Redefining the Eurovision voting process using linear ECC

Roberto Trifiletti, Aarhus University

Joint work with Bernardo David, Irene Giacomelli, Jesper Buus Nielsen Ignacio Cascudo Pueyo

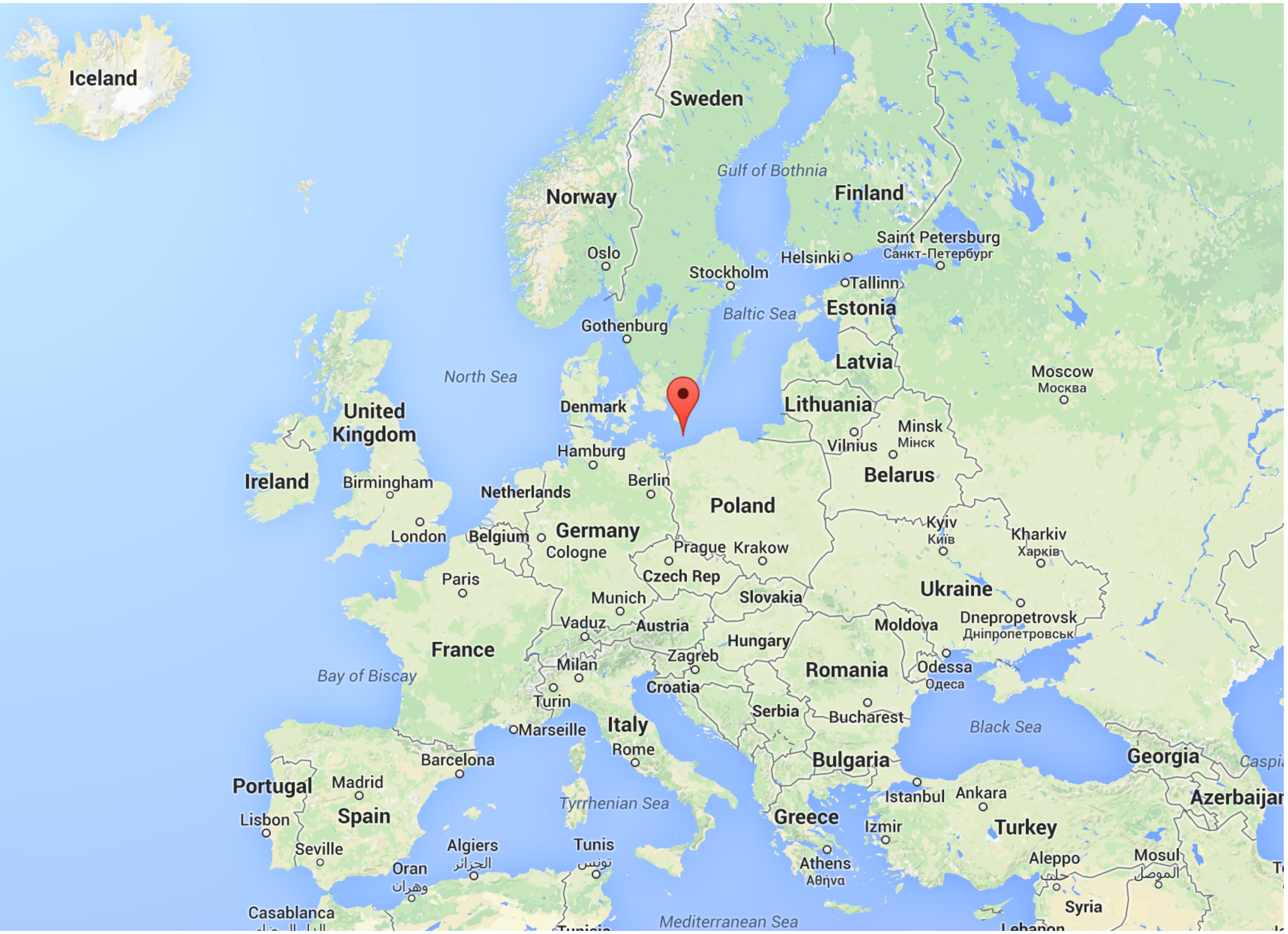
The artists perform

Each in their own way…

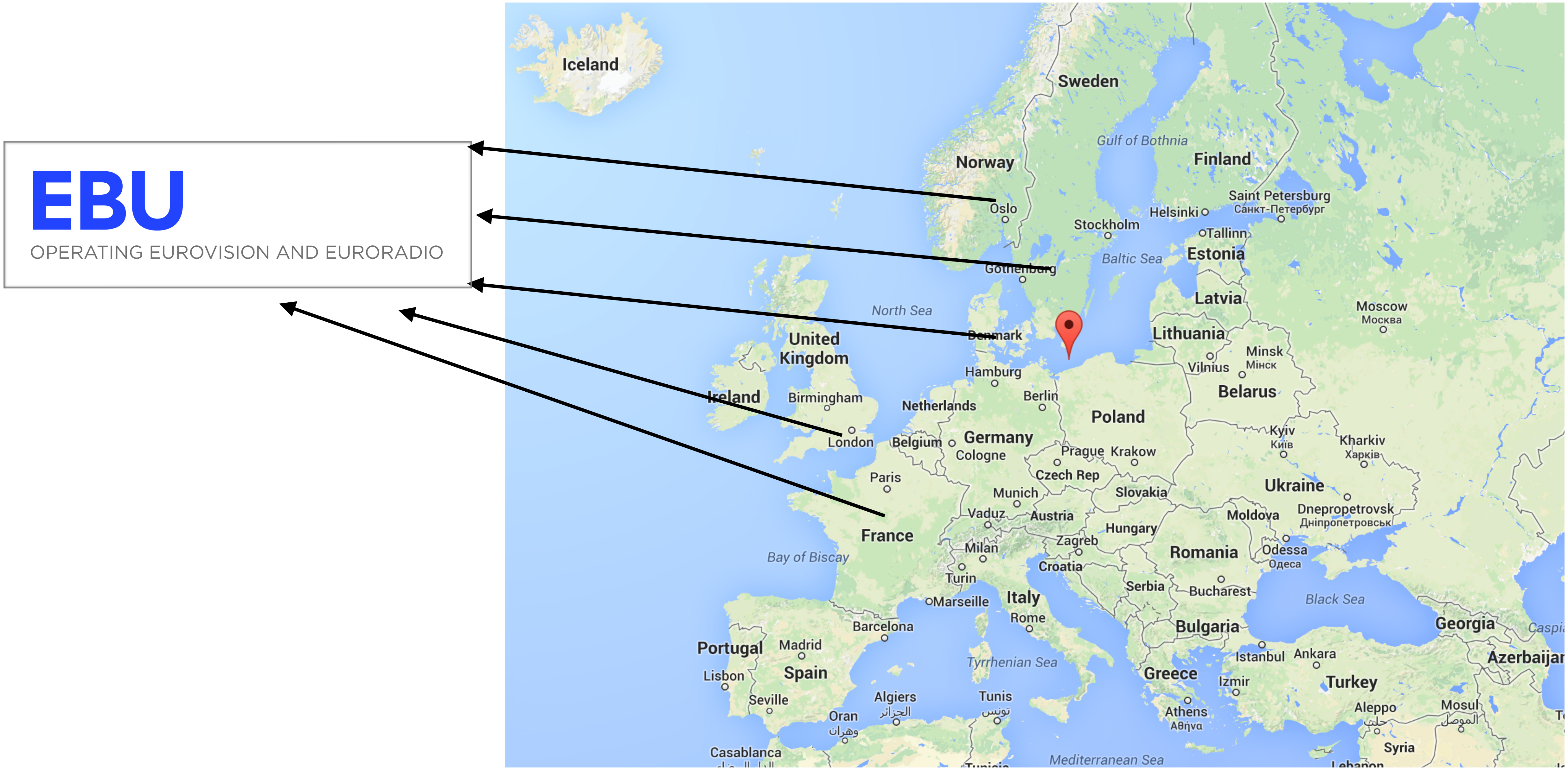
The voting process

EBU

OPERATING EUROVISION AND EURORADIO



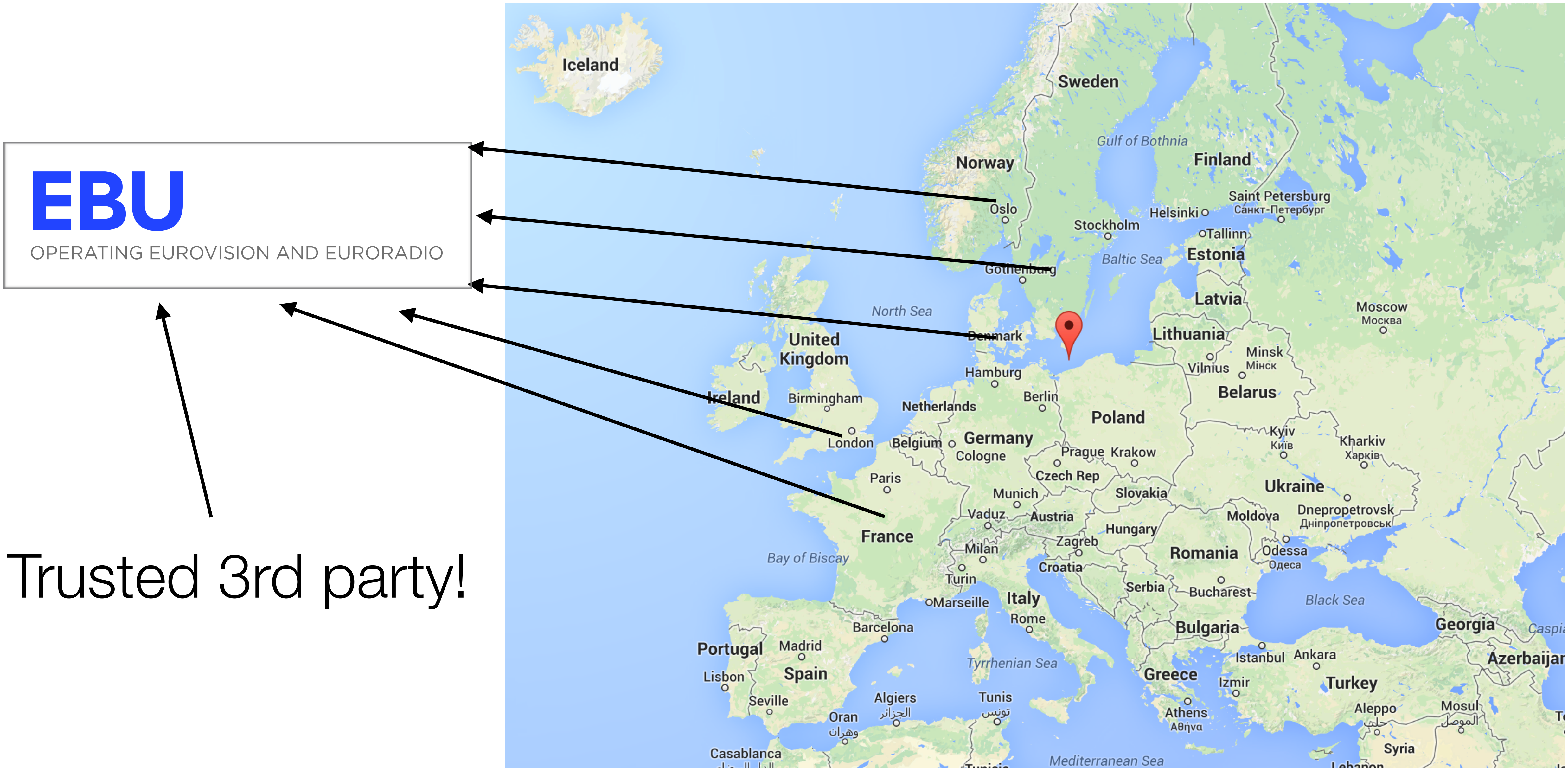
The voting process



EBU

OPERATING EUROVISION AND EURORADIO

The voting process



Trusted 3rd party!

A concrete cheating strategy

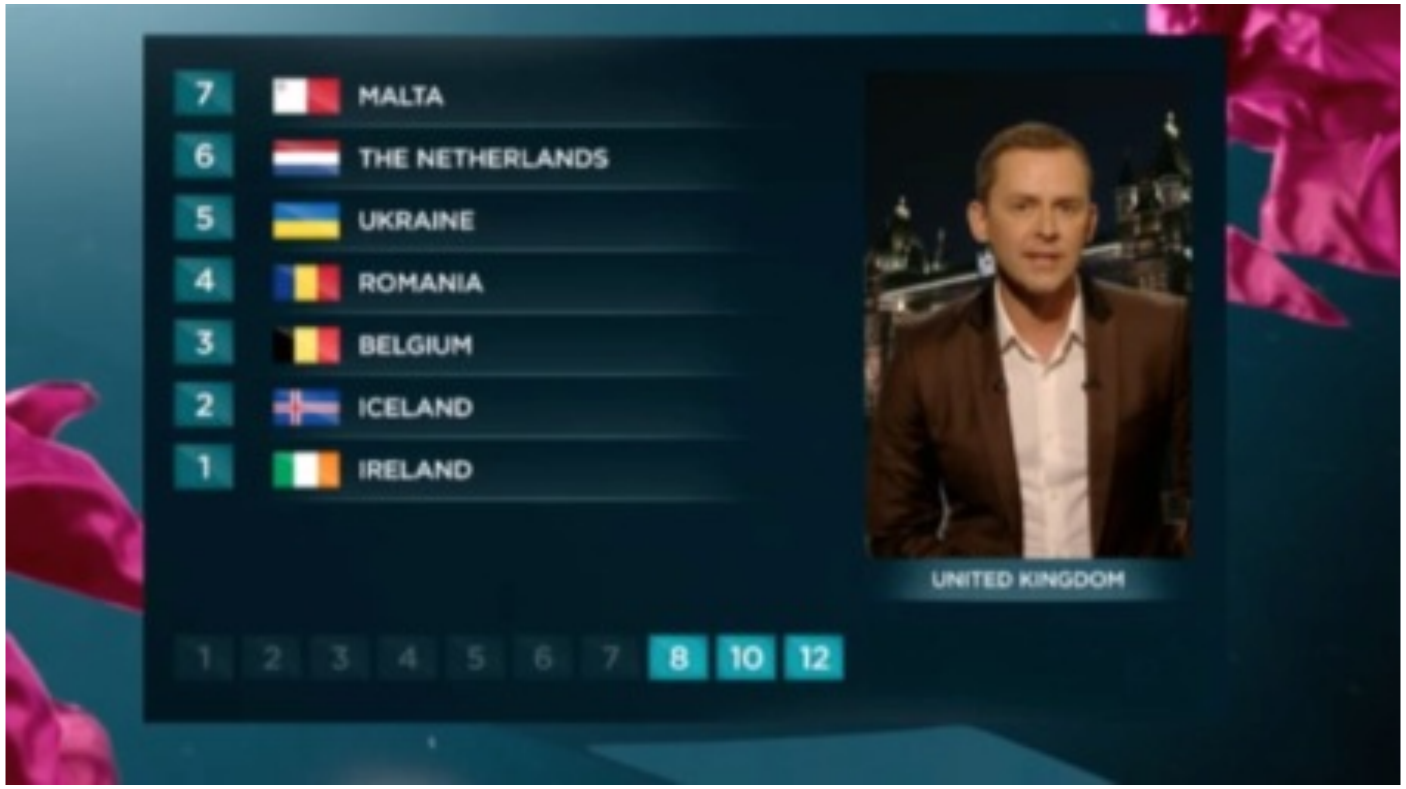
A concrete cheating strategy

- Mole within the EBU who leaks all votes as they come in to the UK

A concrete cheating strategy

- Mole within the EBU who leaks all votes as they come in to the UK

- The UK (as well as their friends) adjust their votes accordingly to maximize their winning probability



7	MALTA
6	THE NETHERLANDS
5	UKRAINE
4	ROMANIA
3	BELGIUM
2	ICELAND
1	IRELAND

The solution

The solution

- Not sending the votes in plain. Commit!

The solution

- Not sending the votes in plain. Commit!
- When done. All countries open to their votes

The solution

- Not sending the votes in plain. Commit!
- When done. All countries open to their votes
- *In addition our solution is additively homomorphic, making it possible to anonymize the entire voting process

The solution

- Not sending the votes in plain. Commit!
- When done. All countries open to their votes
- *In addition our solution is additively homomorphic, making it possible to anonymize the entire voting process
- But might ruin the dramatics of the voting count up

Our Scheme

Our Scheme

- Based on linear ECC

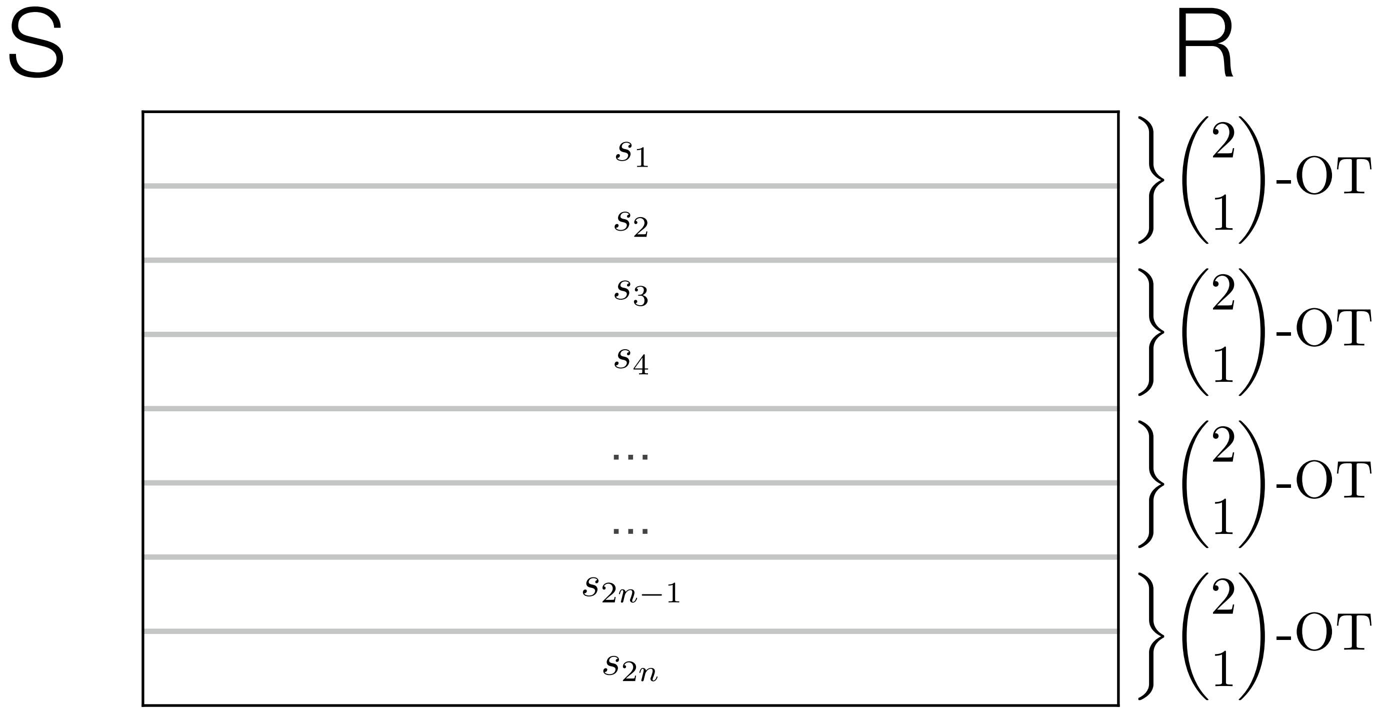
Our Scheme

- Based on linear ECC
- Phrased in OT-hybrid model

Our Scheme

- Based on linear ECC
- Phrased in OT-hybrid model

Do n 1-out-of-2 OT

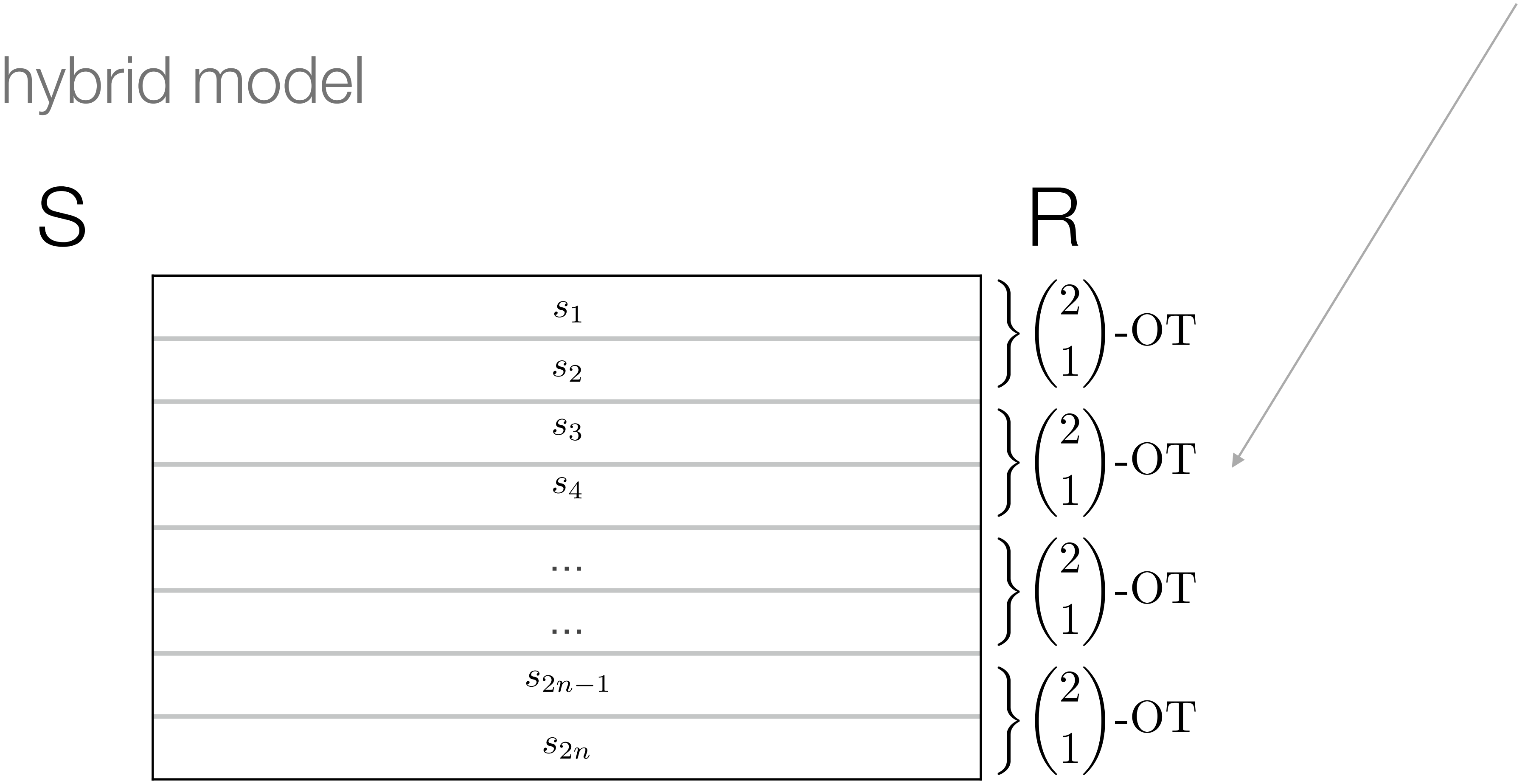


Our Scheme

- Based on linear ECC

Do n 1-out-of-2 OT

- Phrased in OT-hybrid model



S

R

s_1

s_2

s_3

s_4

…

…

s_{2n-1}

s_{2n}

$\binom{2}{1}$-OT

$\binom{2}{1}$-OT

$\binom{2}{1}$-OT

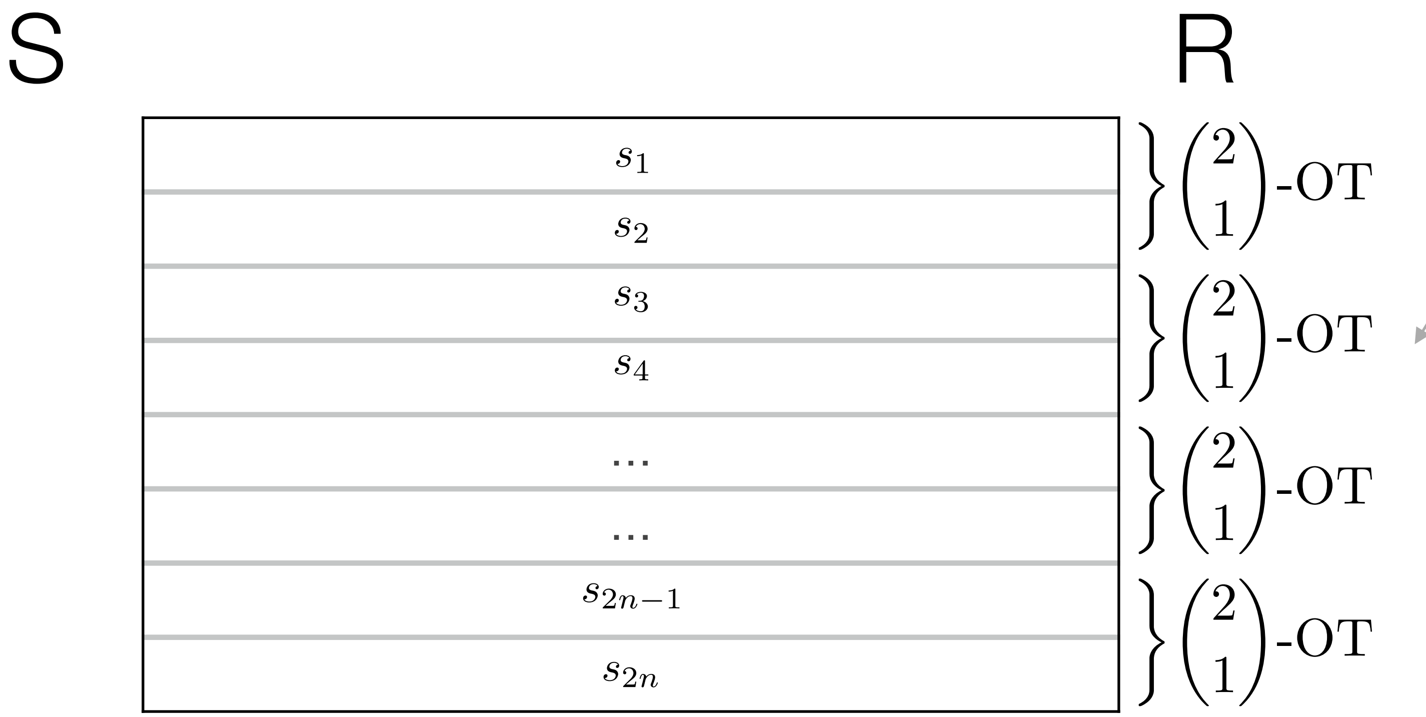
$\binom{2}{1}$-OT

- Means R learns n seeds, based on choice bits in OTs

Our Scheme

- Based on linear ECC
- Phrased in OT-hybrid model

Do n 1-out-of-2 OT



- Means R learns n seeds, based on choice bits in OTs
- Use s_i as seed for PRG and use output y_i as OTP

How to commit

How to commit

- Scheme is based on $[n,k,d]_F$ linear ECC C

How to commit

- Scheme is based on $[n,k,d]_F$ linear ECC C
- Commit to **m**:
  - **z** = C**m**. Now element in F^n

How to commit

- Scheme is based on $[n,k,d]_F$ linear ECC C
- Commit to **m**:
  - **z** = C**m**. Now element in F^n
  - Sample $\mathbf{c_1}$ in_R F^n, set $\mathbf{c_2} = \mathbf{c_1} + \mathbf{z}$ (entry-wise). Additively secret sharing

	$\mathbf{c_1}$
	$\mathbf{c_2}$
+	$\mathbf{z}$

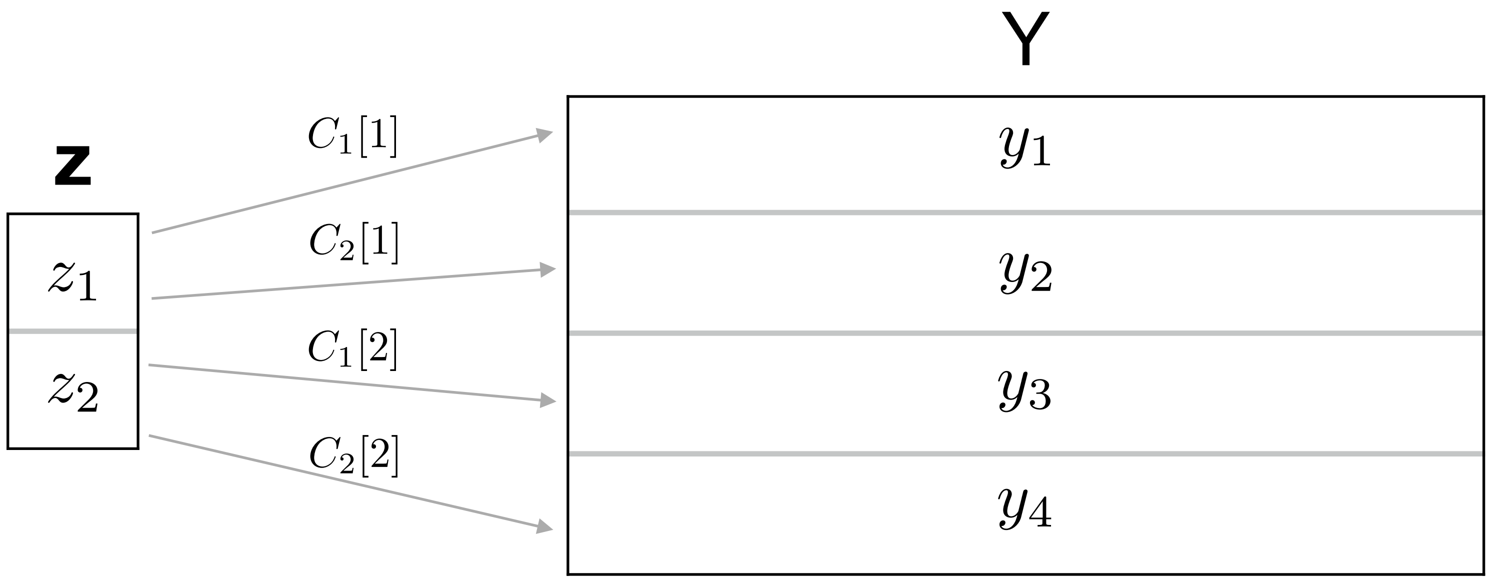
How to commit

- Scheme is based on $[n,k,d]_F$ linear ECC C
- Commit to **m**:
  - **z** = C**m**. Now element in F^n
  - Sample $\mathbf{c_1}$ in$_R$ F^n, set $\mathbf{c_2} = \mathbf{c_1} + \mathbf{z}$ (entry-wise). Additively secret sharing

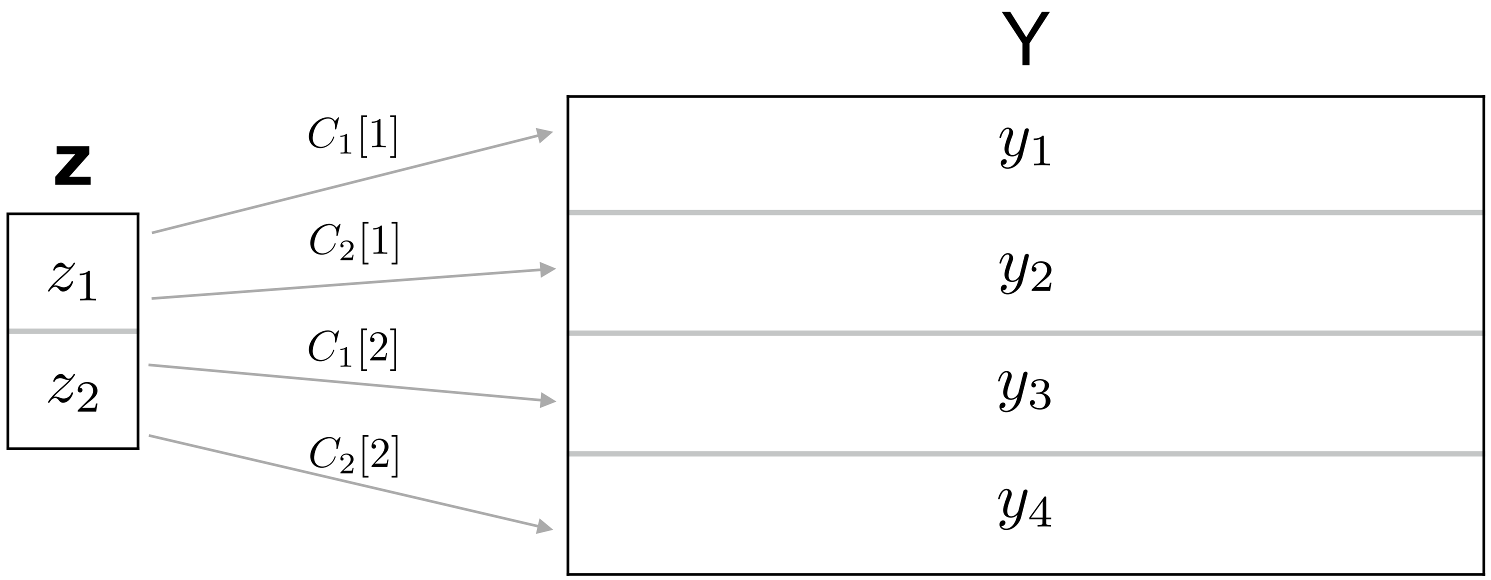
	$\mathbf{c_1}$
	$\mathbf{c_2}$
+	$\mathbf{z}$

  - Entry - and pair-wise pad $\mathbf{c_1}$ and $\mathbf{c_2}$ using the y_i's. Send the padded vectors to R

In a picture

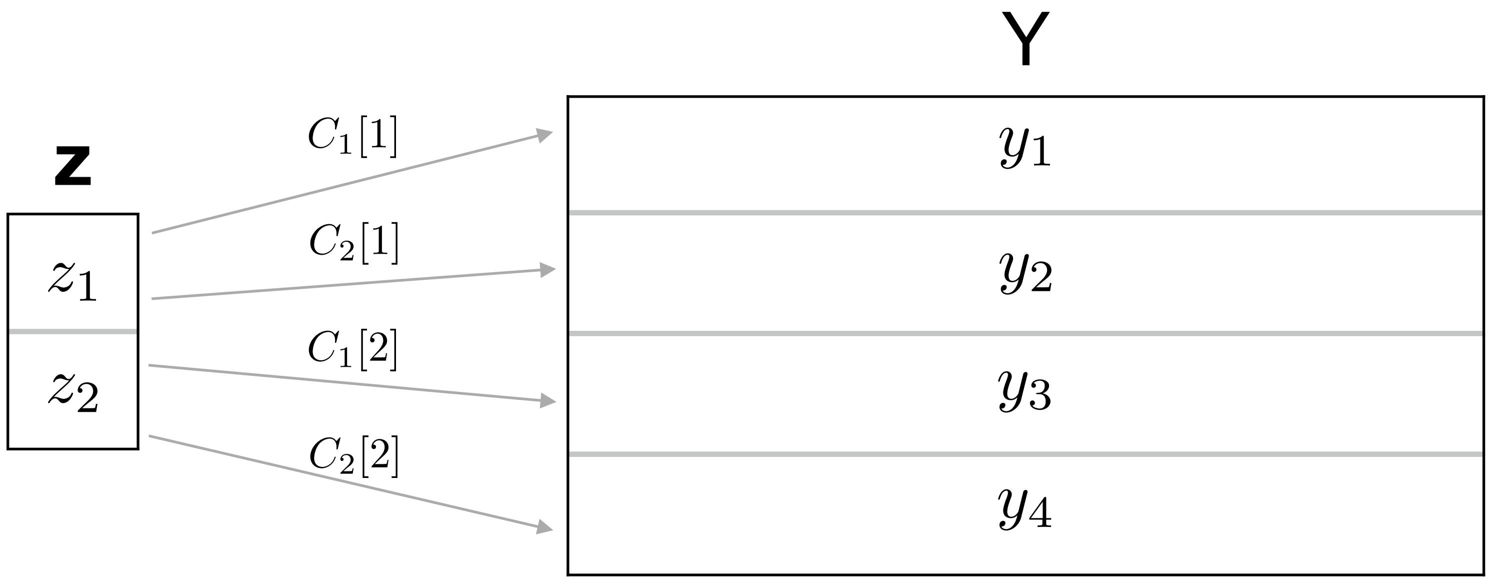


In a picture



- Receiver learns half the shares, i.e. perfectly hiding

In a picture



- Receiver learns half the shares, i.e. perfectly hiding
- Sender unaware which shares are “watched”. Need to change d shares in order to change code-word.
  => Probability of cheating 2^{-d} (more or less)