Infer, Don't Negotiate:

Unilateral ML-Based Cipher Selection for DNSSEC

Stefan Schmid, Haya Schulmann, **Juan Vanerio***, Michael Waidner *juan.vanerio@univie.ac.at

TU Berlin · Goethe-Universität Frankfurt · University of Vienna · TU Darmstadt
ATHENE · Fraunhofer SIT · Austrian Institute of Technology

Infer, don't negotiate

A nameserver can **infer** what a resolver validates,
and serve the strongest algorithm **on its own**.

Security does not depend on prediction accuracy.

Coordination problem
both ends must change

→ each query reveals its sender →

Inference problem
the nameserver decides alone

Problem: stronger algorithms can weaken security

chain verifies
→ accepted

chain fails
→ **SERVFAIL**

no supported algorithm
→ **not validated at all**

Ed448: supported by only **21.8 %** of validating open resolvers.
All others leave an Ed448-only zone unvalidated.

The known remedies are stuck

Negotiation: both ends must change; never deployed.

Signing with everything: **91.28 %** query success.

Result: 98.7 % of signed top-20k domains use one algorithm.

Design: dual-signed zone, middlebox, and oracle

Resolver
unchanged

query →
← only a_m if predicted to validate it, else a_c

Middlebox
the oracle predicts
per query, from its fields

← both signatures

Nameserver
zone signed with
a_c *and* a_m

▼ Middlebox: the oracle learns from behavior

test zones signed with **deliberately invalid** signatures

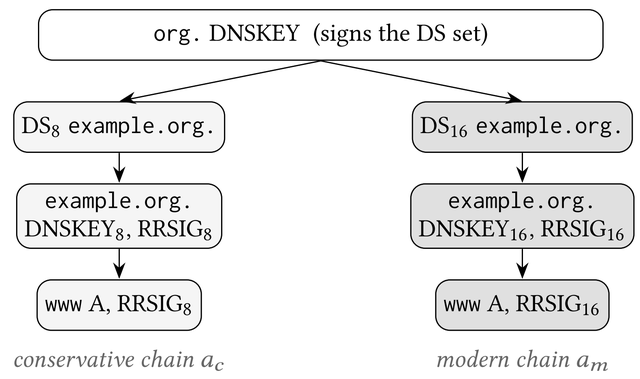
SERVFAIL
⇒ **validates**

answer returned
⇒ **does not**

labels from lab, open, and ad-network resolvers

Random Forest (RF): best for every algorithm;
tree ensembles clearly beat a single tree and k-NN

▼ Nameserver: two chains of trust



a_c = RSASHA256 (8), a_m = Ed448 (16); paper Fig. 1

Feasibility: prediction and availability

Prediction: client sessions unseen in training

Serving **Ed448**: validators' queries that fail

to all **54.5 %**

with RF **1.0 %**

and Ed448 still reaches **49 %** of the validators that support it.

RF accuracy (MCC) on …	Ed25519	Ed448
mostly known resolvers	0.89	0.90
unseen client sessions	0.70	0.47
unseen networks (prefixes)	**0.49**	**0.26**

RF tracks the **software** for Ed25519 (buffer size),
the **network** for Ed448 (AS)

Availability: ∼10M open-resolver addresses

98.77 % query success, vs. 98.93 % dual-signed

Security: a floor independent of the model

wrong "modern"
→ **SERVFAIL**: availability

wrong "conservative"
→ a_c: still validated

never below a_c

I1 DS/DNSKEY never filtered
I2 a_c signature by default
I3 a_c strong, mandatory
I4 state not forgeable
I5 Cookie/TCP first

Errors cost only availability; accuracy sets how many resolvers move forward.
(given validators fail closed, as the standard requires)

Outlook: beyond DNSSEC

Different capabilities · undeployable negotiation · per-peer variants · a safe default

Protocol	Variants served	Infer from
DNSSEC	a_c / a_m signatures	query fields
DKIM	RSA / + Ed25519 signatures	destination domain
Updates (TUF)	classical / PQ signatures	User-Agent
RPKI (RRDP)	objects per suite	User-Agent

also S/MIME; OCSP already standardizes the pattern

Questions for discussion

- **If one side can infer, when do we still need to negotiate?**
- **Is "learn freely above a safe floor" a way to bring ML into other protocols?**
- **How do we build an oracle for networks it has never seen?**

Paper · 2-min video · 15-min talk

Supported by ATHENE; FWF (I-6653, CHIST-ERA GRAPHS4SEC); University of Vienna Doctoral School Computer Science; DFG SPP 2378 ReNO-2 (511099228).