Tailing RFID Tags for Clone Detection

Davide Zanetti[1], Srdjan Capkun[1], and Ari Juels[2]

[1]Institute of Information Security, ETH Zurich, Switzerland
{zanettid,capkuns}@inf.ethz.ch

[2]RSA, The Security Division of EMC
ari.juels@rsa.com

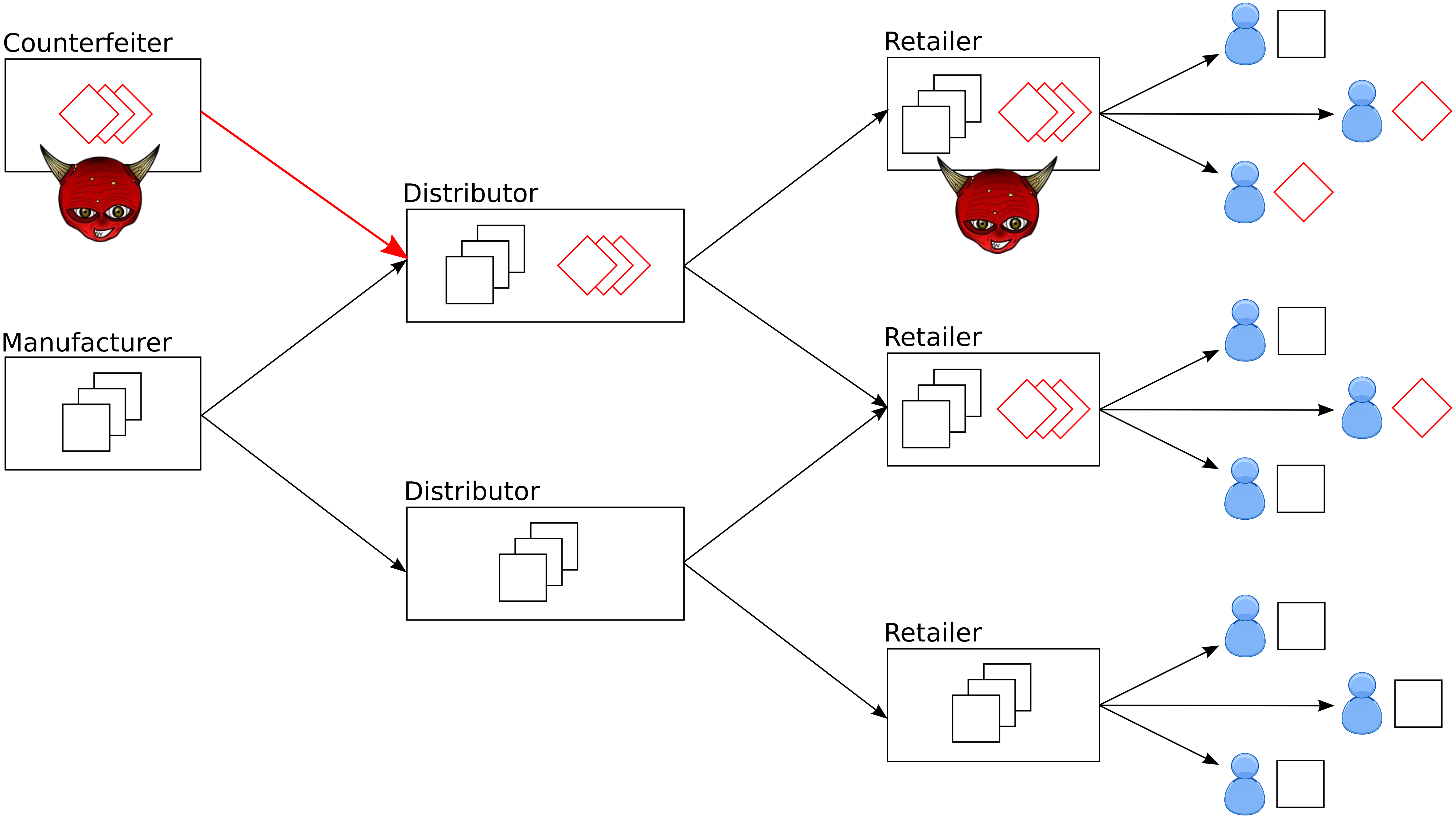
NDSS 2013

San Diego, February 27

Counterfeiting

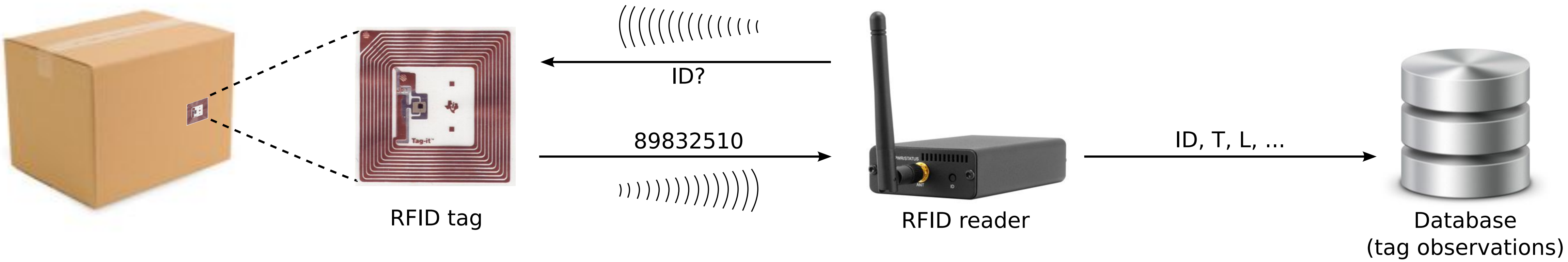
- Financial losses
- Health risks (e.g., using counterfeit pharmaceutical)
- Fraud (useless, defective, of a lower quality, dangerous)

Counterfeiting

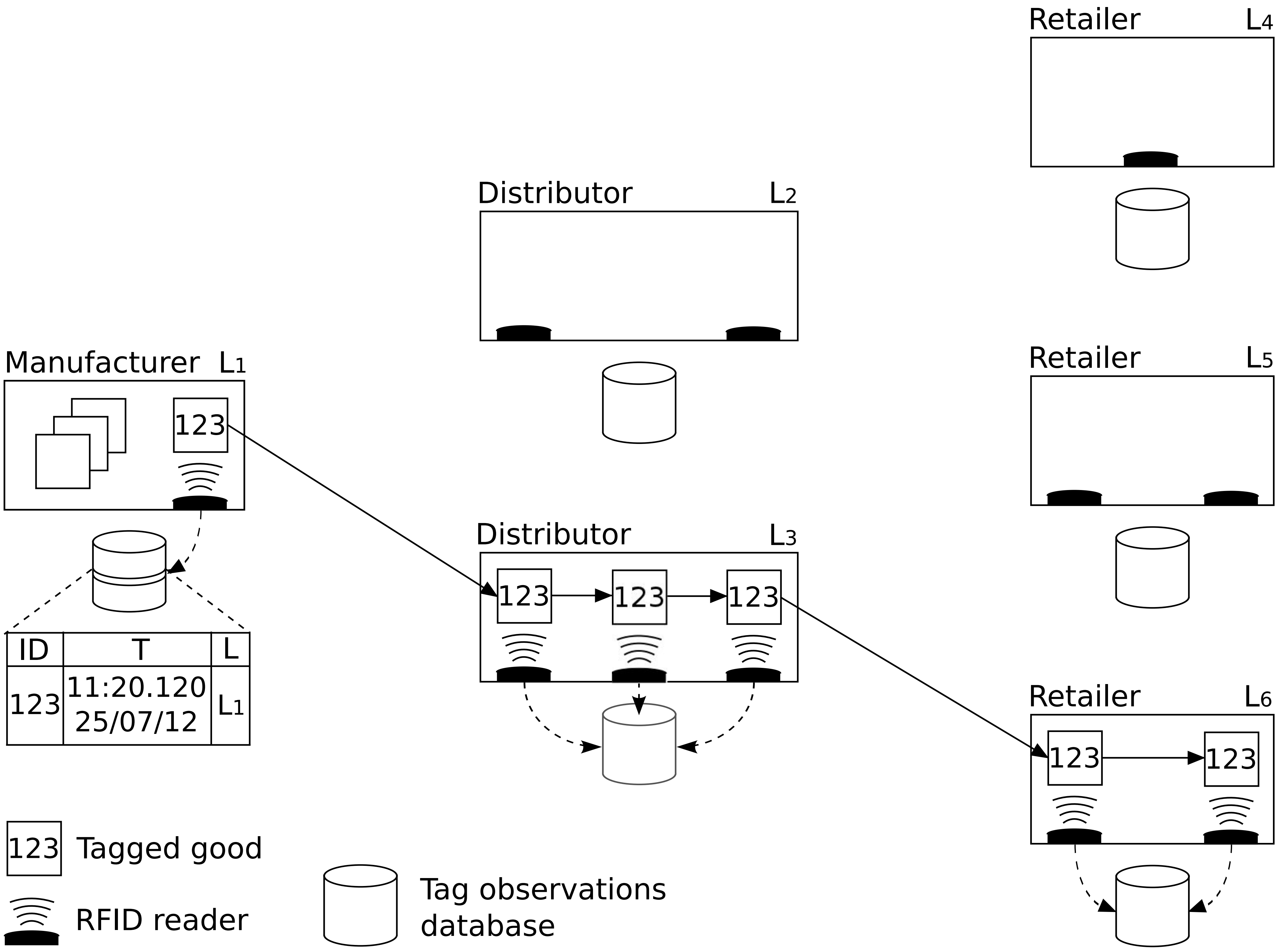


- Distribution through black, grey, and white markets (supply chains)
- Consumers ***trust*** white (and grey) markets

RFID and Supply Chains



RFID and Supply Chains



Manufacturer L_1

Distributor L_2

Distributor L_3

Retailer L_4

Retailer L_5

Retailer L_6

123

ID	T	L
123	11:20.120 25/07/12	L_1

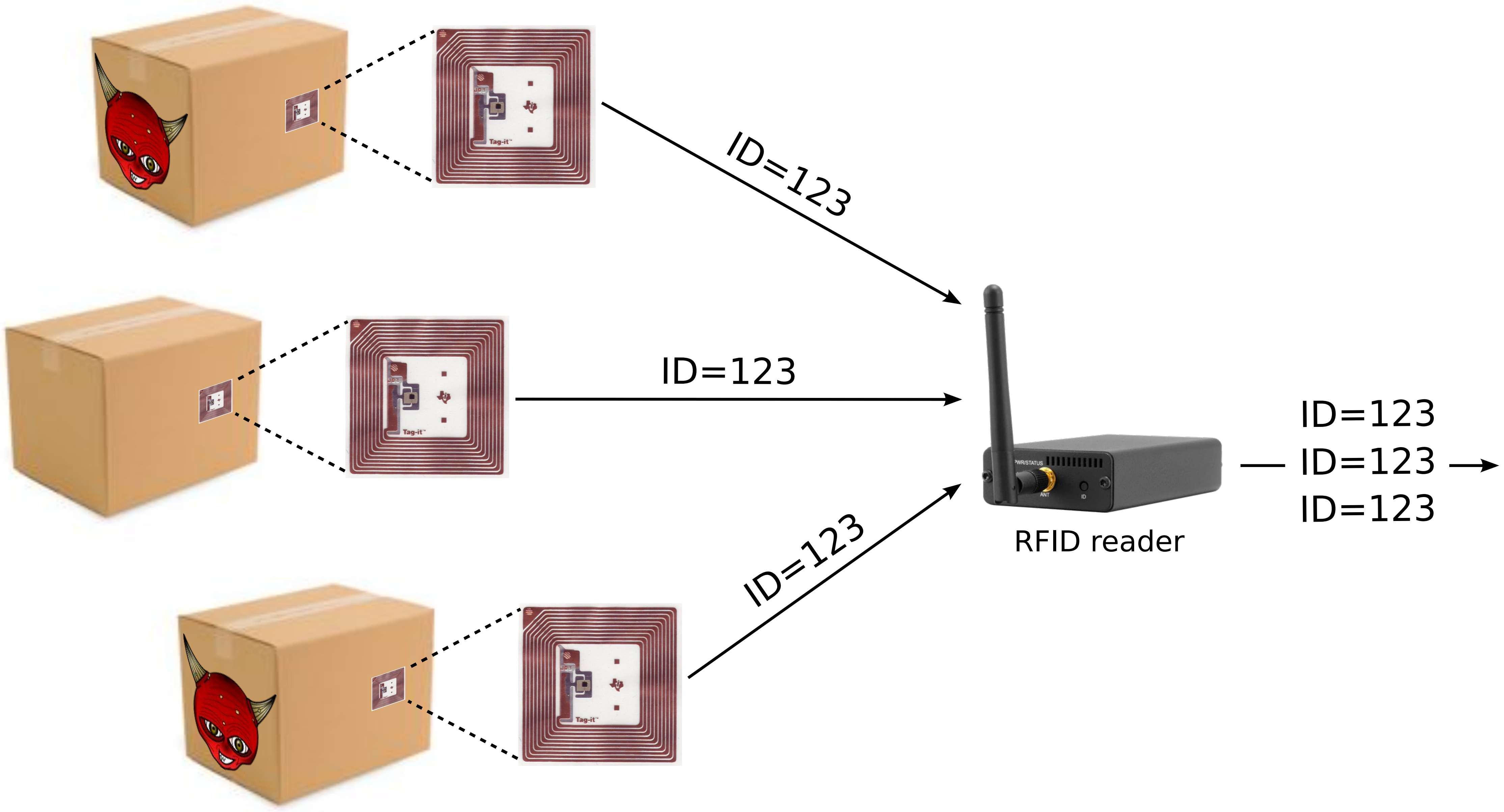
123 Tagged good

RFID reader

Tag observations database

RFID-based (Anti-)counterfeiting

- Tag identification does not guarantee ***authenticity***
- Tag authentication needed to prevent/detect ***counterfeits/clones***



Tag Authentication Solutions

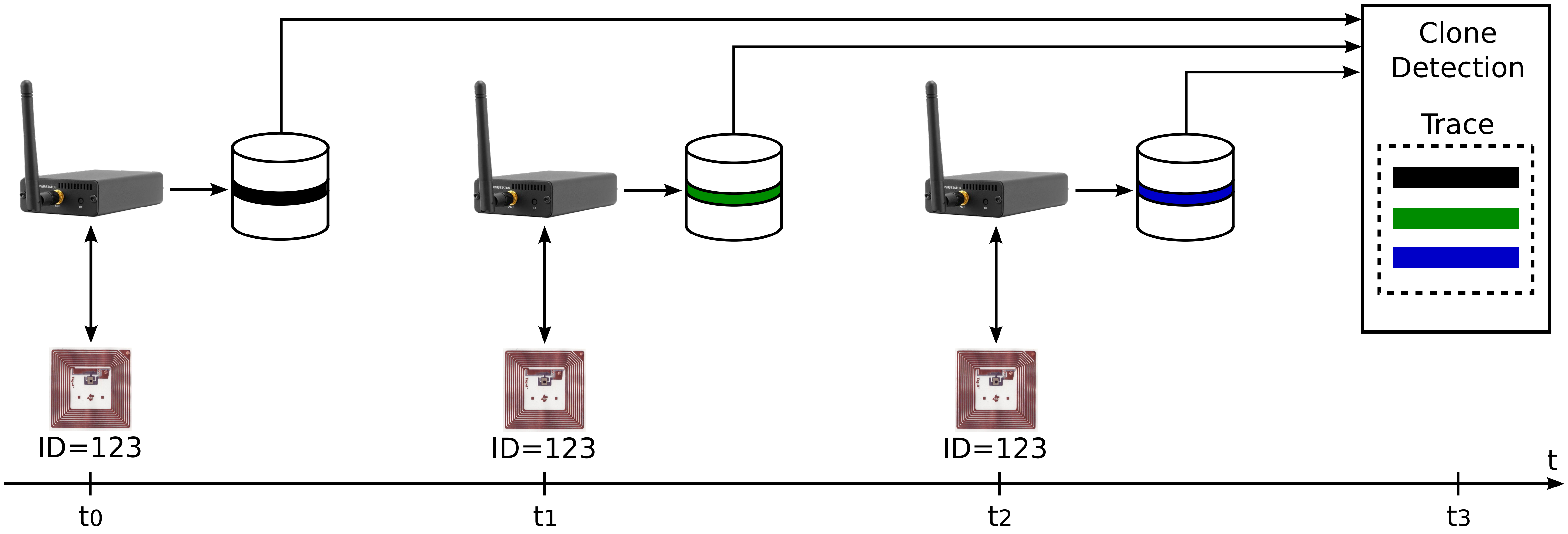
- Tag authentication based on what a tag ***holds***
  - Use crypto (standard or ad-hoc) or (ultra-)lightweight primitives
  - ***Drawbacks***
    - Standard crypto is expensive for supply-chain (low-cost) tags

MD5:	8420 GE
AES (128 bits):	3100-3600 GE
ECC (NIST B-163):	12000 GE
Supply-chain tags (no security):	5000-15000 GE

    - Require non-trivial key-distribution mechanisms
    - Simplified designs led to several key-recovery attacks
    - Require tamper resistance and side-channel protection

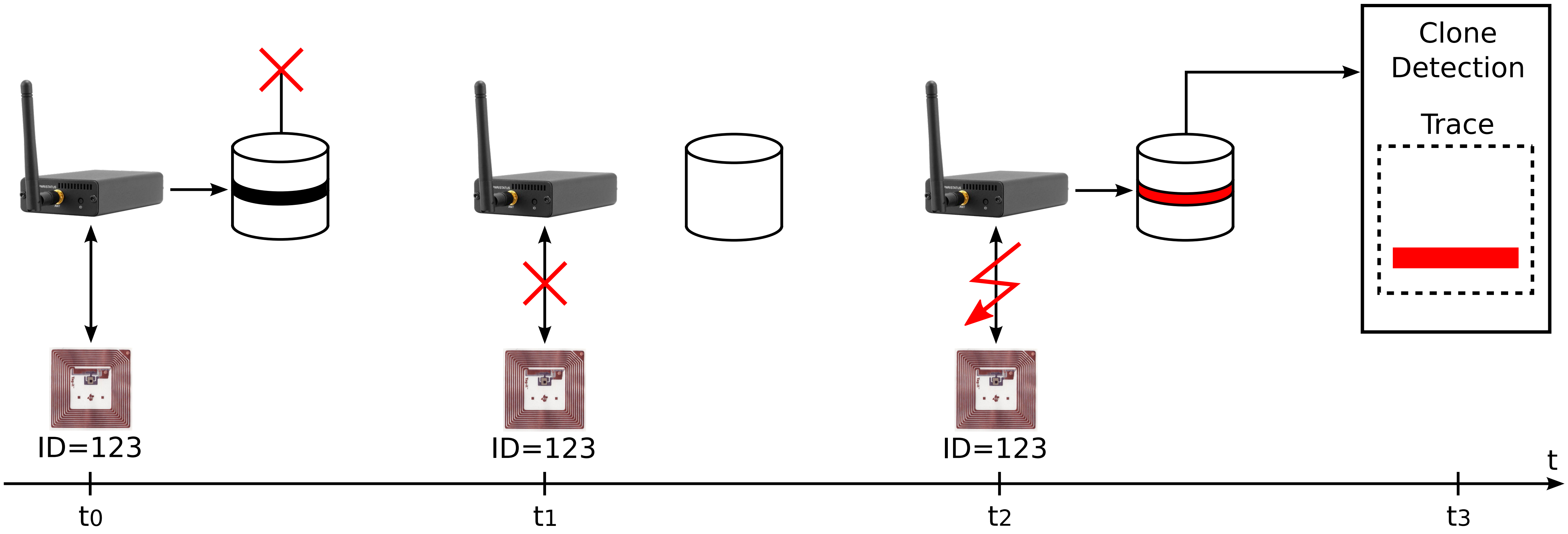
Tag Authentication Solutions

- Tag authentication based on how a tag ***behaves***
  - Clone detection using tracing and plausibility checks
  - Trace: time-sorted collection of tag observations (for an ID)



Tag Authentication Solutions

- Tag authentication based on how a tag ***behaves***
  - Clone detection using tracing and plausibility checks
  - Trace: time-sorted collection of tag observations (for an ID)
- ***Drawbacks:*** false alarms and clone misses due to
  - Missing and corrupted tag observations
  - Tag behavioral deviations



Problem Statement

- Tag authentication / clone detection mechanism:
  - Suitable for low-cost tags and RFID/supply-chain infrastructures
  - Effective under external and internal adversaries
  - Reliable within real-world supply-chain deployments
  - Scalable (front- and back-end operations)

Tailing

- Trace-based clone detection for RFID-enabled supply chains
- Write random values to tags at each tag-reader interaction

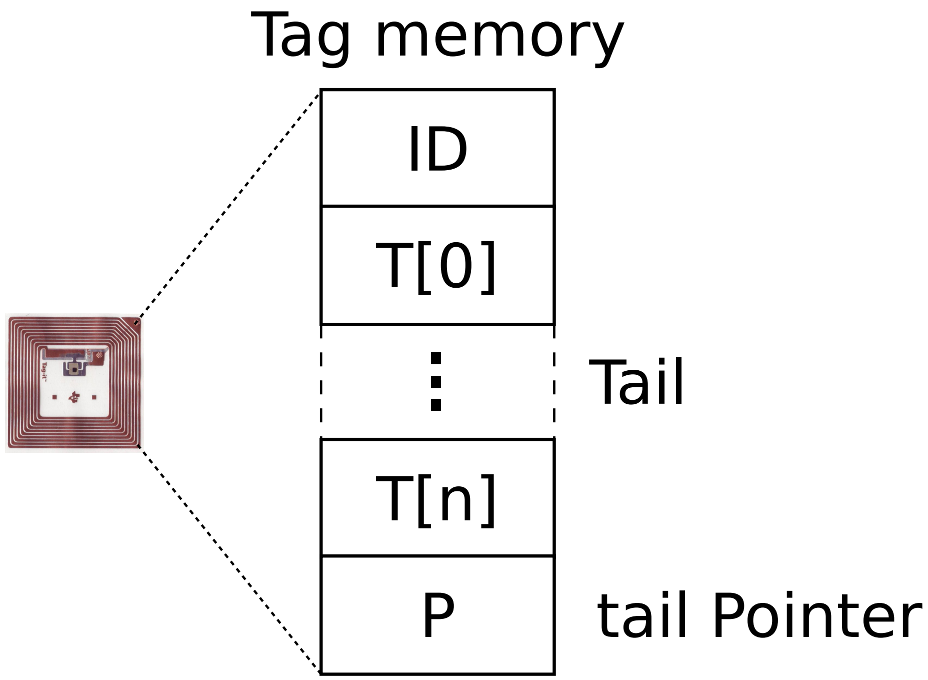
  ➡ Creates in each tag a ***tail*** of random values
- Check how tail evolved over time for ***clone evidence***

Tailing

- Trace-based clone detection for RFID-enabled supply chains
- Write random values to tags at each tag-reader interaction

➡ Creates in each tag a ***tail*** of random values

- Check how tail evolved over time for ***clone evidence***

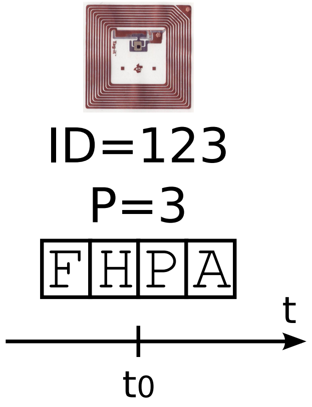


Tailing

- Trace-based clone detection for RFID-enabled supply chains
- Write random values to tags at each tag-reader interaction

➡ Creates in each tag a ***tail*** of random values

- Check how tail evolved over time for ***clone evidence***

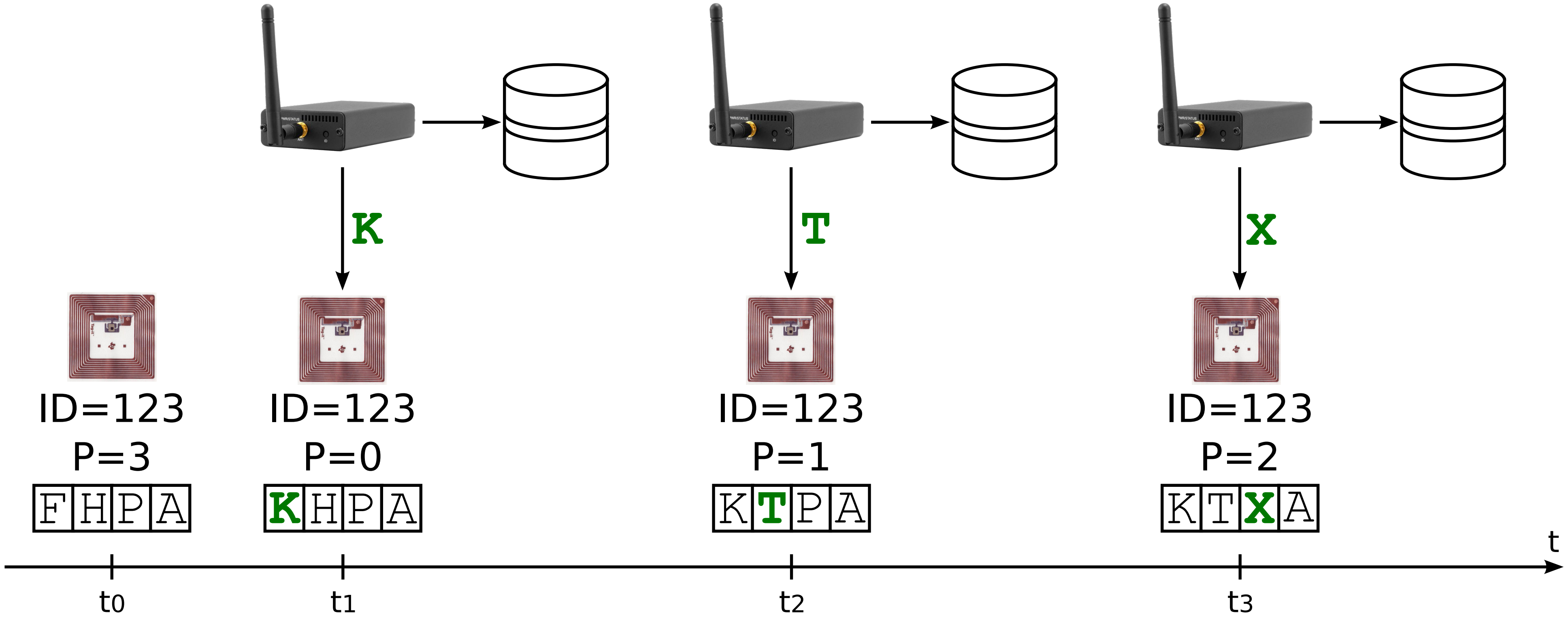


Tailing

- Trace-based clone detection for RFID-enabled supply chains
- Write random values to tags at each tag-reader interaction

➡ Creates in each tag a ***tail*** of random values

- Check how tail evolved over time for ***clone evidence***

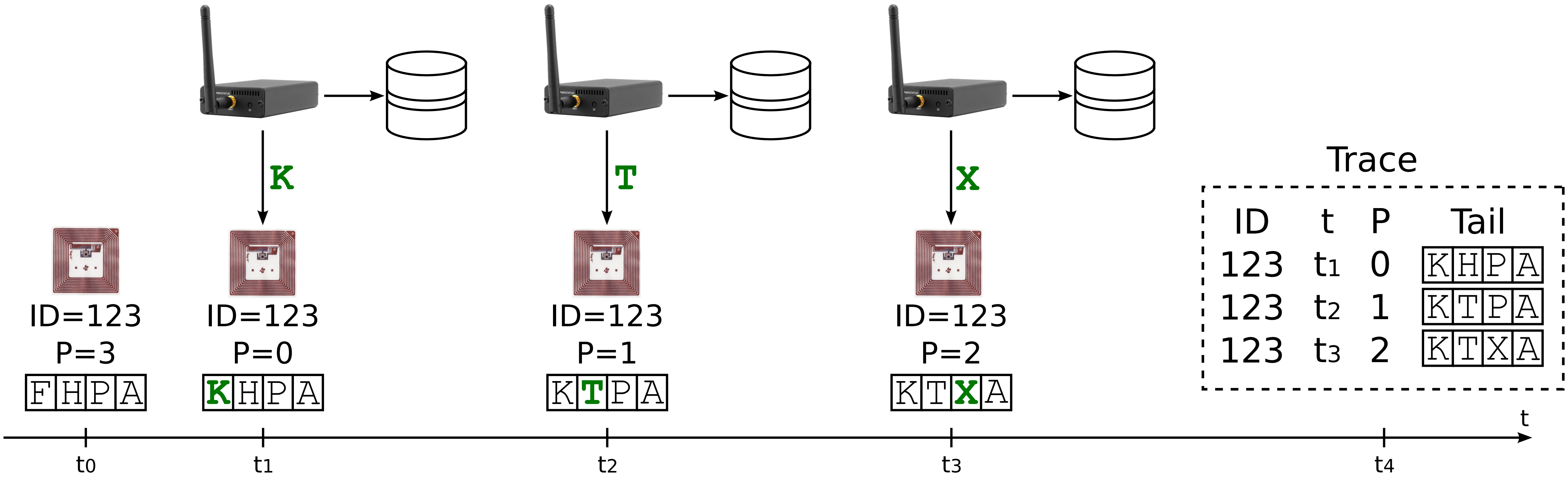


Tailing

- Trace-based clone detection for RFID-enabled supply chains
- Write random values to tags at each tag-reader interaction

➡ Creates in each tag a ***tail*** of random values

- Check how tail evolved over time for ***clone evidence***

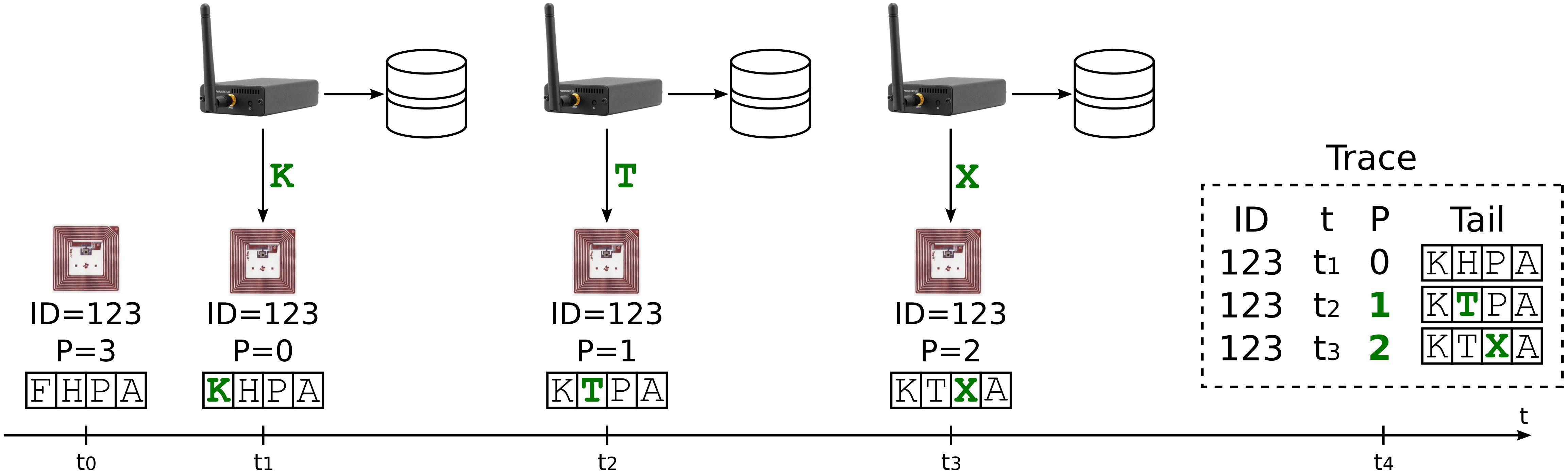


Trace

ID	t	P	Tail
123	t_1	0	KHPA
123	t_2	1	KTPA
123	t_3	2	KTXA

Tailing: Effectiveness

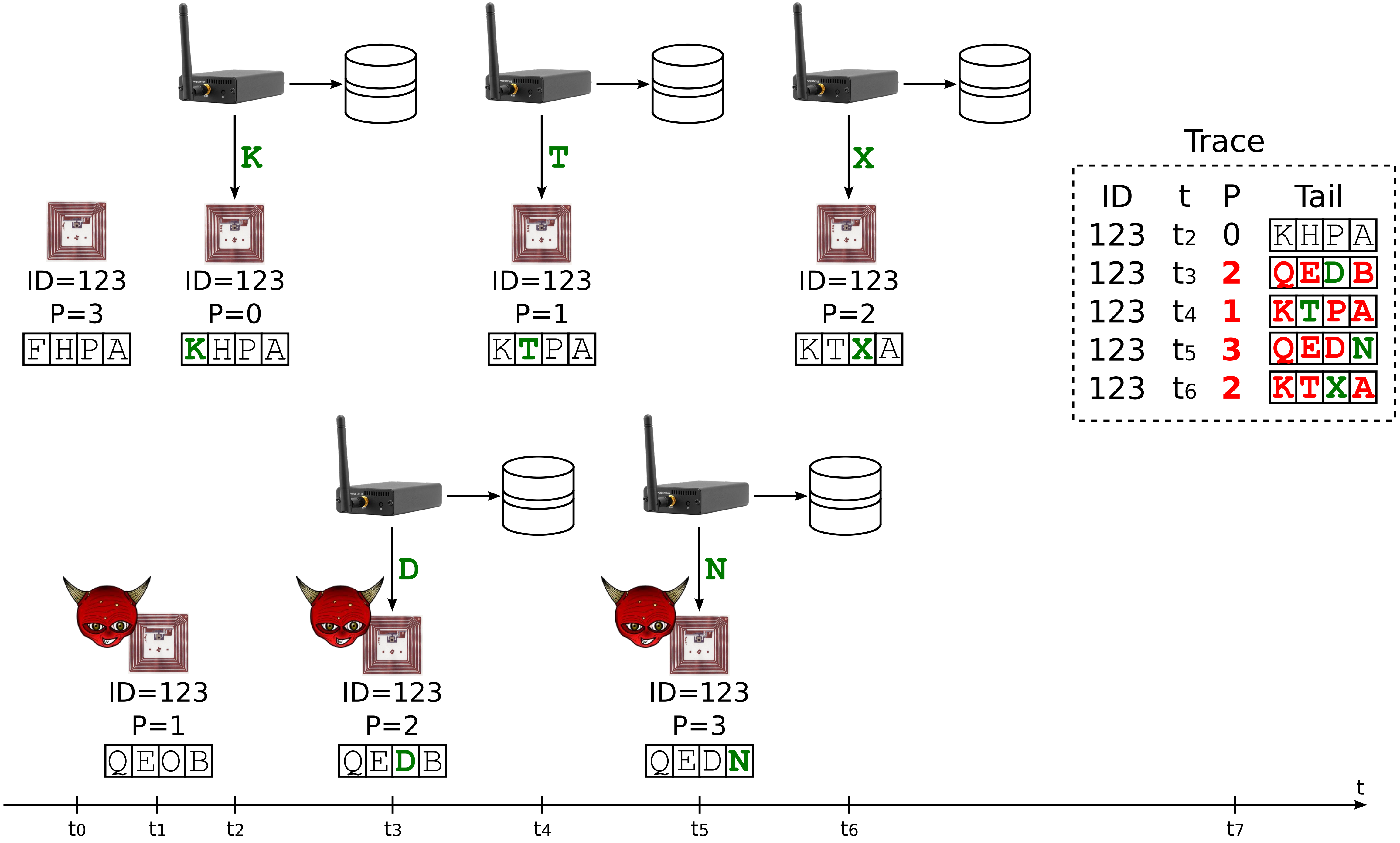
- Tailing builds relationships between consecutive tag observations



ID	t	P	Tail
123	t_1	0	K H P A
123	t_2	**1**	K **T** P A
123	t_3	**2**	K T **X** A

Tailing: Effectiveness

- Tailing builds relationships between consecutive tag observations
- Clones' observations brake them: ***tail/pointer inconsistencies***

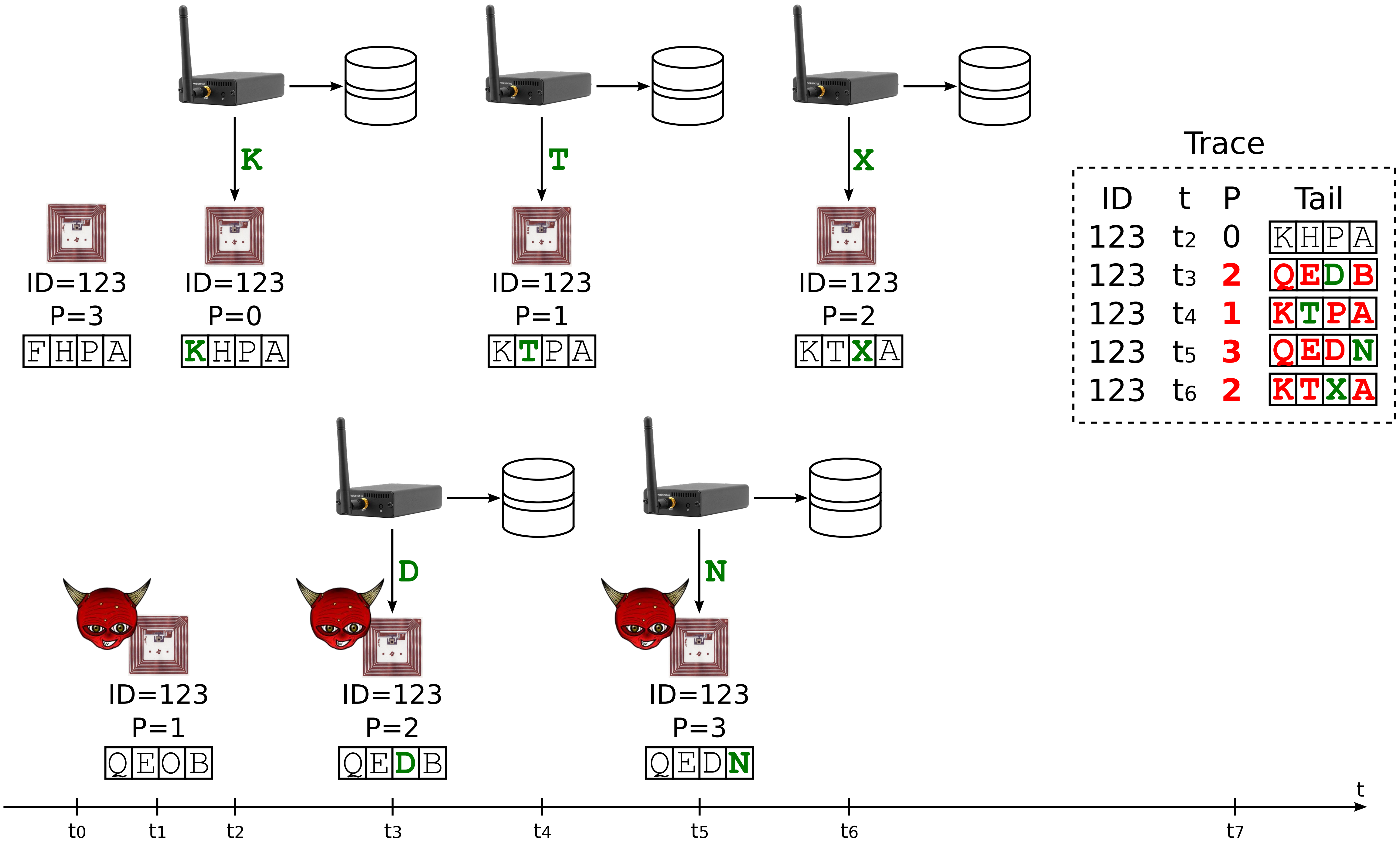


Trace

ID	t	P	Tail
123	t_2	0	KHPA
123	t_3	**2**	**QEDB**
123	t_4	**1**	**KTPA**
123	t_5	**3**	**QEDN**
123	t_6	**2**	**KTXA**

Tailing: Effectiveness

- Tailing effective with external adversaries

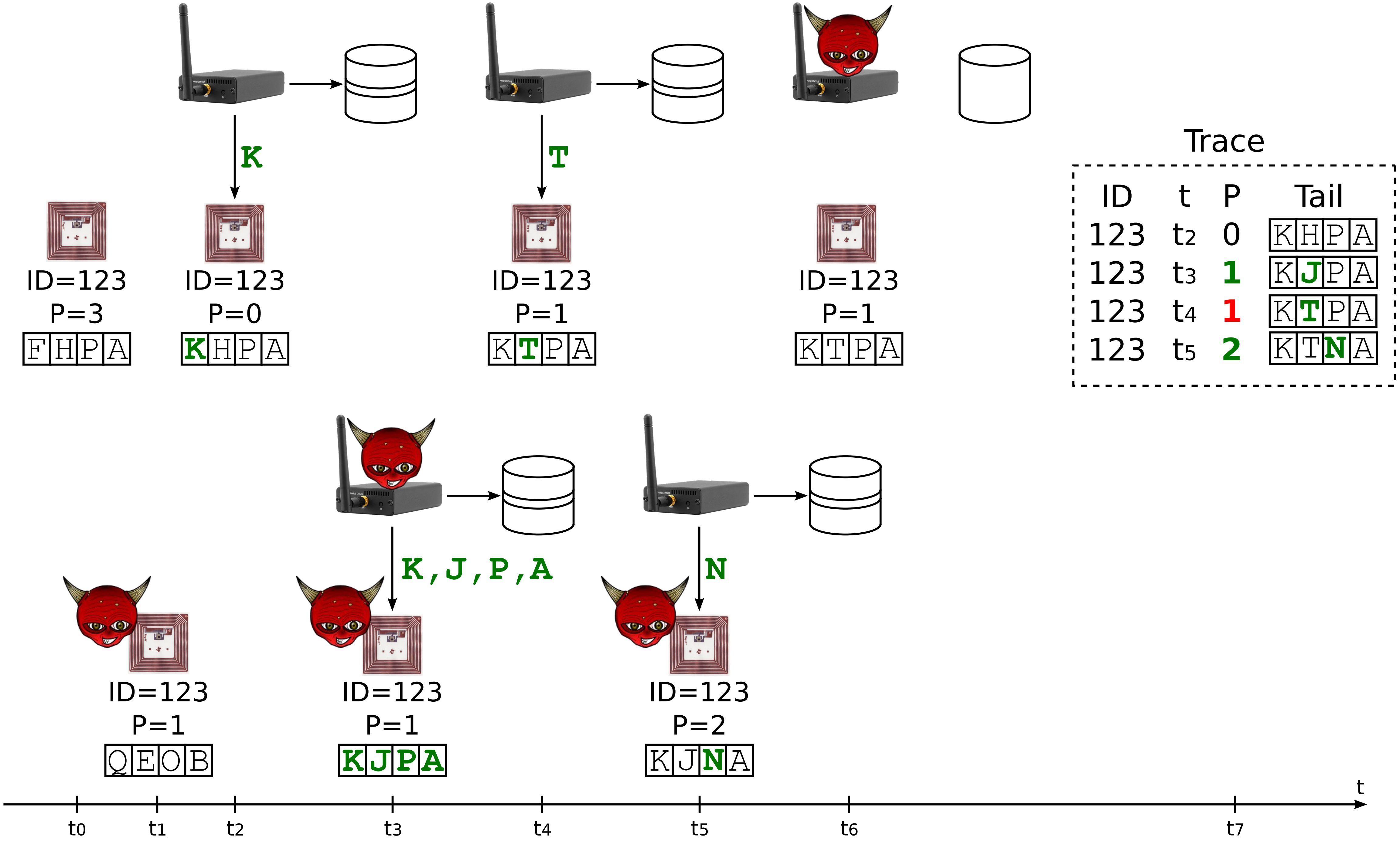


Trace

ID	t	P	Tail
123	t_2	0	KHPA
123	t_3	2	QEDB
123	t_4	1	KTPA
123	t_5	3	QEDN
123	t_6	2	KTXA

Tailing: Effectiveness

- Tailing effective even with internal adversaries:
  - Block readers, inject observations, tamper tag memory



Trace

ID	t	P	Tail
123	t_2	0	KHPA
123	t_3	1	KJPA
123	t_4	1	KTPA
123	t_5	2	KTNA

Tailing: Effectiveness

- Tailing effective even with internal adversaries:
  - Block readers, inject observations, tamper tag memory

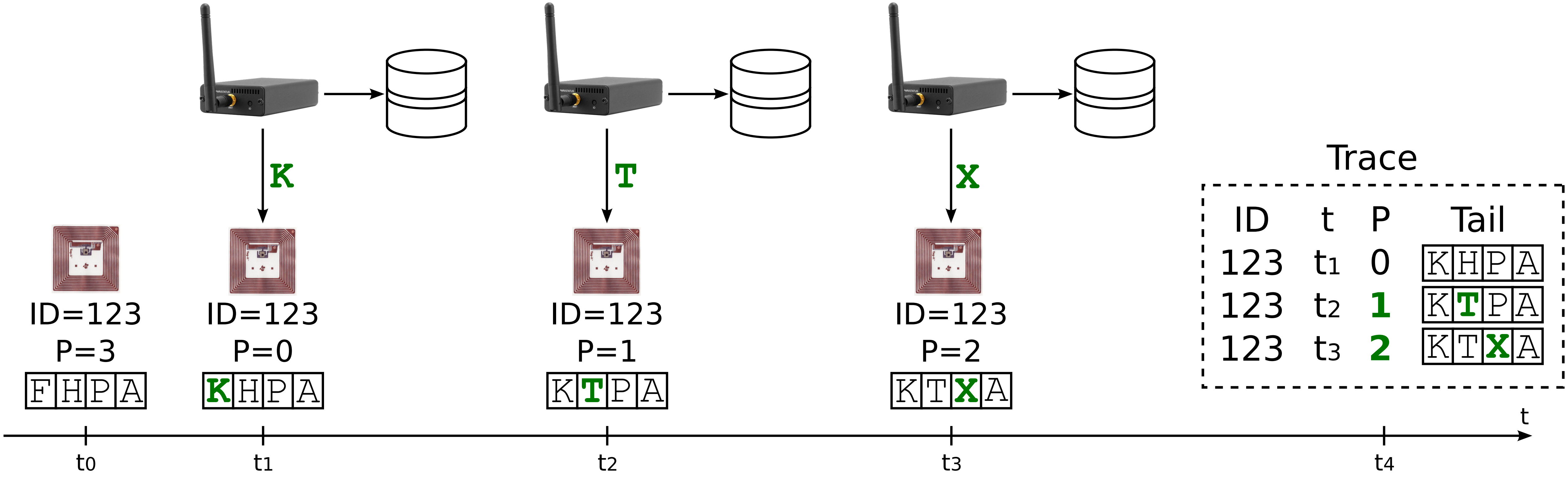
	% Adversary's success probability	# of compromised readers					
		0	1	2	3	4	5
	Inject clones	10^{-7}	-	-	-	-	-
+	Block readers	10^{-6}	0.12	0.81	3.6	12.5	100
+	Inject observations, tag memory tampering	0.19	2.2	14.8	52	89.9	100

Tailing: Reliability

- Tailing does not rely on pre-defined information
  - Uses purpose-built information in the form of tails
  - Not affected by tag behavioral deviations

Tailing: Reliability

- Tailing does not rely on pre-defined information
  - Uses purpose-built information in the form of tails
  - Not affected by tag behavioral deviations
- Gradually randomizing tails preserves symbol discrepancy
  - Creates links also between non-consecutive observations
  - Mitigates negative effect of missing/corrupted tag observations

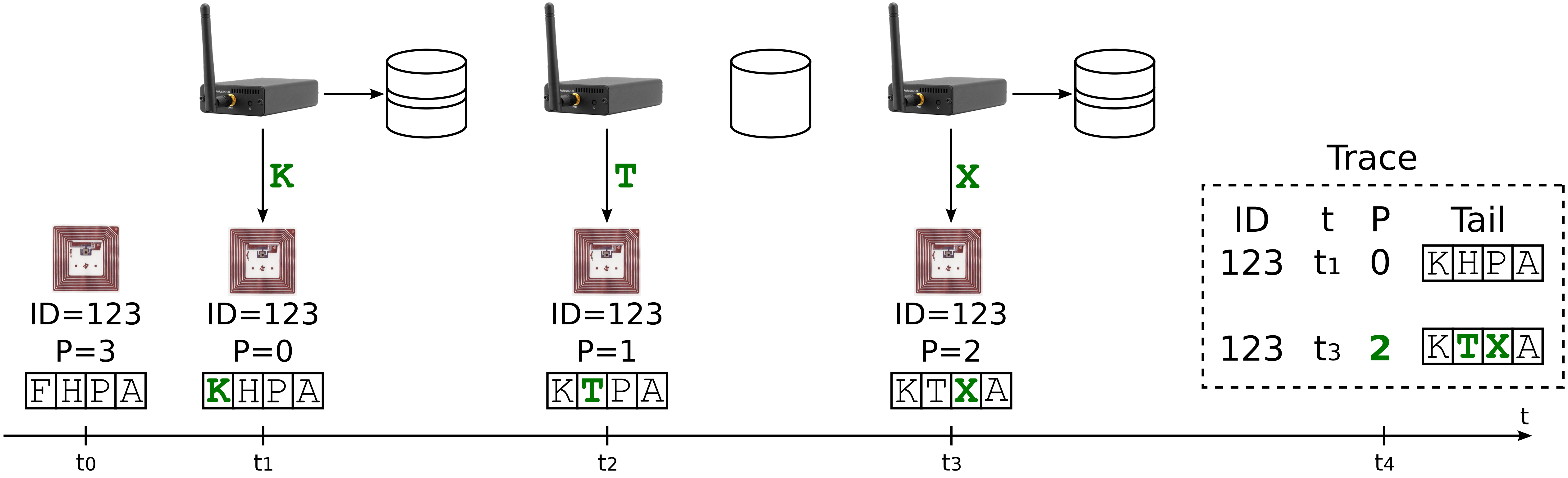


Trace

ID	t	P	Tail
123	t_1	0	K H P A
123	t_2	1	K T P A
123	t_3	2	K T X A

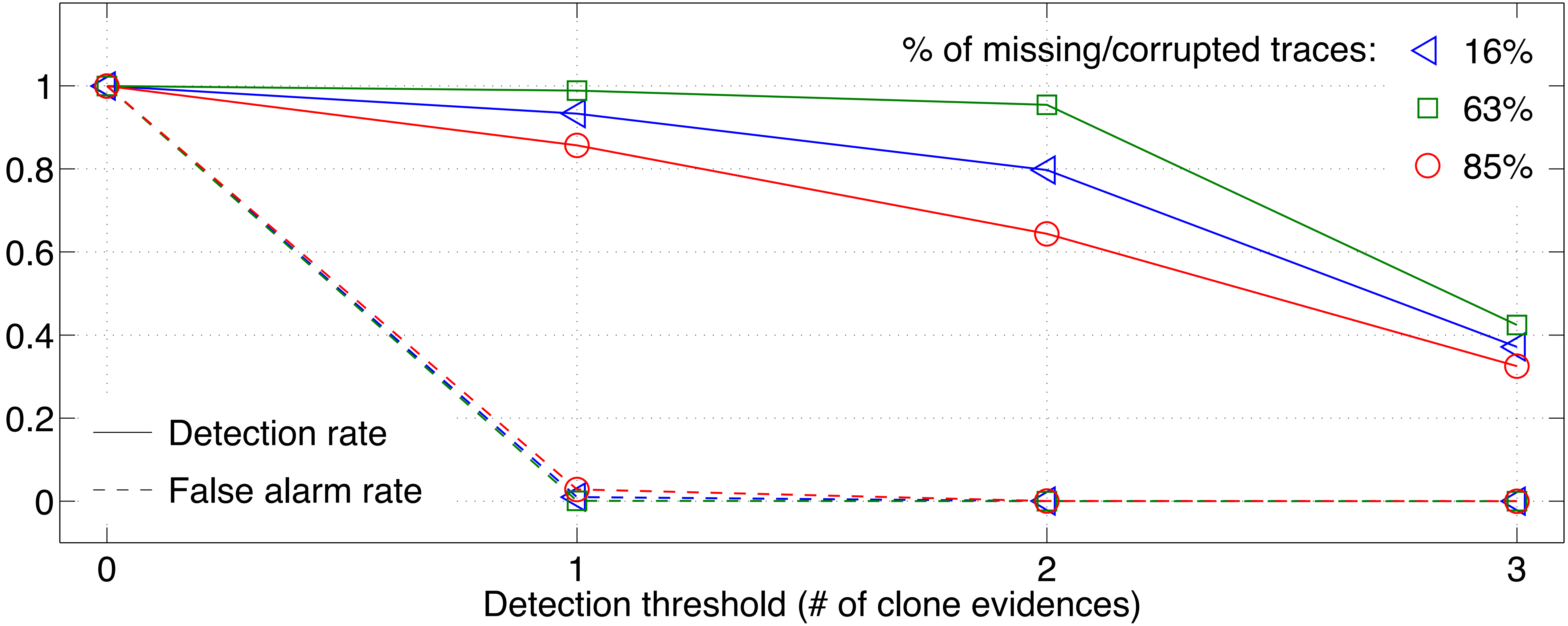
Tailing: Reliability

- Tailing does not rely on pre-defined information
  - Uses purpose-built information in the form of tails
  - Not affected by tag behavioral deviations
- Gradually randomizing tails preserves symbol discrepancy
  - Creates links also between non-consecutive observations
  - Mitigates negative effect of missing/corrupted tag observations



ID	t	P	Tail
123	t_1	0	K H P A
123	t_3	2	K T X A

Tailing: Reliability



Tailing: Performance

- Storage
  - Tailing requires ***little tag memory***, e.g., 8 bits
  - Minimal size increase in back-end databases (tails and pointers)
- Computation
  - Tags perform ***no computation***
  - Readers only perform lightweight operations (PRNG)
  - Trace verification: pairs of consecutive observations
- Communication
  - Tag-reader communication carries extra read/write operations

    ➡ Tag read rate (EPCglobal C1G2): ***45 tags/s***
  - No extra costs on the backend (but slightly larger messages)

Summary and Conclusion

- Tailing:
  - ✓ Suitable for low-cost tags and RFID/supply-chain infrastructures
  - ✓ Effective under external and internal adversaries
  - ✓ Reliable within real-world supply-chain deployments
  - ✓ Scalable (front- and back-end operations)

Thank you for your attention