Eroding RFID Privacy

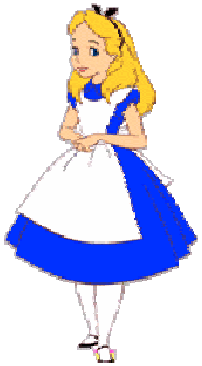
CCC Congress '06

Karsten Nohl

Mr. Jones in 2020

Courtesy: Ari Juels

People Tracking



RFID Privacy: A Multilayer Problem†

Identifying information is leaked from:

- Protocol Layer 
- Physical Layer
- Side-Channels

†paper title, Gildas Avoine, 2005

Private Identification Protocols

Basic hash protocol (Weis et al., 2003)

key: k

nonce: T

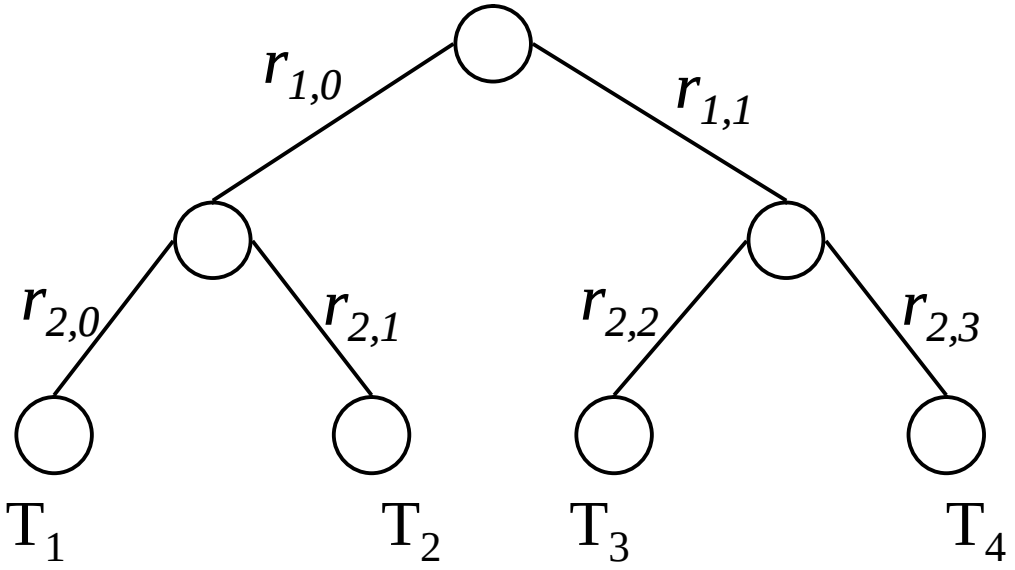
N keys

O(N) hashes

$T, H_k(T)$

Private Identification Protocols

Tree-based hash protocol (Molnar & Wagner, 2004)



O(log N) hashes

Shared secrets compromise privacy

Towards a Realistic Attacker

Stronger success criterion:

Correlate several readings.

But attack also becomes easier:

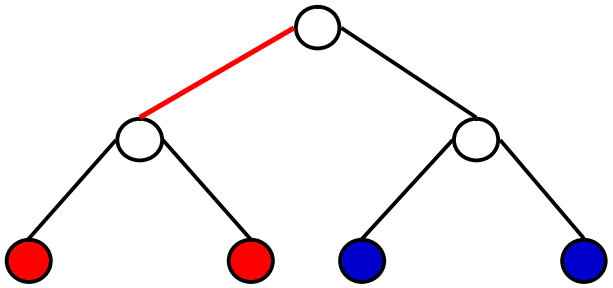
Several tags per person and

Attack focus is limited.

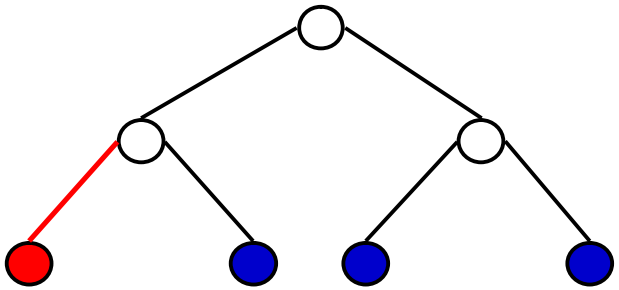
Need good metric for disclosed information.

Privacy Metric

Measure for Disclosed Information



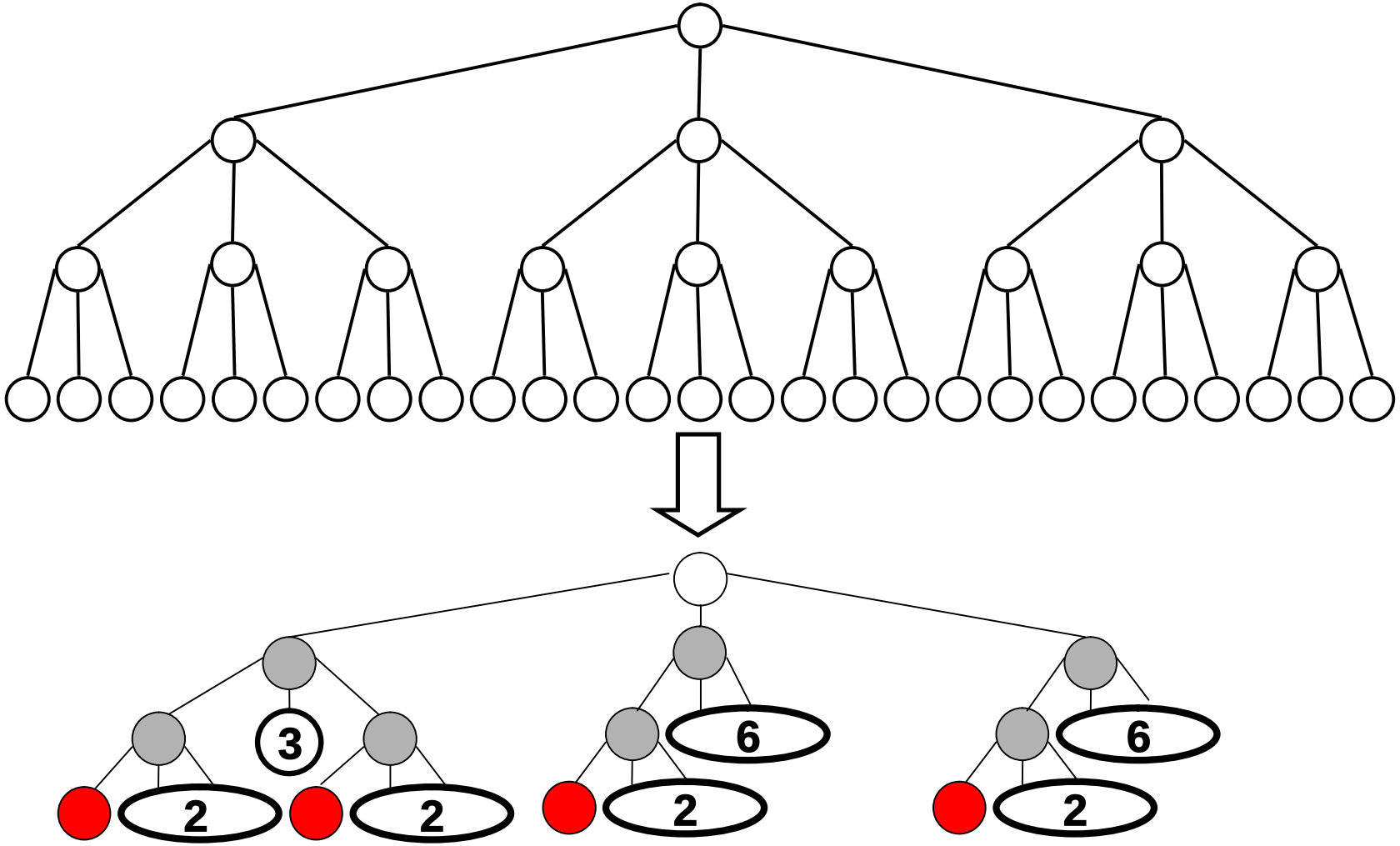
1 bit



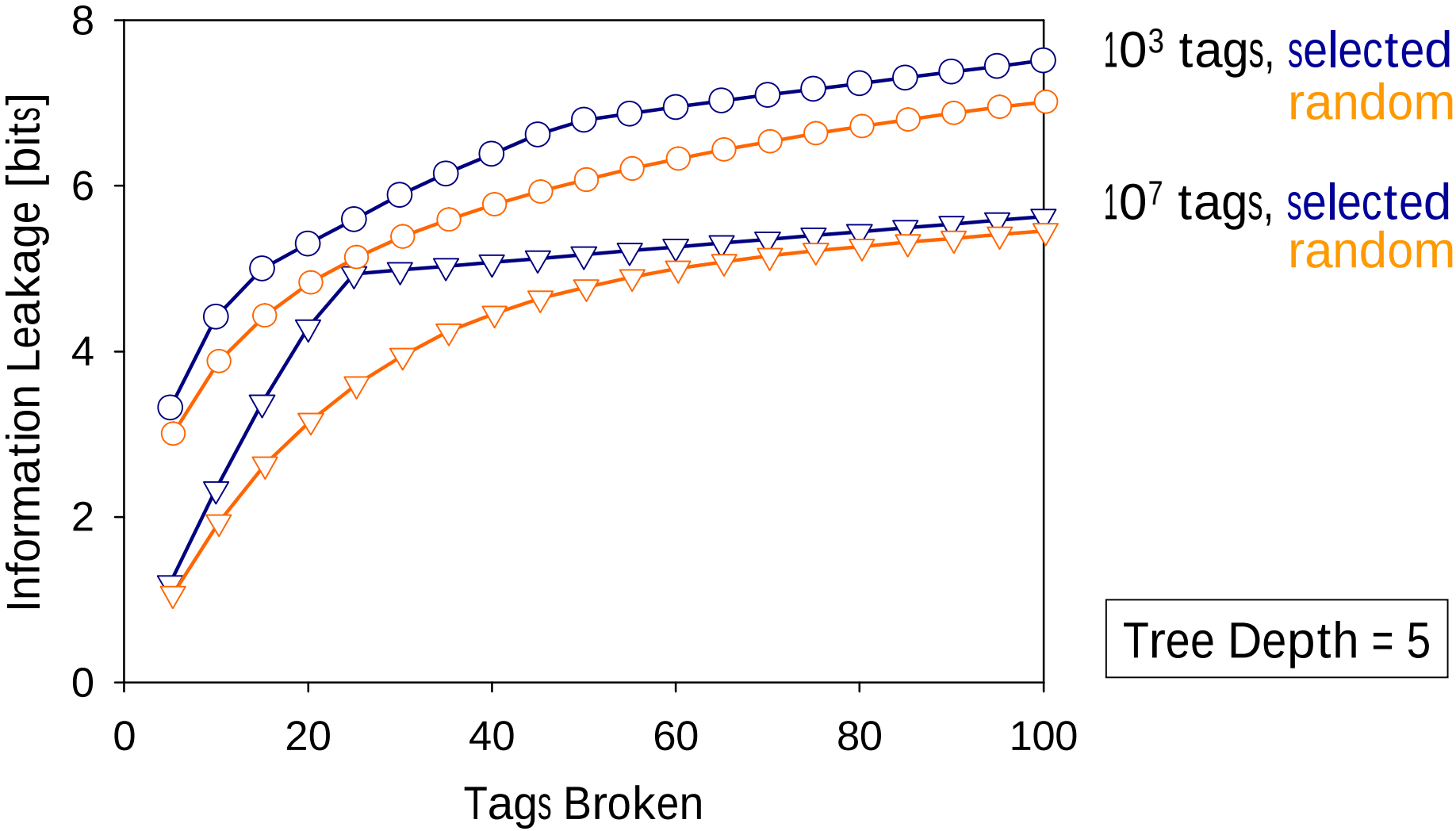
0.81 bit

$= 1/4 \log_2(4)$
$+ 3/4 \log_2(4/3)$

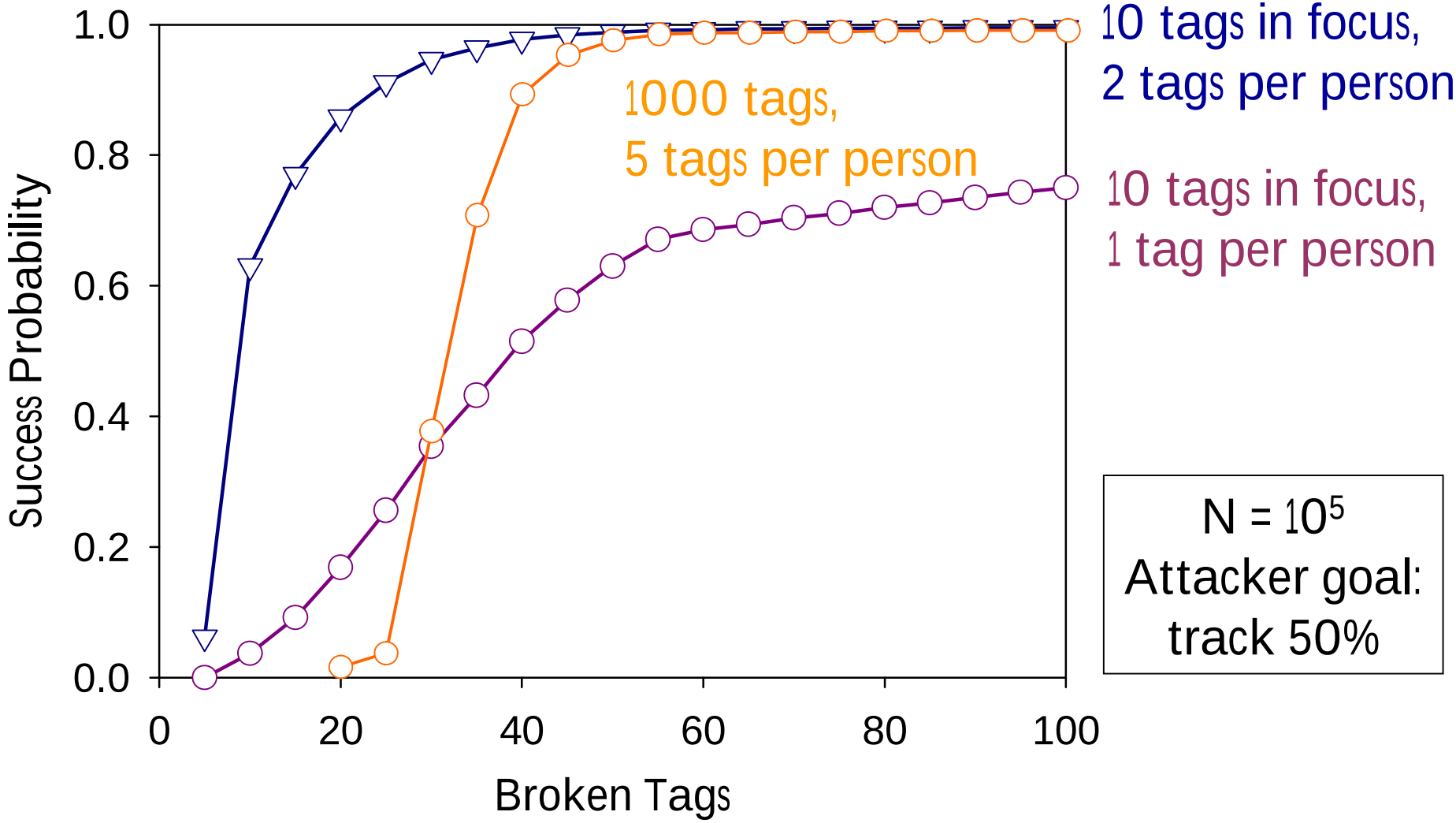
Grouping Tags in Tree



Information from Tree



Tracking Individuals

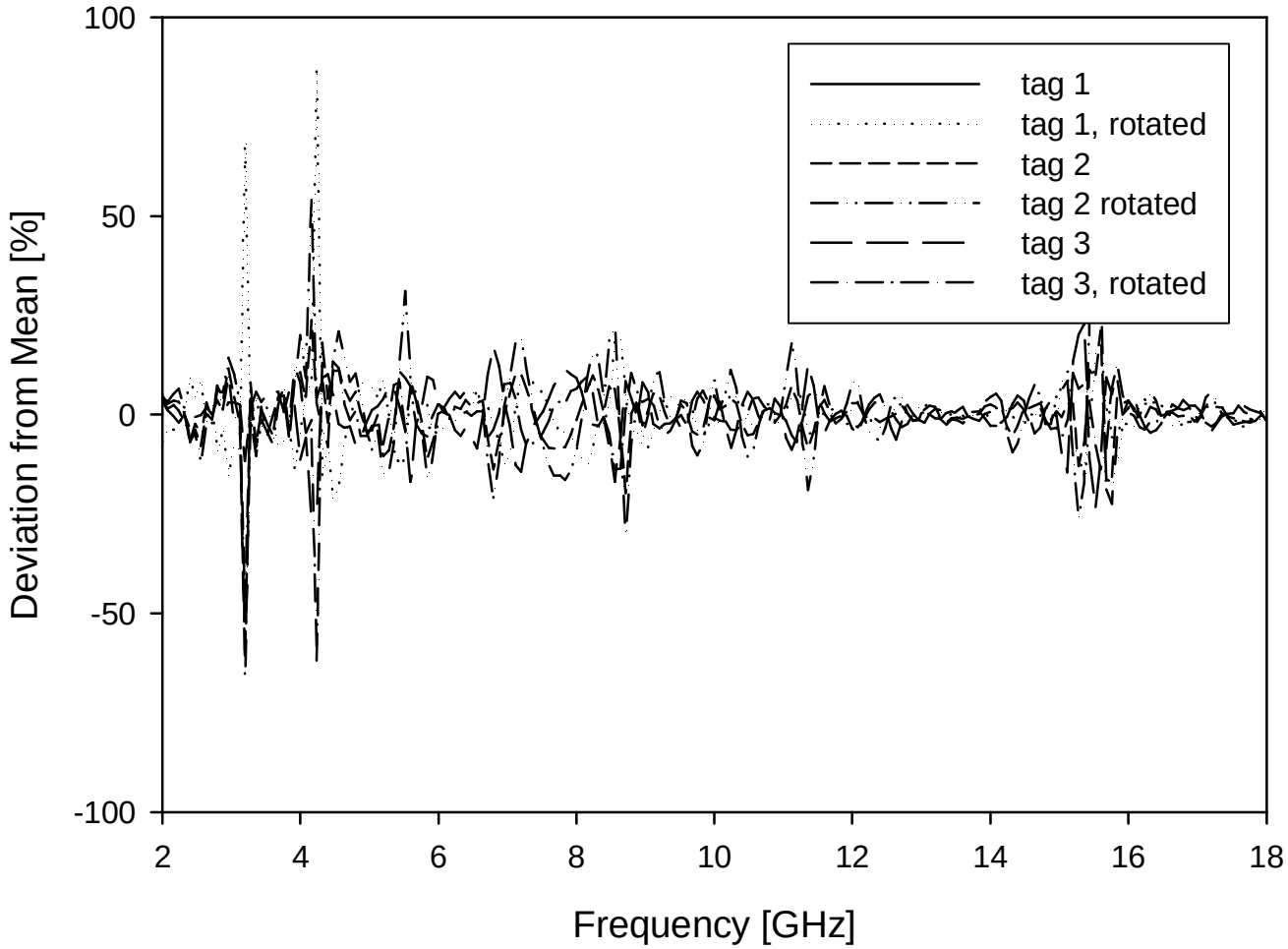


Physical Layer Privacy

Tags must not be distinguishable!

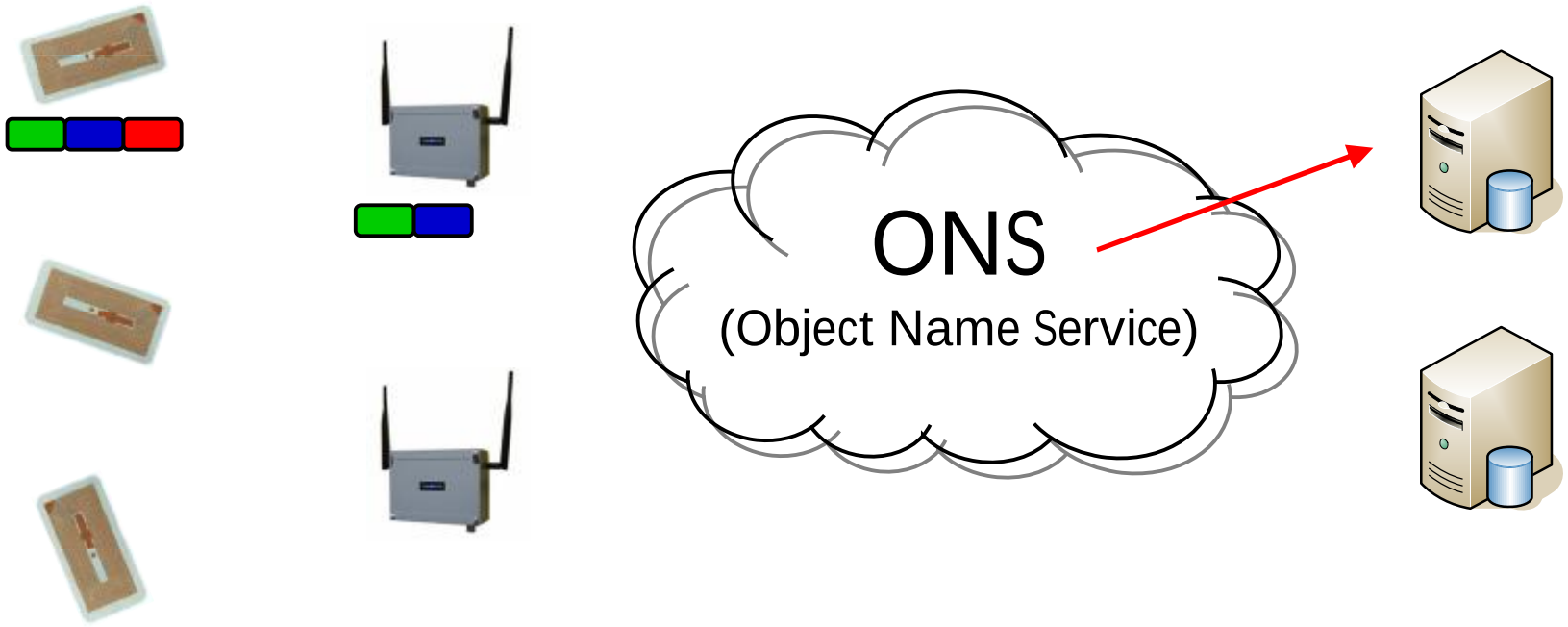
Physical Layer Information

Detectable Variation Among Similar Antenna Shapes



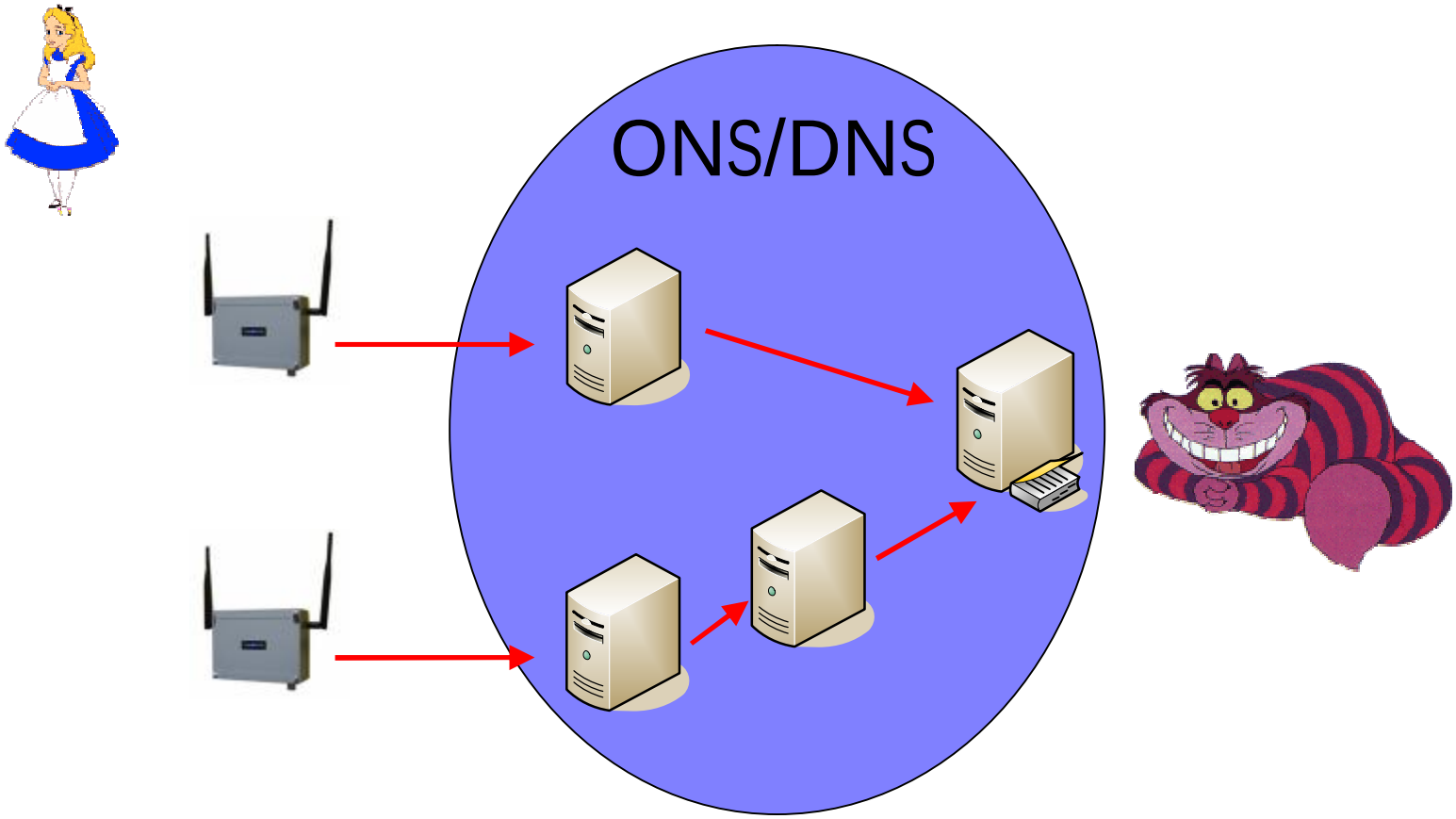
System Level Privacy

RFID System must not leak information!

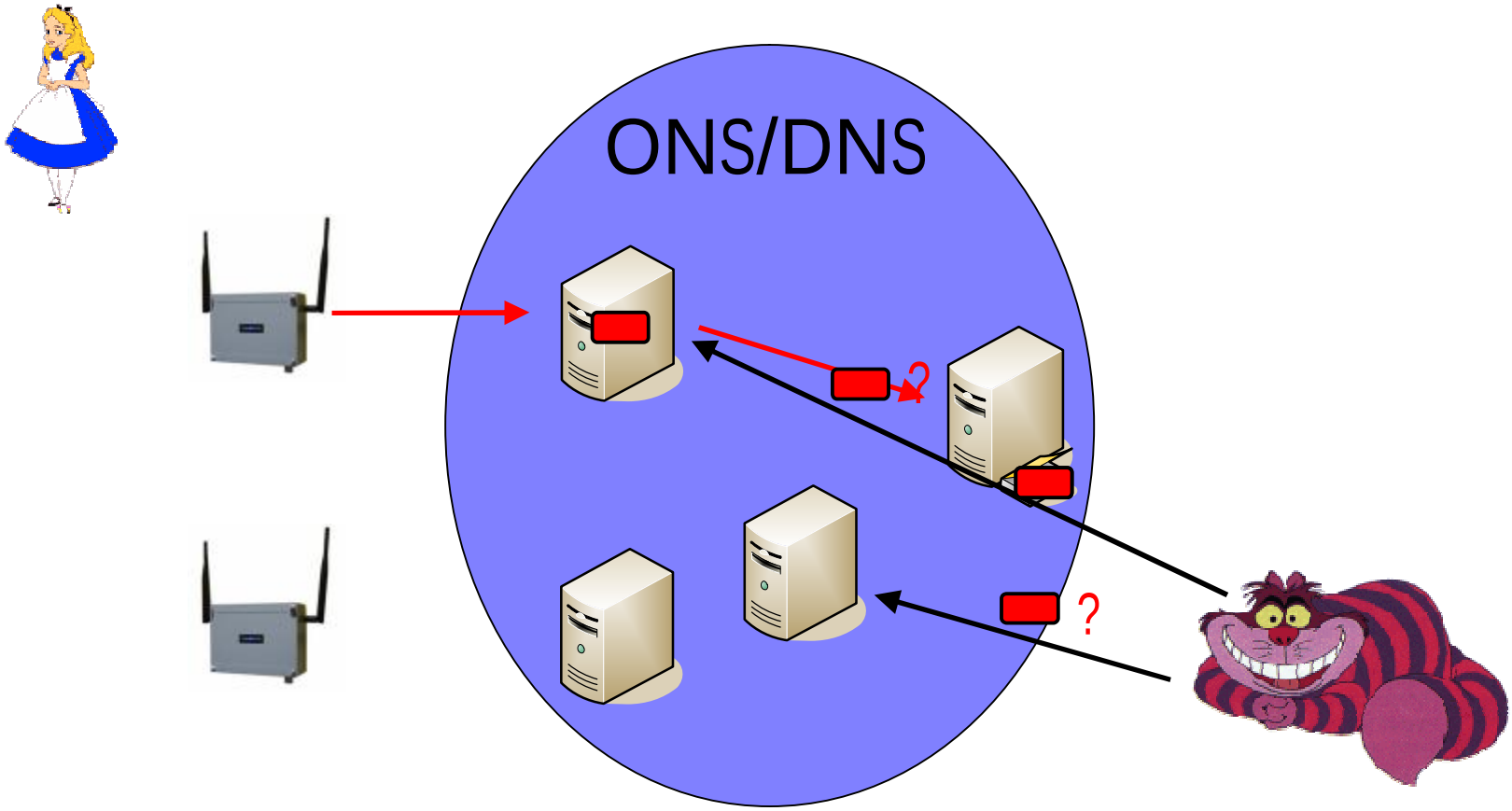


tags readers information lookup information storage

ONS Tracking



Passive ONS Tracking



Conclusion

Sacrificing perfect privacy for scalability appears to be necessary.

Need ways to measure the privacy lost and relate it to realistic attack scenarios.

Questions?

Karsten Nohl
nohl@virginia.edu