DEPRECATED FFDH
Carrick Bartle, Nimrod Aviram, Filippo Valsorda
THE RACCOON ATTACK

- September 2020
- Timing attack
- Uses server as oracle to derive premaster secret
VULNERABLE CIPHER SUITES

• Non-ephemeral Finite Field Diffie-Hellman (FFDH)

• Ephemeral FFDH if public key is reused
VULNERABLE CIPHER SUITES

- Non-ephemeral Finite Field Diffie-Hellman (FFDH)
- Ephemeral FFDH if public key is reused

Already not recommended since they don't provide forward secrecy
ECDH

- Not vulnerable to Raccoon Attack, but:
  - Vulnerable to side-channel attacks, e.g. invalid curve attacks
- Prohibit reuse of ECDHE public keys
ECDH

• Not vulnerable to Raccoon Attack, but:
  • Vulnerable to side-channel attacks, e.g. invalid curve attacks
• Prohibit reuse of ECDHE public keys

Already not recommended since they don't provide forward secrecy
SUMMARY

- FFDH
- Reusing FFDHE and ECHDE keys
- ECDH