A new submission to the SNAKE OIL CRYPTO competition

Roberto Avanzi
@FakeIACR (ad hodorem)
Diego Aranha (our network expert)

ANNOUNCEMENT

- After SPHINCS …
- … and SPHINCS-Haraka …
- … we are introducing a third variant of this high-security post-quantum stateless, gluten-free, kosher, halal, hash-brown-based signature scheme

  (the *brown part* is important)

SPHINC-TER

- We cannot *dump* the specs yet – or ever
- Not only because I am the chief procrastinator (starting tomorrow since 2013)
- It *must* be kept under wraps because….
- **… IT HAS A BACKDOOR !!!!1!11!**
- It will be submitted to J. CRAP-tology
- (if you think this smells fishy… it is not fish)

馬鹿

馬鹿

馬鹿

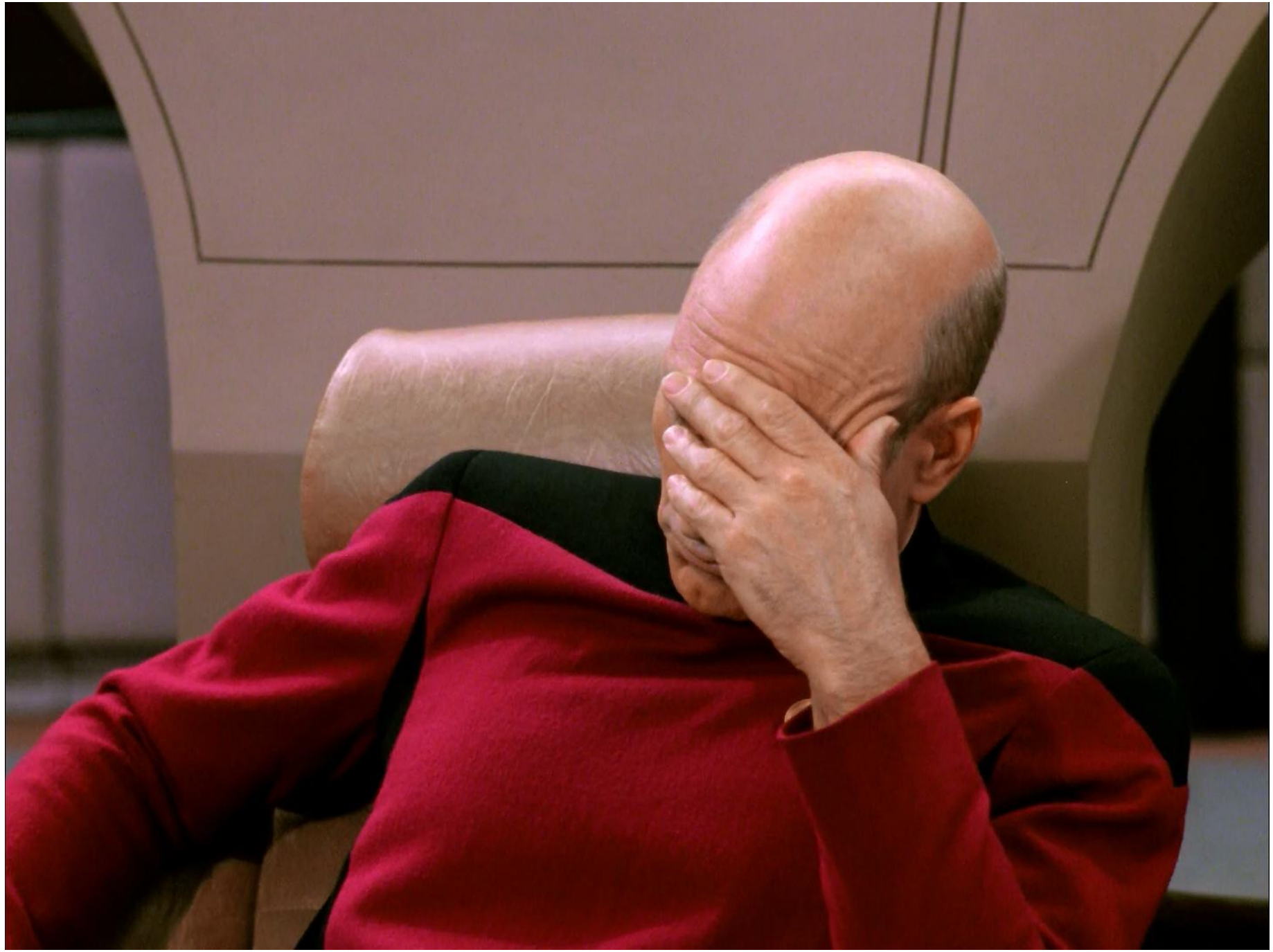
馬鹿

馬鹿

馬鹿

馬鹿

馬鹿



うんち

うんち

うんち

うんち

うんち

うんち

うんち

うんち