Cryptanalysis of OCB2
(ePrint 2018/1040)

Akiko Inoue (NEC Corporation)
Joint work with Kazuhiko Minematsu

Rump session at Asiacrypt 2018, December 2-6, Brisbane Australia
OCB2

• Authenticated Encryption (AE) proposed by Rogaway at Asiacrypt 2004 [Rog04]
• Blockcipher mode with strong features
• Provable security
• Standardized in ISO/IEC 19772

• Three versions. OCB1/2/3
• (all versions of) OCB are widely believed to be secure
Our contributions

• OCB2 can be attacked
  – authenticity is broken
  – independent of the underlying blockcipher

• Simple and practical: one encryption query, then forgery
  – Existential forgery
  – Universal forgery after the first forgery
OCB2

• 2L and 3L : GF(2^n) multiplication by $x$ and $x+1$
• Checksum $\Sigma = M[1] + \ldots + M[m-1] + M[m]$
Minimal Attack

1. First, encrypt \((N, M)\):
   - \(M = \text{len}(0^n) \ || \ M[2]\) for any n-bit \(M[2]\)
   - Get \((C = C[1]C[2], T)\)

2. Decrypt \((N, C', T')\) s.t.
   - \(C' = C[1] + \text{len}(0^n),\)
   - \(T' = M[2] + C[2]\)
   - will be accepted as valid
A flaw in the hybrid argument [Rog04]

• OCB2 relies on the security of XEX* (internal TBC made of blockcipher)

• XEX* is provably secure, but

• This hybrid forces an prohibited use of XEX*

• The security of XEX* does not imply security of OCB2
Extensions and Summary

Follow-ups:
• Poettering (2018/1087) [Pot18]
• Iwata (2018/1090) [Iwa18]
  – Various extensions, such as privacy attack and plaintext recovery

Summary:
• OCB2 is totally broken, practical forgery is possible, and even more
• Not applicable to the general structure of OCB, not applicable to OCB1 and OCB3

👏 Thank you ! 😻