Measuring the quality of DNSSEC deployment

Using longitudinal data from the OpenINTEL platform

UNIVERSITY OF TWENTE.

Northeastern University

SIDN LABS

SURF NET

Goals

- In the **general population**, **DNSSEC remains low**, e.g. deployment in .com, .net, .org **around 1%** [1]

- Some **ccTLDs do** much **better**, with e.g. **.nl** and **.se** having around **half of all domains** using DNSSEC [2]

  - This is likely because they incentivize DNSSEC deployment

- We wanted to study **if organisations that do deploy DNSSEC get it right**, both for the general population and for the ccTLDs with incentives

Longitudinal data

- We used **longitudinal data** from **OpenINTEL** **https://www.openintel.nl/** (new website soon!)

- For the study of **com/net/org**, we used **21 months** of data, for the study of **.se and .nl** we used **14 and 18 months** of data **respectively**.

- **Challenges**:
  - How do we **validate millions of signatures**?
  - How do we **track** complex operations such as **DNSSEC key rollovers**?

- **Solution**:
  - **Use** modern **"big data" technologies**, i.e. Hadoop, Spark and Impala

DNSSEC deployment in general population

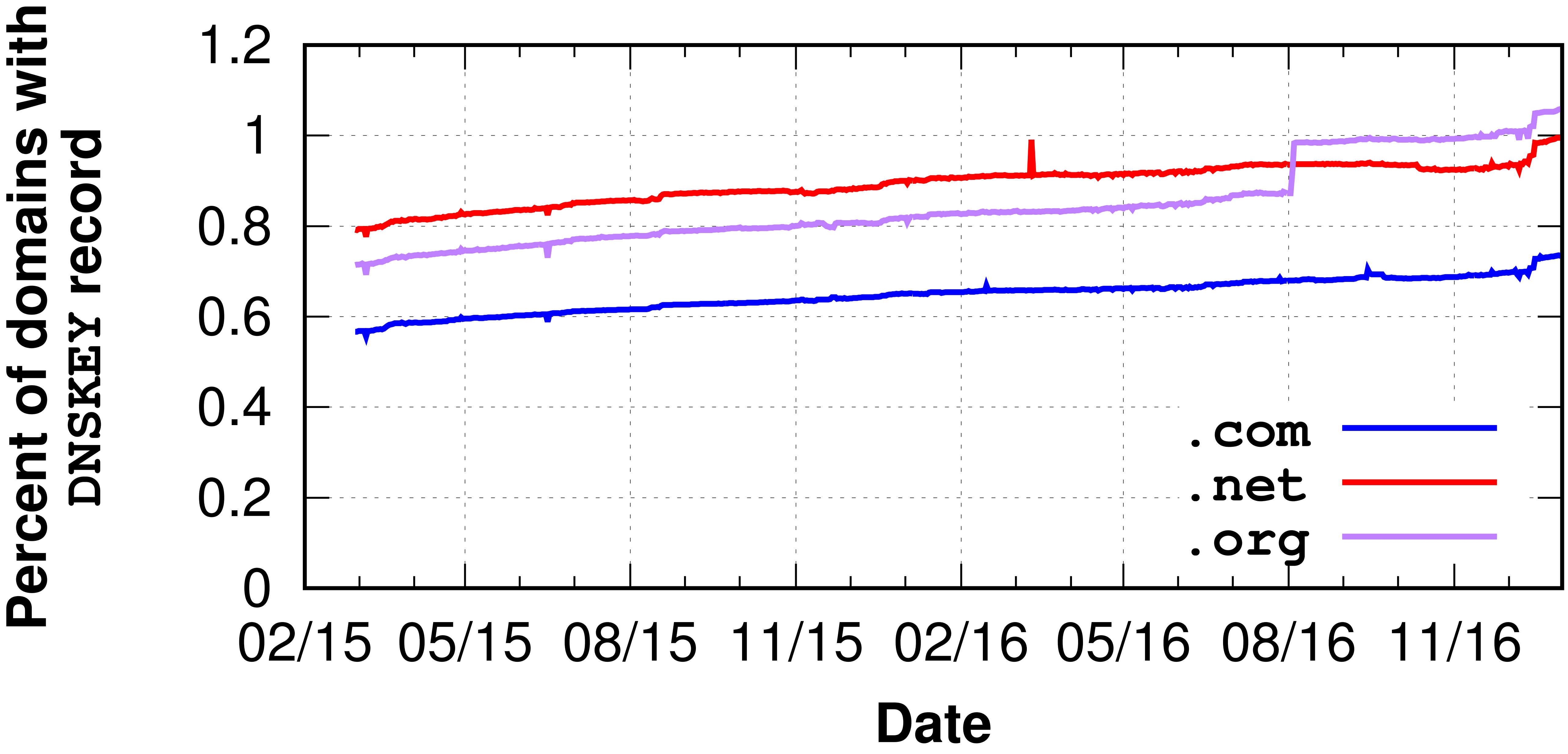


figure from Chung et al. [1]

Takeaway #1:
Lots of domains have no secure delegation

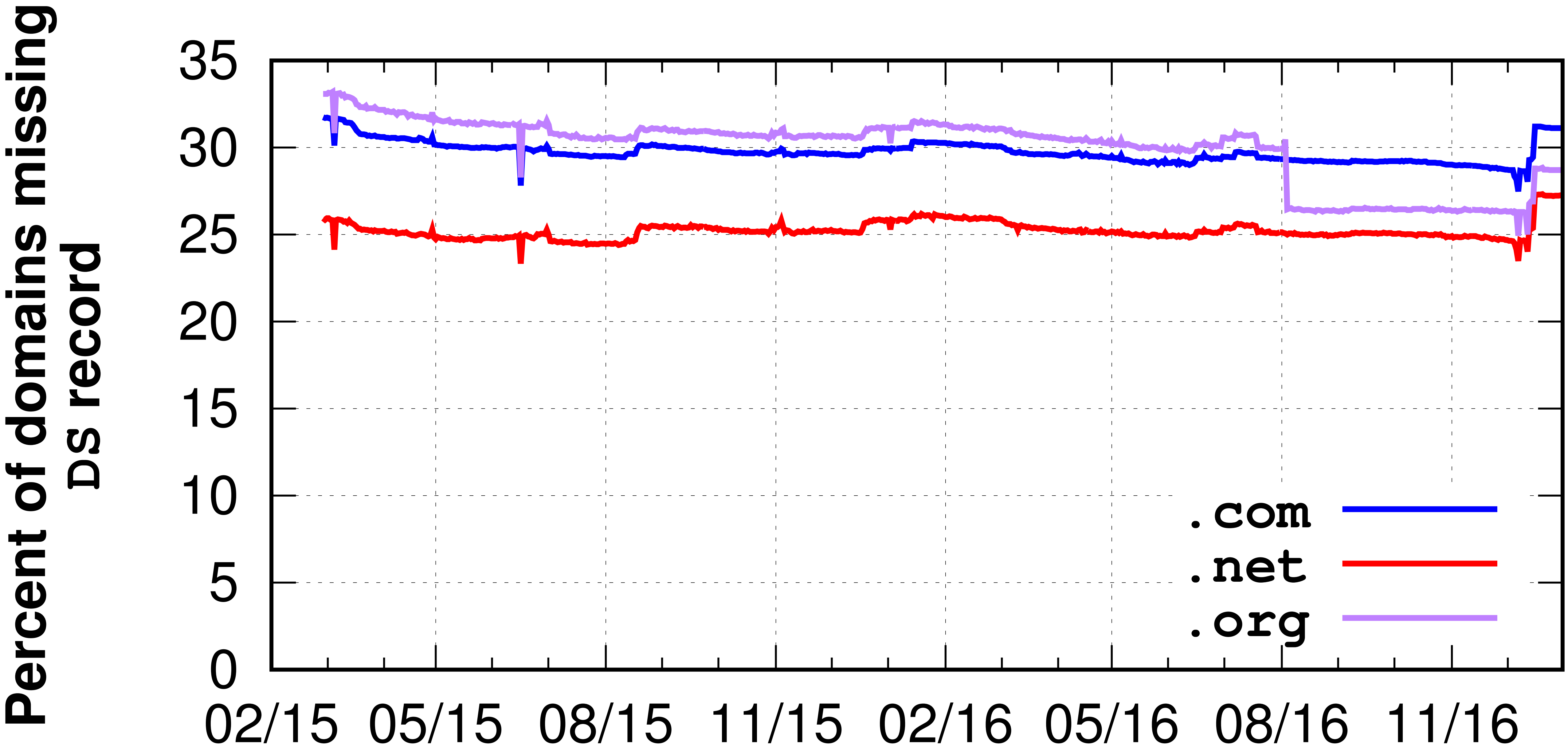


figure from Chung et al. [1]

Takeaway #2:
Most common problem is missing signatures

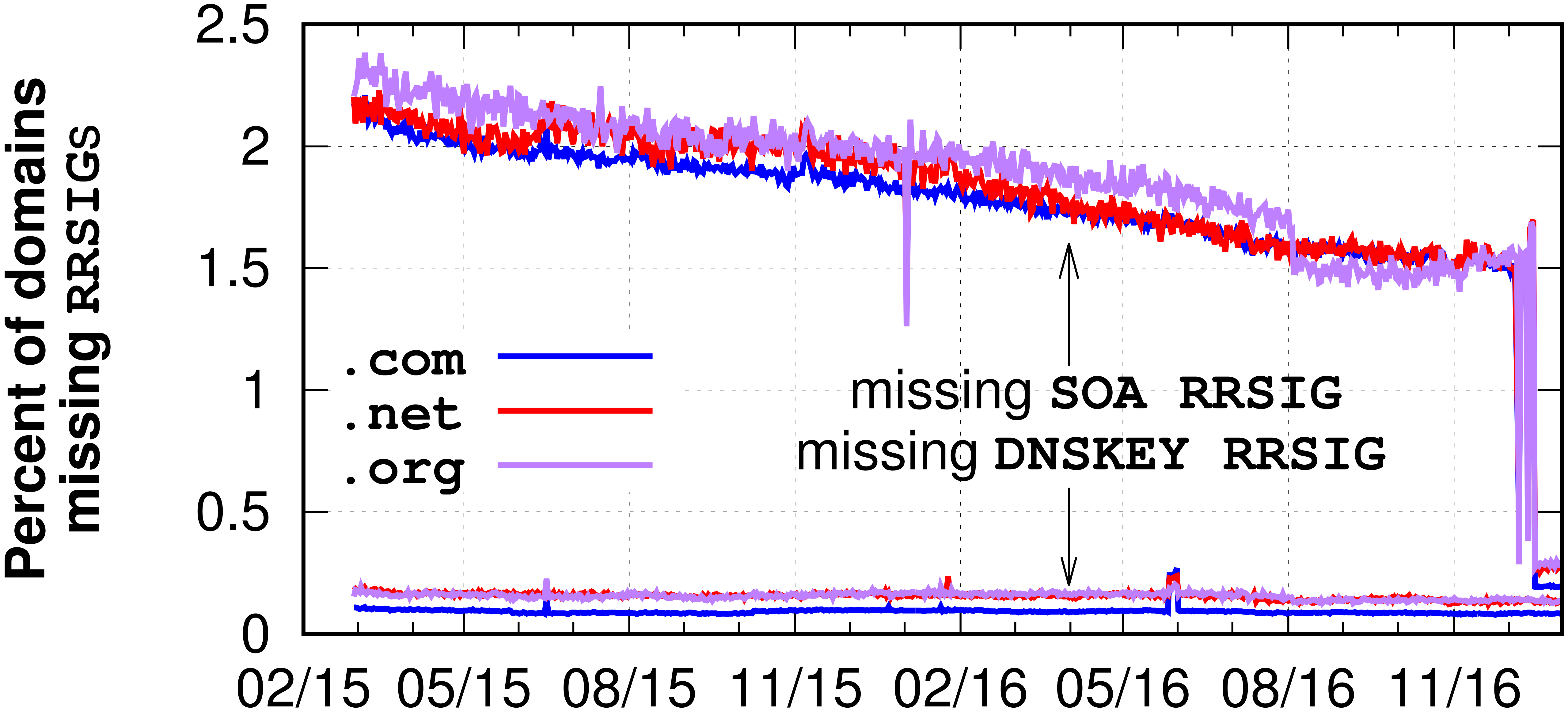


figure from Chung et al. [1]

Takeaway #3:
Actually broken signatures are rare

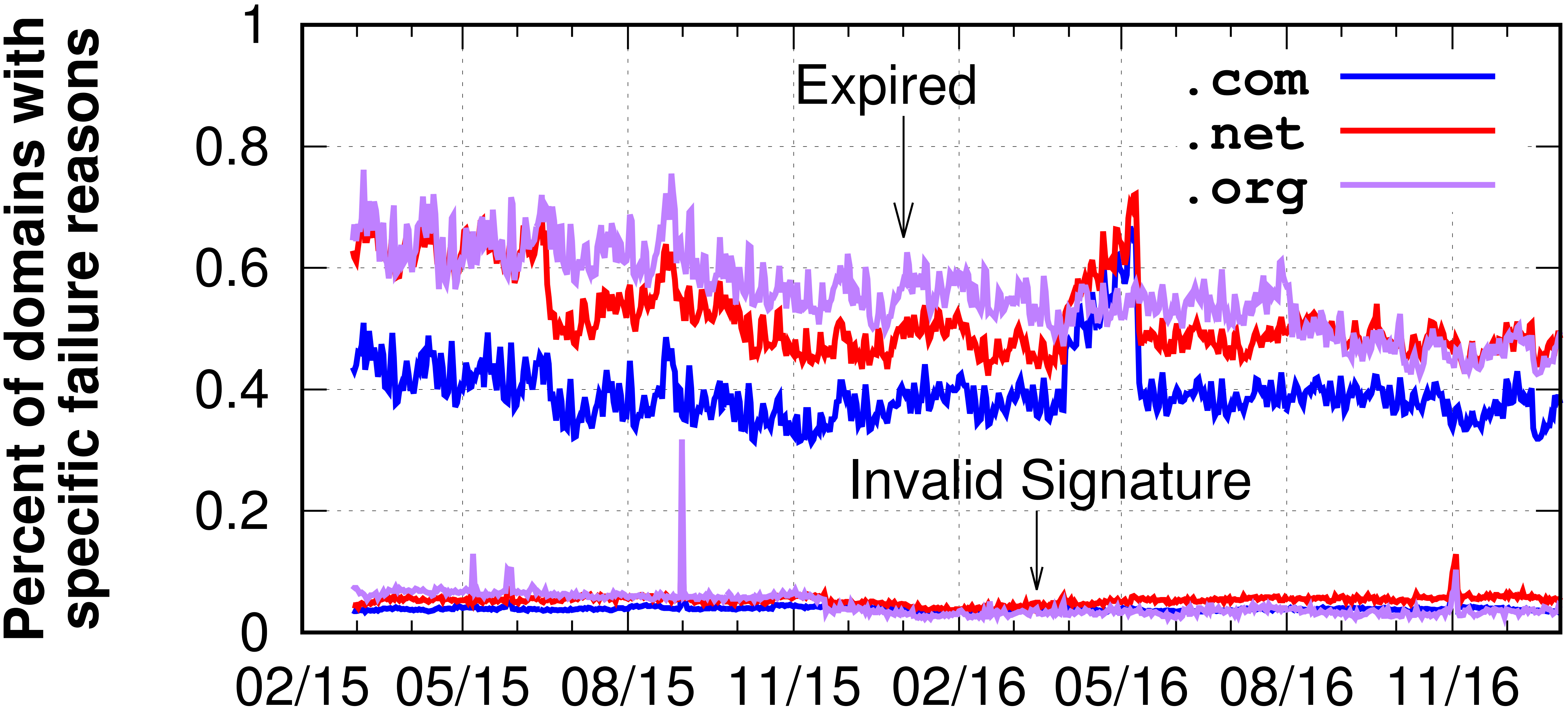


figure from Chung et al. [1]

Takeaway #4: Mismatch between parent and child also rare

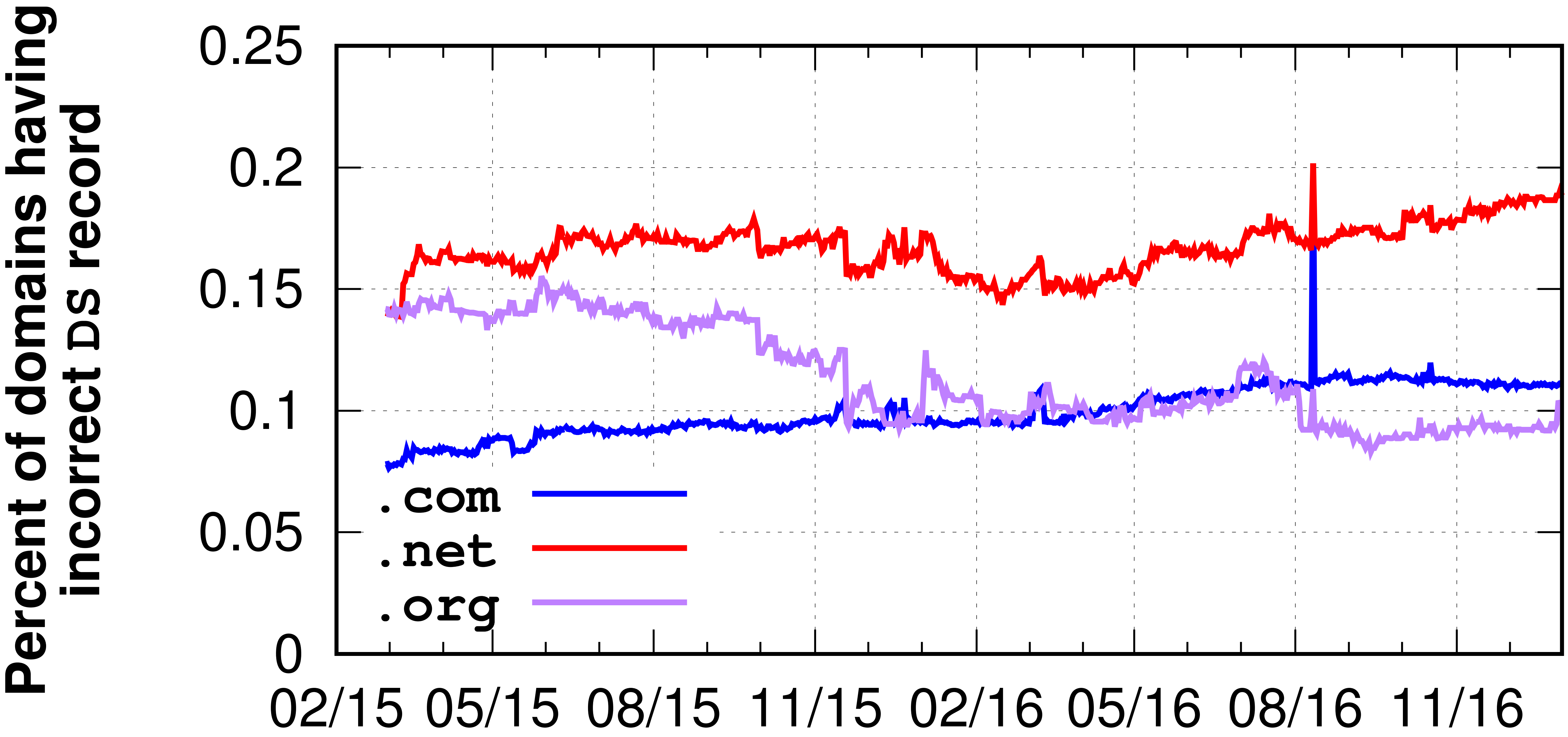
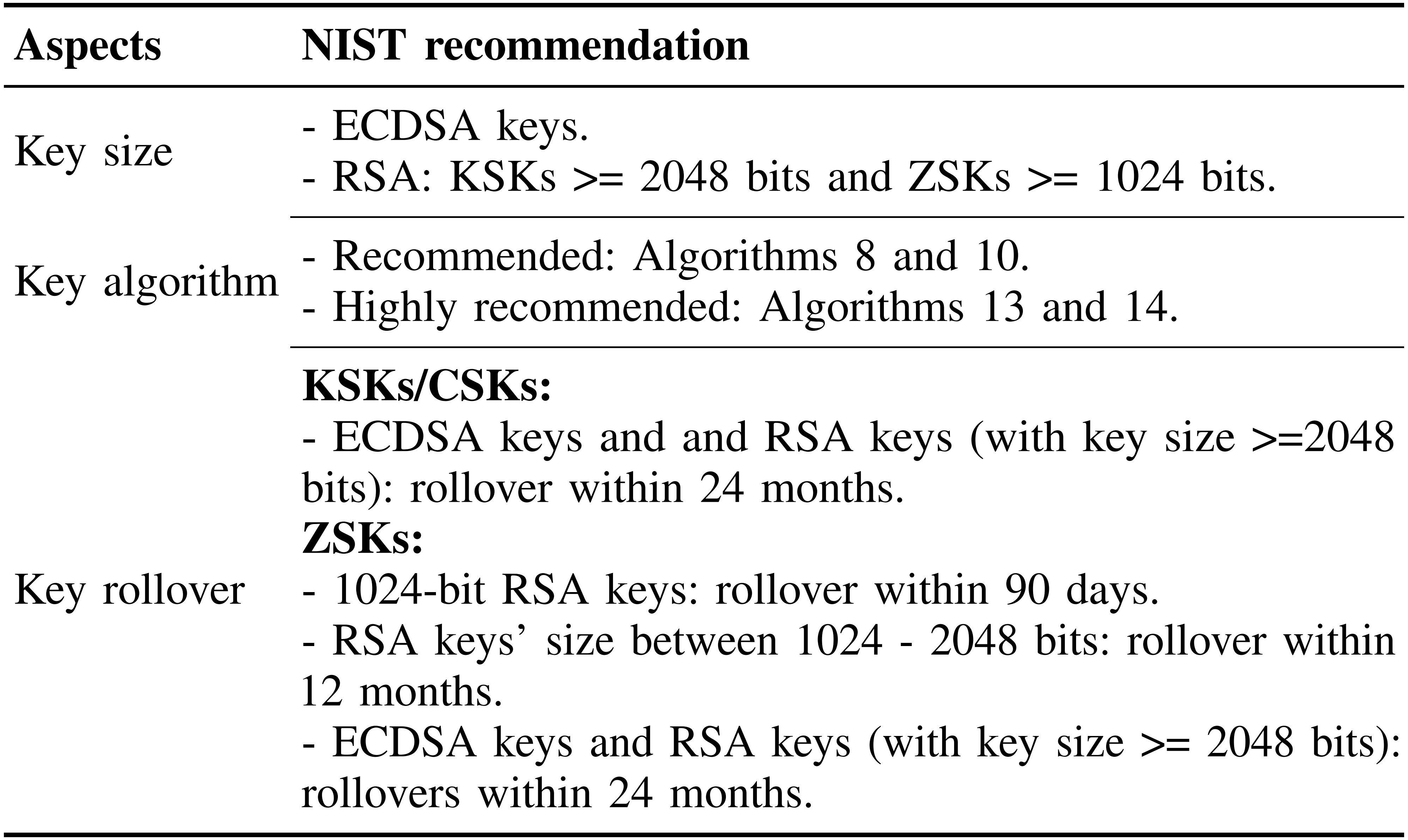


figure from Chung et al. [1]

Quality in ccTLDs with large DNSSEC deployments

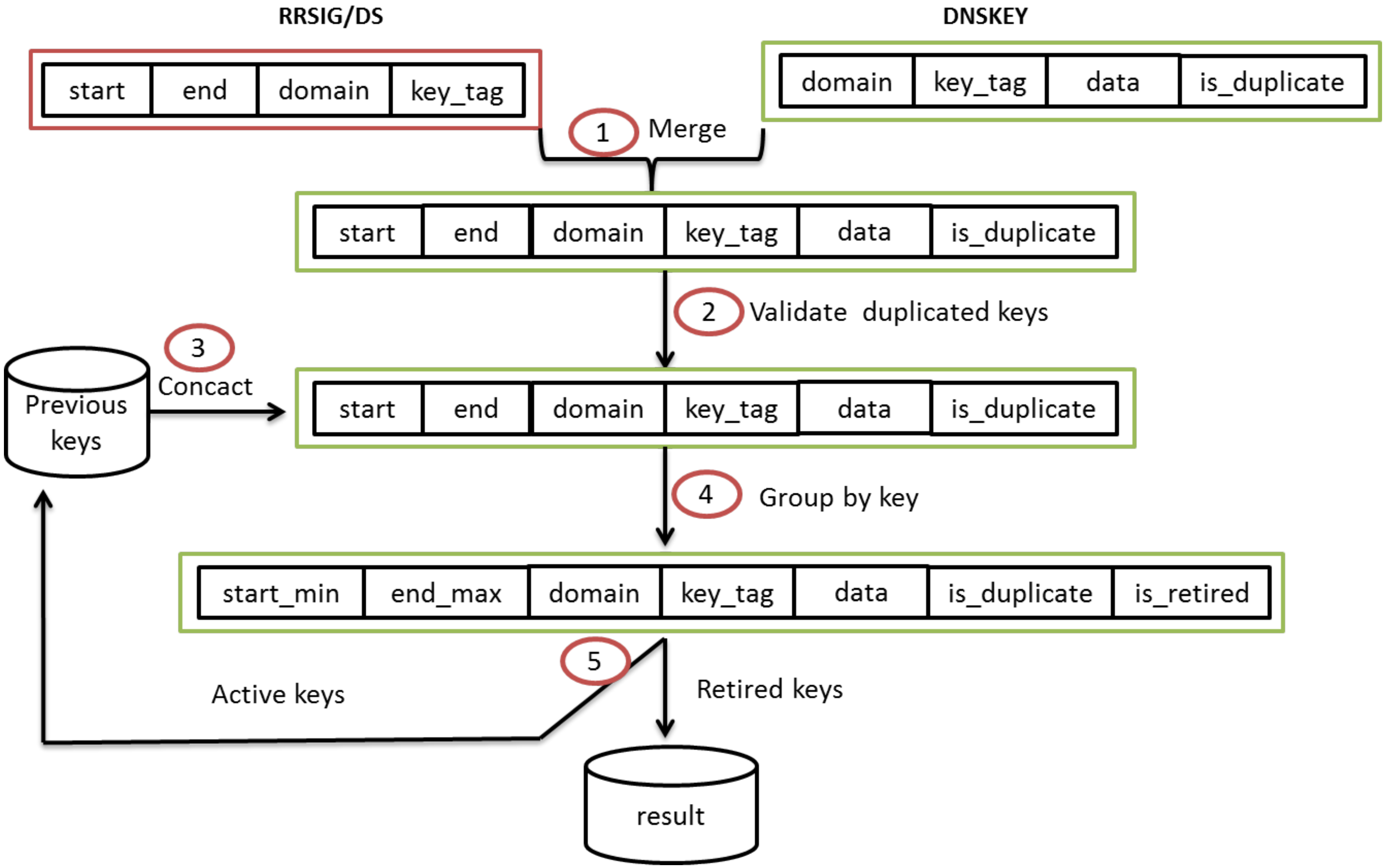
- For quality of DNSSEC deployment in .nl and .se, we use **NIST guidelines as best practice**:



Aspects	NIST recommendation
Key size	- ECDSA keys. - RSA: KSKs >= 2048 bits and ZSKs >= 1024 bits.
Key algorithm	- Recommended: Algorithms 8 and 10. - Highly recommended: Algorithms 13 and 14.
Key rollover	**KSKs/CSKs:** - ECDSA keys and and RSA keys (with key size >=2048 bits): rollover within 24 months. **ZSKs:** - 1024-bit RSA keys: rollover within 90 days. - RSA keys' size between 1024 - 2048 bits: rollover within 12 months. - ECDSA keys and RSA keys (with key size >= 2048 bits): rollovers within 24 months.

Tracking key rollover

- Key rollover takes multiple days, need to check signature records to evaluate if a key is used



Results

.nl

DNS operator	Master NS[†]	#Signed	Algorithm	KSK size	ZSK size	ZSK Rollover
TransIP	*.transip.net.	265,341	✗	✔	⚠[+]	✗
	*.transip.nl.	206,254	✗	✔	⚠[+]	✗
	*.sonexo.eu.	75,256	✔	✔	⚠[+]	✗
	ns0.nl.	50,273	✗	✔	⚠[+]	✗
Metaregistrar BV	*.metaregistrar.nl.	386,913	✔	✔	⚠[+]	✗
Hostnet BV Network	*.hostnet.nl.	359,793	✔	✔	⚠[+]	✗
Cyso Hosting	*.firstfind.nl.	246,385	✔	✔	⚠[+]	✗
Argeweb BV	*.argewebhosting.eu.	101,993	✔	✔	⚠[+]	✗
Openprovider	*.openprovider.nl.	79,367	✔	✔	⚠[+]	✗
Village Media BV	*.webhostingserver.nl.	67,150	✔	✔	⚠[+]	✗
Hosting2GO	*.hosting2go.nl.	64,568	✔	✔	⚠[+]	✗
Flexwebhosting BV	*.flexwebhosting.nl.	60,753	✔	✔	⚠[+]	✗
Internedservices	*.is.nl.	57,033	✔	✔	⚠[+]	✗
Neostrada	*.neostrada.nl.	56,295	✔	✔	⚠[+]	✗
One.com	*.one.com.	55,397	✔	✗	✔	?
PCextreme	*.pcextreme.nl.	50,102	✔	✔	⚠[+]	✗
AXC B.V.	*.axc.nl.	47,861	✔	✔	⚠[+]	✗

.se

DNS operator	Master NS[†]	#Signed	Algorithm	KSK size	ZSK size	ZSK Rollover
Loopia AB	*.loopia.se.	282,604	✔	✔	⚠[+]	✗
One.com	*.one.com.	221,372	✔	⚠[*]	⚠[+]	✗
Binero AB	*.binero.se.	123,131	✔	✔	⚠[+]	✗

Legend: ✔: meets recommendation; ✗: does not meet recommendation; ⚠: only partially meets recommendation; ?: unknown.

[†] The master name server from the SOA records is used to identify the operator, as described in Section III-A.

[*] About half of One.com *.se* domains use unrecommended KSK sizes.

[+] These operators have 1024-bit ZSKs that require regular key rollovers according to the best practice (Tab. II); as the rollover column shows, however, they do not perform key rollover for ZSK.

Results cover large operators responsible for 80% of signed domains

Conclusions and Recommendations

- **DNSSEC deployment** in general **remains low**, with some notable **exceptions among ccTLDs**

- Where DNSSEC is deployed, "real mistakes" are rare, but **best practices are seldom followed**; especially regular key rollovers for weak (1024-bit) keys

- **Recommendations**:
  - **Financial incentives** appear to **work**, that is: they lead to adoption
  - To get high quality adoption, however, **incentives should include mandatory quality requirements** -- the ccTLDs we studied (.nl, .se) are both considering doing this

References

[1] Chung, T., van Rijswijk-Deij, R., Chandrasekaran, B., Choffnes, D., Levin, D., Maggs, B. M., … Wilson, C. (2017). A Longitudinal, End-to-End View of the DNSSEC Ecosystem. In Proceedings of the 26th USENIX Security Symposium (USENIX Security ’17). Vancouver, BC, Canada: USENIX Association.

[2] Le, T., Van Rijswijk-Deij, R., Allodi, L., & Zannone, N. (2018). Economic Incentives on DNSSEC Deployment: Time to Move from Quantity to Quality. In Proceedings of the IEEE Network Operations and Management Symposium 2018. Taipei, Taiwan: IFIP.

Thank you for your attention!
Questions?

acknowledgments: with thanks to
Taejoong Chung and Tho Le

nl.linkedin.com/in/rolandvanrijswijk

@reseauxsansfil

roland.vanrijswijk@surfnet.nl
r.m.vanrijswijk@utwente.nl

UNIVERSITY OF TWENTE.

SURF NET