing and Shor's factoring algorithm",

invited lecture at the course DD2440 Advanced Algorithms (*swe.* "Avancerade Algoritmer"), at KTH, Stockholm, Sweden, 2021-12-08.
(I also provided proposed exercises for the following exercise session.)

- "An introduction to communications security in Sweden", invited lecture at the course "DD2520 Applied cryptography" (*swe.* "Tillämpad kryptografi") at KTH, Stockholm, Sweden, 2022-02-28.
- "On Shor's algorithms, the various derivatives, their implementation and their applications", invited lecture at the course "Advanced quantum algorithms" at WACQT at Chalmers, Göteborg, Sweden, 2022-11-17.
(I also provided proposed exercises for the following exercise session.)
- "An introduction to communications security in Sweden", invited lecture at the course "DD2520 Applied cryptography" (*swe.* "Tillämpad kryptografi") at KTH, Stockholm, Sweden, 2023-02-28.
- "An introduction to communications security in Sweden", invited lecture at the course "DD2520 Applied cryptography" (*swe.* "Tillämpad kryptografi") at KTH, Stockholm, Sweden, 2024-02-28.
- "An introduction to communications security (COMSEC) in Sweden", invited lecture at the course "DD2520 Applied cryptography" (*swe.* "Tillämpad kryptografi") at KTH, Stockholm, Sweden, 2025-02-26.

5. Leadership skills

5.1. Leadership within your organization As the chief cryptographer of the Swedish NCSA, I oversee the area of cryptography as a whole.

The duty falls on me to shape the policy, standards and processes for the area. As previously mentioned, I have for example created a technical document collection, called TDITS, that specifies the policy, standards and processes of the authority for the development of COMSEC systems. It is extensively used by our cryptographic industry, by FMV and by the staff at the Swedish NCSA.

If issues arise within the area of cryptography that are not addressed by our existing policy in TDITS then these are usually escalated to my level for a decision. I then work to ensure that the outcome is reflected in TDITS.

When new COMSEC systems are to be developed I am involved in defining the cryptographic requirements for the systems. The same holds true for components of such systems, such as cryptographic protocols and algorithms. I have also recently done extensive work on defining and leading the development of our new national cryptographic key management.

I work together with Pia Gruvö to define our cryptographic strategy.

I work to shape the policy, standards and processes for cryptography as far as COMSEC is concerned not only nationally within Sweden but also in a broader international context. I have several international roles. For example, I am the Swedish national delegate to the NATO Crypto CaT that handles issues pertaining to cryptography in COMSEC within NATO.

Formally, I am a member of the management group (*swe.* ledningsgrupp) and the strategy group (*swe.* strategigrupp) of the Swedish NCSA. I chair the bi-weekly

meetings of all cryptographers (*swe.* kryptomöten) and I chair the management group for cryptography (*swe.* ledningsgrupp krypto) on which the managers of our groups of cryptographers sit. I furthermore attend all technical council meetings (*swe.* tekniska råd) where technical issue are discussed and technical decisions taken and I attend a variety of other management meetings.

Previously, I used to directly manage cryptographers but this is no longer the case. Instead, I interface with the managers of our groups of cryptographers.

5.2. Leadership in external collaboration projects, for example, with higher education institutions

I am unsure what details, if any, to include here. I am not able to go into much details regarding the external collaboration projects of the Swedish NCSA but I have lead or played instrumental parts in a number of such projects.

I presume that I can mention that I lead the cryptographic research in "Forskning och Teknikuteckling (FoT) Krypto", which is a classified research program funded by the Swedish Armed Forces with participation from FMV, the cryptographic industry in Sweden, and sometimes FOI, universities/institutes, etc.

I interface with the Chief of research (*swe.* forskningschef) of the Swedish Armed Forces on issues related to cryptography (including quantum aspects).

I took part in arranging for the Swedish NCSA and the Swedish Armed Forces to fund a PhD student (Joel Gärtner) in cryptography via CDIS at KTH, and in securing funding for one additional PhD student (who is yet to be recruited).

(More specifically, the PhD student is employed by KTH with funding from the Swedish Armed Forces. The student spends 20% of the time at the Swedish NCSA to interface with the cryptographers and to develop an understanding of the subject area as a whole that would otherwise be unavailable to the student. This approach yielded excellent results in Joel's case. I hope to be able to continue along the same lines in the future with additional students.)

5.3. Leadership experience that you would like to bring to our attention, from both strategic and operative reorganization, as well as experience/knowledge of equal treatment aspects of leadership

I have taken a very active role in reorganizing the technical work within the Swedish NCSA in general, and in growing and reorganizing the subject area of cryptography in particular, during my approximately 18 years at the NCSA.

The Swedish Armed Forces requires all employees to take courses on the topic of equal treatment so I would say that I have a good understanding of the topic.

I have furthermore been engaged in RFSL and other associations that promote LGBT equality since my early teens because I think these issues are important. For instance, I was instrumental in reviving Gaytek at THS at KTH back in 2003, and I served as the vice president of Gaytek for a few years until the association stabilized. Gaytek has since been transformed into Speqtrum.

5.4. Leadership within innovation, entrepreneurship and/or your own company

I consider myself to be quite entrepreneurial. As a pre-high-school teenager, I developed shareware programs that were internationally distributed. This led me to be approached by IT companies, and in turn this led me to start my own company at a very early age to do consultancy work for them.

I have other experiences of doing consultancy work, but for at least the last decade I have focused primarily on my research work and on my principal occupation as a cryptographer at the Swedish NCSA.

6. Collaboration with universities

It should be clear from the above that I have been extensively engaged with universities. I am not quite sure what additional details, if any, that you wish for me to provide under this subject heading.

Publications The below is a complete list of unclassified publications (papers (including pre-prints) and theses; software, interviews, blog posts, etc., are excluded). See also my Google Scholar profile.

- M. Ekerå, Differential cryptanalysis of MD5. MSc thesis, KTH (2008).
- J.-P. Flori, J. Plût, J.-R. Reinhard and M. Ekerå, Diversity and Transparency for ECC. IACR Cryptology ePrint Archive 2015/659 (2015).
- M. Ekerå, Computing information on domain parameters from public keys selected uniformly at random. IACR Cryptology ePrint Archive 2015/879 (2015).
- M. Ekerå. Modifying Shor's algorithm to compute short discrete logarithms. IACR Cryptology ePrint Archive 2016/1128 (2016).
- M. Ekerå and J. Håstad. Quantum algorithms for computing short discrete logarithms and factoring RSA integers. In: PQCrypto 2017. Lecture Notes in Computer Science (LNCS) 10346, 347–363 (2017).
- M. Ekerå. On post-processing in the quantum algorithm for computing short discrete logarithms. Des. Codes Cryptogr. 88(11), 2313–2335 (2020).
- C. Gidney and M. Ekerå. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum 5, 433 (2021)..
- M. Ekerå. Quantum algorithms for computing general discrete logarithms and orders with tradeoffs. J. Math. Cryptol. 15(1), 359–407 (2021).
- M. Ekerå. On completely factoring any integer efficiently in a single run of an order-finding algorithm. Quantum Inf. Proc. 20(6):205 (2021).
- M. Ekerå. On the success probability of quantum order finding. ACM Trans. Quantum Comput. 5(2):11 (2024).
- M. Ekerå and J. Gärtner. Extending Regev's factoring algorithm to compute discrete logarithms. In: PQCrypto 2024. Lecture Notes in Computer Science (LNCS) 14772, 211–242 (2024).
- M. Ekerå. On factoring integers, and computing discrete logarithms and orders, quantumly. PhD thesis, KTH (2024).
- M. Ekerå. Revisiting Shor's quantum algorithm for computing general discrete logarithms. ArXiv pre-print 1905.09084v4 (2024).
- M. Ekerå and J. Gärtner. A high-level comparison of state-of-the-art quantum algorithms for breaking asymmetric cryptography. IACR Commun. Cryptol. 2(1):30 (2025).
- M. Ekerå. On the success probability of the quantum algorithm for the short DLP. ArXiv 2309.01754v2 (2025).

Avtal rörande anknytning som affilierad fakultet

Mellan Kungliga Tekniska Högskolan (KTH) och den Militära underrättelse- och säkerhetstjänsten (Must) som är en del av Försvarsmakten (Myndigheten) (nedan enskilt benämnda ”Part” och gemensamt ”Parterna”) har denna dag träffats följande avtal angående samverkan inom området kryptologi.

1 AFFILIERING

1.1 KTH avser att för tiden **2026-01-01 och längst till och med 2028-12-31** (3 år) anknyta Martin Ekerå (den affilierade), som affilierad fakultet i ämnet kryptologi, under förutsättning att gällande behörighetskrav anses uppfyllda efter sedvanlig behörighetsprövning. Detta avtal avser att bland annat reglera ersättnings- och arbetstidsfrågor samt rätten till de resultat som kan komma att genereras av den affilierade.

2 LÖN OCH ANDRA KOSTNADER

2.1 Den affilierade ska ha rätt att i medeltal avsätta 30% av sin anställning vid Myndigheten för verksamheten som affilierad fakultet vid KTH. Inget avdrag från den affilierades ordinarie lön vid Myndigheten ska göras.

2.2 Beträffande andra kostnader förenade med anknytningen som affilierad fakultet skall detta överenskommas mellan partnerna i förhållande till olika projekt.

3 KTH:S ÅTAGANDE

3.1 För den affilierades verksamhet vid KTH åtar sig KTH att tillhandahålla nödvändiga resurser inklusive lokaler och teknisk utrustning samt se till att verksamhetsförhållandena är i enlighet med gällande lagar, bestämmelser och avtal inom utbildningssektorn och att tillhandahålla tillämpliga säkerhetsföreskrifter som den affilierade ska följa.

4 DEN AFFILIERADES VERKSAMHET

4.1 Den afflierades verksamhet vid KTH ska bedrivas inom området kryptologi och omfatta arbetsuppgifter enligt överenskommelse mellan parterna (bilaga).

4.2 Den affilierade är införstådd med att gränsdragningsproblem kan uppstå i verksamheten och förbinder sig att i sådana fall samråda med ansvarig på berörd institution samt ansvarig chef på Myndigheten. För det fall den affilierades verksamhet kommer att inbegripa

medverkan i samverkansprojekt med annan industri- eller myndighetspart ska ett samverkansavtal tecknas mellan alla i projektet ingående parter.

5 PUBLICERING

5.1 Forskningsresultat som uppkommer i samband med den affilierades verksamhet vid KTH får publiceras fritt i enlighet med gällande vetenskaplig praxis och i övrigt nyttjas i Parternas utvecklings- och forskningsarbete. Inför publicering av forskningsresultat som den affilierade kan ha varit med och genererat ska Myndigheten få ett utkast av publikationen för granskning. Myndigheten äger att inom en månad från mottagandet av utkastet begära att publiceringen fördröjs i syfte att Parterna ska komma överens om att undanta sekretessbelagda uppgifter som Myndigheten identifierar. Har Myndigheten inte gjort någon invändning mot publiceringen inom en månad är publiceringen tillåten. En publicering kan som längst fördröjas med tre (3) månader från det att Myndigheten lämnat invändning mot publiceringen.

6 ÄGANDERÄTT

6.1 Äganderätt till resultat som den affilierade ensam generar med stöd av finansiering enligt detta avtal tillkommer den affilierade. Rättigheter som den affilierade genererar tillsammans med anställd eller student vid KTH tillfaller respektive rättighetshavare enligt lag. Gemensamt genererat resultat kan således bli gemensamt ägt.

6.2 KTH har rätt att fritt och utan att utge ersättning nyttja samtliga resultat för forskning, utveckling och undervisning.

7 ANSVAR

7.1 Part ansvarar för skada eller förlust som denne uppsåtligen eller av vårdslöshet vållat den andre Parten under utförandet av detta avtal eller genom att bryta mot detta avtal. Ansvaret omfattar inte ersättning för indirekt skada eller förlust, förlust till följd av att resultatet inte kan nyttjas på avsett sätt eller följdskador såsom inkomstbortfall, utebliven vinst och kapitalkostnader. Part ansvarar endast för skada som har upptäckts inom ett (1) år efter avtalets upphörande.

8 SEKRETESS

8.1 Parterna är införstådda med att offentlighetsprincipen gäller vid KTH. Undantag härifrån kan endast ske i den utsträckning offentlighets- och sekretesslagen så medger.

9 AVTALSTID

9.1 Avtalet gäller från och med den dag då utnämning som affilierad fakultet sker till och med den tidpunkt som beslutet om utnämning anger. En förutsättning är också att den affilierade samtidigt är anställd vid Myndigheten. För det fall den affilierades anställning vid Myndigheten upphör, upphör detta avtal automatiskt att gälla samma datum som anställningen upphör. Myndigheten äger skyldighet att informera KTH för det fall den affilierades anställning är på väg att upphöra.

9.2 I samband med en eventuell prövning av frågan om förlängd affiliering ska även frågan om förlängning av villkoren i detta avtal prövas.

10 TVIST

10.1 Tvist angående detta avtal ska lösas mellan Parterna.

11 GODKÄNNANDE

11.1 Parterna godkänner avtalet genom sina underskrifter.

_____	_____
2025-	**2025-**
Myndigheten	**Skolchef , Kungliga Tekniska Högskolan**

Jag har tagit del av detta avtal och förbinder mig att med avseende på allt som berör mina rättigheter och skyldigheter enligt detta avtal följa vad som avtalats mellan Parterna.

_____

2025-
Den affilierade

Enclosure to the affiliation agreement for Martin Ekerå

This enclosure provides relevant background and states the intent behind and expected outcome of the affiliation of Martin Ekerå to KTH.

Mailing address	Visiting address	Telephone	Fax	E-mail, Internet
Försvarsmakten	Lidingövägen 24	+46-(0)8-788 75 00	+46-(0)8-788 77 78	exp-hkv@mil.se
SE-107 85 STOCKHOLM				www.mil.se
SWEDEN				

Background for context

The Swedish National Communications Security Authority (NCSA) is a function within Must, which is in turn a part of Swedish Armed Forces ("Myndigheten"). The Swedish NCSA directs and coordinates government activities related to communications security (COMSEC).

This includes activities related to so-called "secure cryptographic functions" (*swe.* "säkra kryptografiska funktioner") — ranging from cryptographic algorithm and protocol development to the development, evaluation and approval of complete COMSEC systems (*swe.* signalskyddssystem).

By Swedish law, if classified information (*swe.* säkerhetsskyddsklassificerade uppgifter) is to be communicated to an information system that is beyond the operator's control, the information must be encrypted with a COMSEC system approved by the Swedish NCSA.

The Swedish NCSA advises the government offices (*swe.* Regeringskansliet) on cryptography, and acts as a CCA/NCSA and NDA in the EU/NATO.

For example, the Swedish NCSA evaluates and approves COMSEC system for EU classified information up to C-UE/EU-C, and is one of five appropriate qualified authorities (AQUAs) within the EU that provide policy guidance on cryptography and are responsible for carrying out second-party evaluations for EU approvals of COMSEC systems us to TS-UE/EU-TS.

The Swedish NCSA furthermore approves COMSEC systems for NATO classified information up to NC, and interfaces with SECAN for obtaining approvals up to CTS within NATO.

As NDA, the Swedish NCSA produces and distributes cryptographic keys.

—

Martin Ekerå is currently serving as the chief cryptographer of the Swedish NCSA, overseeing the area of cryptography as a whole.

Since his employment in 2007 he has served in various roles as a cryptographer within the Swedish NCSA, and has thus accumulated approximately 18 years of experience. During this time, he has been extensively involved in classified research and development work. Unfortunately, it is not possible to provide further details on this work.

Martin Ekerå did an MSc in engineering physics at KTH 2003–2008, with exchange studies at the EPFL. He did a PhD in computer science at KTH 2016–2025 (at half pace) with a specialization in quantum cryptanalysis and post-quantum cryptography. During this time, Martin Ekerå established himself as a leading international figure within the field of quantum cryptanalysis. He had amassed over 1000 citations at the time of defending his thesis in late October 2024.

Intent and primary topics

The intent of creating this affiliation is to allow Martin Ekerå to:

- Continue researching quantum cryptanalysis, and post-quantum secure cryptography and cryptography more broadly when relevant in the context of his role at the Swedish NCSA, whilst keeping track of the evolution of cryptographically relevant large-scale fault-tolerant quantum computers.

  (This will serve to strengthen the posture of KTH within quantum computing, whilst at the same time respecting the restriction that the Swedish NCSA is primarily interested in cryptography.)

- Maintain a link between the Swedish NCSA and the "cryptography group" at KTH,[1] with the aim of maintaining a viable group at KTH.

  As a first step, we are now looking to employ one PhD student (provided we get a good applicant), financed by the Swedish NCSA and the Swedish Armed Forces via CDIS, and advised by Johan Håstad with Martin Ekerå as "co-advisor" or similar.

  This includes participating in regular meetings (approximately 1h every two weeks) of the cryptography group, primarily to support the new PhD student and to discuss research.

- Occasionally give talks/lectures/interviews related to his research, and to cryptography and COMSEC more broadly when relevant in the context of his role at the Swedish NCSA.

  For instance, Martin Ekerå usually gives an invited lecture at the "DD2520 Applied cryptography" course every year about COMSEC in Sweden, and he has previously also been a guest lecturer at "DD2440 Avancerade algoritmer", and at MSc and PhD courses in quantum computing given by WACQT at Chalmers with virtual participation from other European universities.

Time allocation: On average 30% of the work time should be devoted to the affiliation (whilst allowing for a considerable variation between weeks).

Duration of the arrangement: At most 3 years (for exact dates, see the agreement), after which a new arrangement can hopefully be made. The aim to is for Martin Ekerå to be able to proceed to a role as "adjungerad professor" or "docent", or similar, fairly quickly. Although Martin Ekerå recently took out a PhD, he has considerable merits and past experience as indicated in the background section, and somehow it must be possible to take this into account. (In order to maintain a group, fairly rapid advancement appears necessary, especially in light of Johan Håstad's planned retirement.)

[1] It is doubtful whether a group can be said to currently exist at KTH.

§ X Beslut om fastställande av utbildningsplaner HT26, tilläggsbeslut för CDATE, CMETE, TIVNM

(HS-2025-2537)

Fakultetsnämnden beslutar om tillägg till beslutet HS-2025-1370 att fastställa kurslistor och text för studenter som antas höstterminen 2026 enligt bilagor för följande program inom grundutbildningen:

1. **Civilingenjörsutbildning i datateknik (CDATE)**
   Endast nya kurskoder för några mattekurser är ändrade.

2. **Civilingenjörsutbildning i medieteknik (CMETE)**
   Tillägg av en punkt med en förklarande text för åk 3 om förkunskaper till de nyinförda mastermappningarna, samt ändring av kurskod för obligatorisk kurs; SK1140 ersätts av SK1141 Teknisk Fotografi 4,0 hp, dvs nytt kursnamn och kurskod men kursinnehållet är detsamma.

3. **Masterprogram, ICT Innovation (TIVNM)**
   EIT Digital har skickat ut en ny läroplan till spåransvarig Jan Gulliksen, avseende studenter som börjar på Människa dator interaktion (HCI) från september 2026. Informationen behöver därför uppdateras så att KTH:s kurslista överensstämmer med EIT Digitals kurslista.

Bilaga 1: Kurslista

Civilingenjörsutbildning i datateknik (CDATE)

Årskurs 1

Kommentar till kurslistan
I årskurs 1 läses 60 hp obligatoriska kurser.
DD1390 läses under tre år, varav 2 hp läses i årskurs 1.

Obligatoriska kurser

DD1390 Programsammanhållande kurs i datateknik 6 hp
DA1600 Ingenjörsmässigt skrivande 4,5 hp
DD1337 Programmering 7 hp
DD1338 Algoritmer och datastrukturer 6 hp
DD1349 Projektuppgift i introduktion till datalogi 3 hp
DD1396 Parallellprogrammering i introduktion till datalogi 3 hp
DH1623 Människa-datorinteraktion, grundläggande teori 4,5 hp
SF1624 Algebra och geometri 7,5 hp
SF1625 Envariabelanalys 7,5 hp
SF1626 Flervariabelanalys 7,5 hp
Ny kurskod Matematik, baskurs, med diskret matematik 7,5 hp

Årskurs 2

Kommentar till kurslistan
I årskurs 2 läses 60 hp obligatoriska kurser.

Obligatoriska kurser
DD1390 Programsammanhållande kurs i datateknik 6 hp
DD1366 Programmeringsparadigm 6 hp
DD1367 Programvarukonstruktion i projektform 9 hp
DD1368 Databasteknik för D 6 hp
IS1500 Datorteknik och komponenter 9 hp
ME1010 Organisation och kunskapsintensivt arbete 6 hp
SF1547 Numeriska metoder, grundkurs 6 hp
SF1935 Sannolikhetsteori och statistik med tillämpning inom maskininlärning 7,5 hp
DD1351 Logik för dataloger 7,5 hp

Årskurs 3

Kommentar till kurslistan
I årskurs 3 läses 45 hp obligatoriska kurser och 15 hp valfria kurser.

Obligatoriska kurser
DD1390 Programsammanhållande kurs i datateknik 6 hp
AL1504 Hållbar utveckling för datateknik 7,5 hp
DA150X Examensarbete inom datateknik, grundnivå 15 hp
DD2350 Algoritmer, datastrukturer och komplexitet 9,5 hp
ID1200 Operativsystem 6 hp
Ny kurskod Diskret matematik 6 hp

Årskurs 4

Kompletterande information
Under årskurs 4-5 läses ett masterprogram och då följs det programmets utbildningsplan.

Årskurs 5

Kompletterande information
Under årskurs 4-5 läses ett masterprogram och då följs det programmets utbildningsplan.

Bilaga 1: Kurslista

Civilingenjörsutbildning i medieteknik (CMETE)

Årskurs 1

Kommentar till kurslistan
DM1578 läses över tre år varav 3 hp läses i åk 1.

Obligatoriska kurser

DM1578 Programintegrerande kurs i medieteknik 7 hp
DH1609 Kommunikation och information 7,5 hp
DM1579 Medieproduktion 6 hp
DM1581 Introduktion till medieteknik 6 hp
SF1624 Algebra och geometri 7,5 hp
SF1625 Envariabelanalys 7,5 hp
DD1318 Programmeringsteknik och tekniska beräkningar 9 hp
SF1626 Flervariabelanalys 7,5 hp
SK1120 Vågrörelselära 6 hp

Årskurs 2

Obligatoriska kurser

DM1578 Programintegrerande kurs i medieteknik 7 hp
DD1320 Tillämpad datalogi 6 hp
DH1622 Människa-datorinteraktion, inledande kurs 7,5 hp
DM1135 Multimediasystem och signaler 7,5 hp
DM1580 Videoteknik 6 hp
DM1588 Sensorprogrammering för medieteknik 6 hp
DM1590 Maskininlärning för medieteknik 7,5 hp
DT1175 Ljud 7,5 hp
SF1919 Sannolikhetsteori och statistik 6 hp
SK1141 Teknisk fotografi 4 hp

Årskurs 3

Kommentar till kurslistan:
ME2016 och ME2163 är obligatoriska för behörighet till master i industriell ekonomi (TINEM).

Obligatoriska kurser

DM1578 Programintegrerande kurs i medieteknik 7 hp
DH2642 Interaktionsprogrammering och dynamiska webben 7,5 hp
DM128X Examensarbete inom medieteknik, grundnivå 15 hp
DM1595 Programutveckling för interaktiva medier 7,5 hp
DM2573 Hållbarhet och medieteknik 7,5 hp
ME1003 Industriell ekonomi, grundkurs 6 hp
ME1042 Entreprenörskap inom Media och IKT 1,5 hp

Villkorligt valfria kurser

AK2203 Media mellan teknik och kultur 7,5 hp
DD1354 Modeller och simulering 6 hp
DD1380 Javaprogrammering för Pythonprogrammerare 1,5 hp
DD2352 Algoritmer och komplexitet 7,5 hp
DH2323 Datorgrafik med interaktion 6 hp
DM1998 Ingenjörsinriktad yrkesträning 13 hp
DM2556 Interkulturell kommunikation 7,5 hp
DM2624 Människocentrerad teknik för funktionshinder 7,5 hp
DM2720 Hållbar Informations- och kommunikationsteknik (IKT) i praktiken 7,5 hp
DT2112 Talteknologi 7,5 hp
DT2212 Musikakustik 7,5 hp
LS1464 Retorik - konsten att övertyga 7,5 hp
ME2016 Project Management: Leadership and Control 6 hp
ME2163 Ledarskap och organisering i olika miljöer 6 hp
SF1662 Diskret matematik 7,5 hp

Information om villkorligt valfria kurser
Minst 13 hp av de villkorligt valfria kurserna ska läsas, bland dessa kan även kurser i språk eller interkulturell kompetens väljas vid KTH Språk och kommunikation

Årskurs 4

Kompletterande information
Under årskurs 4-5 läses ett masterprogram och då följs det programmets utbildningsplan.

Årskurs 5

Kompletterande information
Under årskurs 4-5 läses ett masterprogram och då följs det programmets utbildningsplan.

Please use the table below to update your programme structure. You can skip course codes for now if they haven't been assigned yet, and feel free to insert extra rows where necessary.

Existing data: https://masterschool.eitdigital.eu/human-computer-interaction-and-design/entry-exit
We are updating this page centrally, using the same format.

Structure:
Entry: 36ects Technical Major (incl. 3-6ects Intro to XR), 24ects I&E Minor
Exit: 1. Semester 24ects Technical Major (specialization), 6ects I&E Minor (I&E Study)
2. semester 30ects Master's Thesis

Academic coordinator name and bio (update existing one if need be)

Name: Jan Gulliksen
Bio: Jan Gulliksen is a professor in Human Computer Interaction and a Vice President for Digitalization at KTH Royal Institute of Technology, Stockholm, Sweden. He is conducting research in usability, accessibility, user-centered systems design, digitalization and digital work environment problems. He has been serving as the chairman of the digital commission of Sweden between 2012-2016 for the minister of Digitalization at the Ministry of the Enterprise and is now a member of the Digitalization Council for the Ministry of Infrastructure. He has also been working as a Digital Champion of Sweden for the European Commission since 2012. He was also a member of the EU High Level Group on the impact of Horizon 2020 and preparing for Horizon Europe, the so called "Lamy group" and as such contributed to the report Fab-Lab-App.

Link to local programme website (update existing one if need be)

Url:

ENTRY YEAR

First semester

Compulsory major courses

Course code, Course name	ECTS
Human-Computer Interaction, Introductory Course	7,5
Introduction to XR	3
Research Methodology and Scientific Writing (Can be taken in year 1 or in year 2)	7.5
Multimodal Interaction and Interfaces	7.5

Optional major courses

Course code, Course name	ECTS
Cooperative IT-design	9
Human Perception for Information Technology	7.5
Evaluation Methods in Human-Computer Interaction	6

I&E minor courses

Course code, Course name	ECTS
Internet Marketing	7.5
Entrepreneurship for Engineers	6

Second semester

Compulsory major courses

Course code, Course name	ECTS
Extended Reality in Theory and Practice	7.5
Computer Game Design	6
Computer Graphics and Interaction	6

Optional major courses

Course code, Course name	ECTS
Human-Computer Interaction, Research Seminars	3
Interaction Design Methods	7.5
Human-centered technologies for disabilities	7.5

I&E minor courses

Course code, Course name	ECTS
Business Development Lab of Entrepreneurship Engineers	9
Summer course Entrepreneurship for Engineers	4

EXIT YEAR

Specialization name and description:

Name: XR and applied business-oriented HCI
Description: Extended Reality (XR)—encompassing Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR)—is reshaping how we interact with digital content across education, entertainment, training, and simulation. This program introduces students to the foundational principles and cutting-edge practices in XR, with a focus on interaction, collaborative design processes, and user-centered development. Students will explore the design and implementation of immersive experiences through hands-on projects that emphasize gaming mechanics, training in simulated environments, and real-time user testing. A central component of the curriculum is understanding and applying interaction paradigms unique to XR, such as controller-free input, locomotion techniques, and redirection strategies, which are essential for creating intuitive and accessible virtual experiences. Through collaborative workshops, learners will engage in multidisciplinary teams to conceptualize, prototype, and iterate XR applications. The program emphasizes design thinking and agile development methodologies to prepare students for real-world challenges in XR development. Special attention is given to evaluating usability, performance, and human factors, ensuring that the solutions developed are both functional and user-oriented.

Compulsory courses

Course code, Course name	ECTS
Advanced Graphics and Interaction	9
Research Methodology and Scientific Writing (Can be taken in year 1 or in year 2)	7.5
Degree Project in Computer Science and Engineering, specialising in ICT Innovation, Second Cycle	30

Optional courses

Course code, Course name	ECTS
Physical Interaction Design and Realisation	7.5
Multimodal Interaction and Interfaces	7.5
Advanced Topics in Visualization and Computer Graphics	6

I&E study

Course code, Course name	ECTS (6)
ICT Innovation Study Project	6

§ X Beslut om ändring av CMETEs utbildningsplaner kull HT23, HT24, HT25

(HS-2025-2538)

I utbildningsplanen för civilingenjörsutbildningen i medieteknik (CMETE) kull HT26 beslutades om fyra nya mappningar av masterprogram. Programansvarig Roberto Bresin önskar att dessa mappningar även ska gälla för kullarna HT23, HT24 och HT25. Motiveringen till att erbjuda de nya mastermappningarna till tre tidigare kullar är för att bredda området för medieteknikstudenterna och att påvisa att medieteknik behövs i bredare kontexter. De fyra programansvariga för de nya mappade programmen önskar ta emot CMETE-studenter redan från hösten 2026, och ser fram mot att få medietekniska kompetenser och kunskaper till sitt område.

Fakultetsnämnden beslutar om tillägg av mappningarna för civilingenjörsutbildningen i medieteknik (CMETE) retroaktivt för kullarna HT23, HT24 och HT25, enligt följande:

Utbildningens omfattning och innehåll

”De avslutande två åren läses inom ett masterprogram. Utbudet av valbara masterprogram kan komma att förändras. Studenter på programmet har platsgaranti på nedanstående sju kopplade masterprogram.

På följande tre kopplade masterprogram leder de obligatoriska och villkorligt valfria kurserna till uppfyllande av examenskraven för civilingenjörsexamen i medieteknik:

- *Interaktiv Medieteknik (TIMTM)*
- *Maskininlärning (TMAIM)*
- *Hållbar digitalisering (TDIGM)*

På de fyra kopplade masterprogrammen nedan ges mycket goda förutsättningar att välja kurser i syfte att uppfylla examenskraven för civilingenjörsexamen i medieteknik. Beroende på studentens kursval inom programmet kan det bli nödvändigt att utnyttja delar av eller hela det valfria utrymmet till att läsa kurser i ämnen centrala för teknikområdet medieteknik i syfte att uppfylla examenskraven.

Valet av kurser inom teknikområdet ska godkännas av programansvarig för civilingenjörsprogrammet i en sa˚kallad individuell studieplanering. Därtill ska specifikationen av examensarbetet godkännas av programansvarig, innan påbörjande av arbetet, i syfte att säkerställa att det behandlar en forskningsfråga som är central för teknikområdet medieteknik. Detta gäller för följande kopplade masterprogram:

- *lndustriell ekonomi (TINEM).*
- *Teknikbaserad entreprenörskap (TTBEM).*
- *Teknik, arbete och hälsa (TTAHM), spår: Human Factors Ergonomics Track (HFE).*
- *Idrottsteknologi (TIDTM).”*

§ X Beslut om ändring av utbildningsplan för TIELA

(HS-2025-2628)

Fakultetsnämnden beslutar att revidera utbildningsplan gällande kurslistor för studenter som antas höstterminen 2024, 2025 och 2026 för följande program inom grundutbildningen:

- **Högskoleingenjörsutbildning i elektroteknik, Flemingsberg (TIELA)**
  Borttag av den villkorligt valfria kursen ME2083 Vattenkraft- teknik, ekonomi, hållbarhet 7,5 hp i kurslista för åk 3 för TIELA i utbildningsplanen för HT24, HT25 och HT26 då kursen är vilande.