Security & Privacy in Voice Biometrics and Beyond

da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP

TECHNISCHE
UNIVERSITÄT
DARMSTADT

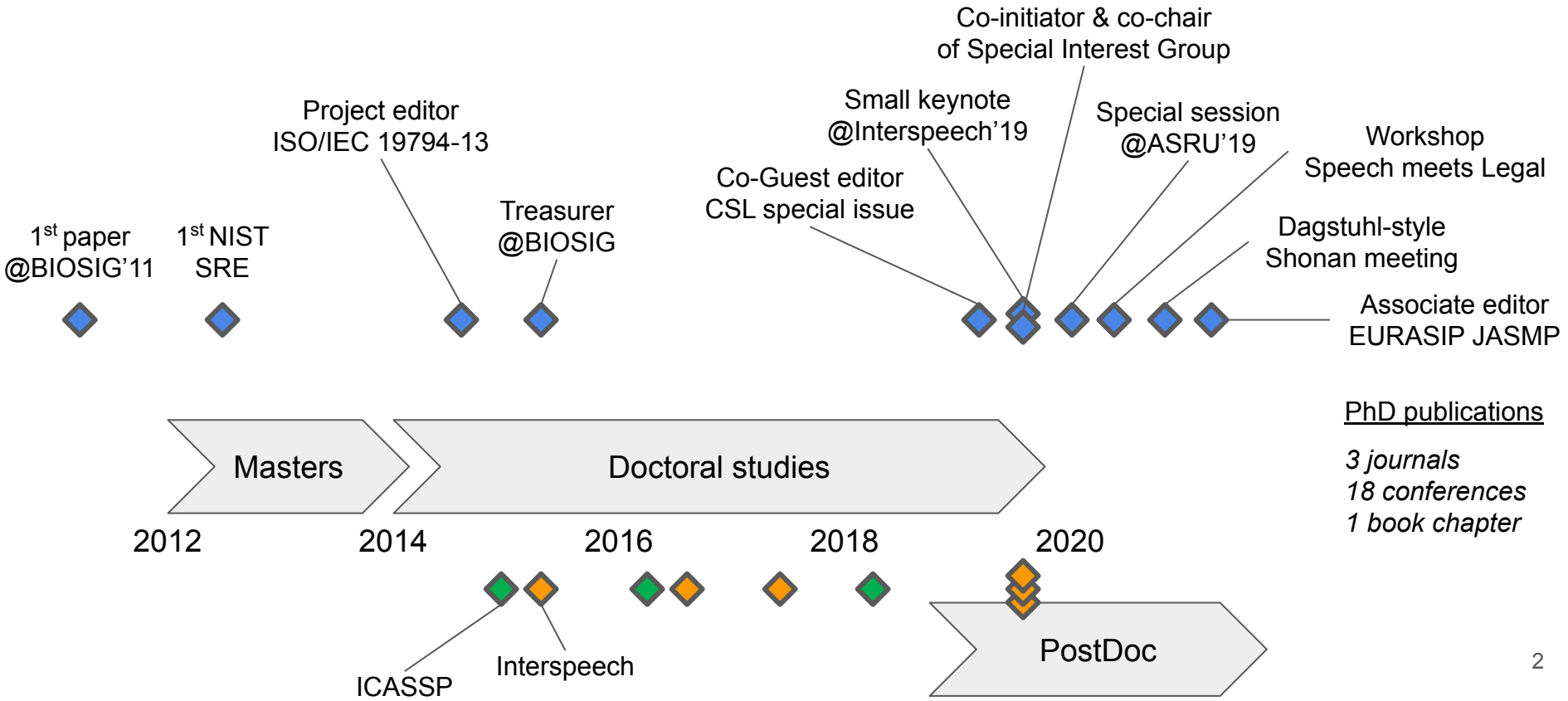
EURECOM
Sophia Antipolis

Andreas Nautsch

Research: Hochschule Darmstadt
Doctorate: TU Darmstadt
PostDoc: EURECOM

European Biometrics Max Snijder, Research, and Industry Awards 2020
2020-09-16 — Virtual Conference

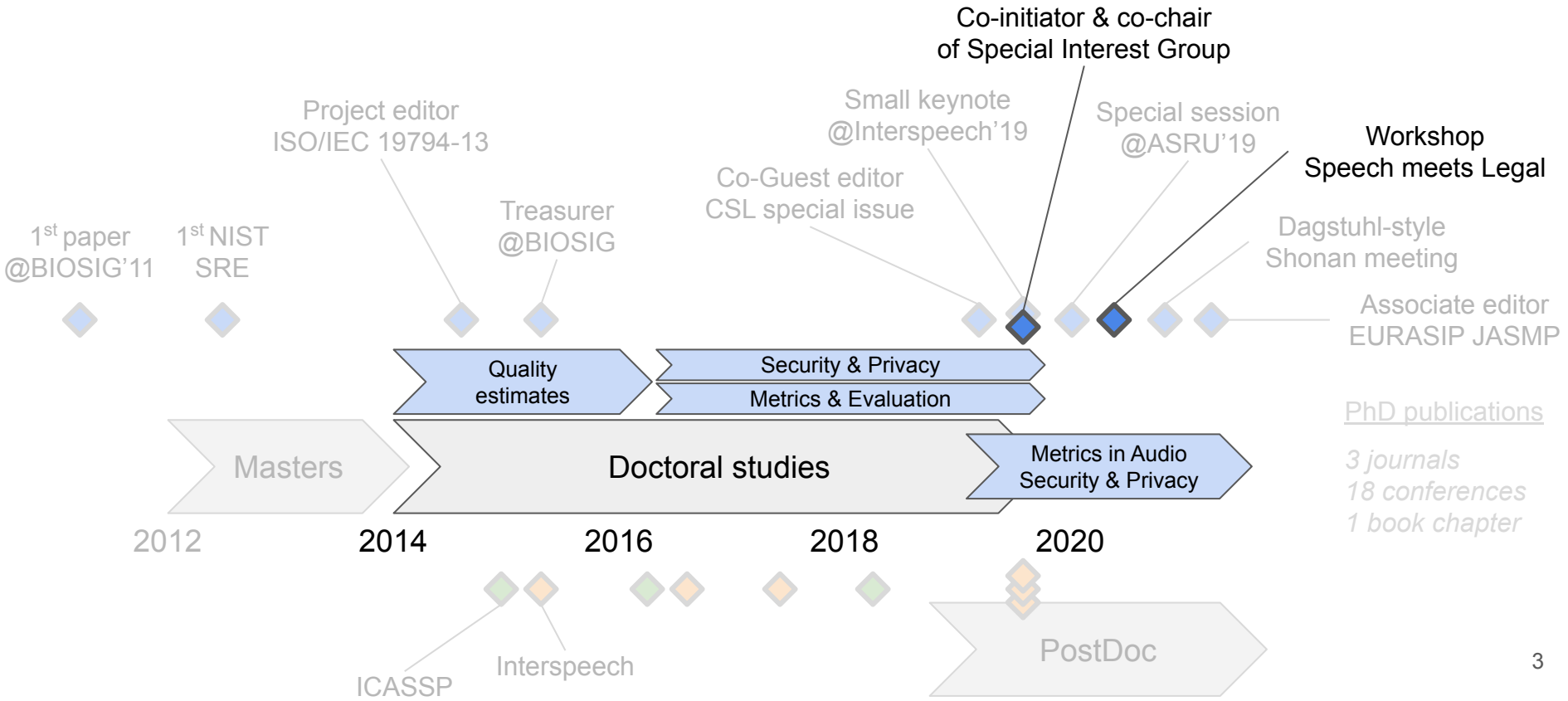
My CV & research leadership



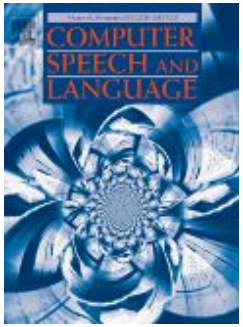
PhD publications

3 journals
18 conferences
1 book chapter

Outline of my research achievements



Doctoral studies



IEEE

SIGNAL PROCESSING LETTERS

Best paper award

Computer Speech and Language

An official publication of the International Speech Communication Association (ISCA)

Most Downloaded Computer Speech and Language Articles

The most downloaded articles from Computer Speech and Language in the last 90 days.

August - December 2019

Preserving privacy in speaker and speech characterisation - Open access

November 2019

Andreas Nautsch | Abelino Jiménez | Amos Treiber | Jascha Kolberg | Catherine Jasserand | Els Kindt | Héctor Delgado | Massimiliano Todisco | Mohamed Amine Hmani | Aymen Mtibaa | Mohammed Ahmed Abdelraheem | Alberto Abad | Francisco Teixeira | Driss Matrouf | Marta Gomez-Barrero | Dijana Petrovska-Delacrétaz | Gérard Chollet | Nicholas Evans | Thomas Schneider | Jean-François Bonastre | Bhiksha Raj | Isabel Trancoso | Christoph Busch

GRAZ – AUSTRIA
SEPTEMBER 15th – 19th 2019
INTERSPEECH
2019

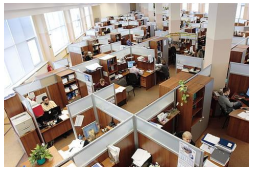
PRIVACY PRESERVING MACHINE LEARNING

CCS 2019 Workshop
London, November 15

Interspeech 2019 — "Survey talk" — small keynote
https://www.youtube.com/watch?v=mywNMwZfbDo

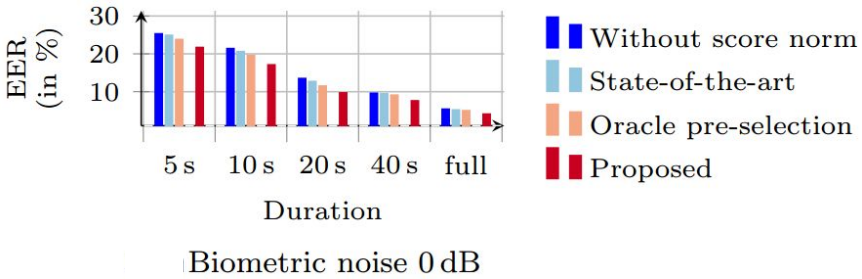
Quality estimates



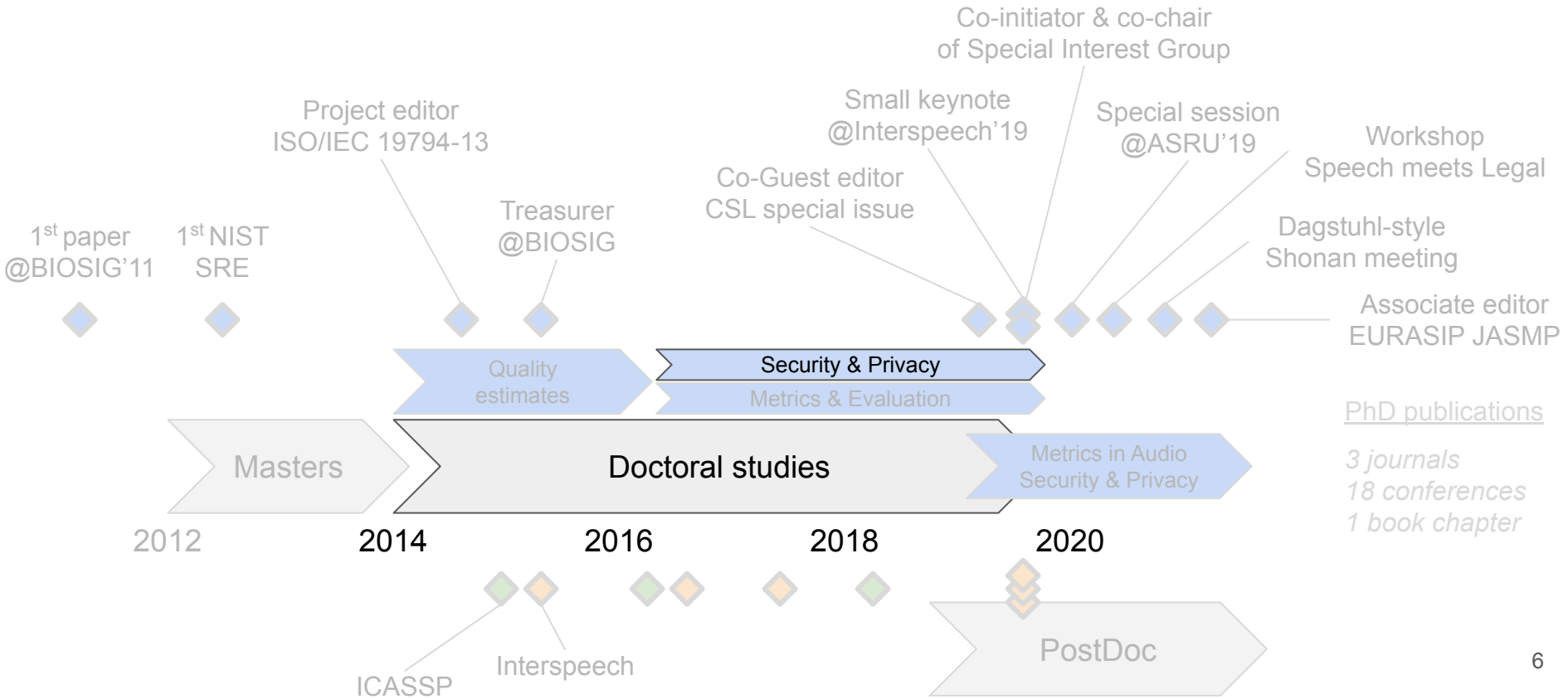



- Environments can change every session
- 2012 NIST SRE
  - Tasks: a) known vs. unknown identification b) large-scale dataset c) *varying quality*
  - Participants: large fusions, rise of i-vectors & *adaptive score calibration*
- My contributions: studies on I4U team's dataset (1996-2010 NIST SREs)
  - Collision probability
  - Parsimonious score calibration
  - Robustness: ambient vs. biometric noise
  - Pre-selection in score normalisation

0 dB & clean speech from NOIZEUS

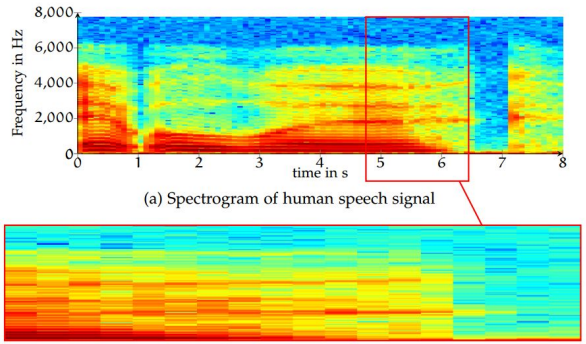


Outline of my research achievements

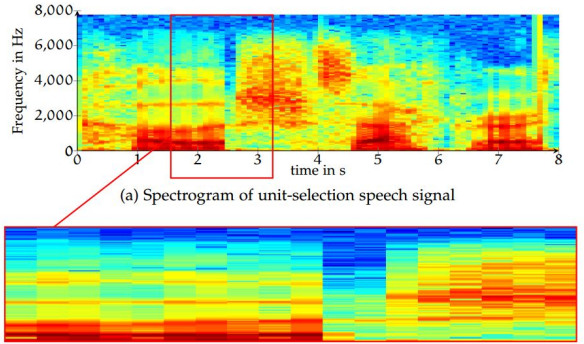


Contribution to security

- ASVspoof 2015 challenge (metric: EER)
  - ISO/IEC IS 30107 family “Presentation Attack Detection”
  - Focus: “unit-selection attack” (strongest among 10 attacks)
- Contribution: 1st Voice-PAD method on unfiltered speech signals
  - Proposed: wavelet & Fourier analysis with SVM & GMM classification
  - Baseline (8.5%) — training & validation on German (7.1%) — ASVspoof 2015 (11.7%)



(a) Spectrogram of human speech signal



(a) Spectrogram of unit-selection speech signal

Contribution to privacy

- Privacy-preservation w/o loss of …
  - Recognition performance
  - Real-time response
- ISO/IEC IS 24745 “Biometric Information Protection”

State-of-the-art comparator

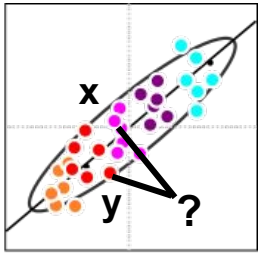


Figure based on Prince: www.computervisionmodels.com

Paillier homomorphic encryption

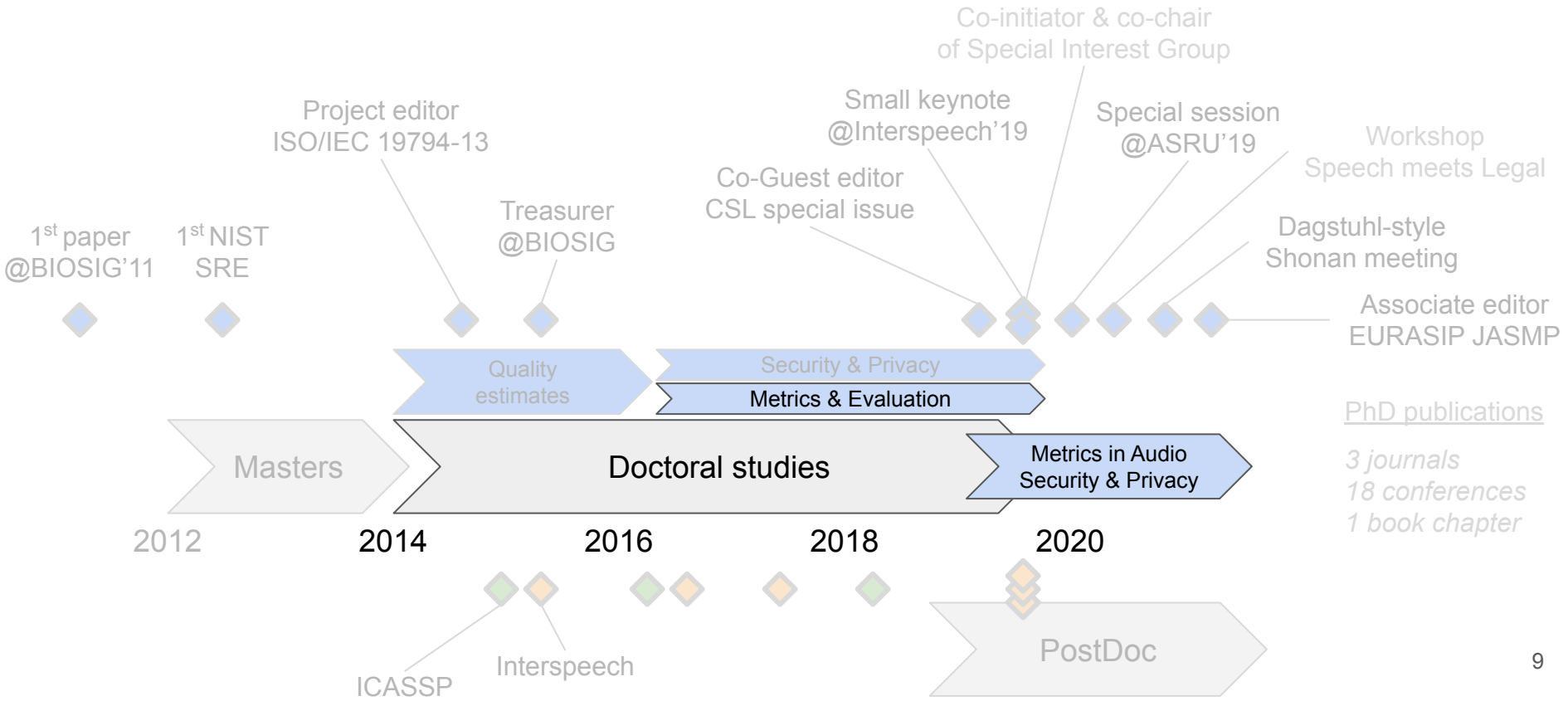
$$Enc_{pk}(x) \boxplus Enc_{pk}(y) = Enc_{pk}(x+y)$$

“compute all-at-once” approach
Slow computation
Fast communication

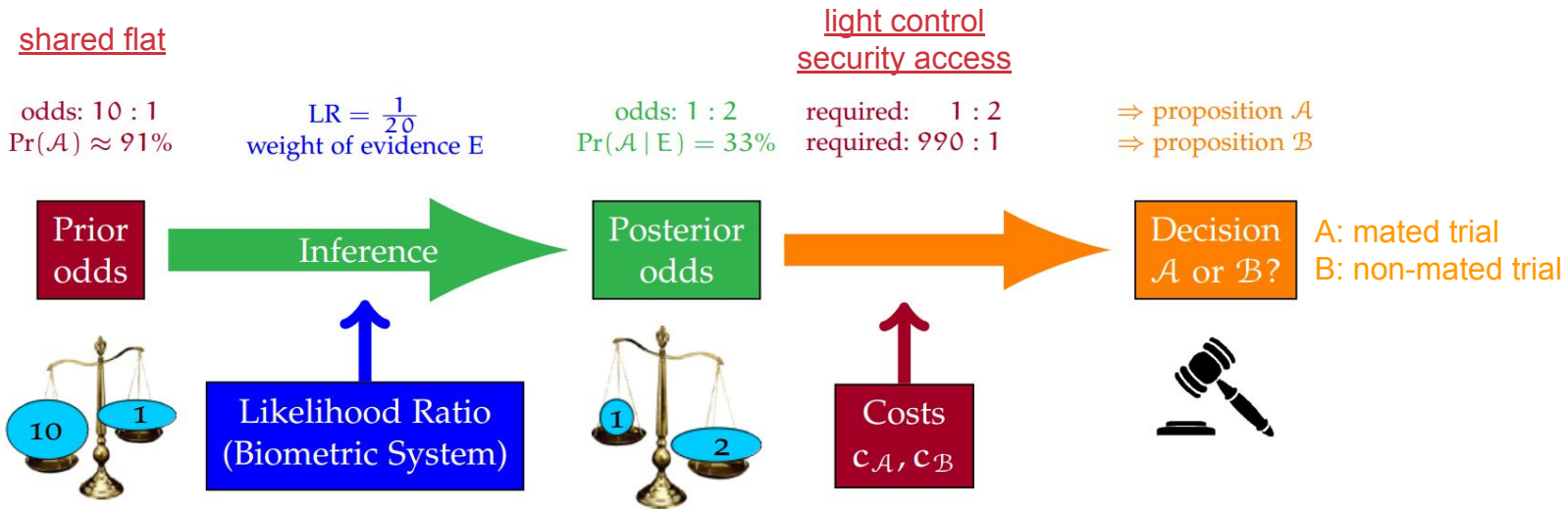
“compute bit-by-bit” approach
Fast computation
Slow communication

Secure Two-Party Computation

Outline of my research achievements

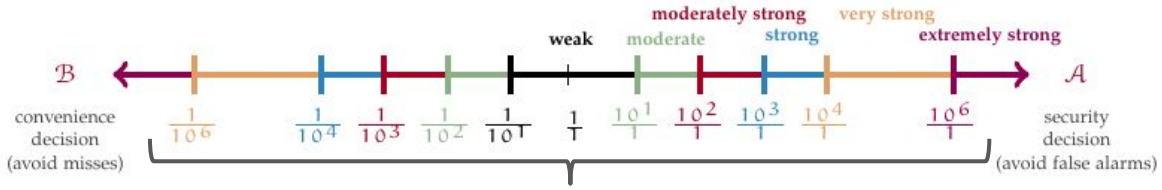


Textbook Bayesian decision theory



Bridging between paradigms

- Frequentist & Bayesian paradigms driven by …
  - Error rates (e.g., SC 37)
  - Decision trade-offs (e.g., forensic sciences)
- Contribution — answers to
  - Which scales of decision trade-offs are supported by which error rate trade-offs?
  - Relation: error rate plots to priors & costs?



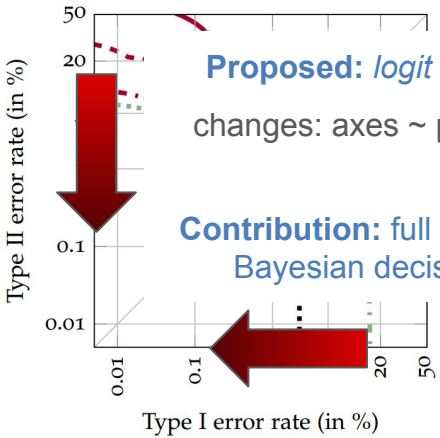
ENFSI scale; next step: from scores to thresholds

ISO/IEC JTC 1

ISO/IEC JTC 1/SC 37

Biometrics

ENFSI — EUROPEAN NETWORK OF FORENSIC SCIENCE INSTITUTES



Proposed: *logit* axes scaling

changes: axes ~ priors & costs

Contribution: full interrelation of Bayesian decision theory

Metrics in Audio Security & Privacy

ASVspoof 2019: Future Horizons in Spoofed and Fake Audio Detection

Massimiliano Todisco[1], Xin Wang[2], Ville Vestman[3,6], Md Sahidullah[4], Héctor Delgado[1], Andreas Nautsch[1], Junichi Yamagishi[2,5], Nicholas Evans[1], Tomi Kinnunen[3], Kong Aik Lee[6]

GRAZ – AUSTRIA
SEPTEMBER 15th – 19th 2019

INTERSPEECH 2019

Introducing the VoicePrivacy Initiative

N. Tomashenko[1], B. M. L. Srivastava[2], X. Wang[3], E. Vincent[4], A. Nautsch[5], J. Yamagishi[3,6], N. Evans[5], J. Patino[5], J.-F. Bonastre[1], P.-G. Noé[1], M. Todisco[5]

Co-organiser of two research challenges

INTERSPEECH 2020
Cognitive Intelligence for Speech Processing

IEEE/ACM TRANSACTIONS ON

AUDIO, SPEECH, AND LANGUAGE PROCESSING

Tandem Assessment of Spoofing Countermeasures and Automatic Speaker Verification: Fundamentals

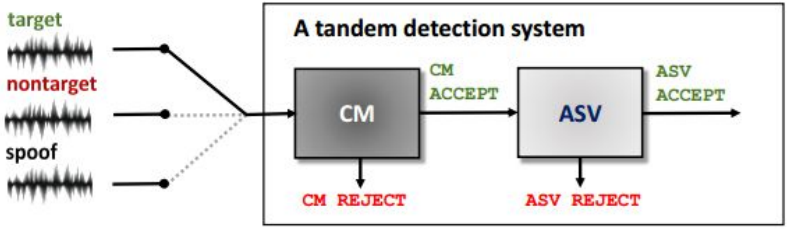
Tomi Kinnunen, *Member, IEEE,* Héctor Delgado, *Member, IEEE,* Nicholas Evans *Member, IEEE,* Kong Aik Lee, *Senior Member, IEEE,* Ville Vestman, Andreas Nautsch, *Member, IEEE,* Massimiliano Todisco, *Member, IEEE,* Xin Wang, *Member, IEEE,* Md Sahidullah *Member, IEEE,* Junichi Yamagishi, *Senior Member, IEEE,* and Douglas A. Reynolds, *Fellow, IEEE*

The Privacy ZEBRA: Zero Evidence Biometric Recognition Assessment

Andreas Nautsch[1], Jose Patino[1], Natalia Tomashenko[2], Junichi Yamagishi[3], Paul-Gauthier Noé[2], Jean-François Bonastre[2], Massimiliano Todisco[1] and Nicholas Evans[1]

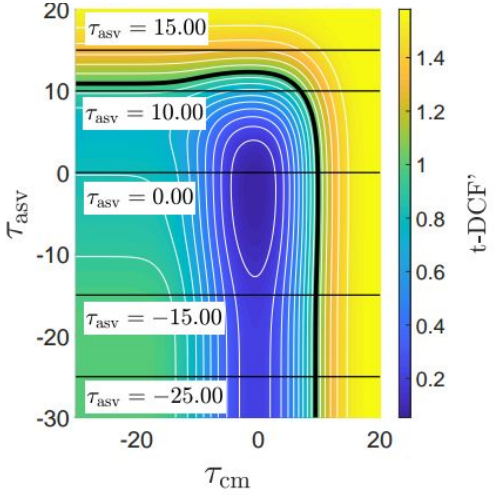
Metrics: ASVspoof 2019

- Previous editions 2015 & 2017: EER
- 2019 inspired by NIST SREs's: Detection Cost Function (DCF)
  - Biometric sub-system + countermeasure ⇒ tandem DCF (t-DCF)



	Actual class	Tandem decision	Unit cost
a.	Target	REJECT (by ASV)	C_{miss}
b.	Nontarget	ACCEPT	C_{fa}
c.	Spoof	ACCEPT	$C_{\text{fa,spoof}}$
d.	Target	REJECT (by CM)	C_{miss}

Actual class	Asserted prior
Target	π_{tar}
Nontarget	π_{non}
Spoof	π_{spoof}
	$\Sigma = 1$



Terminology in speech communication jargon

ASVspoof: highly collaborative consortium

ASVspoof 2019: spoofing countermeasures for the detection of synthesized, converted and replayed speech

Andreas Nautsch, *Member, IEEE,* Xin Wang, *Member, IEEE,* Nicholas Evans, *Member, IEEE,* Tomi Kinnunen, *Member, IEEE,* Ville Vestman, Massimiliano Todisco, *Member, IEEE,* Héctor Delgado, Md Sahidullah, *Member, IEEE,* Junichi Yamagishi, *Senior Member, IEEE,* and Kong Aik Lee, *Senior Member, IEEE*

** submitted to:*

IEEE Biometrics Council

IEEE TRANSACTIONS ON BIOMETRICS, BEHAVIOR, AND IDENTITY SCIENCE

Tandem Assessment of Spoofing Countermeasures and Automatic Speaker Verification: Fundamentals

Tomi Kinnunen, *Member, IEEE,* Héctor Delgado, *Member, IEEE,* Nicholas Evans *Member, IEEE,* Kong Aik Lee, *Senior Member, IEEE,* Ville Vestman, Andreas Nautsch, *Member, IEEE,* Massimiliano Todisco, *Member, IEEE,* Xin Wang, *Member, IEEE,* Md Sahidullah *Member, IEEE,* Junichi Yamagishi, *Senior Member, IEEE,* and Douglas A. Reynolds, *Fellow, IEEE*

ASVspoof 2019: A large-scale public database of synthesized, converted and replayed speech

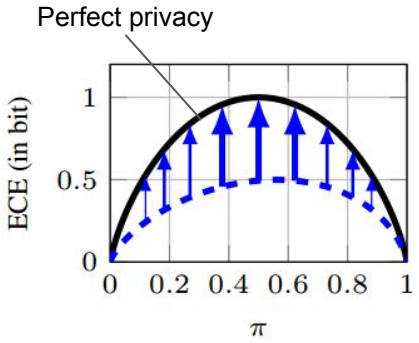
Xin Wang [a], Junichi Yamagishi [1, a, b], Massimiliano Todisco [1, c], Héctor Delgado [1, c], Andreas Nautsch [1, c], Nicholas Evans [1, c], Md Sahidullah [1, d], Ville Vestman [1, e], Tomi Kinnunen [1, e], Kong Aik Lee [1, f], Lauri Juvela [g], Paavo Alku [g], Yu-Huai Peng [h], Hsin-Te Hwang [h], Yu Tsao [h], Hsin-Min Wang [h], Sébastien Le Maguer [i], Markus Becker [j], Fergus Henderson [j], Rob Clark [j], Yu Zhang [j], Quan Wang [j], Ye Jia [j], Kai Onuma [k], Koji Mushika [k], Takashi Kaneda [k], Yuan Jiang [l], Li-Juan Liu [l], Yi-Chiao Wu [m], Wen-Chin Huang [m], Tomoki Toda [m], Kou Tanaka [n], Hirokazu Kameoka [n], Ingmar Steiner [o], Driss Matrouf [p], Jean-François Bonastre [p], Avashna Govender [b], Srikanth Ronanki [q], Jing-Xuan Zhang [r], Zhen-Hua Ling [r]

ASVspoof 2019: Future Horizons in Spoofed and Fake Audio Detection

Massimiliano Todisco[1], Xin Wang[2], Ville Vestman[3,6], Md Sahidullah[4], Héctor Delgado[1], Andreas Nautsch[1], Junichi Yamagishi[2,5], Nicholas Evans[1], Tomi Kinnunen[3], Kong Aik Lee[6]

Metrics: VoicePrivacy 2020

- Modify audio: biometrics should fail & speech recognition should work
  - 1st edition
  - Conventional metrics do not suffice (e.g., EER, DCF, C_{llr}, …)
- Contribution: Zero Evidence Biometric Recognition Assessment (ZEBRA)
  - Inspired by speaker recognition & forensic sciences
  - Shannon: if prior = posterior knowledge ⇒ perfect privacy



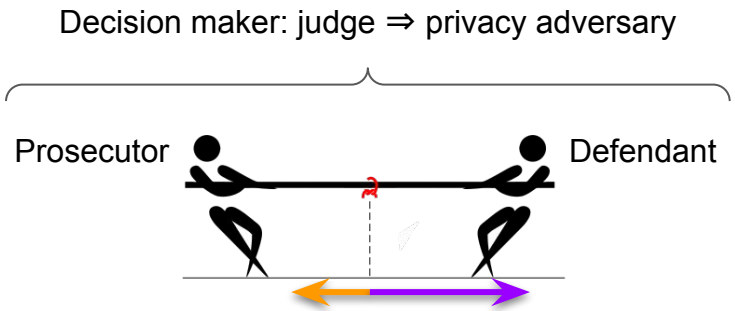
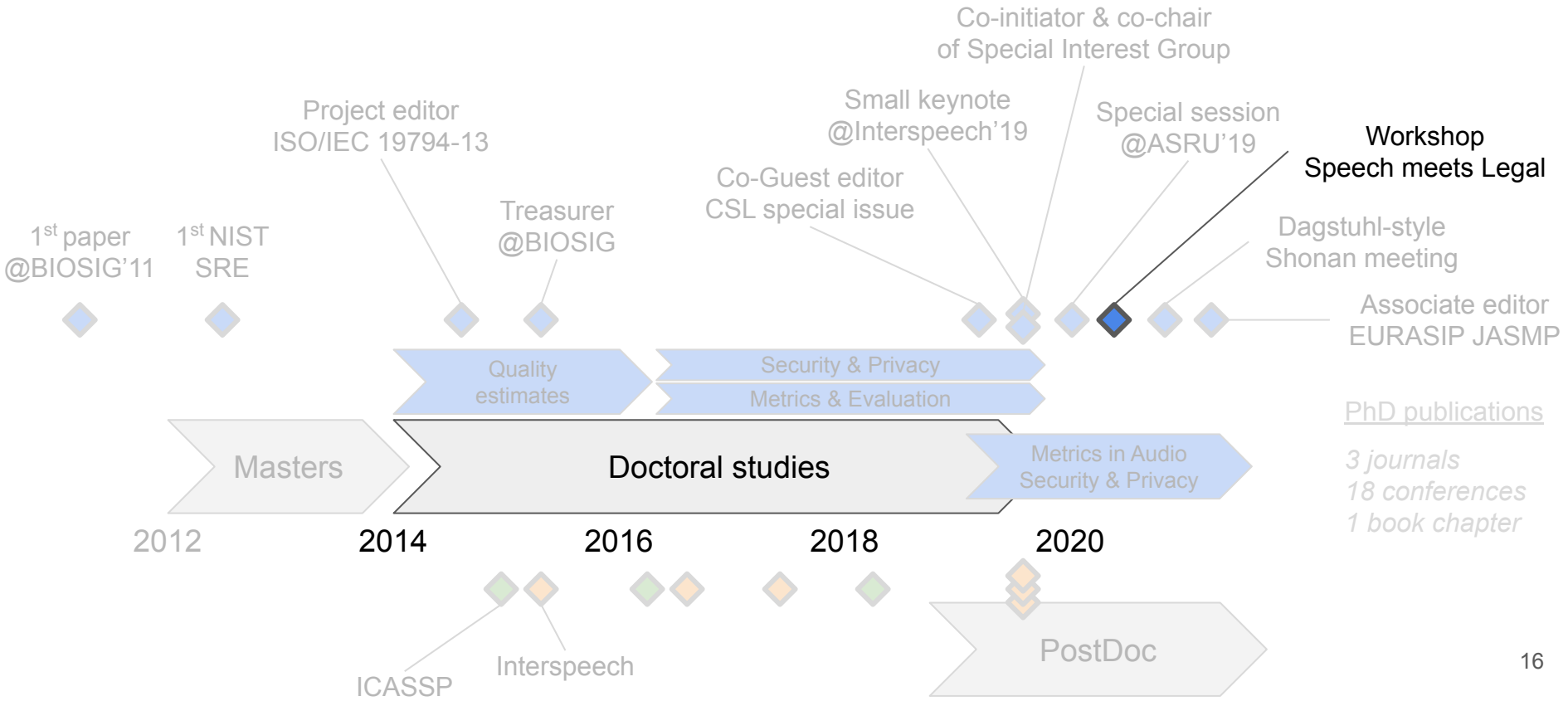


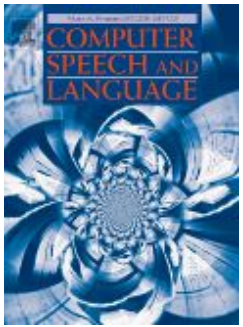
Figure based on wikimedia.org

Picture taken in Heidelberg Zoo, 2020

Outline of my research achievements



Workshop:
Speech meets Legal experts



GRAZ – AUSTRIA
SEPTEMBER 15th – 19th 2019
INTERSPEECH
2019

NII SHONAN MEETING

NO.170

[Cancelled] Privacy, Ethics, and Legislation for Speech Communication

Shonan Village Center
March 23 - 27, 2020 (Check-in: March 22, 2020)

Organizers

Stephan Sigg
Aalto University, Finland

Andreas Nautsch
EURECOM, France

Junichi Yamagishi
National Institute of Informatics Japan

Shout outs for support, encouragements & advice to:
Nick Evans, Els Kindt, Catherine Jasserand, Isabel Trancoso, Korbinian Riedhammer, Adriana Stan

ELSEVIER

Computer Speech & Language

Volume 58, November 2019, Pages 441-480

Preserving privacy in speaker and speech characterisation ☆

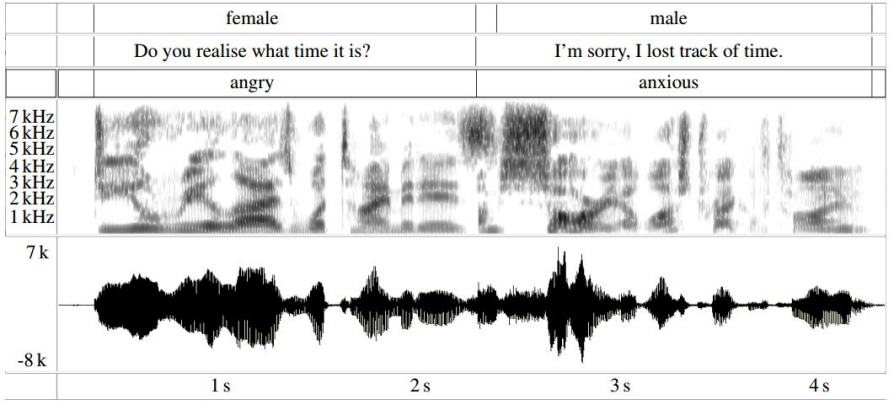
Andreas Nautsch [a, f] ✉, Abelino Jiménez [b], Amos Treiber [c], Jascha Kolberg [a], Catherine Jasserand [d], Els Kindt [e], Héctor Delgado [f], Massimiliano Todisco [f], Mohamed Amine Hmani [g], Aymen Mtibaa [g], Mohammed Ahmed Abdelraheem [h], Alberto Abad [i], Francisco Teixeira [j], Driss Matrouf [k], Marta Gomez-Barrero [a], Dijana Petrovska-Delacrétaz [g], Gérard Chollet [h, g], Nicholas Evans [f], Thomas Schneider [c], Jean-François Bonastre [l], Bhiksha Raj [m], Isabel Trancoso [j], Christoph Busch [a]

Biometrics
Study of the Law
Cryptography

Speaker recognition
Speech communication

The GDPR & speech data: first steps

- Privacy, a Legal Perspective
  - What are ‘privacy’ and ‘data protection’?
  - When does data qualify as ‘biometric data’?
  - When is data ‘sensitive’?
  - Legal grounds to process sensitive data?
- Privacy, a Technical Perspective
  - What is speech [in] communication?
  - How is speech data captured, processed and stored?
  - Why is speech data sensitive?
  - What safeguards are there?
- Need for Taxonomies (7 proposed)



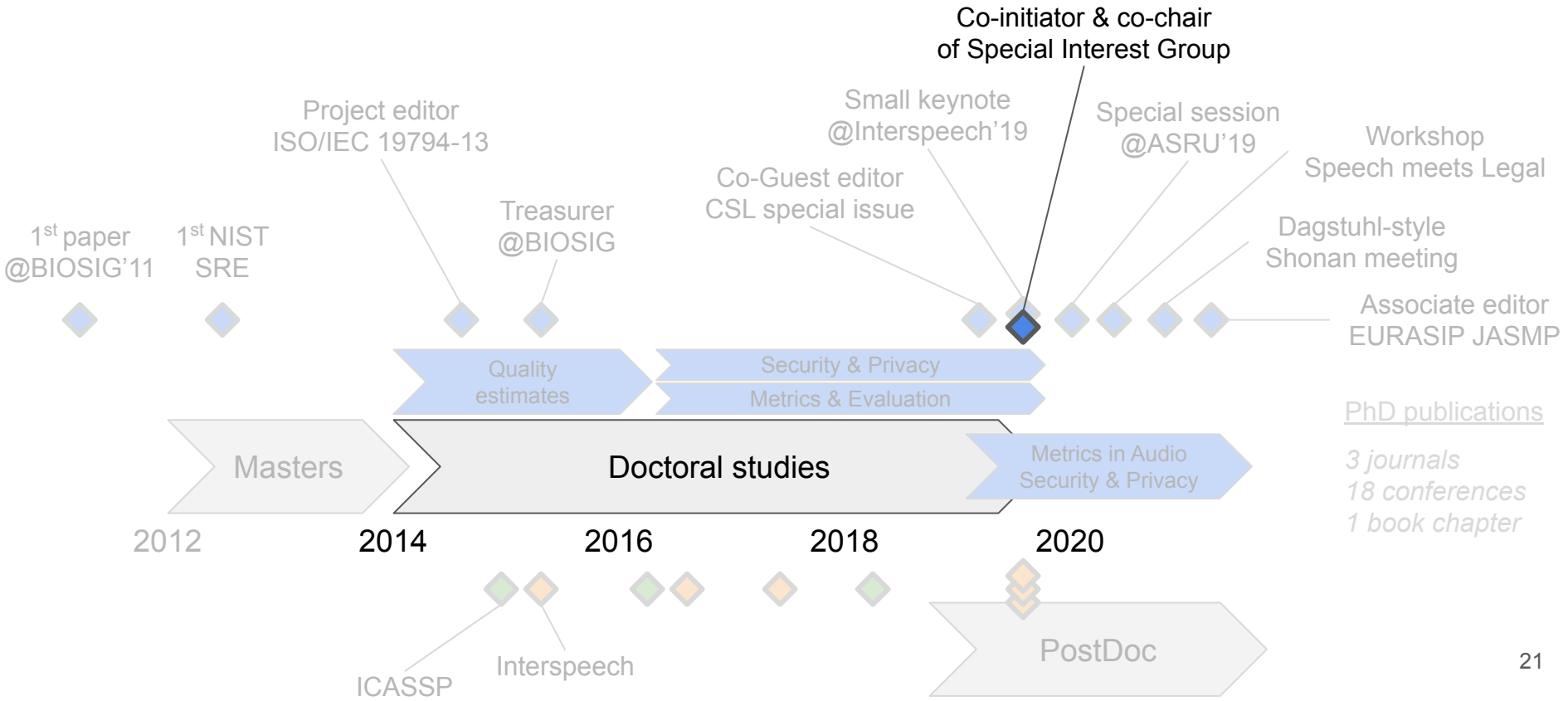
Sound extracted from https://www.eslfast.com/robot/audio/dailylife/dailylife1901.mp3

Speech meets Legal experts workshop

- Lead organiser
- Morning session: four presentations
  - "SPEAKER — privacy preserving speech assistance made in Germany"
  - "Patient and audio data in clinical speech therapy"
  - "Views of the EDPS on speech and data protection"
  - "Speech data and the GDPR: First reflections from a legal perspective"
- Afternoon session: open discussion

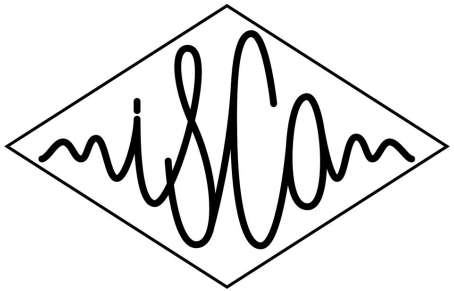
Presenters: Birgit Brüggemeier (Fraunhofer IIS),
Korbinian Riedhammer (TH Nürnberg),
Thomas Zerdick (European Data Protection Supervisor; Head IT policy),
Catherine Jasserand (University of Groningen)

Outline of my research achievements



Security and Privacy in Speech Communication

Special Interest Group
of the

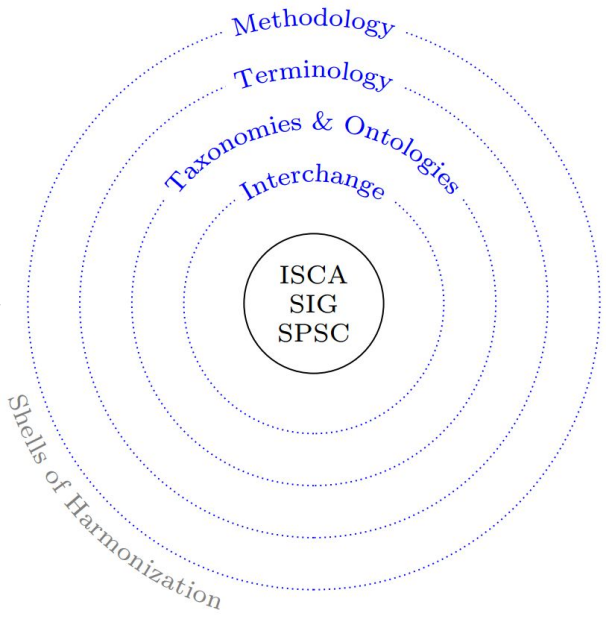


International Speech
Communication Association (ISCA)

Research Areas

- Speech Communication
- Ethics & Study of the Law
- HCI with Speech as Medium
- Cybersecurity

Understanding Security & Privacy



Dissemination

- Qualitative Research
- Popular Science
- Quantitative Research

Security & Privacy in Speech Communication

- Established @ Interspeech 2019
- 93 members as of September 2020
- Dissemination
  - www.spsc-sig.org
  - E-mail list
  - Webinars
  - LinkedIn
  - Twitter
- Join us

  simply drop me an email: nautsch@eurecom.fr

Tom Bäckström

Chair

Andreas Nautsch

Secretary/Co-Chair

da/sec
BIOMETRICS AND INTERNET-SECURITY
RESEARCH GROUP

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACULTY OF COMPUTER SCIENCE

TECHNISCHE
UNIVERSITÄT
DARMSTADT

ATHENE
National Research Center
for Applied Cybersecurity

European
Association for
Biometrics
eab
Human Identity in Europe

LOEWE
Exzellente Forschung für
Hessens Zukunft

EURECOM
Sophia Antipolis

ISO/IEC JTC 1
ISO/IEC JTC 1/SC 37
Biometrics

Thank you :)

Questions?

Co-initiator & secretary/co-chair of ISCA SIG
"Security & Privacy in Speech Communication"

Co-guest editor for ASVspoof special issue in Computer Speech & Language

Associate editor: EURASIP Journal on Audio, Speech, and Music Processing

Project editor: ISO/IEC IS 19794-13:2018
"Biometric data interchange formats — Part 13: Voice data"

Cited by

	All	Since 2015
Citations	282	281
h-index	9	9
i10-index	8	8