40 years Advances in Cryptology: How Will History Judge Us?

Yvo Desmedt

Univ. of Texas at Dallas
USA

University College London
UK

August 18, 2020

1. Cryptology today

Today most research at Crypto is assumption based.

History note: we are not the first assumption based "science."

Indeed:

1. Cryptology today

Today most research at Crypto is assumption based.

History note: we are not the first assumption based "science."

Indeed:

a. Astrology assumed that the earth was the center of the universe. We had to wait until Copernicus to have this assumption challenged.

b. Alchemists assumed there were 5 elements, being (in the West): earth, water, air, fire, and aether (added by Aristotle).

2. How did we challenge our assumptions?

Cryptanalysis challenges our assumptions.

2. How did we challenge our assumptions?

Cryptanalysis challenges our assumptions.

At Crypto in the 1980's 33-48% of the papers were on cryptanalysis.

As in Garey-Johnson:

I can't find an efficient attack, but neither can all these famous cryptanalysts.

3. How do we prepare for the future?

We want Post-Quantum security!!

However, despite 26 years of research since Shor's algorithm (1994) we still do not have a large quantum computer!! Could this just be science fiction?

4. How do we challenge our assumptions today?

Today, we have significantly less papers on cryptanalysis, e.g., at Crypto 2012 only 6%.

We no longer follow a Garey-Johnson like approach, but instead:

4. How do we challenge our assumptions today?

Today, we have significantly less papers on cryptanalysis, e.g., at Crypto 2012 only 6%.

We no longer follow a Garey-Johnson like approach, but instead:

We just trust NIST.

5. Where did some of the famous cryptanalysts go?

Hendrik Lenstra

No fundamental progress on factoring since he is no longer working on it, i.e., 1990.

Ernie Brickell

Retired.

Adi Shamir

Sidetracked by sidechannels

Don Coppersmith

Classified

since he moved to IDA.

Jim Reeds

Classified

since he moved to IDA.

Andrew Odlyzko

Switched to Economic Aspects of Security.

6. Some recent progress on cryptanalysis

Only on a few topics was substantial progress made, e.g., on:

- breaking hash functions, such as MD-4, MD-5, SHA-1,
- breaking discrete logarithm over $\mathbf{F}_{2^k}$,
- breaking several Multilinear Maps.

No substantial progress on several problems for decades. However, Jim Massey might be correct when he stated:

> Hard problems are the problems that nobody works on.

7. State of the art of cryptology

With so little research on cryptanalysis, we do not know whether we are standing on thin ice!

8. Conclusions

It took 300 years to break Vigenere cipher. So, it is too early to celebrate after 40 years.

If we do not want to be judged by history as naive, we should work much harder towards breaking cryptosystems, and IACR should:

- have more PC Chairs in the area,
- require that 50% of the Best Paper Awards are for cryptanalysis,
- encourage workshops and summer schools on the topic,
- encourage funding agencies to increase unclassified funding in the area (today close to $0 in USA[1]).

[1] See Appendix for my e-mail to NIST on this issue.

9. Recommended reading

The following texts should be required reading for all PhD students in crypto:

[1] E. Brickell and A. M. Odlyzko. Cryptanalysis: A survey of recent results. *Proc. IEEE*, 76(5), pp. 578–593, May 1988.

[2] E. F. Brickell and A. M. Odlyzko. Cryptanalysis: A survey of recent results. In G. J. Simmons, editor, *Contemporary Cryptology*, pp. 501–540. IEEE Press, New York, 1992.

[3] D. Kahn. Modern cryptology. *Scientific American*, 215(1), pp. 38–46, July 1966.

[4] D. Kahn. *The Codebreakers*. MacMillan Publishing Co., New York, 1967.

A. Appendix: April 12, 2018 e-mail to Lily Chen at NIST

Dear Lily,

as I pointed out on April 11, 2018, most talks at PQCrypto 2018 have been given by researchers from *outside* the USA. By having a call for post-quantum proposals, NIST has boosted academic research in the field of post-quantum cryptography, but so far, only for researchers *outside* the USA. Indeed, many academics attended from outside the USA got funding from their funding agencies. Some US academics who attended, as myself, used their startup money to fund attendance. So, currently, very few academic researchers in the US are working on post-quantum cryptography.

To address this situation, it is important to have a Post-Quantum dedicated call for proposals for research.

. . .

Best Regards,

Yvo