Eli and I in New York Times

The CBCM mode of operation designed by IBM, USA, was almost included in the ANSI X9.52 Triple-DES Modes of Operation standard. ANSI is the American National Standards Institute. Eli and I broke the scheme which was withdrawn from the standard after our attack.

Eli Biham and I had known each other for 7-8 years at that time. We were both very productive and published many papers at the prestigious crypto-events. We were also competing against each other trying to publish the best results. A sound competition!

We were on our way home from the annual Crypto conference, held every year in Santa Barbara in California. IBM had published a variant of Triple-DES, which had a fourth key in an attempt to get even better security than Triple-DES.

The US standardization body ANSI had accepted the IBM proposal and had produced a draft standard. The world was invited to comment on the draft.

Eli and I were waiting for a bus heading for LAX, the airport in Los Angeles. The ride is a few hours, three maybe? One of us suggested to look at the CBCM mode and maybe, hopefully break it. We brainstormed for a bit, couldn't get to it…… I remember insisting to Eli that if we were to break this scheme with a low complexity, we had to somehow find a way to *undo* the extra fourth encryption and some-other-how isolate a single DES encryption and do exhaustive search on this. An exhaustive search for one DES-key could be done, but a search over two or three DES keys was not possible and still isn't. We ping-pong'ed back and forth and threw ideas up in the air. In the end it was Eli that made the discovery that made us yell "YES". A bijection has a fixed point with some good probability, but the question was how to detect such a fixed point for an inner encryption in a triple encryption scheme. This was not easy to see at first, but this is what we discovered. The complexity of the attack is high and requires many chosen plaintexts and lots of memory, so it may not be an attack that will be executed in real-life right now. But IBMs proposal was an attempt to lift the security of triple-DES by introducing a fourth encryption, but our attack showed that this was wrong.

As a consequence of our attack, ANSI decided to remove the CBCM mode from the proposed standard. Later the news of our findings was shown on the webpage of New York Times and the day after there was an article in the real printed newspaper (not on the frontpage, though).

LRK 2019.