LCS35 Time-Lock Crypto Puzzle

Ronald L. Rivest

MIT

May 15, 2019

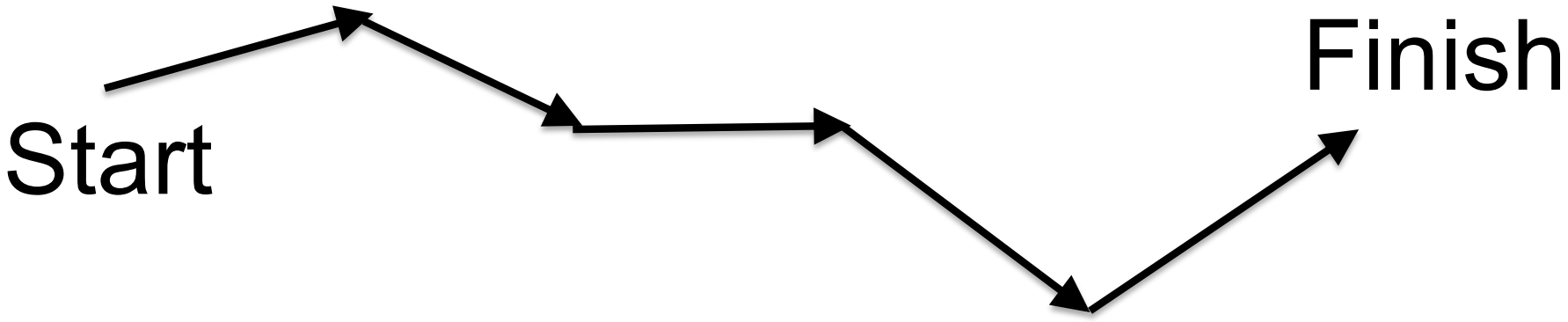
Outline

- Rivest-Shamir-Wagner puzzle design
- LCS 35th Celebration (April 12-13, 1999)
- Creation of LCS35 Time Capsule Crypto Puzzle
- Solution(s)

Can two women have a baby in 4.5 months?

Intrinsically Sequential Computations

- Can’t be sped up using parallelism
- Can be created to require a certain chosen number of operations (in series)



Time-Lock Puzzle Design

- Create $n = pq$ as product of two primes
- Choose t as number of operations required
- Publish (n, t) as puzzle description
- Puzzle: compute $2^{2^t} \pmod n$
- Method (repeated squarings):
  - $a_0 = 2 \ (mod \ n)$
  - $a_i = a_{\{i-1\}}^2 (mod \ n)$ for $i = 1, 2, \ldots, t$
  - Solution is a_t

Embedding a message *M*

- Puzzle creator knows prime factors p, q
- Puzzle creator can compute a_t quickly
- Publish

$$C = M \oplus a_t$$

(Here $\oplus$ denotes "exclusive or".)

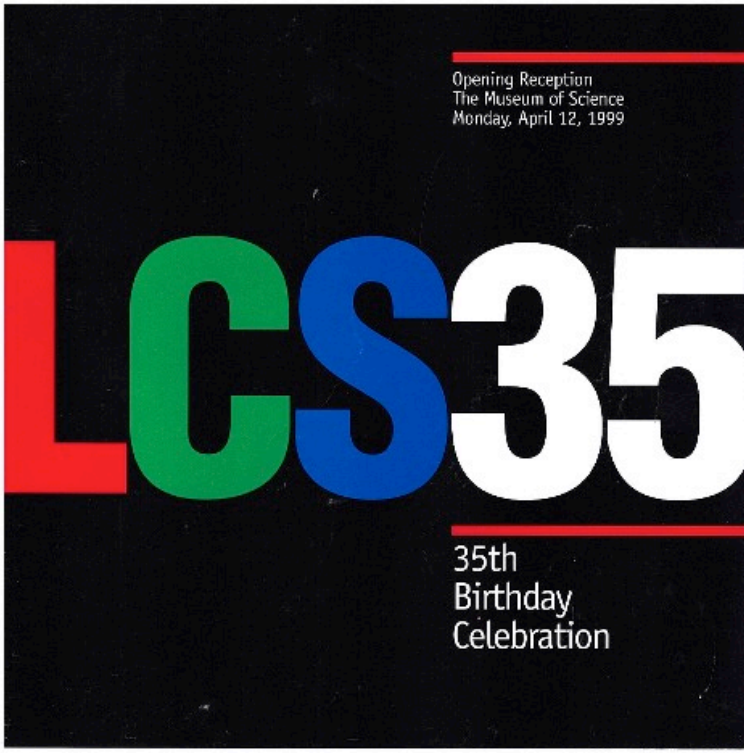
- Puzzle solver can compute a_t (with t squarings), and then compute

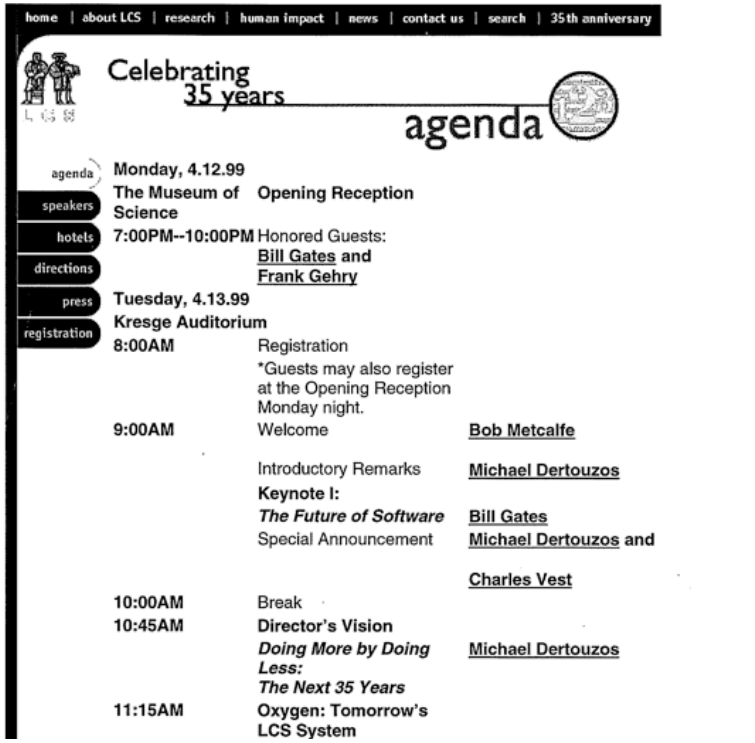
$$M = C \oplus a\_t$$

- (Rivest, Shamir, Wagner 1996)

LCS 35th Celebration
April 12-13, 1999

- Laboratory for Computer Science created 1963 as “Project MAC”
- Mike Dertouzos, Director 1974--2001





Time Capsule & Puzzle

- Celebration featured a Gehry-designed “time capsule” with significant artifacts from LCS history, to be opened in “35 years”.
- Actually, capsule to be opened when “Time Capsule Crypto-Puzzle” I supplied was solved.
- So, I needed to create a “35-year puzzle”…

Choosing puzzle parameters n, t

- Choose n as product of two 1024-bit primes.
- 3000 squarings/second in 1999 (Java)
- Moore's Law model:

  22.0% faster / year until 2012 (13x total), then

  7.5% faster / year thereafter (5x total)
- Squarings (first year) = 94.6G
- Squarings (total, 35 years) = t

$$t = 79685186856218 \approx 80T$$

Time Capsule Created & Loaded

Bill Gates

Solution !!!

Solution!!

– Bernard Fabrot
  - Solved April 15, 2019 (exactly 20 years from LCS35th!)
  - Email April 16, 2019
  - Software-based approach
  - 3 years + 3 months of computation
  - Message = “!!! Happy Birthday LCS !!! (numeric values)”

Second solution (!!!)

"Cryptophage" collaboration

- Supranational (Simon Peffers)
- Sabanci University (Turkey) (Erdinc Ozturk)
- Ethereum Foundation (Justin Drake)
- Protocol Laboratories (Jeromy Johnson)

- Email April 17, 2019 (one day later!)
- Solved May 10, 2019
- FPGA-based approach
- 2 months of computation

Next

- Presentation of awards
- Presentation by Bernard Fabrot
- Presentation by Simon Peffers
- Break (Food & Drink in R&D Lounge)
- Opening & Refreshing of Time Capsule (Daniela Rus, CSAIL Director)
- [Thanks to Lauralyn Smith and Shacie Garcia for organizational help]
- [Thanks to Terrapass for carbon offset]