CRYPTO IN 2030

Jean-Jacques Quisquater

UCL CRYPTO

Rump session CRYPTO 2015, Santa Barbara

TODAY CRYPTO 2015

- Conference
- Number 35 (each year since 1981)
- I just wanted to say Ha …
- But there is a birhday attack!

THE ATTACK: HAPPY BIRTHDAY

See https://en.wikipedia.org/wiki/Happy_Birthday_to_You

"Happy Birthday to You" first appeared in print in 1912

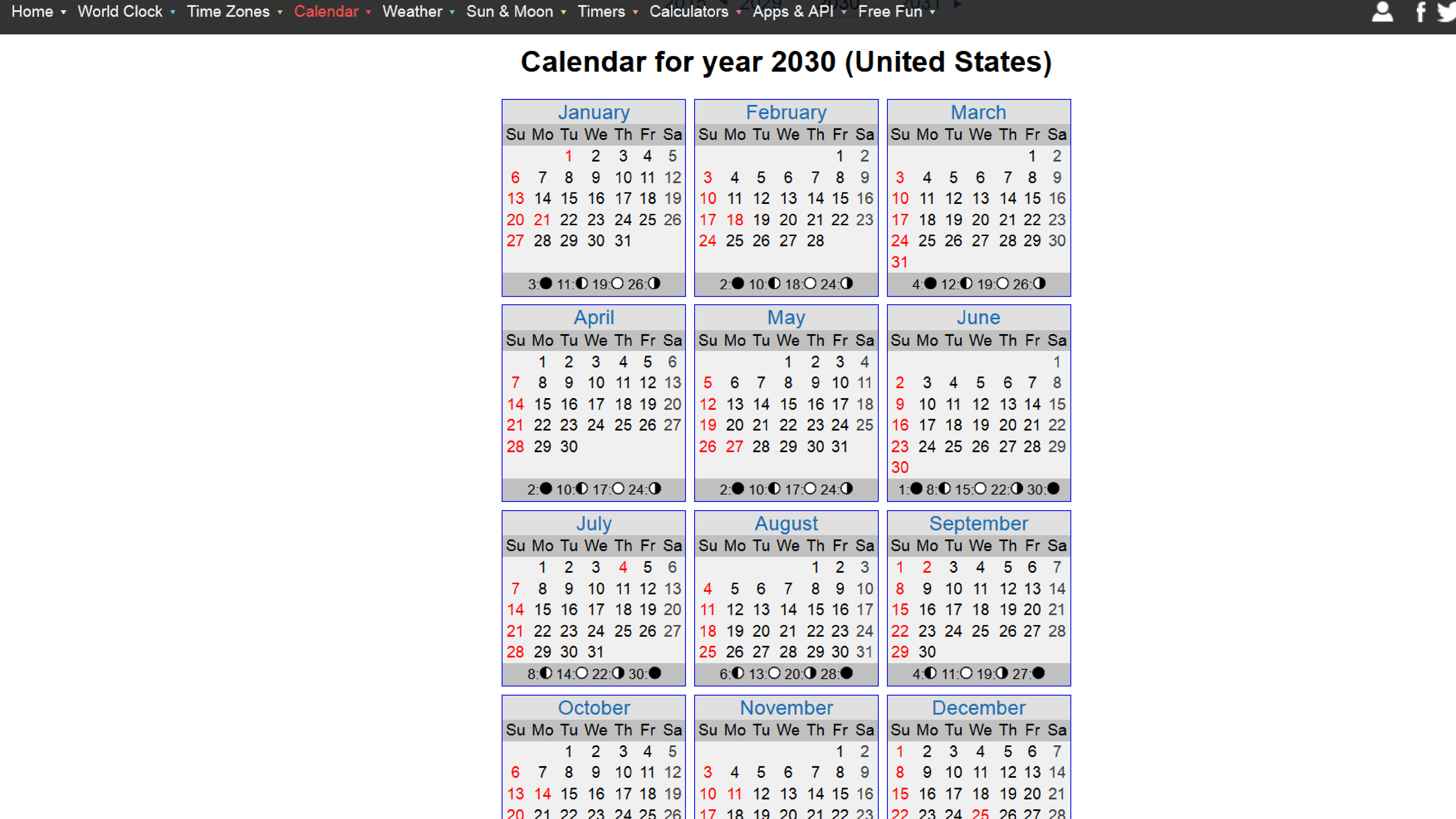
Based on the 1935 copyright registration, Warner claims that the United States copyright will not expire until **2030** (31 December 2016 in Europe)

unauthorized public performances of the song are technically illegal unless royalties are paid to Warner

(get $ 2 millions each year …)

WAITING UNTIL 2030 …

- So we can imagine what CRYPTO 2030 will be
- Not so different (see 2000 and today)
- When?



Calendar for year 2030 (United States)

January

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

3:● 11:◐ 19:○ 26:◑

February

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28		

2:● 10:◐ 18:○ 24:◑

March

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

4:● 12:◐ 19:○ 26:◑

April

Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

2:● 10:◐ 17:○ 24:◑

May

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

2:● 10:◐ 17:○ 24:◑

June

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

1:● 8:◐ 15:○ 22:◑ 30:●

July

Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

8:◐ 14:○ 22:◑ 30:●

August

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

6:◐ 13:○ 20:◑ 28:●

September

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

4:◐ 11:○ 19:◑ 27:●

October

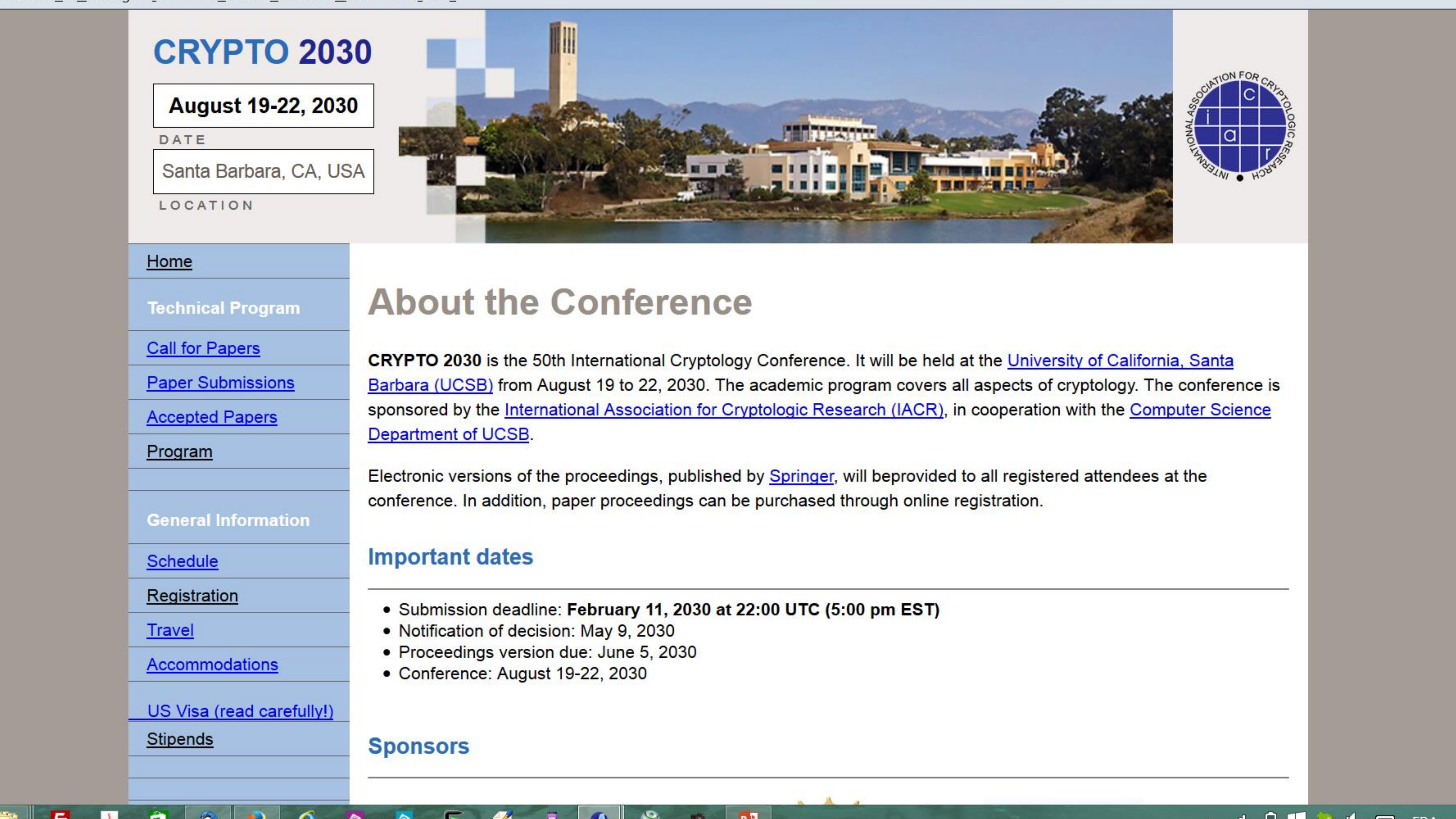
Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26

November

Su	Mo	Tu	We	Th	Fr	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23

December

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28



CRYPTO 2030

August 19-22, 2030

DATE

Santa Barbara, CA, USA

LOCATION

About the Conference

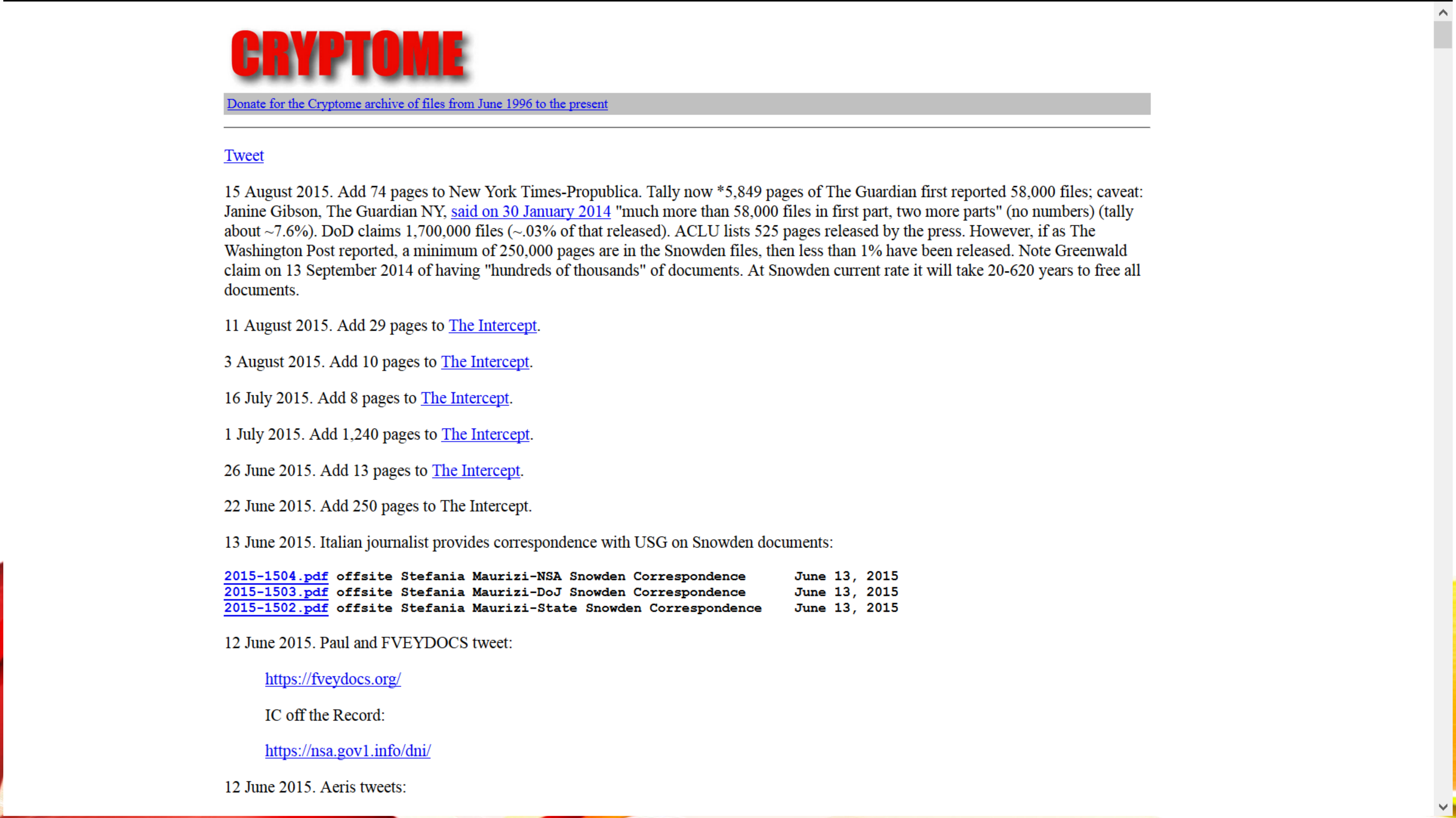
CRYPTO 2030 is the 50th International Cryptology Conference. It will be held at the University of California, Santa Barbara (UCSB) from August 19 to 22, 2030. The academic program covers all aspects of cryptology. The conference is sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the Computer Science Department of UCSB.

Electronic versions of the proceedings, published by Springer, will beprovided to all registered attendees at the conference. In addition, paper proceedings can be purchased through online registration.

Important dates

- Submission deadline: **February 11, 2030 at 22:00 UTC (5:00 pm EST)**
- Notification of decision: May 9, 2030
- Proceedings version due: June 5, 2030
- Conference: August 19-22, 2030

Sponsors



CRYPTOME

Donate for the Cryptome archive of files from June 1996 to the present

Tweet

15 August 2015. Add 74 pages to New York Times-Propublica. Tally now *5,849 pages of The Guardian first reported 58,000 files; caveat: Janine Gibson, The Guardian NY, said on 30 January 2014 "much more than 58,000 files in first part, two more parts" (no numbers) (tally about ~7.6%). DoD claims 1,700,000 files (~.03% of that released). ACLU lists 525 pages released by the press. However, if as The Washington Post reported, a minimum of 250,000 pages are in the Snowden files, then less than 1% have been released. Note Greenwald claim on 13 September 2014 of having "hundreds of thousands" of documents. At Snowden current rate it will take 20-620 years to free all documents.

11 August 2015. Add 29 pages to The Intercept.

3 August 2015. Add 10 pages to The Intercept.

16 July 2015. Add 8 pages to The Intercept.

1 July 2015. Add 1,240 pages to The Intercept.

26 June 2015. Add 13 pages to The Intercept.

22 June 2015. Add 250 pages to The Intercept.

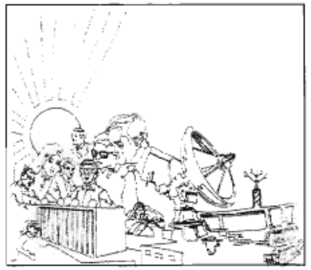
13 June 2015. Italian journalist provides correspondence with USG on Snowden documents:

```
2015-1504.pdf offsite Stefania Maurizi-NSA Snowden Correspondence      June 13, 2015
2015-1503.pdf offsite Stefania Maurizi-DoJ Snowden Correspondence      June 13, 2015
2015-1502.pdf offsite Stefania Maurizi-State Snowden Correspondence    June 13, 2015
```

12 June 2015. Paul and FVEYDOCS tweet:

> https://fveydocs.org/
>
> IC off the Record:
>
> https://nsa.gov1.info/dni/

12 June 2015. Aeris tweets:



NATIONAL SECURITY AGENCY

CRYPTOLOG

~~Classified by NSA/CSSM 123-2~~
~~Declassify on: Originating Agency's~~
~~DeterminationRequired~~

~~THIS DOCUMENT CONTAINS~~
~~CODEWORD MATERIAL~~

~~TOP SECRET~~

EUROCRYPT '92

P.L. 86-36

[redacted]

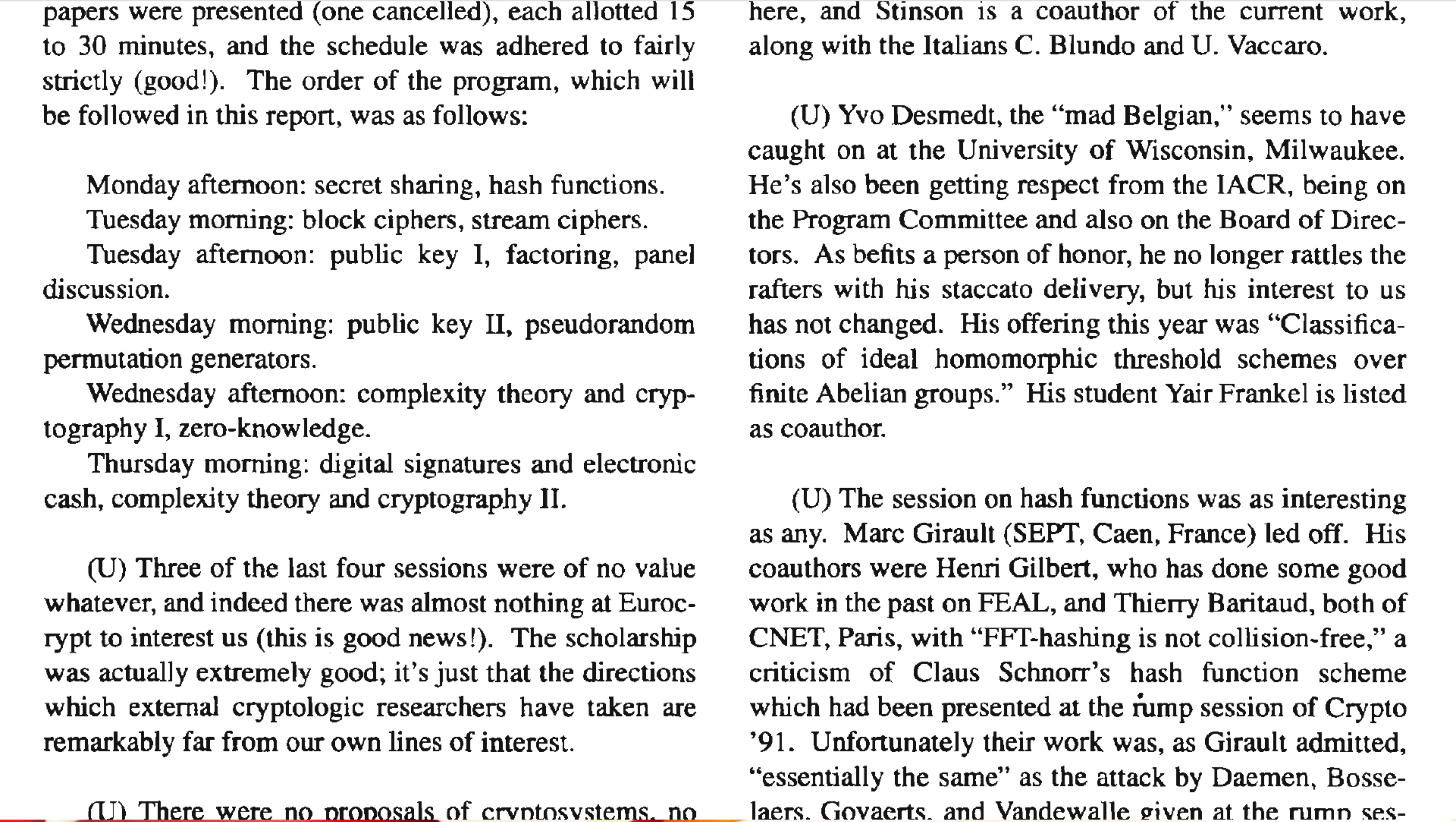
(U) Eurocrypt '92 continued the string of successful congresses sponsored by the IACR (International Association for Cryptologic Research). For the first time, the meeting was hosted by an Eastern (Central?) European country: the venue was Balatonfüred, Hungary; the dates, 24-28 May 1993.

(U) Attendance was announced as 253, but a preliminary registration list which was circulated contained only 240 names. From that preliminary list, we have the following accounting, by home address, of the registrants:

Germany	42
U.S.A.	30
France	27
Hungary	15

(U) There were some prominent "cryptologists" who did not attend: Adi Shamir of Israel (we've heard that he may by preparing a book, probably containing his work on "differential cryptanalysis"); Ron Rivest and Silvio Micali of MIT; Canada's Claude Crépeau and Gilles Brassard; Gus Simmons of Sandia; Agnes Chan of Northeastern; David Chaum of CWI, Amsterdam; Louis Guillou of France, and Ivan Dåmgard of Denmark. All of these have been more or less regular attnedants at previous IACR meetings. Three world-class mathematicians attended: Arjen Lenstra of Bellcore, Harald Niederreiter of Austria, and Andrew Odlyzko of Bell Labs.

(U) The General Chairman was Tibor Nemetz of the Mathematics Institute, Hungarian Academy of Sciences. I understand that some people experienced difficulties



papers were presented (one cancelled), each allotted 15 to 30 minutes, and the schedule was adhered to fairly strictly (good!). The order of the program, which will be followed in this report, was as follows:

Monday afternoon: secret sharing, hash functions.

Tuesday morning: block ciphers, stream ciphers.

Tuesday afternoon: public key I, factoring, panel discussion.

Wednesday morning: public key II, pseudorandom permutation generators.

Wednesday afternoon: complexity theory and cryptography I, zero-knowledge.

Thursday morning: digital signatures and electronic cash, complexity theory and cryptography II.

(U) Three of the last four sessions were of no value whatever, and indeed there was almost nothing at Eurocrypt to interest us (this is good news!). The scholarship was actually extremely good; it's just that the directions which external cryptologic researchers have taken are remarkably far from our own lines of interest.

(U) There were no proposals of cryptosystems, no

here, and Stinson is a coauthor of the current work, along with the Italians C. Blundo and U. Vaccaro.

(U) Yvo Desmedt, the "mad Belgian," seems to have caught on at the University of Wisconsin, Milwaukee. He's also been getting respect from the IACR, being on the Program Committee and also on the Board of Directors. As befits a person of honor, he no longer rattles the rafters with his staccato delivery, but his interest to us has not changed. His offering this year was "Classifications of ideal homomorphic threshold schemes over finite Abelian groups." His student Yair Frankel is listed as coauthor.

(U) The session on hash functions was as interesting as any. Marc Girault (SEPT, Caen, France) led off. His coauthors were Henri Gilbert, who has done some good work in the past on FEAL, and Thierry Baritaud, both of CNET, Paris, with "FFT-hashing is not collision-free," a criticism of Claus Schnorr's hash function scheme which had been presented at the rump session of Crypto '91. Unfortunately their work was, as Girault admitted, "essentially the same" as the attack by Daemen, Bosselaers, Govaerts, and Vandewalle given at the rump ses-

ANONYMOUS SUBMISSIONS

- So Forget it ! All former reviews were recently published … thanks to cryptoleaks, Snowden, aso

- At CRYPTO 2030, there was a true problem because all submitted papers and reviews leaked 10 days before the conference. Ambiance!

PUBLISHING

- Only the BEST PAPER is published on paper!
- Springer got Thomson Reuters Web of Science in 2027, so now eprint is now getting a high citation index.

HOW MANY TRACKS FOR TALKS?

- Between 1 and 2 (not everytime),

- Videos of each one: so with your computer you also follow the other one ☺

- Virtual poster sessions with video allowed for people not able to be physically there.

RUMP SESSION

RUMP SESSION

There were too many good submissions to the rump session. So …

RUMP SESSION

There were too many good submissions to the rump session. So …

NEW for 2030: 2 rump session tracks in parallel:

RUMP SESSION

There were too many good submissions to the rump session. So …

NEW for 2030: 2 rump session tracks in parallel:

- Rump Session A: RSA: broken systems and jokes

RUMP SESSION

There were too many good submissions to the rump session. So …

NEW for 2030: 2 rump session tracks in parallel:

- Rump Session A: RSA: broken systems and jokes
- Rump session B: RSB: songs and new results

RUMP SESSION

There were too many good submissions to the rump session. So …

NEW for 2030: 2 rump session tracks in parallel:

- Rump Session A: RSA: broken systems and jokes
- Rump session B: RSB: songs and new results

- Both directed by Dan Bernstein and Tanja Lange

DAN
BERN