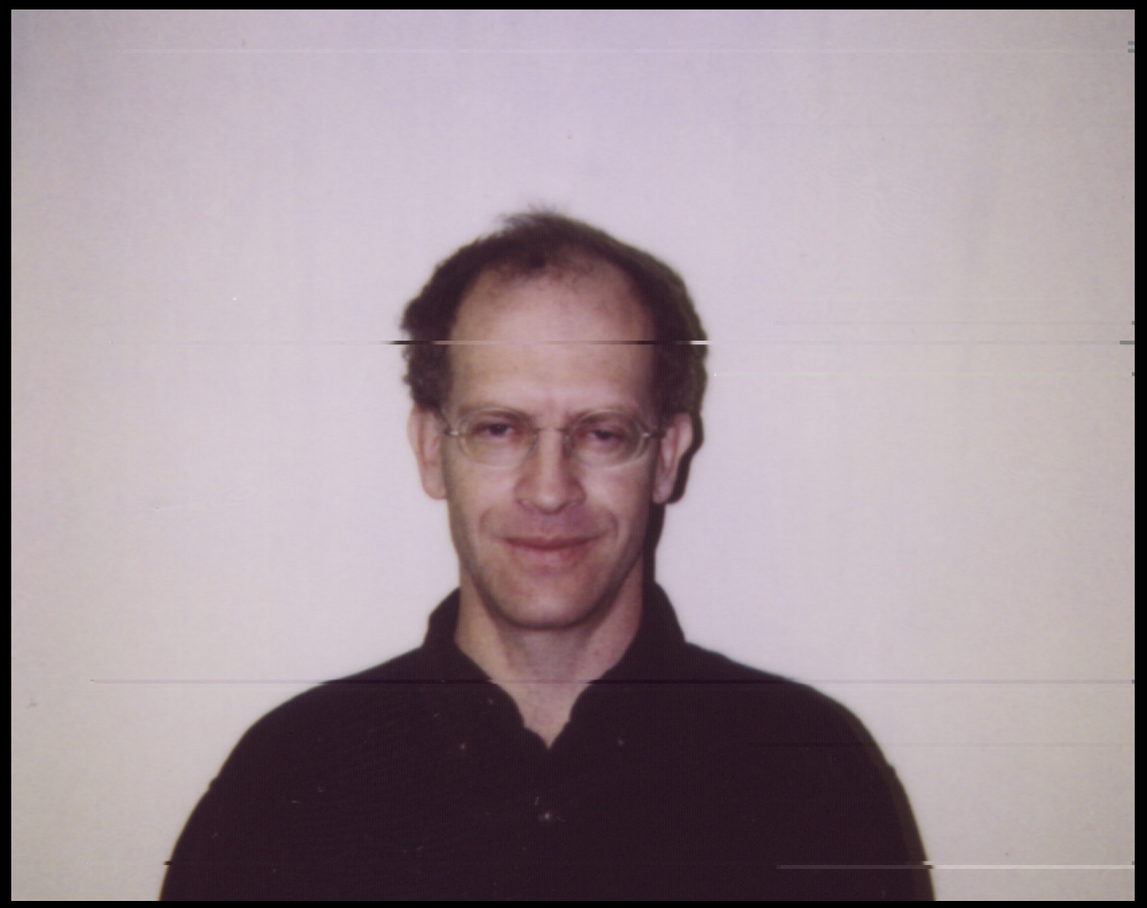
ICSI
30th anniversary celebration

Mike Luby
ICSI Theory group
1988-1999



Theory Group permanent staff

- Richard Karp

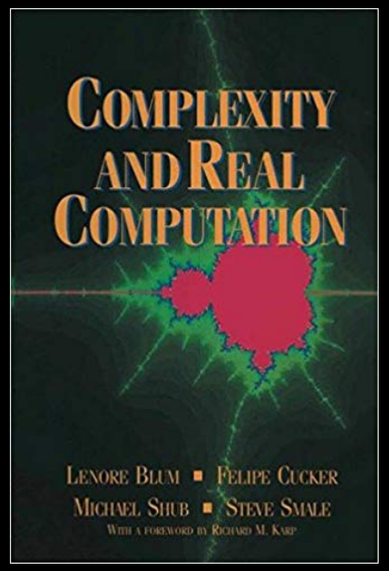
NP-completeness

Algorithms

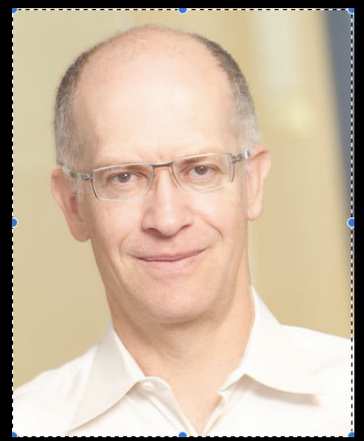
Randomized algorithms

Computational Molecular Biology and Genomics

- Lenore Blum



- Michael Luby



Statement from Professor Karp

My association with ICSI began in 1988 when Founding Director Jerry Feldman decided to include an Algorithms group at the institute. I was the initial group leader, succeeded by Mike Luby, Lenore Blum was a charter member of the group, and Jerry provided significant financial support that allowed the group to run a thriving visiting program for many years.

In 1998, Scott Shenker's invitation to join the excellent ICSI Networking Group enabled me to work out my return to Berkeley from the University of Washington, and I remained happily at ICSI until 2012. I will always be grateful to Director Nelson Morgan for his personal support and enlightened leadership throughout this period.

Visitors

- Professors from Distinguished Full to Just Starting, Researchers, Postdocs, Graduate students, from sponsor countries (Germany, Italy, …) and elsewhere (U.S., Israel, Canada, Sweden, …)
- A Snapshot: Friedhelm Meyer auf de Heide, Marek Karpinski, Emo Welzl, Amin Shokrollahi, Alberto Marchetti-Spacamella, Volker Stemann, Johannes Bloemer, Avi Wigderson, Oded Goldreich, Nati Linial, Amos Fiat, Noga Alon, Johan Hastad, Allan Borodin, Alistair Sinclair, …

My focus at ICSI

- Cryptography and Security
- Coding Theory
- Transmission Protocols

- Parallel and Distributed Computation
- Derandomizing Algorithms
- Monte Carlo Algorithms for Hard Counting Problems
- Self-Testing/Correcting Programs
- Optimal Simulation
- Neural and Belief Networks
- Online Algorithms

Deconstructing Luby

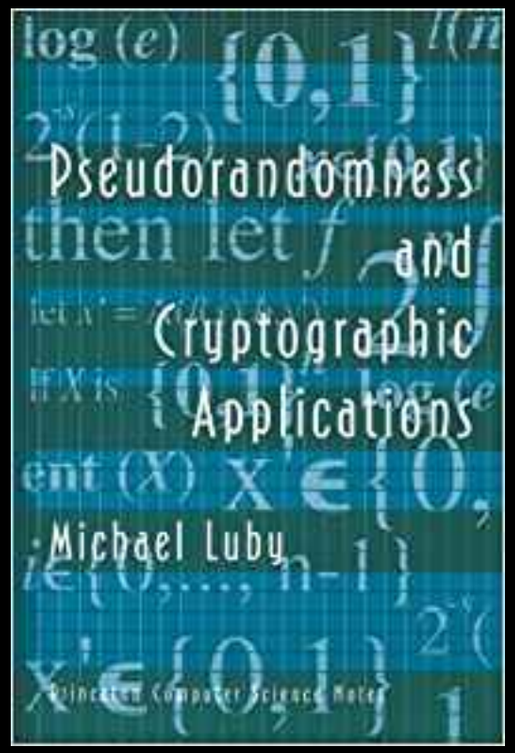
one can and cannot use
a trick used by Luby
the one used by Luby
obtaining the expected
Luby's method to make
what is desired
behavior of the greedy
still adhering
Luby's techniques
take advantage of the freedom
brute force is too
possible with the Luby
give ourselves a fighting chance
observe that Luby

by Prabhakar Ragde

Published in the Volume 22, Number 2, Spring 1991 issue of SIGACT News.

Cryptography

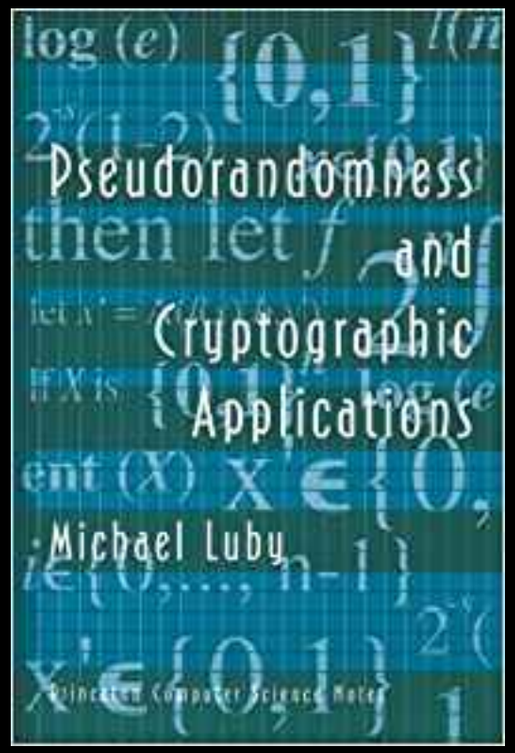
Pseudorandomness and Cryptographic Applications
Michael Luby
Princeton Computer Science Notes
Princeton University Press
David R. Hanson and Robert E. Tarjan, Editors,
Princeton University Press, January 1996



A Pseudorandom generator from any one-way function
Johan Hastad, Russell Impagliazzo, Leonid Levin, Michael Luby
STOC, 1989, SIAM J. on Computing, 1999

Cryptography

Pseudorandomness and Cryptographic Applications
Michael Luby
Princeton Computer Science Notes
Princeton University Press
David R. Hanson and Robert E. Tarjan, Editors,
Princeton University Press, January 1996



A Pseudorandom generator from any one-way function
Johan Hastad, Russell Impagliazzo, Leonid Levin, Michael Luby
STOC, 1989, SIAM J. on Computing, 1999

SIAM Outstanding Paper Prize (2003)

Coding Theory

Practical Loss-Resilient Codes
Michael G. Luby, Michael Mitzenmacher, Amin Shokrollahi, Daniel Spielman, Volker Stemann, STOC, 1997

Analysis of Low Density Codes and Improved Designs Using Irregular Graphs
Michael G. Luby, Michael Mitzenmacher, Amin Shokrollahi, Daniel Spielman
ICSI TR-97-045,1997, STOC, 1998

Improved Low-Density Parity-Check Codes Using Irregular Graphs and Belief Propagation
Michael G. Luby, Michael Mitzenmacher, Amin Shokrollahi, Daniel Spielman
ICSI TR-97-044, 1997. IEEE International Symposium on Information Theory, 1998

Coding Theory

Practical Loss-Resilient Codes
Michael G. Luby, Michael Mitzenmacher, Amin Shokrollahi, Daniel Spielman, Volker Stemann, STOC, 1997

Analysis of Low Density Codes and Improved Designs Using Irregular Graphs
Michael G. Luby, Michael Mitzenmacher, Amin Shokrollahi, Daniel Spielman
ICSI TR-97-045,1997, STOC, 1998

Improved Low-Density Parity-Check Codes Using Irregular Graphs and Belief Propagation
Michael G. Luby, Michael Mitzenmacher, Amin Shokrollahi, Daniel Spielman
ICSI TR-97-044, 1997. IEEE International Symposium on Information Theory, 1998

Multiple awards and medals
Basis for RaptorQ codes
Basis for LDPC codes used at physical layer in 5G

Transmission Protocols

Priority Encoding Transmission
Andres Albanese, Johannes Bloemer, Jeff Edmonds, Michael Luby, Madhu Sudan
FOCS, 1994, IEEE Transactions on Information Theory, 1996

A Digital Fountain Approach to Reliable Distribution of Bulk Data
John Byers, Michael Luby, Michael Mitzenmacher, Ashu Rege
ICSI Technical Report TR-98-005, 1998, ACM SIGCOMM, 1998

A Modular Analysis of Network Transmission Protocols
Micah Adler, Yair Bartal, John Byers, Michael Luby, Danny Raz
Proceedings of the Israeli Symposium on Theory of Computing and Systems, 1997

Transmission Protocols

Priority Encoding Transmission
Andres Albanese, Johannes Bloemer, Jeff Edmonds, Michael Luby, Madhu Sudan
FOCS, 1994, IEEE Transactions on Information Theory, 1996

Original motivation for the coding work

A Digital Fountain Approach to Reliable Distribution of Bulk Data
John Byers, Michael Luby, Michael Mitzenmacher, Ashu Rege
ICSI Technical Report TR-98-005, 1998, ACM SIGCOMM, 1998

ACM SIGCOMM Test of Time Award (2009)

A Modular Analysis of Network Transmission Protocols
Micah Adler, Yair Bartal, John Byers, Michael Luby, Danny Raz
Proceedings of the Israeli Symposium on Theory of Computing and Systems, 1997

Key component to some of the streaming work at Qualcomm

Some Success Stories

Christian Leicher
THEN:
- Visiting member of the ICSI Network Group
- Key contributor to the PET project

NOW:
- President and CEO of Rohdes and Schwarz, Munich

Alistair Sinclair
THEN:
- Visiting postdoc of the ICSI Theory Group
- Key contributor to randomized algorithm research

NOW:
- Founding Associate Director of the Simons Institute for Theory of Computing
- Professor at UC Berkeley

Some Success Stories

Paul Dagum
THEN:
- My PhD Student in ICSI Theory Group (from Toronto)
- Key contributor to randomized algorithms

NOW:
- Founder and CEO of MindStrong

Amin Shokrollahi
THEN:
- Visiting postdoc of the ICSI Theory Group
- Key contributor to coding theory

NOW:
- Professor at EPFL, Lausanne Switzerland
- Founder and CEO of Kandou

Digital Fountain

Overview

- Startup based in Bay Area, 1999-2009
- LT codes, Raptor codes (IETF RFC 5053) and more advanced variants
- Reliable delivery and video streaming software using Raptor codes

Deployments

- Digital dailies for major studios (Harry Potter, Lord of the Rings, Fast and Furious, …)
- Defense apps (Rescue of Jessica Lynch, Globalhawk,…)
- IPTV deployments (NTTs in Japan, Netherlands)
- Satellite data delivery (USPS, Sirius/XM)


HOTEL

Qualcomm

Overview

- Acquired Digital Fountain in 2009
- RaptorQ codes (IETF RFC 6330)
- Video streaming, distributed storage

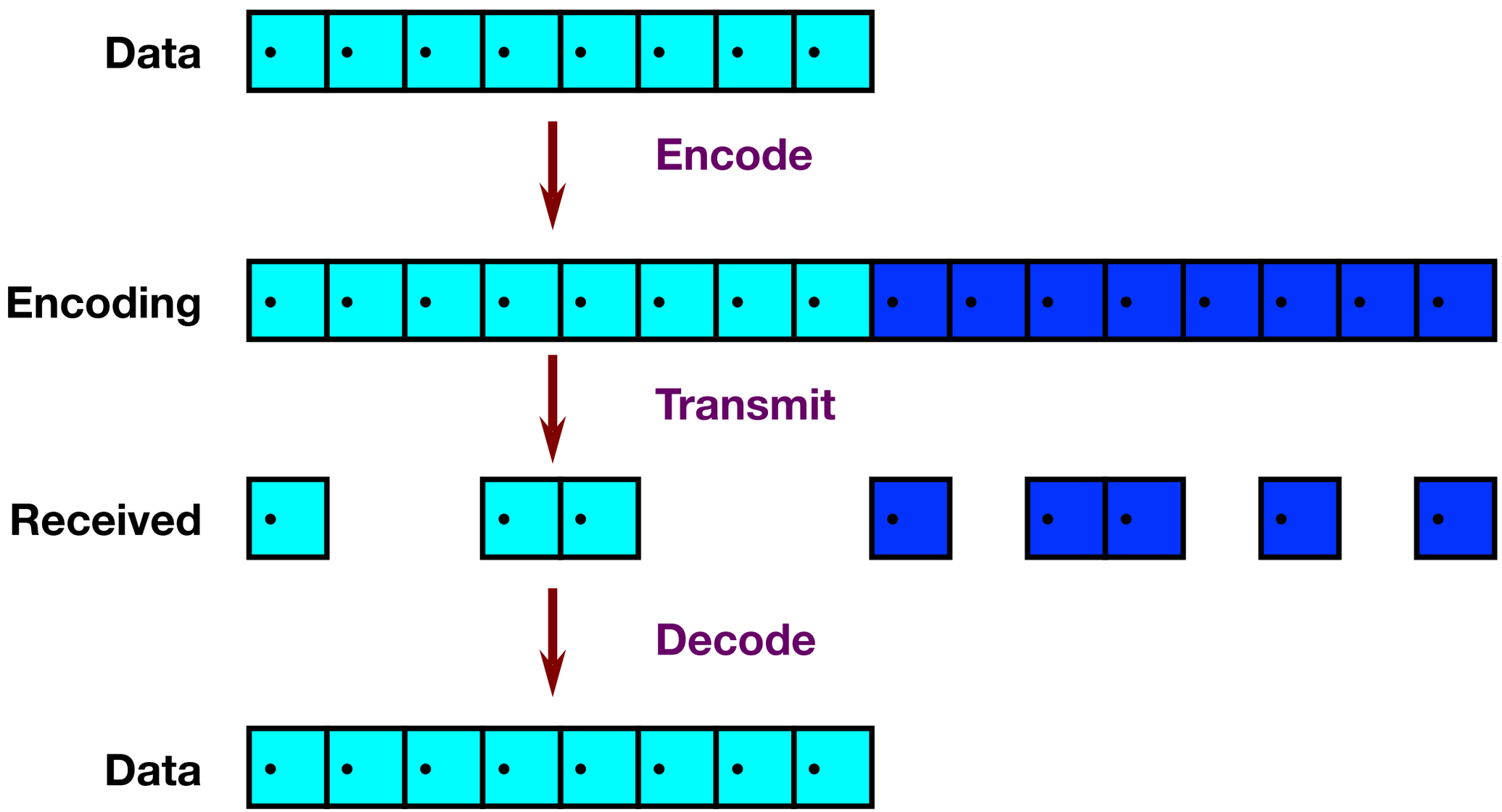
Deployments

- 3GPP Multimedia Broadcast/Multicast Services
- Licensed for a variety of use cases, commercial and defense


QUALCOMM
SEARCH BERKELEY
10/05/2012


Berkeley
Trevor Darrell
Berkeley
Bom Hartmann
10/05/2012

Erasure Code



What is a fountain code?

- Generate as much encoding as desired
- Recover data from the minimal possible encoding
  - It doesn’t matter what is received or lost
  - It only matters that enough is received

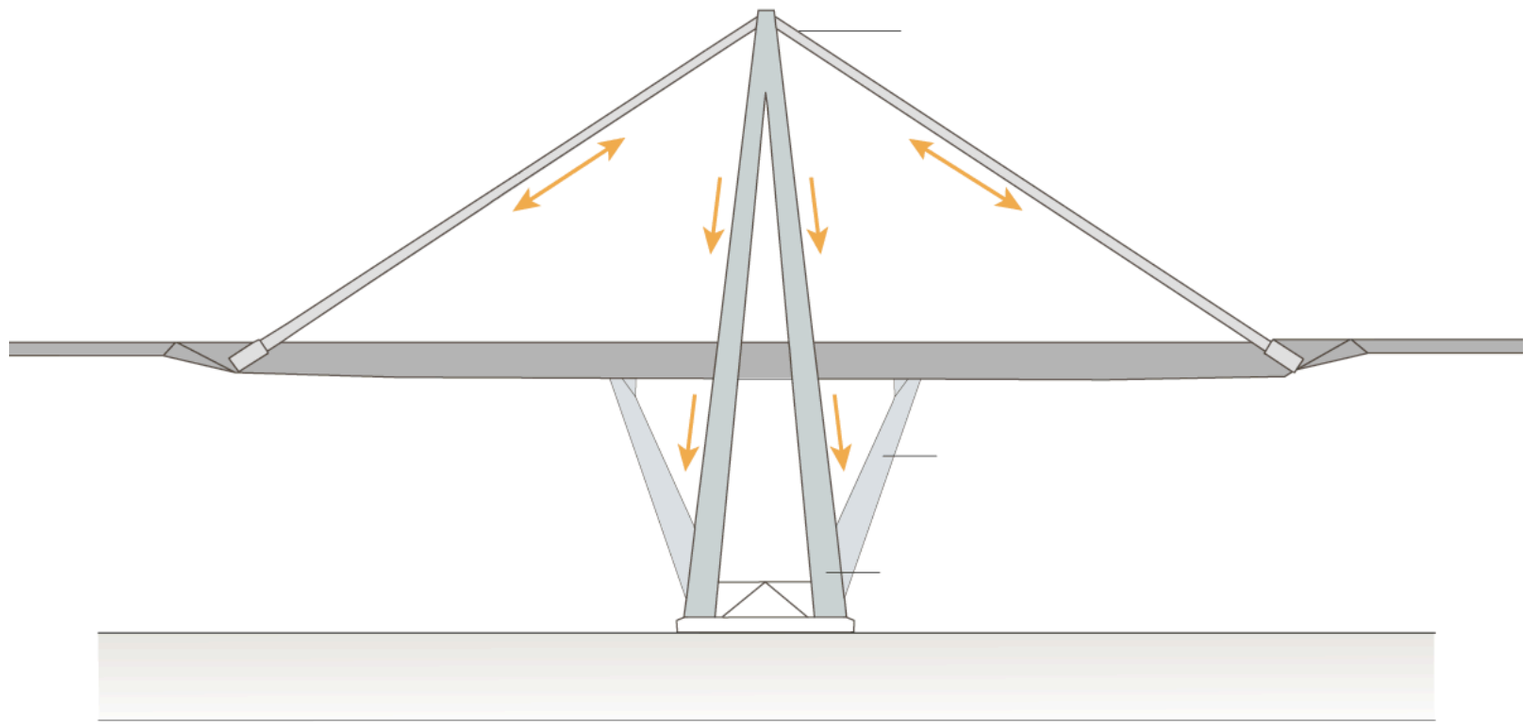
Raptor and RaptorQ properties

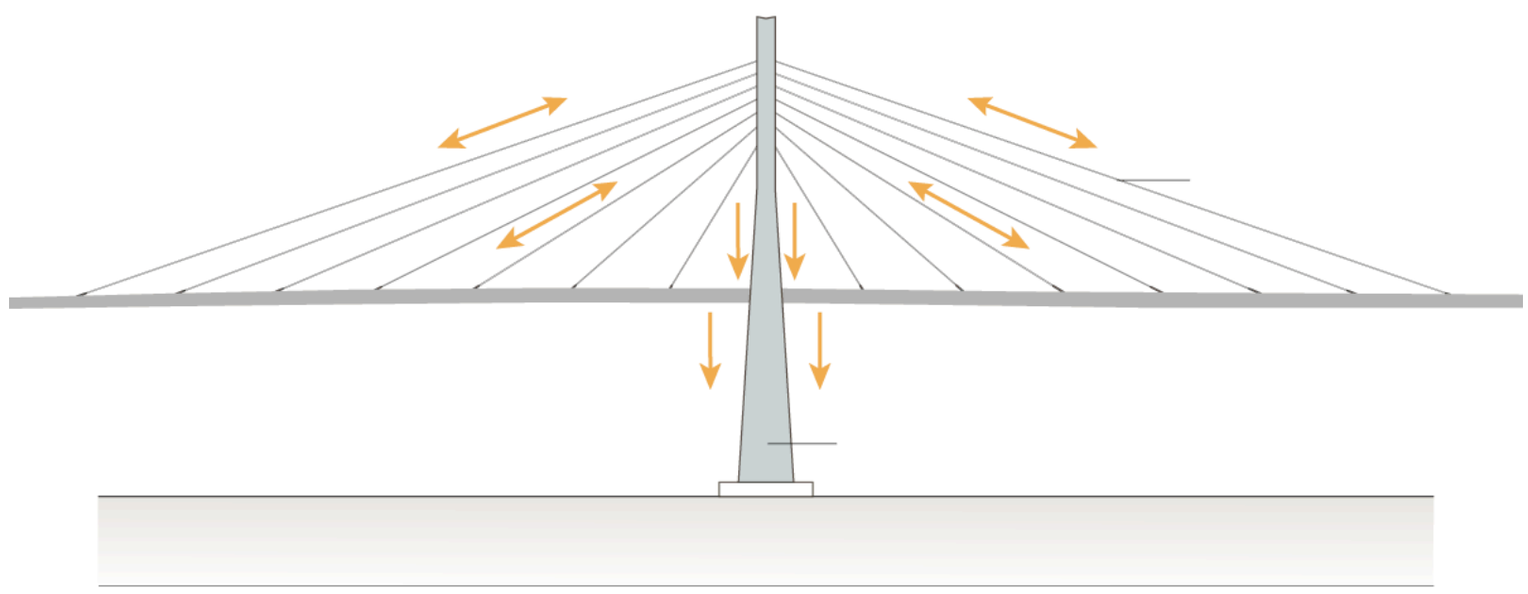
- Raptor codes
  - ➢ Fountain codes
  - ➢ Good recovery properties – like a random code over GF(2)
  - ➢ **Linear time encoding and decoding — 10+ Gbps on a single core**
  - ➢ **Standardized – IETF RFC 5053, 3GPP Multimedia Broadcast/Multicast Services**

- RaptorQ codes
  - ➢ Fountain codes
  - ➢ **Great recovery properties – like a random code over GF(256)**
  - ➢ Linear time encoding and decoding — 10+ Gbps on a single core
  - ➢ **Standardized – IETF RFC 6330, Advanced Television Systems Committee 3.0**

An analogy to civil engineering

How the Morandi Bridge (Genoa) compares to modern bridges





ICSI — Codornices Project

- Team launched project September 2018
- Develop high performance implementation of RaptorQ
- Develop application software around RaptorQ
- Develop software that support various standards RaptorQ use cases

Codornices Team

Pooja Aggarwal **Lorenz Minder**

Thanks!