ASVspoof 2015:

Automatic Speaker Verification Spoofing and Countermeasures Challenge

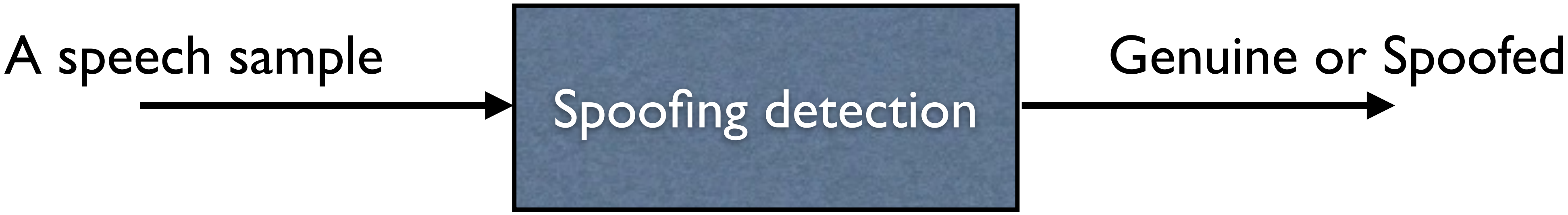
http://www.spoofingchallenge.org/

Zhizheng Wu[1], Tomi Kinnunen[2], Nicholas Evans[3], Junichi Yamagishi[1]

[1]University of Edinburgh, UK
[2]University of Eastern Finland, Finland
[3]EURECOM, France

The challenge task

- **Spoofing detection**
  - **To develop algorithms to discriminate between natural and spoofed speech**



Database: overview

- Clean data without channel or background noise
  - To focus on spoofing

- A subset of SAS corpus with additional processing
  - removing broken files
  - trimming some silence frames

- Consisting of both genuine and spoofed speech
  - spoofed speech is modified from the original speech by voice conversion or speech synthesis algorithms

Zhizheng Wu, Ali Khodabakhsh, Cenk Demiroglu, Junichi Yamagishi, Daisuke Saito, Tomoki Toda, Simon King, "SAS: A speaker verification spoofing database containing diverse attacks", ICASSP 2015

Database: subsets

- Training data
  - a dataset of audio files with known ground-truth which can be used to train or learn systems which can distinguish between genuine and spoofed speech

- Development data
  - a dataset of audio files with known ground-truth which can be used for the development of spoofing detection algorithms

- Evaluation data
  - a dataset of audio files with no ground-truth and which must be processed to produce scores

Database: subsets

- **Number of non-overlapping speakers and utterances in each subset**

	# speakers		# utterances	
	Male	Female	Genuine	Spoofed
Training	10	15	3750	12625
Development	15	20	3497	49875
Evaluation	20	26	9404	184000

To encourage gender- and speaker-independent spoofing detection

Database: spoofing algorithms

- **Summary of spoofing algorithms implemented**

	# utterances			Algorithm	Vocoder
	Training	Development	Evaluation		
Genuine	3750	3497	9404	None	None
S1	2525	9975	18400	VC :Frame-selection	STRAIGHT
S2	2525	9975	18400	VC: Slope-shifting	STRAIGHT
S3	2525	9975	18400	SS: HMM	STRAIGHT
S4	2525	9975	18400	SS: HMM	STRAIGHT
S5	2525	9975	18400	VC: GMM	MLSA
S6	0	0	18400	VC: GMM	STRAIGHT
S7	0	0	18400	VC: GMM	STRAIGHT
S8	0	0	18400	VC:Tensor	STRAIGHT
S9	0	0	18400	VC: KPLS	STRAIGHT
S10	0	0	18400	SS: unit-selection	None

Database: known and unknown

- Known attacks: S1 - S5
  - available in the training and development sets

- Unknown attacks: S6 - S10
  - only appear in the evaluation set

Evaluation metric

- **Average Equal Error Rate (EER)**

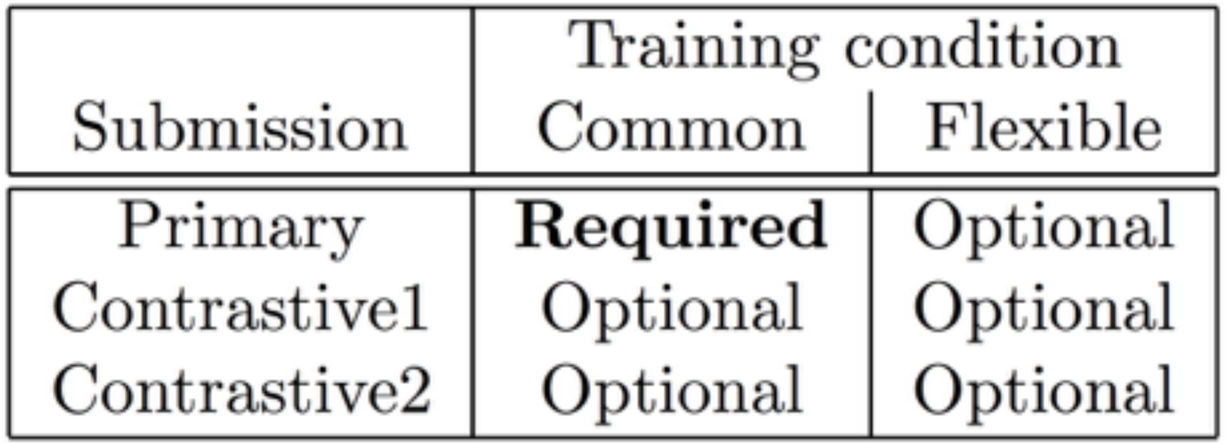
$$
\begin{aligned}
P_{\mathrm{fa}}(\theta) &= \frac{\#\{\text{spoofed trials with score} > \theta\}}{\#\{\text{total spoofed trials}\}} \\
P_{\mathrm{miss}}(\theta) &= \frac{\#\{\text{genuine trials with score} \leq \theta\}}{\#\{\text{total genuine trials}\}}
\end{aligned}
$$

$$
\mathrm{EER} = P_{\mathrm{fa}}(\theta_{\mathrm{EER}}) = P_{\mathrm{miss}}(\theta_{\mathrm{EER}})
$$

  - **Calculate an EER for each spoofing algorithm, and average across all the EERs**

Evaluation task

- **Each participant is allowed to submit up to six systems**
  - **Only the primary score under the common training condition is used for ranking**

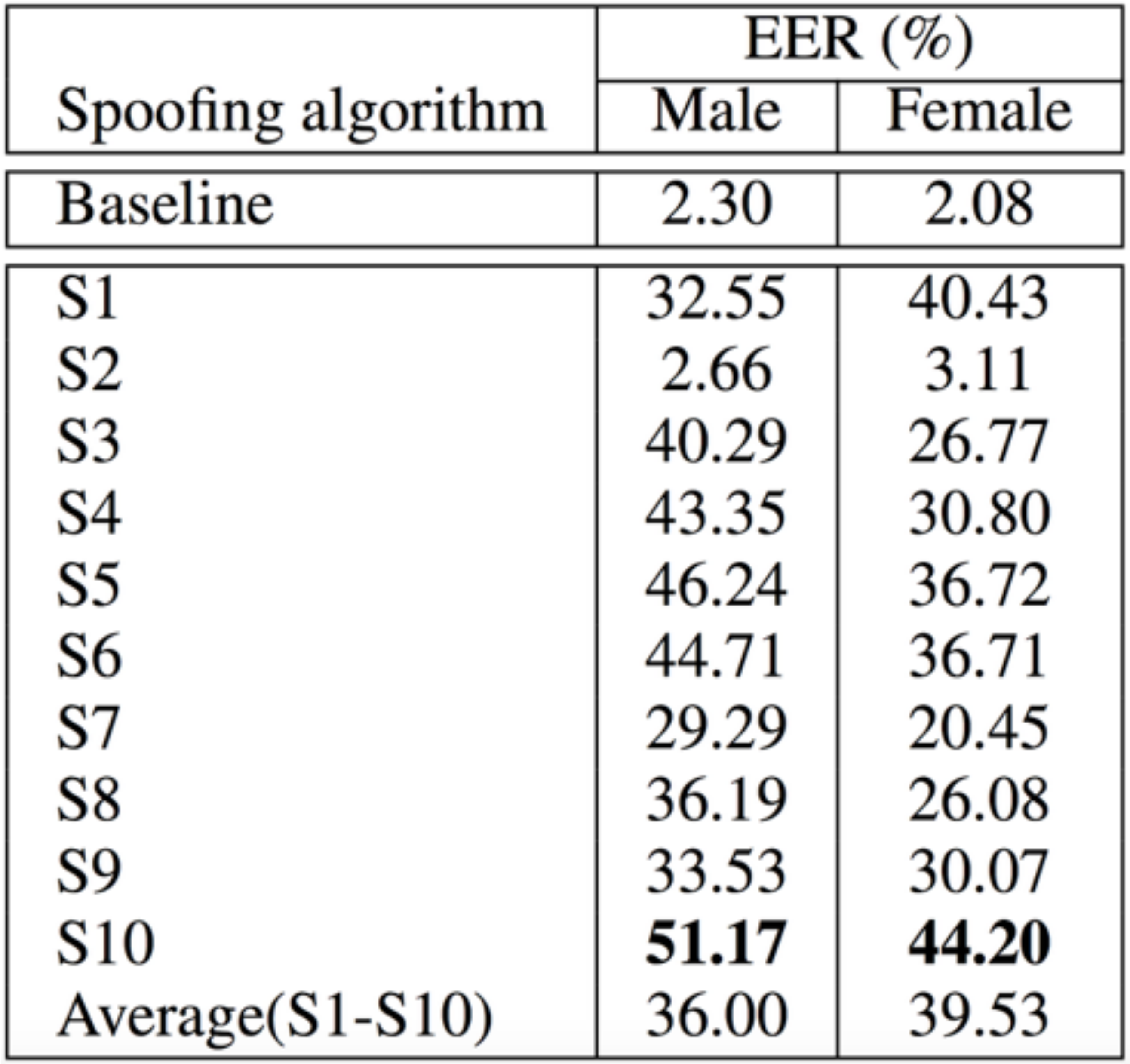


Submission	Training condition	
	Common	Flexible
Primary	**Required**	Optional
Contrastive1	Optional	Optional
Contrastive2	Optional	Optional

  - **Common condition: can only use the defined training data**
  - **Flexible condition: can use any training data**

Speaker verification performance

- **State-of-the-art i-vector-PLDA system**



Spoofing algorithm	EER (%)	
	Male	Female
Baseline	2.30	2.08
S1	32.55	40.43
S2	2.66	3.11
S3	40.29	26.77
S4	43.35	30.80
S5	46.24	36.72
S6	44.71	36.71
S7	29.29	20.45
S8	36.19	26.08
S9	33.53	30.07
S10	**51.17**	**44.20**
Average(S1-S10)	36.00	39.53

All the spoofing algorithms increase the EERs considerably!

The challenge participation

- 28 teams from 16 countries requested the challenge database
- 16 teams submitted results by the deadline
- Received 16 primary submissions and 27 additional submissions

Challenge results

- **Equal error rates (EERs) of the primary tasks from 16 teams**

	Equal Error Rates (EERs)		
Team	Known attacks (S1 - S5)	Unknown attacks (S6 - S10)	Average (all)
A	0.408	2.013	1.211
B	0.008	3.922	1.965
C	0.058	4.998	2.528
D	0.003	5.231	2.617
E	0.041	5.347	2.694
F	0.358	6.078	3.218
G	0.405	6.247	3.326
H	0.67	6.041	3.355
I	0.005	7.447	3.726
J	0.025	8.168	4.097
K	0.21	8.883	4.547
L	0.412	13.026	6.719
M	8.528	20.253	14.391
N	7.874	21.262	14.568
O	17.723	19.929	18.826
P	21.206	21.831	21.518

Challenge results

- **Results with/without S10**

	Equal Error Rates (EERs)		
Team	Average (all)	Average (without S10)	S10
A	1.211	0.402	8.490
B	1.965	0.008	19.571
C	2.528	0.076	24.601
D	2.617	0.003	26.142
E	2.694	0.060	26.393
F	3.218	0.400	28.581
G	3.326	0.360	30.021
H	3.726	0.021	37.068
I	3.898	0.703	32.651
J	4.097	0.029	40.708
K	4.547	0.203	43.638
L	6.719	3.478	35.890
M	14.391	12.482	31.574
N	14.568	11.299	43.991
O	18.826	16.304	41.519
P	21.518	18.786	46.102

Challenge results

- **Team names**

	Equal Error Rates (EERs)			
Team	Average (all)	Average (without S10)	S10	Team name
A	1.211	0.402	8.490	DA-IICT
B	1.965	0.008	19.571	STC
C	2.528	0.076	24.601	SJTU
D	2.617	0.003	26.142	NTU
E	2.694	0.060	26.393	CRIM
F	3.218	0.400	28.581	
G	3.326	0.360	30.021	
H	3.726	0.021	37.068	
I	3.898	0.703	32.651	
J	4.097	0.029	40.708	
K	4.547	0.203	43.638	
L	6.719	3.478	35.890	
M	14.391	12.482	31.574	
N	14.568	11.299	43.991	
O	18.826	16.304	41.519	
P	21.518	18.786	46.102	

Free 'lunch'!

- System descriptions are available online now
  - http://www.spoofingchallenge.org
- The challenge database is publicly-available to everyone for free
  - Including the spoofing detection protocol as well as speaker verification protocol (Bonus to everyone!)
  - link: http://data.cstr.ed.ac.uk/antispoofing2015/
  - User name: test
  - Password: test

  - A permanent DOI link is coming soon (our data repository assistant is working on it)

Conclusions

- The first challenge is highly successful in attracting significant participation
  - At least 10 companies are interested in the database

- Most of the participants achieved good results on known attacks, however, many of them got higher error rates on unknown attacks

- There is still a long way to go towards a real generalised countermeasure

Acknowledgement

- Thank the following colleagues from providing spoofing materials
  - Dr. Daisuke Saito from University of Tokyo, Japan
  - Prof. Tomoki Toda from Nagoya University, Japan
  - Prof. Zhen-Hua Ling from University of Science and Technology of China
  - Mr Ali Khodabakhsh and Dr. Cenk Demiroglu from Ozyegin University, Turkey

- Protocol validation (conduct pilot evaluation)
  - Dr. Md Sahidullah, Dr. Cemal Hanilci, Mr. Aleksandr Sizov from University of Eastern Finland

Please come back at 10:30 to discuss the future :)