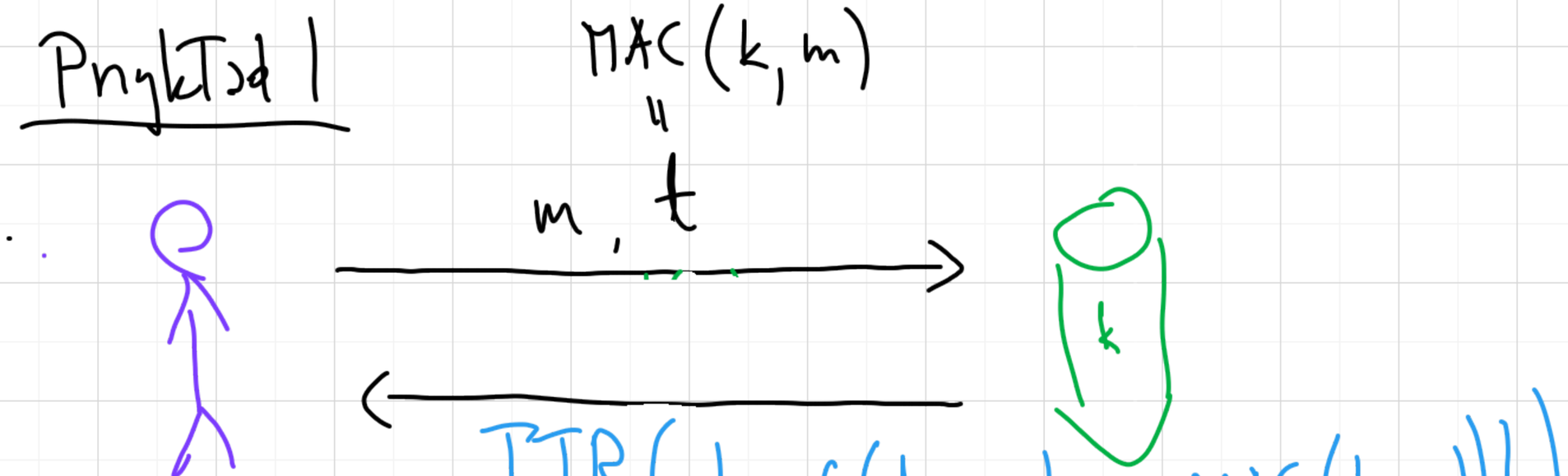
Side-channel attacks

Pomysł 1



Constant-time implementations

$\forall_{x,y\ |x|=|y|}\ T(A(x)) = T(A(y))$

```
compare(A, B)
    for a, b in zip(A, B):
        if a != b
            return False
    return True
```

Problem: nic jest constant-time!

```
Vrfy(k, m, t)
    t' = MAC(k, m)
    return MAC(k, t) == MAC(k, t')
```

+1 +1

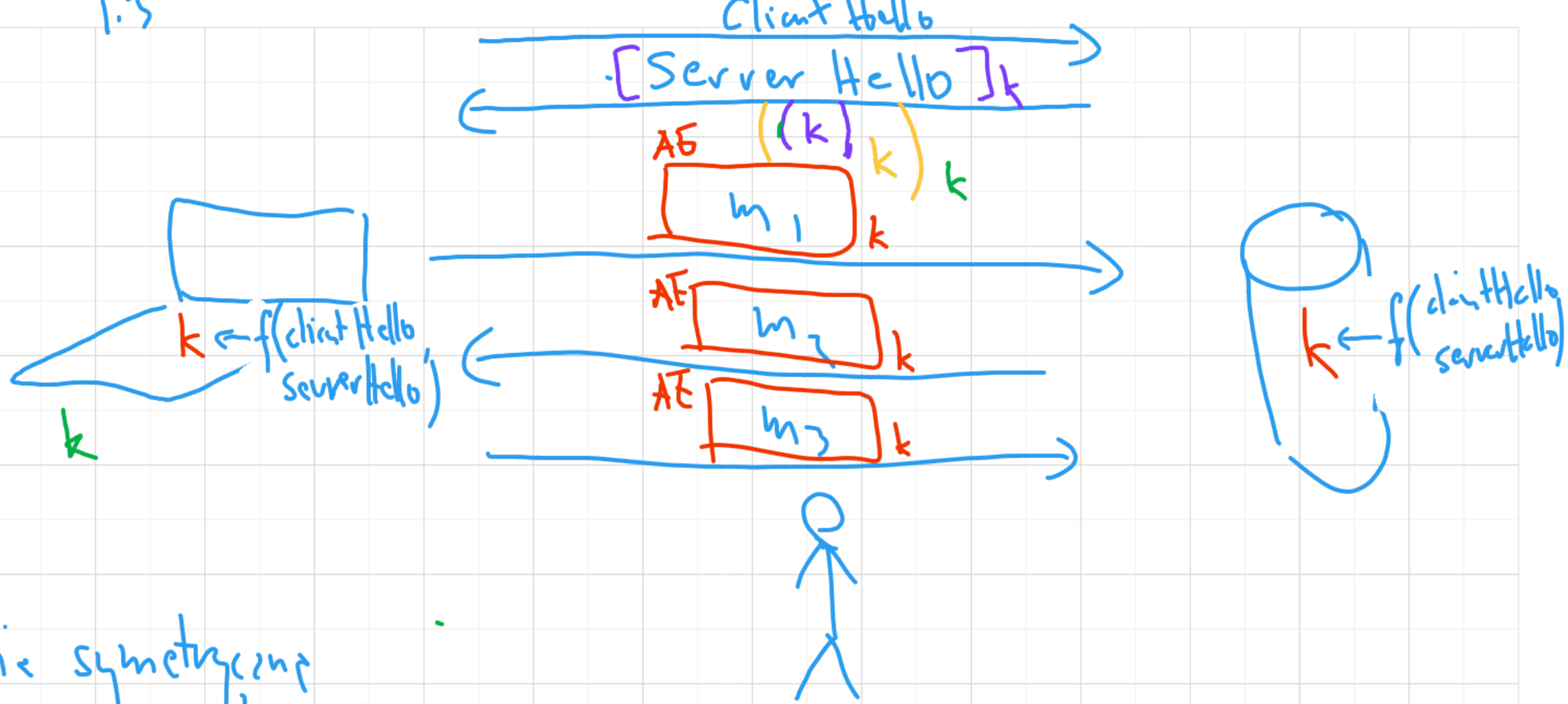
```
Compare(A, B)
    result = 0
    for a, b in zip(A, B):
        result |= ord(a) ^ ord(b)
    return result == 0
```

+1

TLS

Bear SSL

1.3



Kryptografie symetryczna
AE (AES-GCM/...)

Kryptografie asymetryczna
Key Exchange (DHE, RSA)
Signature (DSA, RSA, ...)