Hamilton Institute

How I broke AES (Advanced Encryption Standard)---if I did it

Dr Warren D. Smith
Center for Range Voting
http://www.rangevoting.org

Monday, February 2nd, 2009

Abstract:
We describe a new simple but more powerful form of linear cryptanalysis. It appears to break AES (and undoubtedly other cryptosystems too, e.g. SKIPJACK).
• But the break is "nonconstructive".
• Even if this break is broken (due to the underlying models inadequately approximating the real world) we explain how AES still could contain "trapdoors" which would make cryptanalysis unexpectedly easy for anybody who knew the trapdoor.

We then discuss how to use the theory of BLECCs to build cryptosystems provably
- not containing trapdoors of this sort,
- secure against our strengthened form of linear cryptanalysis,
- secure against "differential" cryptanalysis,
- secure against D.J. Bernstein's timing attack.

Using this technique we prove a fundamental theorem: it is possible to thus-encrypt N bits with security 2^(cN), via an circuit Q_N containing <= cN two-input logic gates and operating in <= c log(N) gate-delays, where Q_N is constructible in polynomial (in N) time.

Venue: Seminar Room, Hamilton Institute, Rye Hall, NUI Maynooth

Time: 2.00 - 3.00pm (followed by tea/coffee)

Travel directions are available at www.hamilton.ie

IEEE CC Ireland Chapter