From: Vincenzo Iozzo <[redacted]>
Subject: practical kleptography
Sent: Sunday, September 14, 2014 1:17:59 PM
Cc: "jeffrey E." <jeevacation@gmail.com>, Joshua Cooper Ramo [redacted]
To: Joichi Ito <[redacted]>

The speaker is somewhat biased (you can guess in which direction), but this explains how some of the elliptic curves suggested by NIST were allegedly backdoored.

It's pretty high level, so don't need a lot of crypto understanding for it:
https://www.usenix.org/conference/woot14/technical-sessions/presentation/practical-kleptography

Besides the technical/crypto part it's a very good way to understand how certain processes within the US govt work