$(SAC)^{25}$ – A Retrospective

Carlisle Adams
August 16, 2018

Beginnings

Stafford Tavares

Idea (early 1990s):

- *Canadian venue for crypto research*
- *Small, friendly workshop*
- *“discussion atmosphere”*

What to call it?

- Stafford and one of his students, Art Webster, defined a property that they called the “Strict Avalanche Criterion” (SAC) in a paper published at Crypto 1985
  - SAC is a formalization of the “avalanche effect” (a concept explored by Shannon and named by Feistel) and incorporates the notion of “completeness”

Avalanche

Small disturbance leads to large, unpredictable change

SAC: if a single input bit is complemented, each output bit changes with probability $p = 0.5$

http://nsidc.org/cryosphere/snow/science/avalanches.html

What to call the workshop?

- "Avalanche effect" and "SAC" were fundamental and important work for symmetric cipher design (particularly s-box design), but Crypto and Eurocrypt were receiving lots of submissions from many other exciting advances in the field

  (zero knowledge protocols, secret sharing schemes, digital signatures, elliptic curve computations, etc., etc.)

- "Selected Areas in Cryptography" (SAC) ☺

Organizers of the first SAC Workshop

Stafford Tavares

Henk Meijer

Paul Van Oorschot

Carlisle Adams

Walter Light Hall

Queen's University at Kingston

May 5-6, 1994

Governance

- SAC Organizing Board
  - 9 members, each serving a 3-year term. One member is the Board Chair.
  - Each year, the terms of 3 members end. Each of these members may be replaced, or may serve another term.
- SAC Conference
  - 3 permanent topics, plus a 4th topic that can vary from year to year.
- SAC Co-Chairs
  - Normally 2 fully-cooperating co-chairs, although from 2001 typically one (Canadian) has primary responsibility for local arrangements, and one (residing outside Canada) focuses on the technical program.
- SAC Financial Management
  - Each conference is budgeted to break even (any surpluses are accumulated in a long-term account).

Note: after a few years…

Stafford Tavares

Henk Meijer

Paul Van Oorschot

Carlisle Adams

SAC: "Stafford And Carlisle" Workshop ☺

Growth

Growth: Location

Kingston, ON (1994) (5)

Ottawa, ON (1995) (5)

Waterloo, ON (2000) (3)

Toronto, ON (2001) (2)

St. John's, NF (2002) (2)

Montreal, QC (2006) (2)

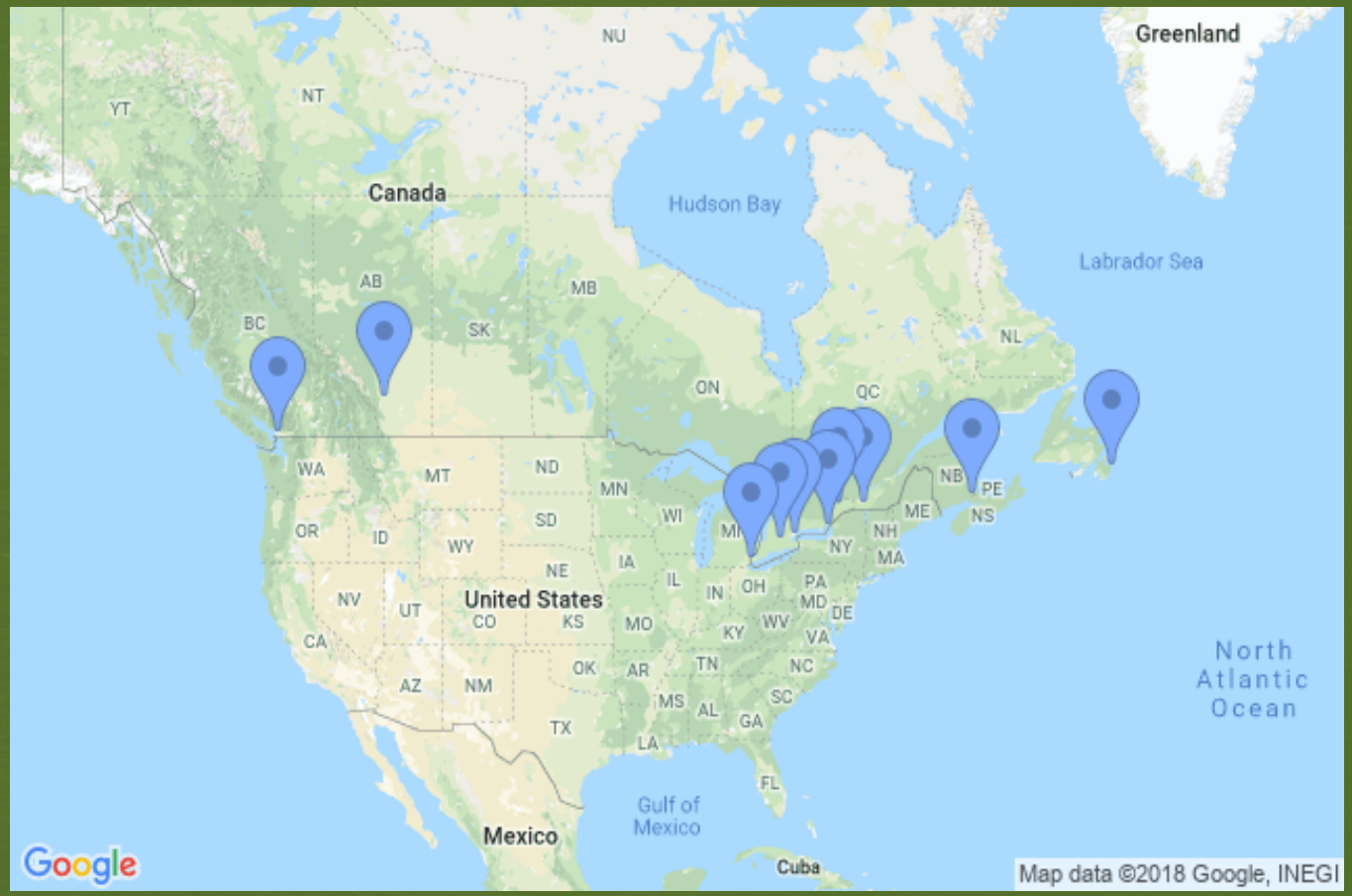
Sackville, NB (2008) (2)

Calgary, AB (2009) (2)

Windsor, ON (2012) (1)

Burnaby, BC (2013) (1)

Co-chairs: C. Adams, H. Heys, L. Keliher, A. Youssef (11 times out of 25!)



Growth: Timing

- Move from May to August (just before Crypto) in 1996
- Move from 2-day to 3-day format in 2013
- Move to 5-day format in 2015

Growth: Scope

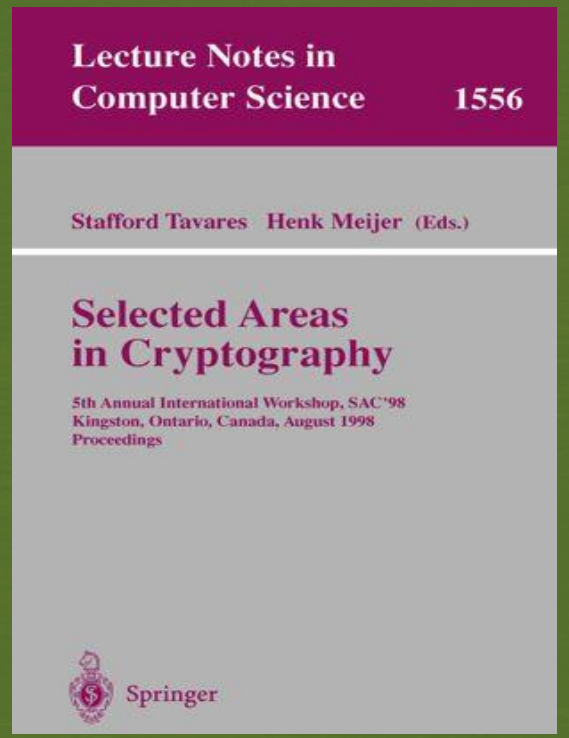
SAC Summer School (S3)

- Opportunity to gain in-depth knowledge in topics of SAC
- World-class researchers give extended talks in their areas of specialty
- Focused, but relaxed, learning environment

Special thanks to Orr Dunkelman!

Growth: Status

- Springer LNCS proceedings (1998)
- "In Cooperation with IACR" (2006)
- SAC permanent website (2010)
  - Special thanks to Aleks Essex!
- "Workshop" → "Conference" (2011)



In Cooperation with IACR

Impact

Impact: Acceptance Rates (%)

Average: 36.6

Average (since 2002): 28.9

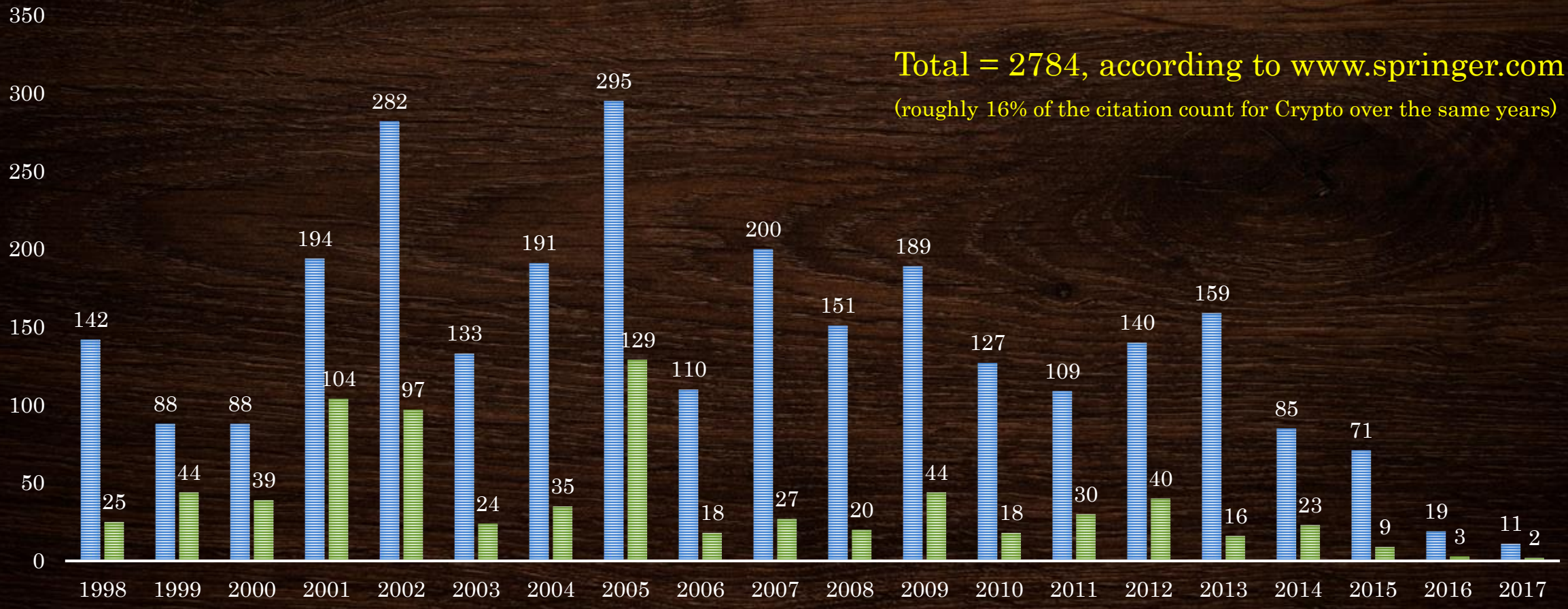
Impact: Participation

- E.g., 2014: 30 countries represented

- E.g., 2016: 70 participants
  - 30 students, 40 non-students
  - 27 Canadian, 43 international

- Each year: Good mix of industry / government / academia

Impact: Citations (on August 2nd, 2018)



Total = 2784, according to www.springer.com

(roughly 16% of the citation count for Crypto over the same years)

Citations for LNCS Proceedings

Top-cited paper in Proceedings

Impact: Invited Speakers

Jacques Patarin
Andrey Bogdanov
Phong Nguyen
Jan Camenisch
Nicolas Courtois
Paulo Barreto
Avi Rubin
Paul Syverson
Dan Bernstein
Hugh Williams
Kaisa Nyberg
Nigel Smart
Mihir Bellare
Miles Smid
Keith Martin
Serge Vaudenay
Eli Biham
Vincent Rijmen
Anne Canteaut
Doug Stinson
Steve Babbage
David Wagner
Richard Kemmerer
Chris Peikert
Kristin Lauter
Pierrick Gaudry
Bart Preneel
Adi Shamir
Alfred Menezes
Yevgeniy Dodis
Alexandra Boldyreva
Michael Wiener
Joseph Silverman
Phil Zimmermann
Gaetan Leurent
Virgil Gligor
Dan Boneh
Helena Handschuh
Mike Reiter
Lars Knudsen
Antoine Joux
Moti Yung
Andreas Enge
Ian Goldberg
Francesco Regazzoni
Douglas Stebila
Stafford Tavares

"Who's who" of the cryptography/security/privacy fields!

Highlights

Special Memories

- People (and papers)

https://www.google.com/search?q=pictures+of+cartoons+listening+to+a+seminar&tbm=isch&imgil=UMHWua7lTCJlvM%253A%253Bpsd4tTFKqm5EVM%253Bhttps%25253A%25252F%25252Fblogs.synopsys.com%25252Fthelisteningpost%25252F2010%25252F05%25252Fif-a-picture-says-a-thousand-words%25252F&source=iu&pf=m&fir=UMHWua7lTCJlvM%253A%252Cpsd4tTFKqm5EVM%252C_&biw=1366&bih=603&usg=__c-cNnAgDC8vwiCp0R3SSKx9hEYo%3D&ved=0CDsQyjdqFQoTCIiq877z3ccCFcldHgodv4kL0g&ei=ktTpVYiZMMm7eb-TrpAN#imgrc=-CCkZLDs5aUIDM

Special Memories

- People (and papers)
- Invited talks
- Locations
- Banquets and social events
- …

- But one particular memory stands out above all the others…

SAC, August 14-15, 2003

- The 10th SAC was hosted in Ottawa by Mitsuru Matsui and Robert Zuccherato
- Lots of worrying about the hundreds of small details associated with organizing a workshop
- On the 14th, everything went perfectly all day…

… and then at 4:10 p.m. the projector went out!

- *"At the time, it was the world's second most widespread blackout in history…. The outage … affected an estimated 10 million people in Ontario and 45 million people in eight U.S. states."*

(https://en.wikipedia.org/wiki/Northeast_blackout_of_2003)

States and provinces that experienced power outages (https://en.wikipedia.org/wiki/Northeast_blackout_of_2003)

Toronto, on the evening of August 14, 2003 (https://en.wikipedia.org/wiki/Northeast_blackout_of_2003)

SAC, August 14-15, 2003

- In Ottawa, the blackout lasted until late in the day on August 15th (i.e., until the end of SAC) ☺
  - For the banquet on Thursday evening, the conference staff at Carleton University quickly improvised beautifully
  - All the Friday talks were done in an "unplugged" format with blackboards and chalk
- Instead of being a disaster, there was a warm, intimate, collegial atmosphere and 2003 turned out to be one of my favourite SACs!

Future

Looking Ahead…

- SAC has had a successful past and is seeing an exciting present; there is every reason to expect a bright future!

- I encourage all participants – those who organize, and those who contribute their research / expertise / presence – to keep moving SAC forward, but never forget its roots & character

- What makes SAC special?
  - High-quality research
  - Small, friendly group of attendees
  - Hobnob with the big names in the field

To Sum Up

- *It has been a terrific and rewarding 25 years*
- *I look forward to lots of exciting SAC Conferences in the years to come!*

Thank you!