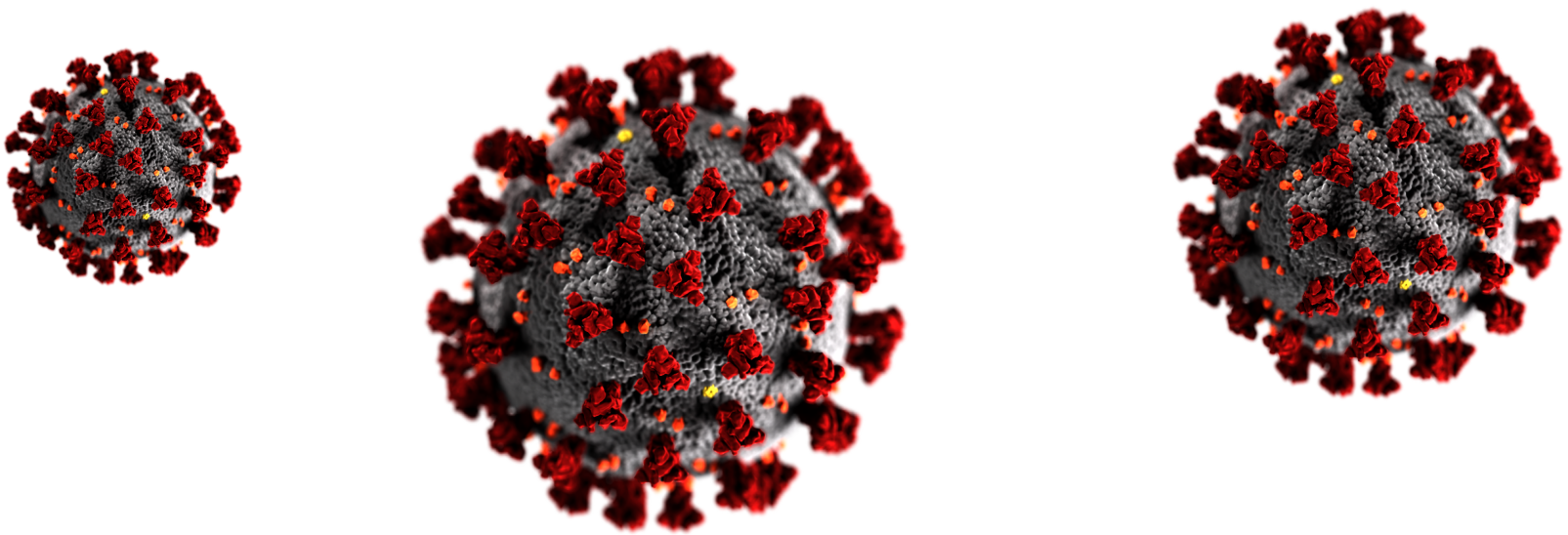
Replay, Relay and Inverse-Sybil Attacks on Proximity Tracing Apps

Krzysztof Pietrzak

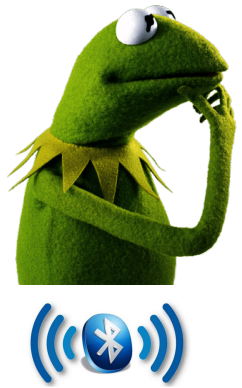
IST AUSTRIA
Institute of Science and Technology



2020 Eurocrypt Rump Session, May 13th, Living Room

Proximity Tracing

Proximity Tracing



. . .
8GD45AF3
. . .

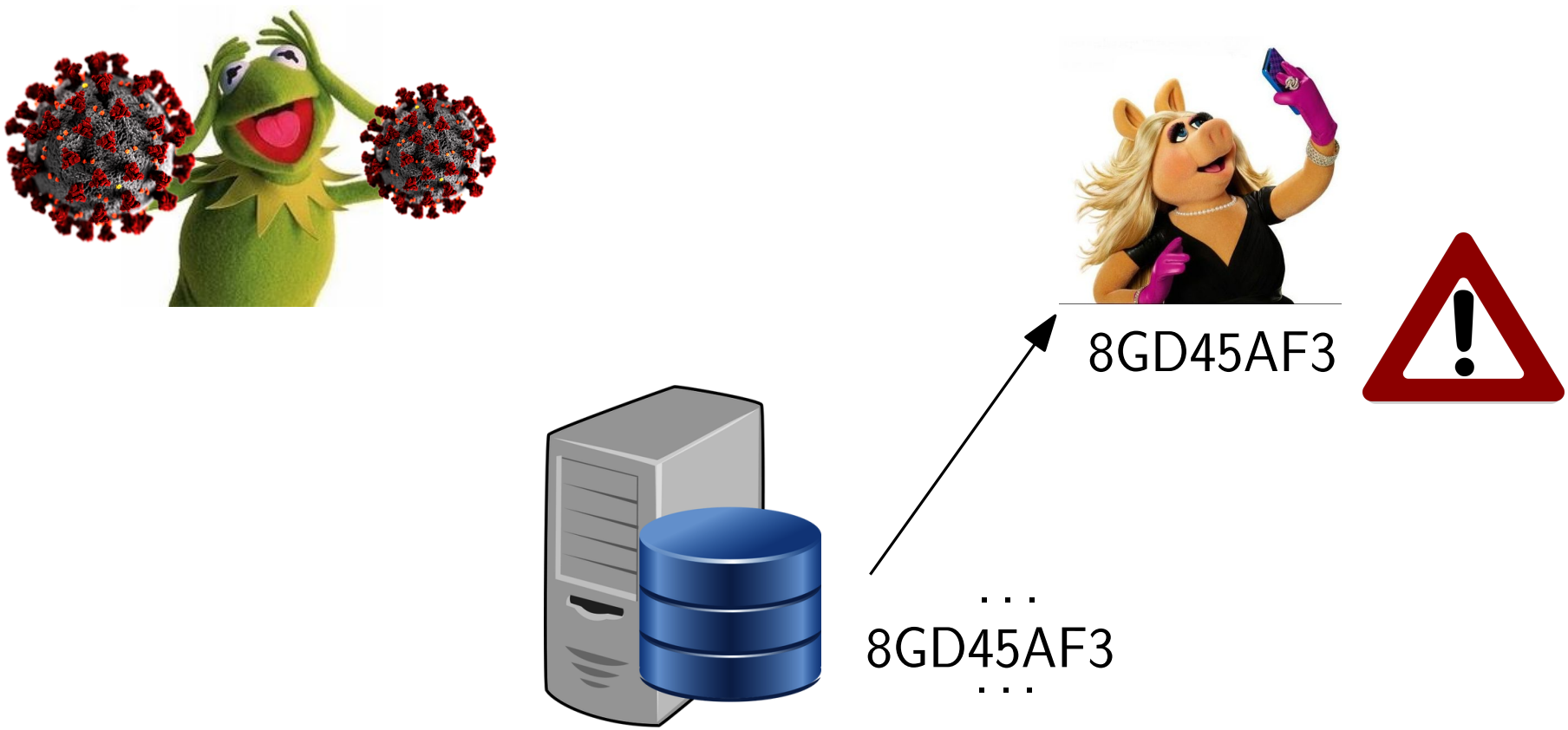
8GD45AF3

8GD45AF3

. . .
8GD45AF3
. . .

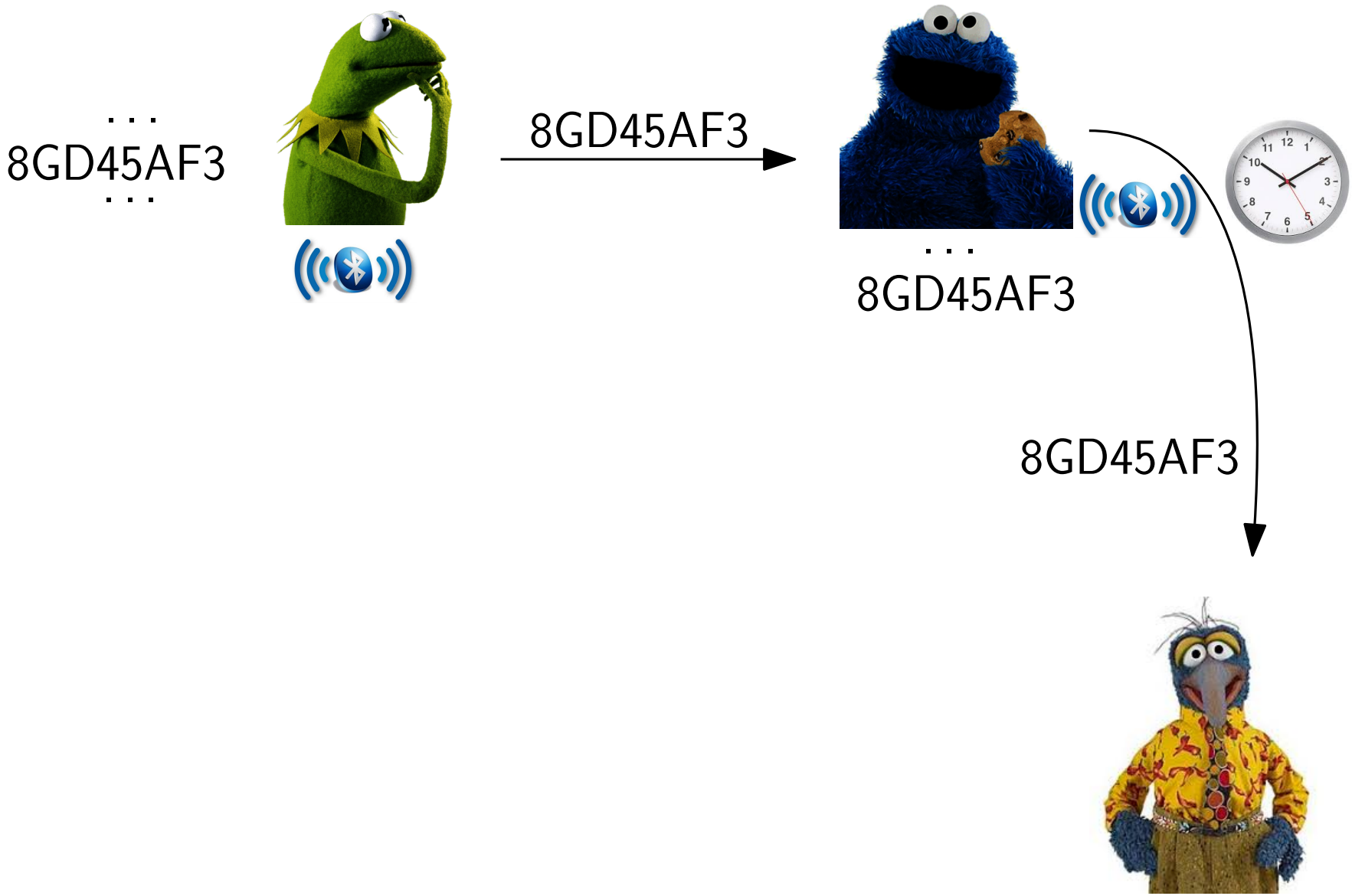
. . .
8GD45AF3
. . .

Proximity Tracing

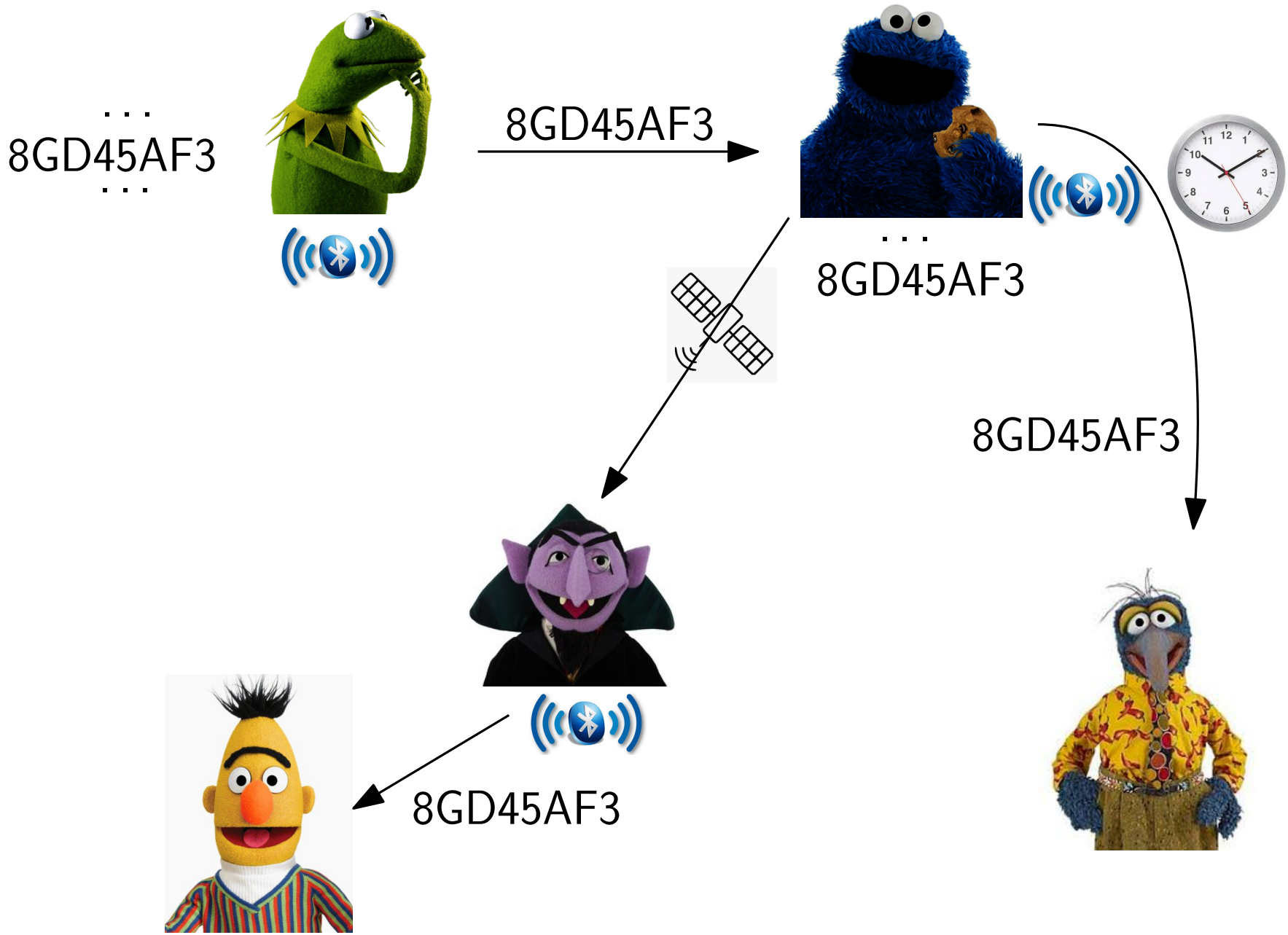


Replay and Relay Attacks

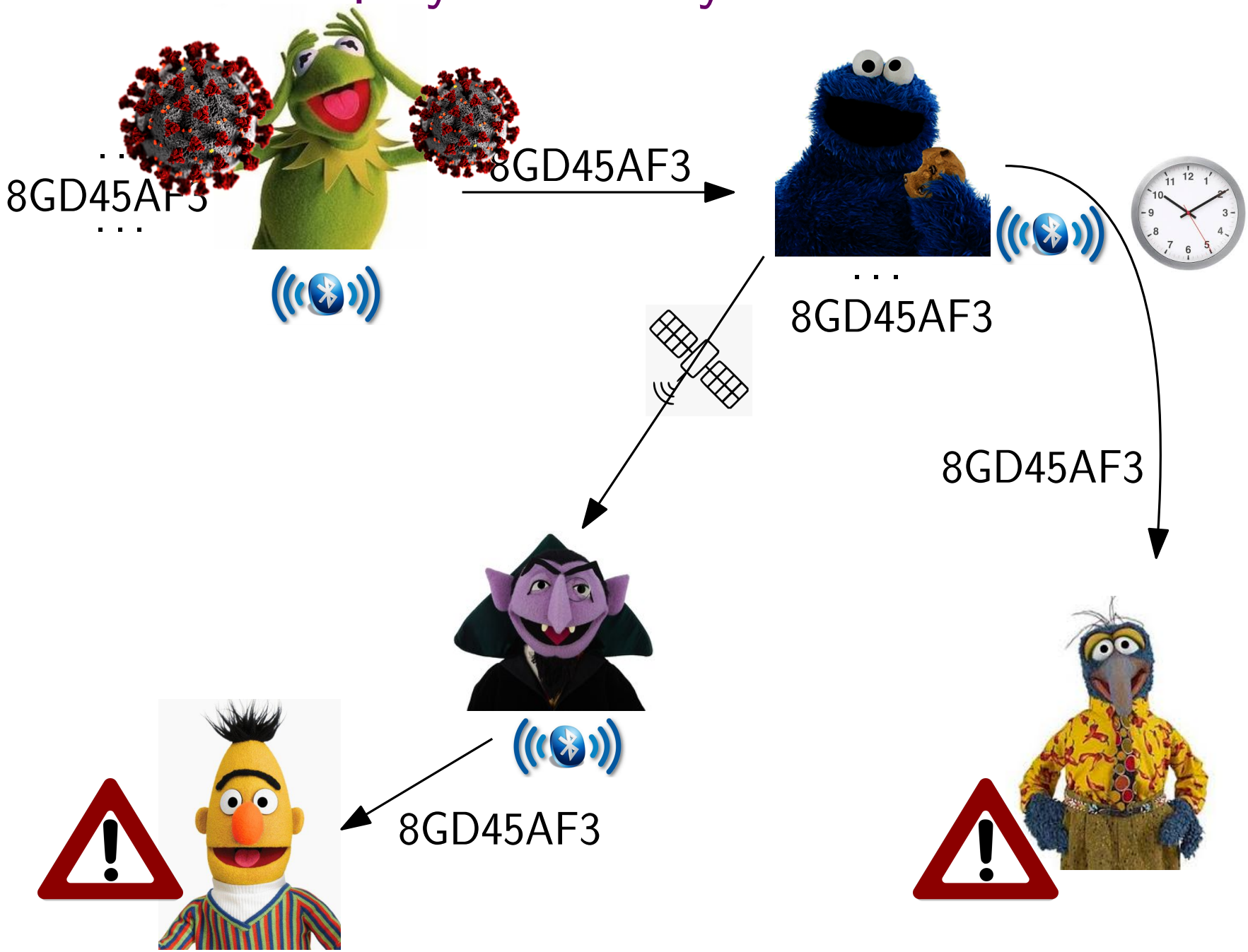
Replay and Relay Attacks



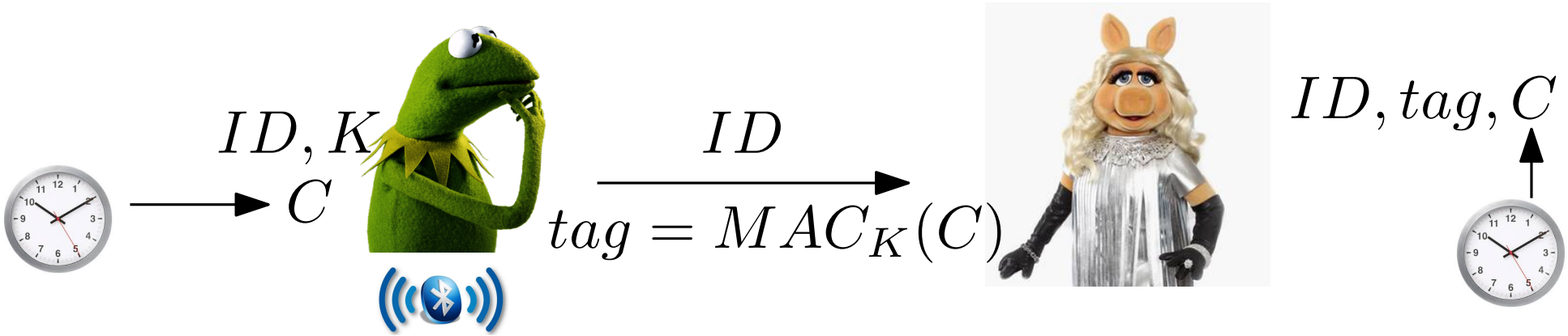
Replay and Relay Attacks



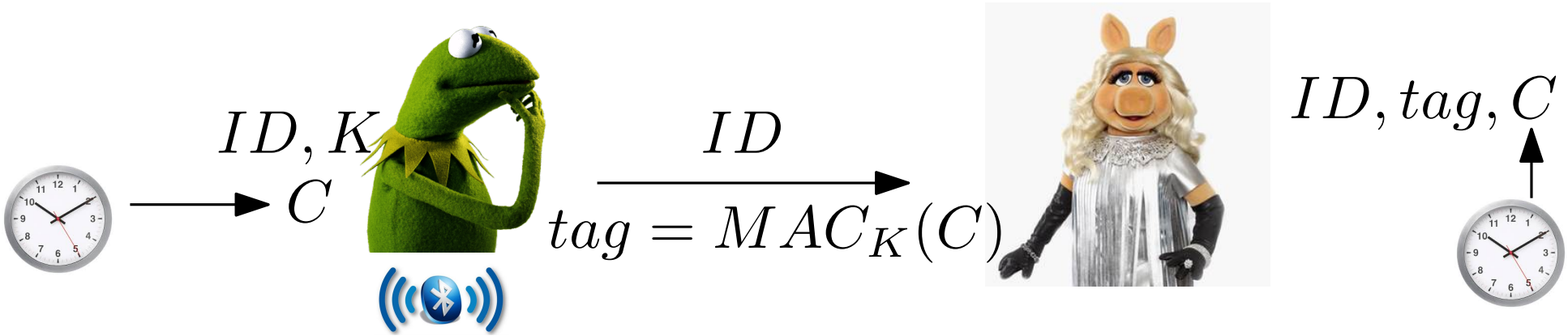
Replay and Relay Attacks

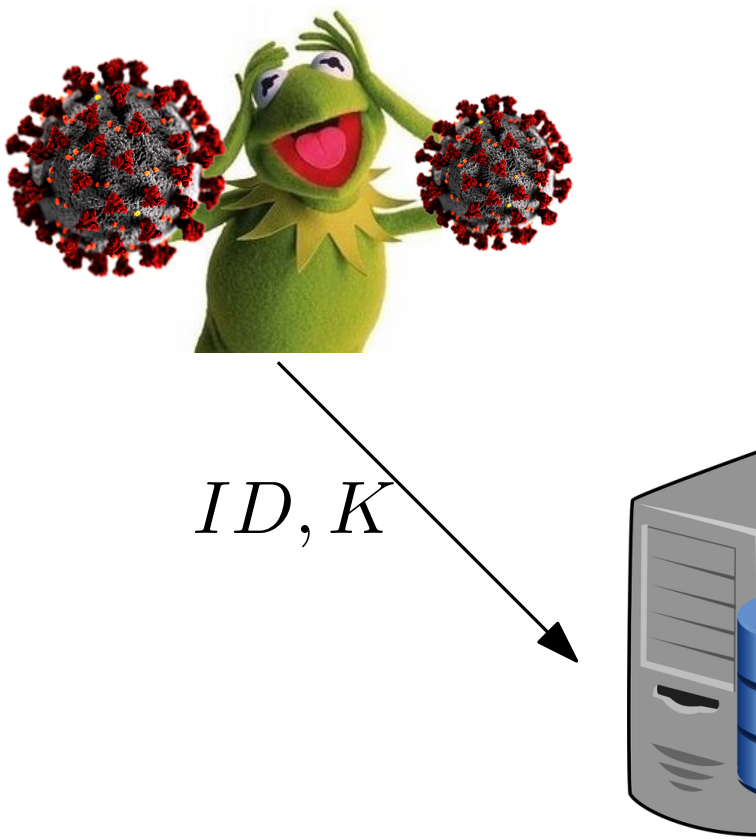


Preventing Relay and Replay Attacks without Privacy

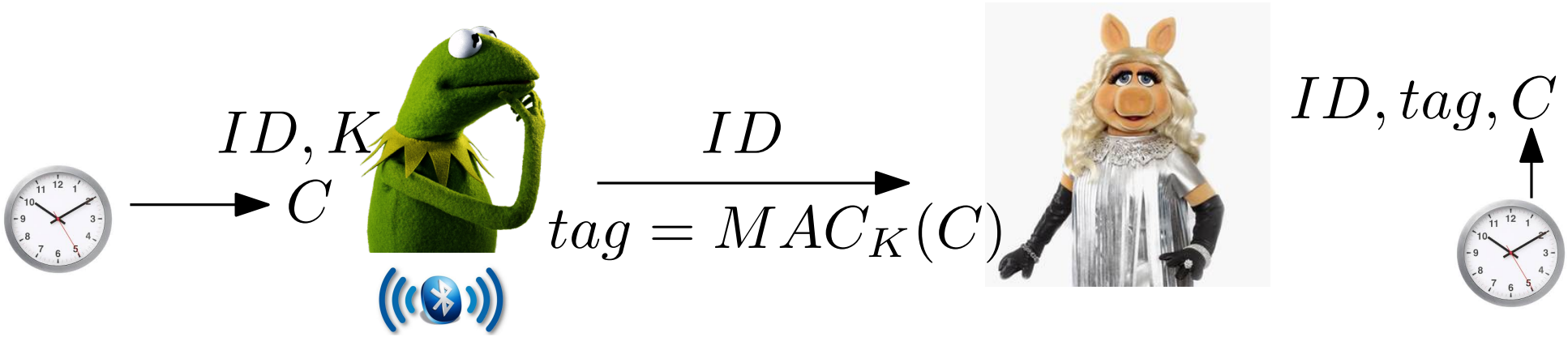


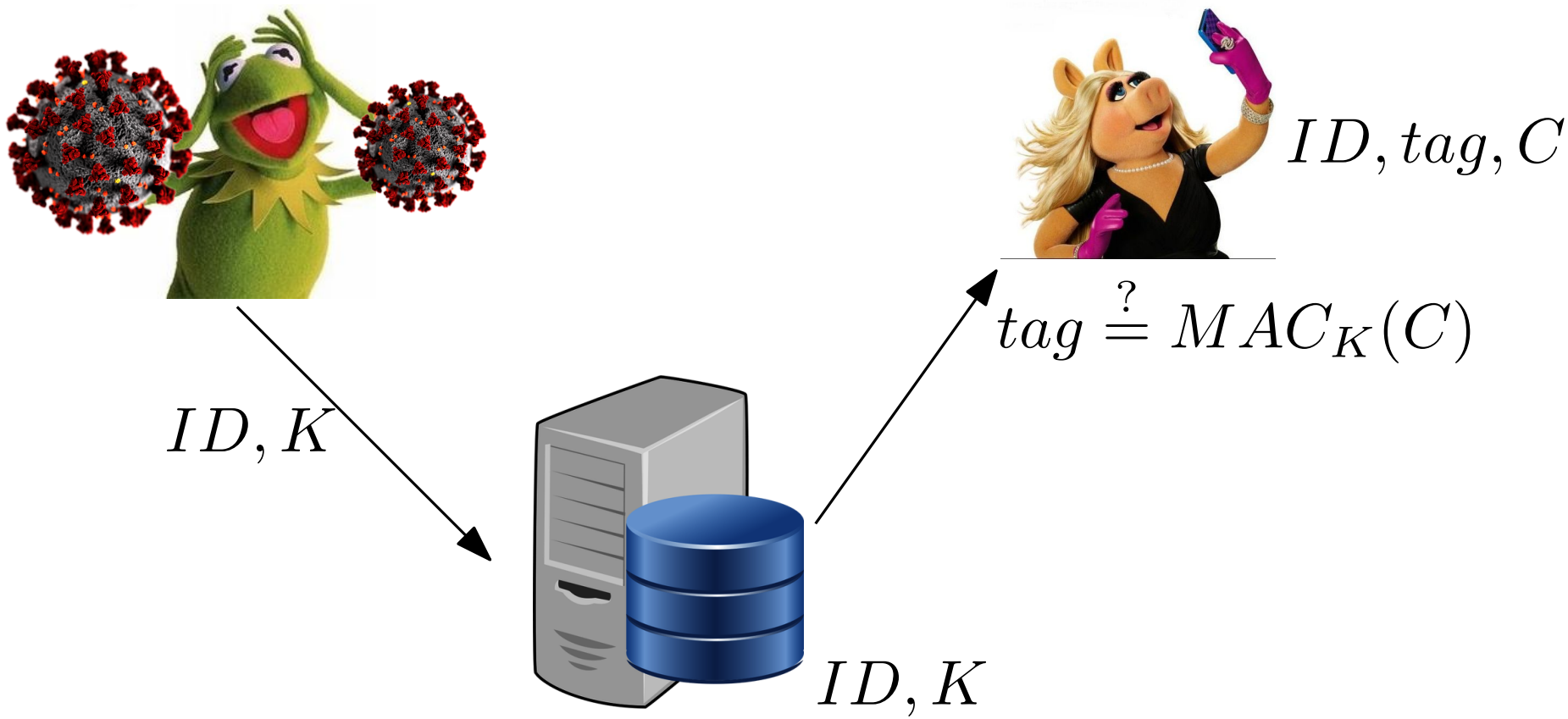
Preventing Relay and Replay Attacks without Privacy



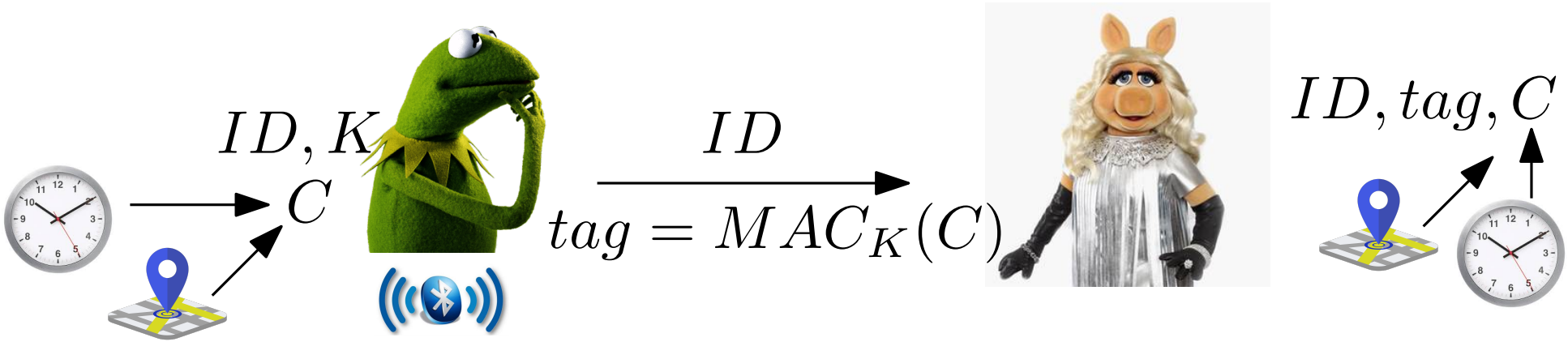


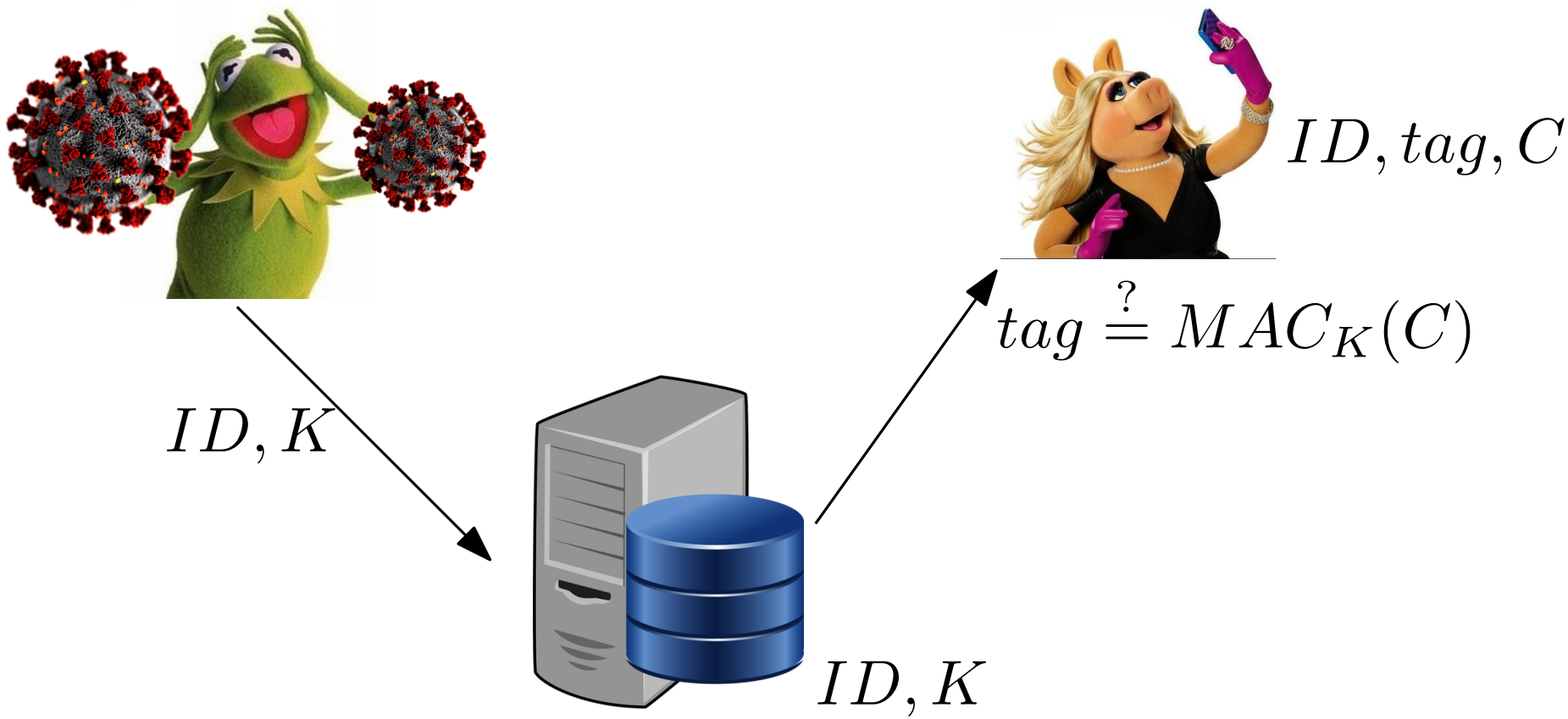
Preventing Relay and Replay Attacks without Privacy



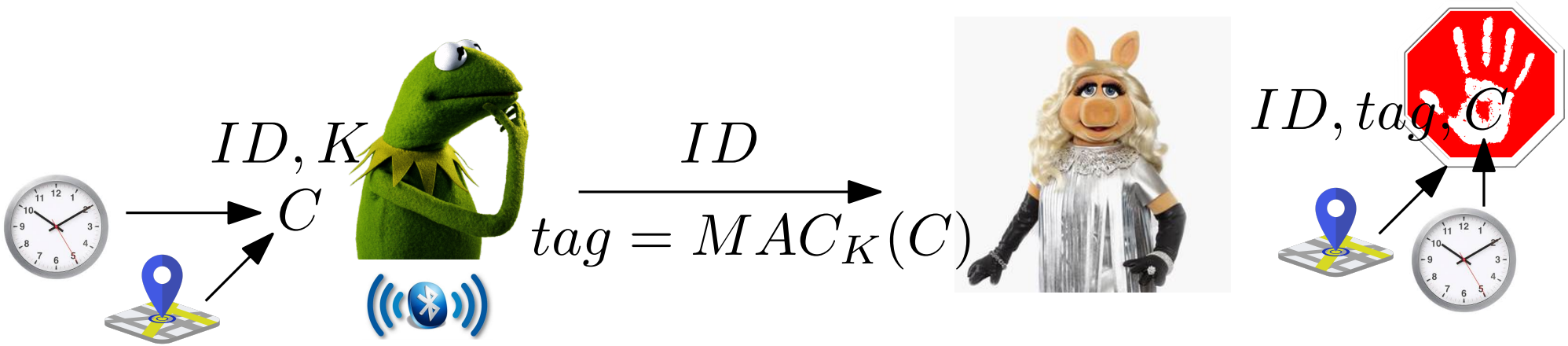


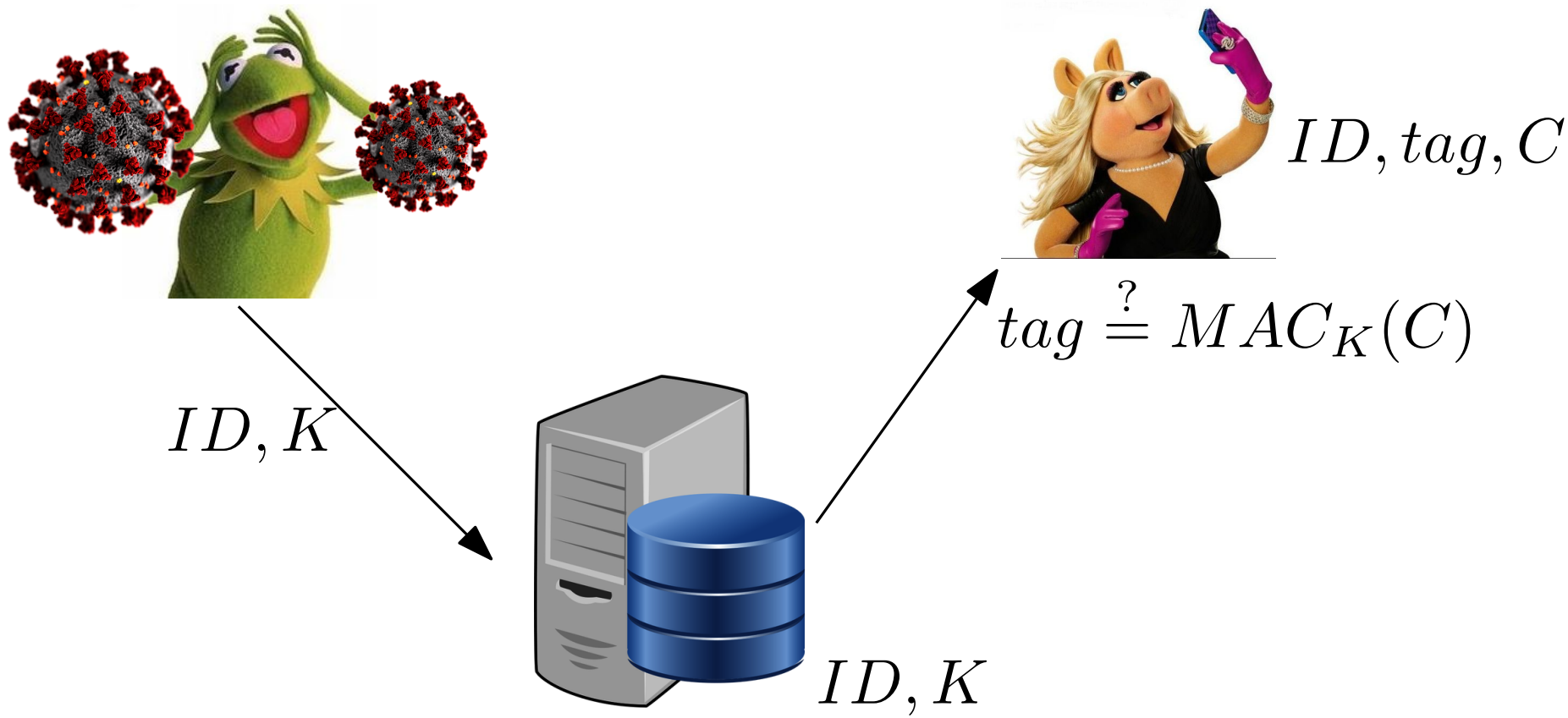
Preventing Relay and Replay Attacks without Privacy



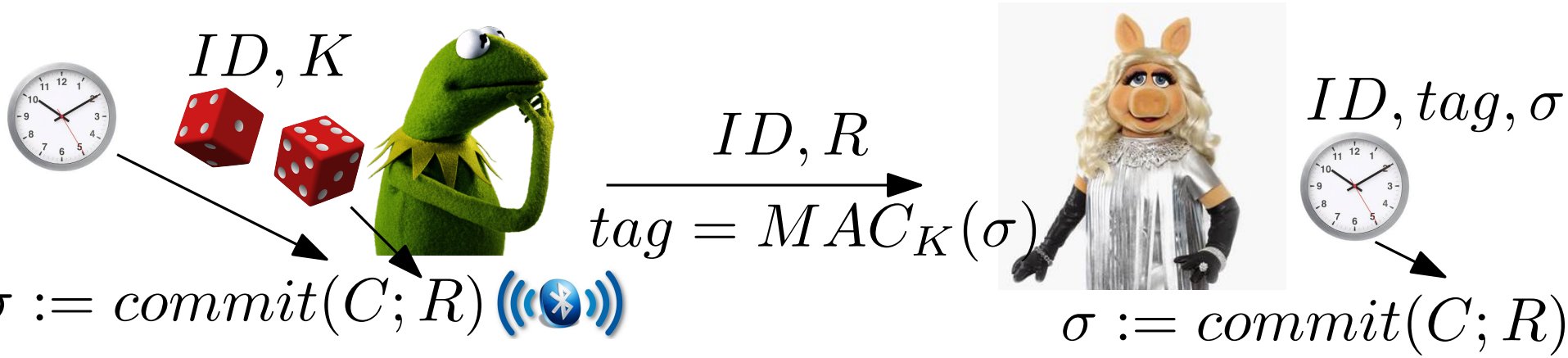


Preventing Relay and Replay Attacks without Privacy

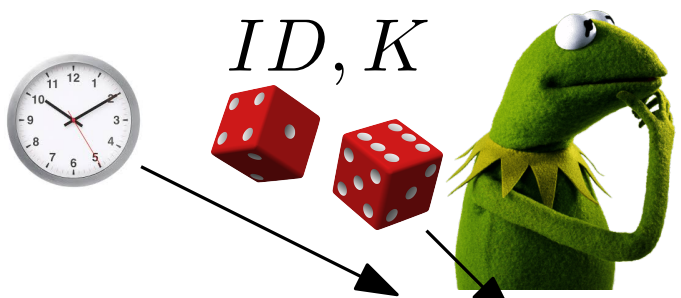




Delayed Authentication (eprint 2020/418)



Delayed Authentication (eprint 2020/418)



ID, K

$\sigma := commit(C; R)$

ID, R

$tag = MAC_K(\sigma)$

ID, tag, σ

$\sigma := commit(C; R)$

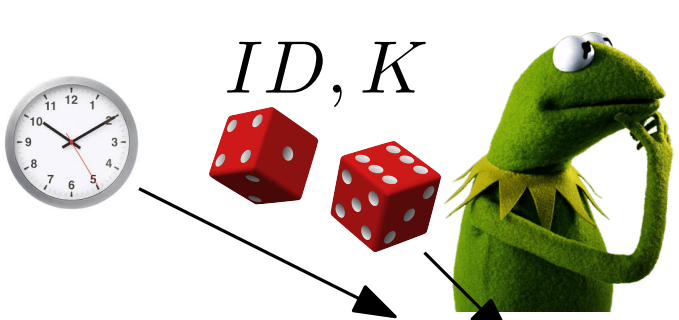
ID, K

ID, K

$tag \stackrel{?}{=} MAC_K(\sigma)$

ID, tag, σ

Delayed Authentication (eprint 2020/418)



ID, K

$\sigma := commit(C; R)$

ID, R

$tag = MAC_K(\sigma)$

ID, tag, σ

$\sigma := commit(C; R)$

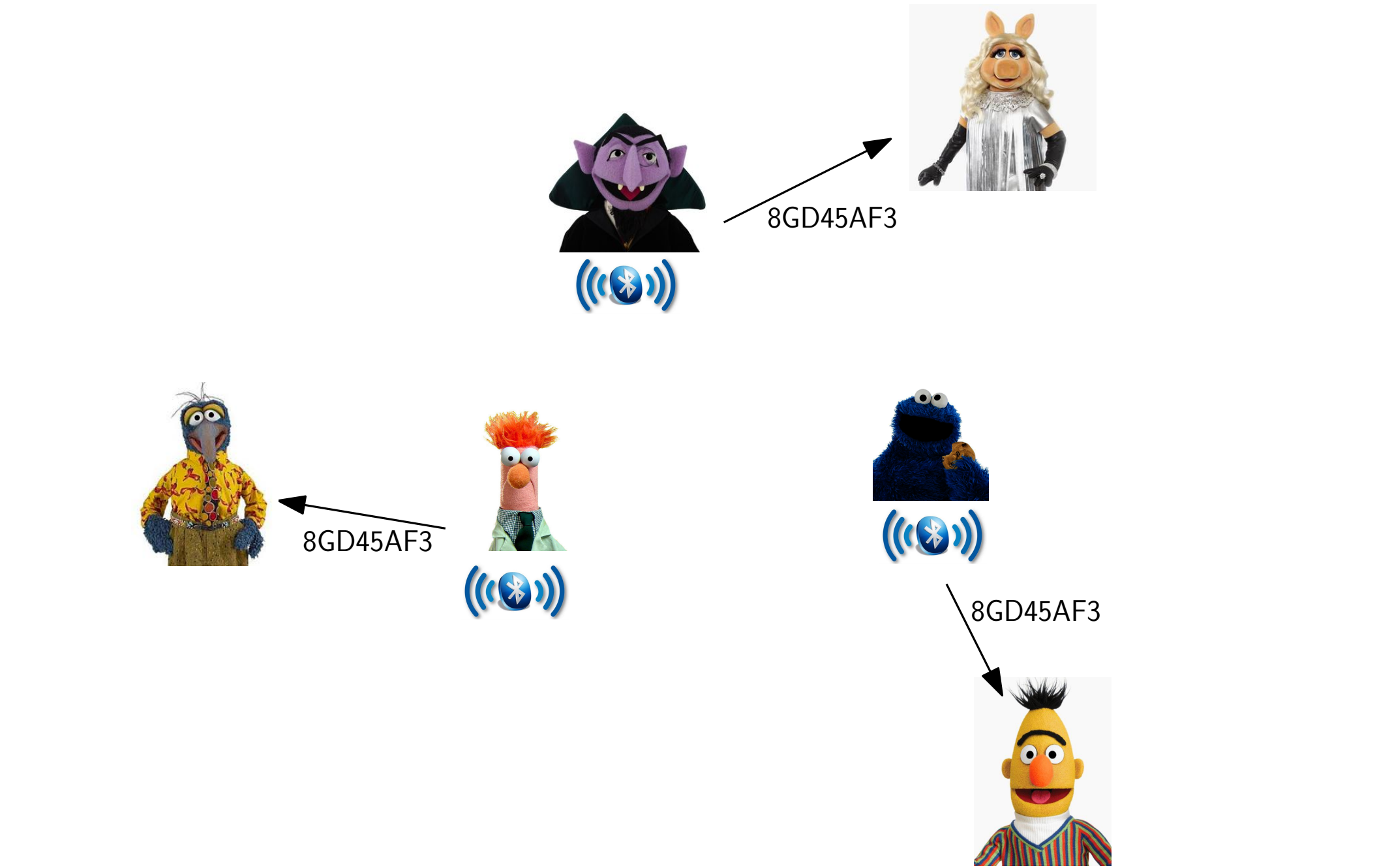
ID, K

ID, K

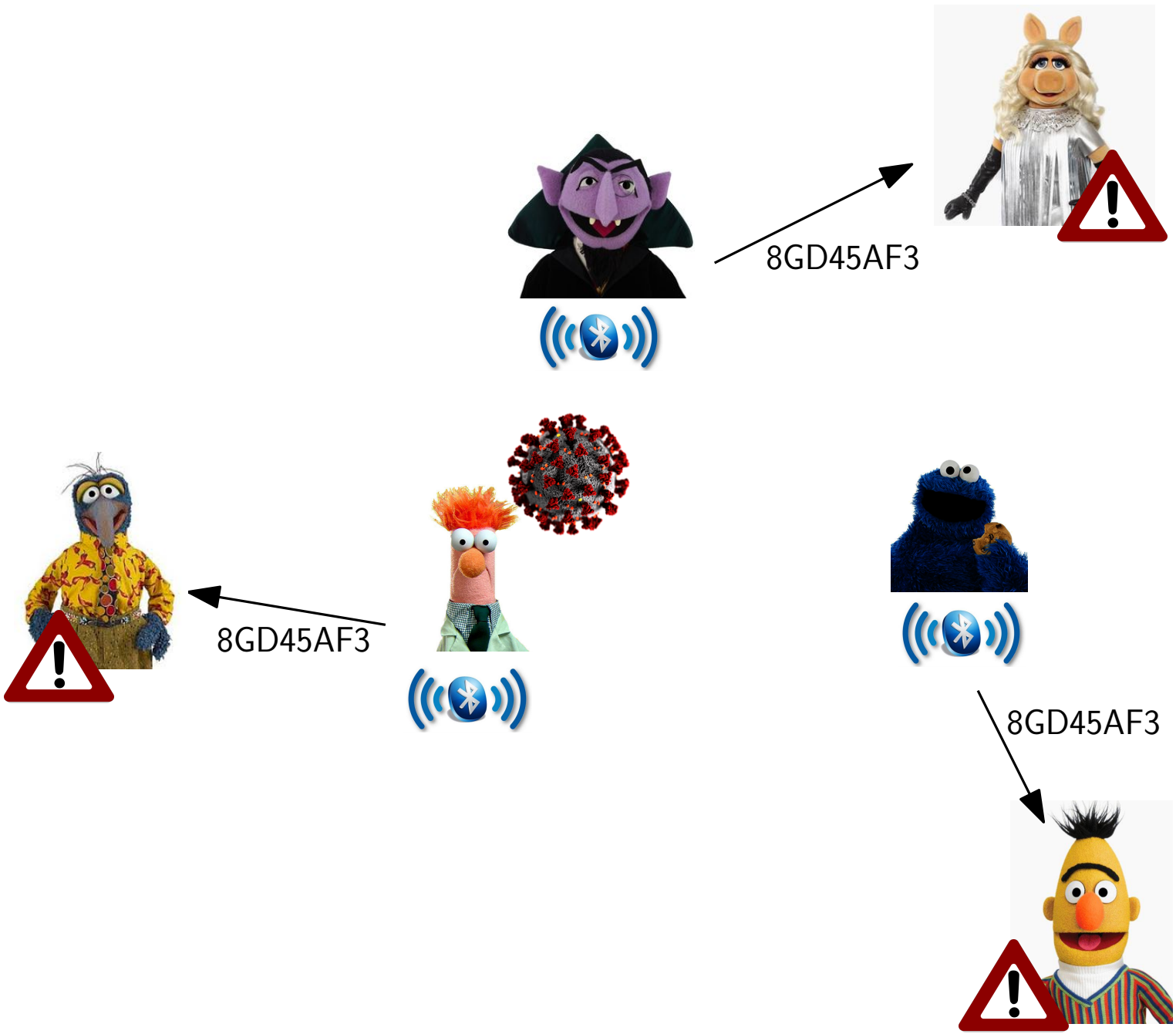
ID, tag, σ

$tag \stackrel{?}{=} MAC_K(\sigma)$

Inverse Sybil Attacks



Inverse Sybil Attacks



Inverse Sybil Attacks

https://github.com/DP-3T/documents/issues/295