# Side-Channel Attacks

Infer values of the system under execution based on its physical side-effects.

- Timing Attacks [1]
- Power Analysis Attacks
- Electromagnetic Analysis Attacks

[1] Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. Paul Kocher. CRYPTO 1996

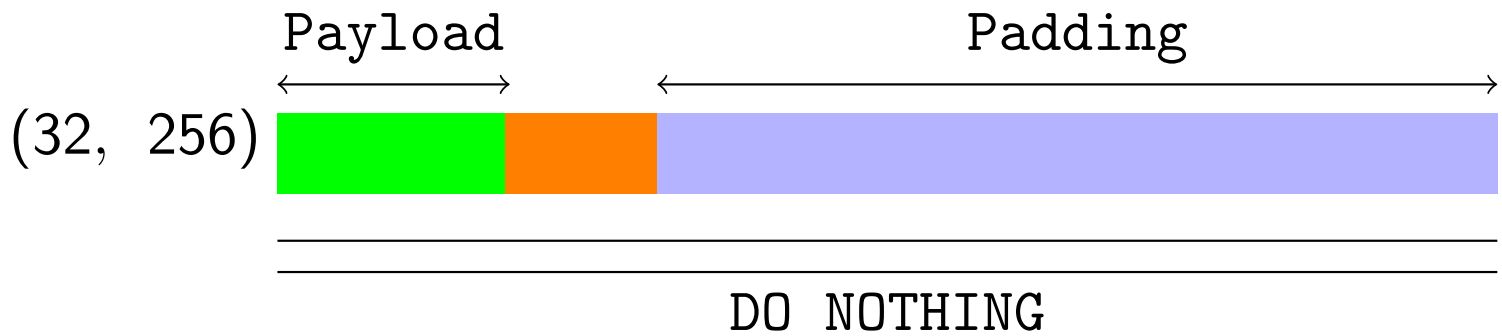
# Timing Attacks on TLS

## Attacker Model: MITM over the network

1. Resides in the same LAN segment as the targeted TLS client/server.
2. Injects ciphertexts of its own.
3. Observes *total* time required to process a TLS record.
4. Doesn't reside in the same multi-core processor.

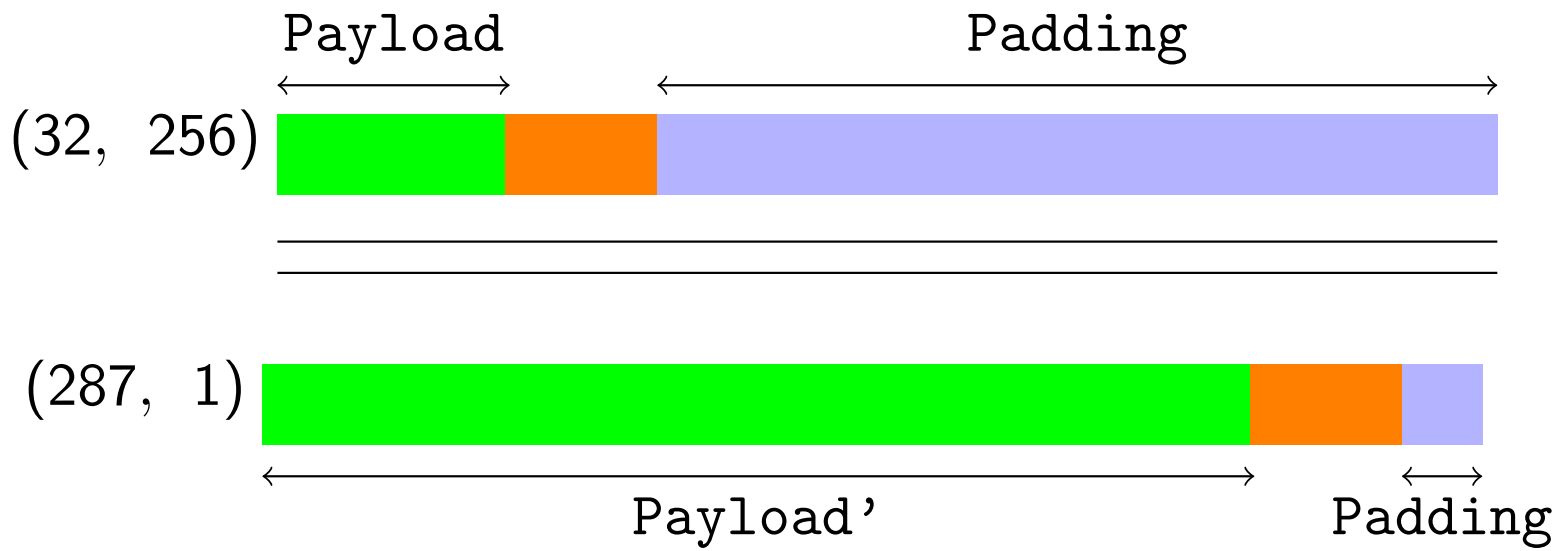
# Padding Oracle Timing Attack

**if** padding check succeeds **then**
  check the MAC
**else**
  **return**



# Padding Oracle Timing Attack (Band-Aid Fix)

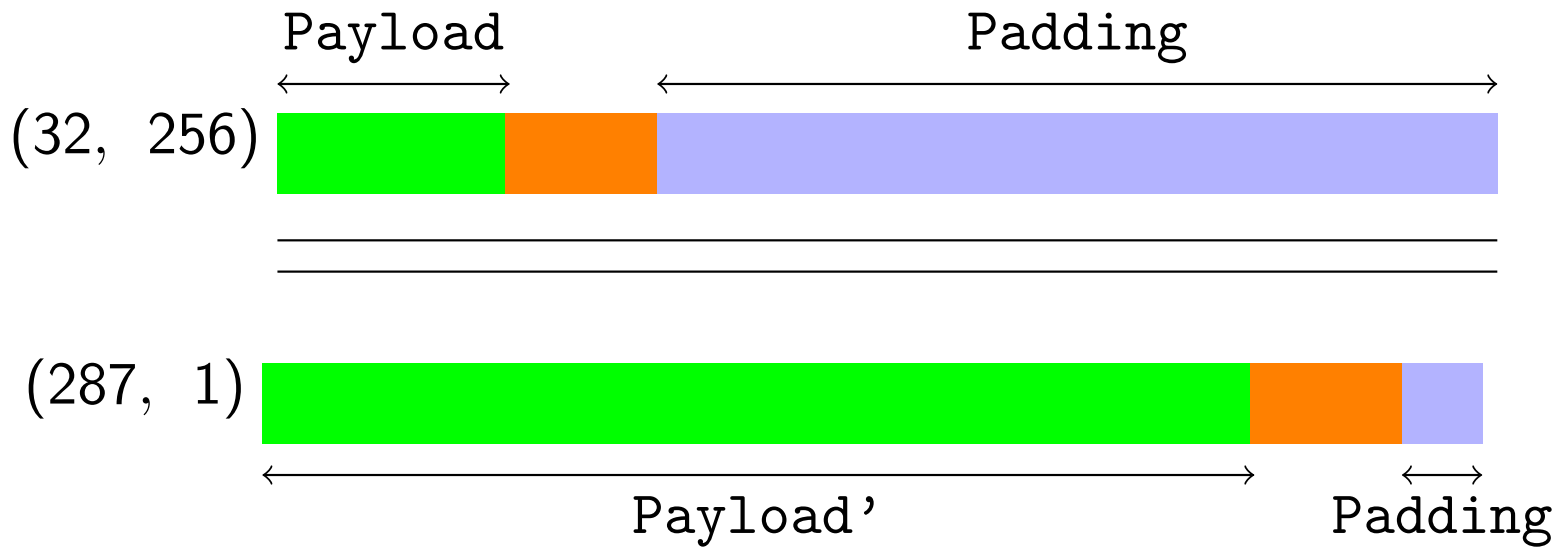
**if** padding check succeeds **then**
  check the MAC
**else**
  check the MAC (assuming 0 padding)
  **return**



*The best way is to compute the MAC even if the padding is incorrect, and only then reject the packet.*
*For instance, if the pad appears to be incorrect, the implementation might assume a zero-length pad and then compute the MAC. This leaves a small timing channel, since MAC performance depends to some extent on the size of the data fragment, but it is not believed to be large enough to be exploitable, due to the large block size of existing MACs and the small size of the timing signal.*

TLS 1.2

# Lucky 13 [2]




$$\#hash\_rounds = \left\lfloor \frac{Payload - 55}{64} \right\rfloor + 4$$

[2] Lucky Thirteen: Breaking the TLS and DTLS Record Protocols. AlFardan, Paterson. S&P 2013