Securing the last mile of DNS with CGA-TSIG

Marc Buijsman

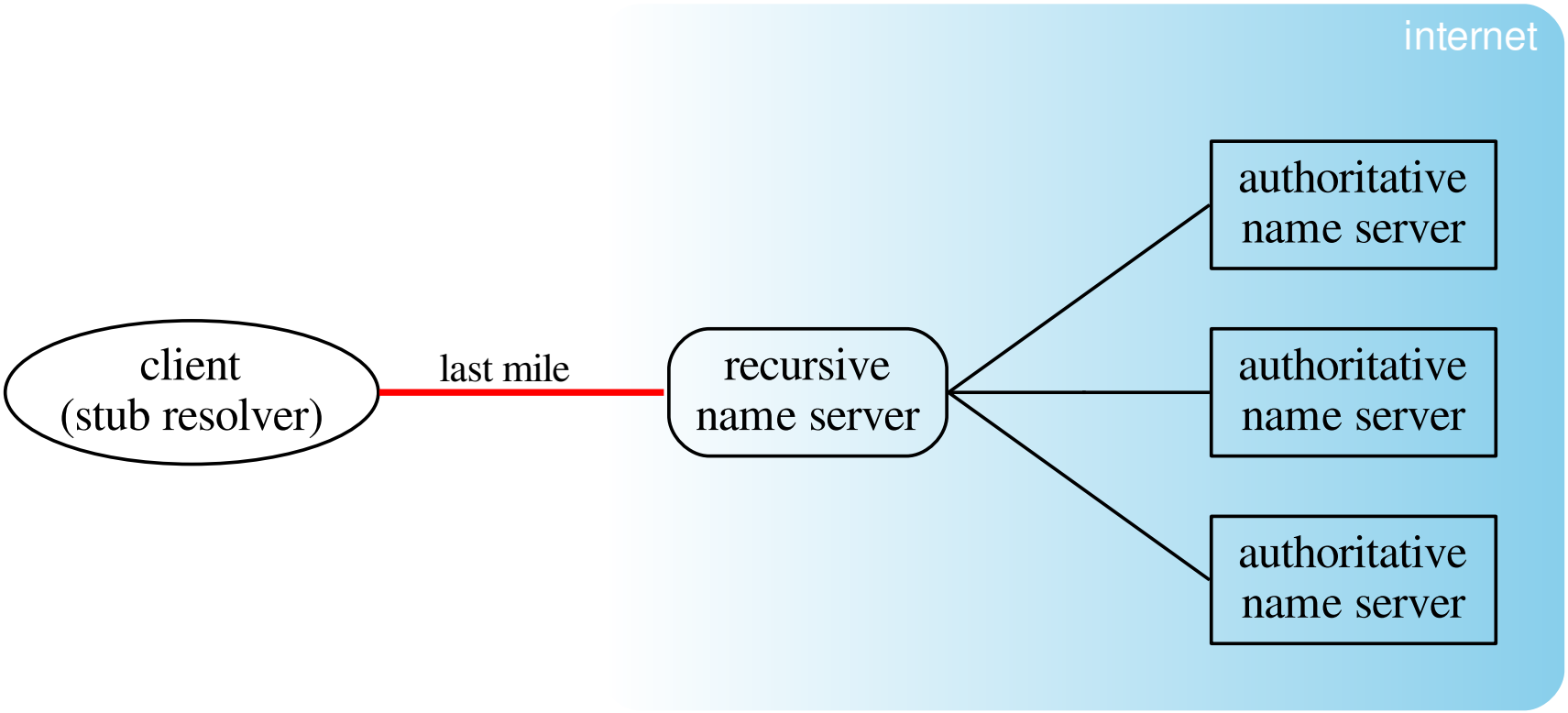
UNIVERSITEIT VAN AMSTERDAM

MASTER SYSTEM & NETWORK ENGINEERING

19 December 2013

Problem statement

- "last mile" not secured



Problem statement

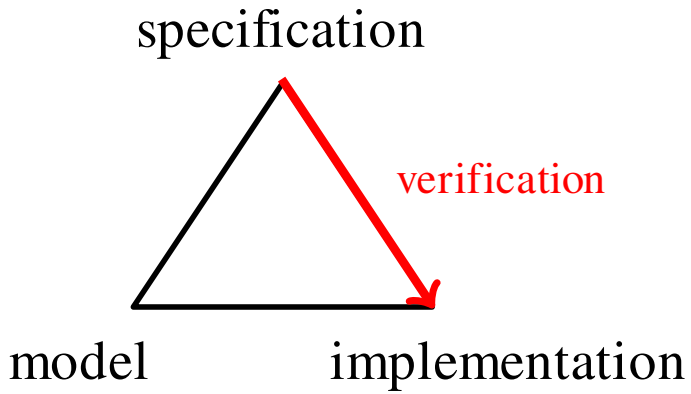
- do local resolution
  - requires local server
- DNSSEC
  - requires root key
  - validating stub
- DNSCurve
  - not widely deployed
  - needs server support
- TSIG
  - DNS message authentication
  - shared key
  - not scalable

Problem statement

- new proposal: CGA-TSIG
- research question:

  Is CGA-TSIG an adequate solution to the last mile problem?

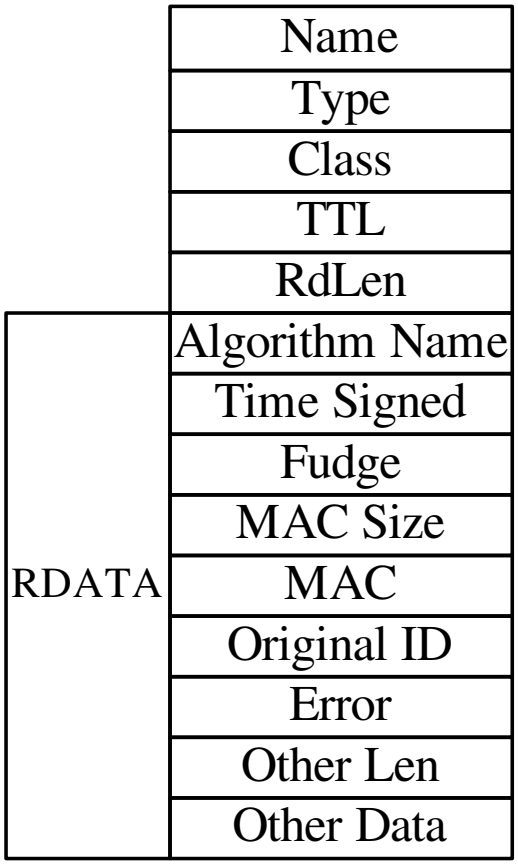
  - *Does CGA-TSIG provide the necessary security?*
  - *Is the CGA-TSIG specification correct?*



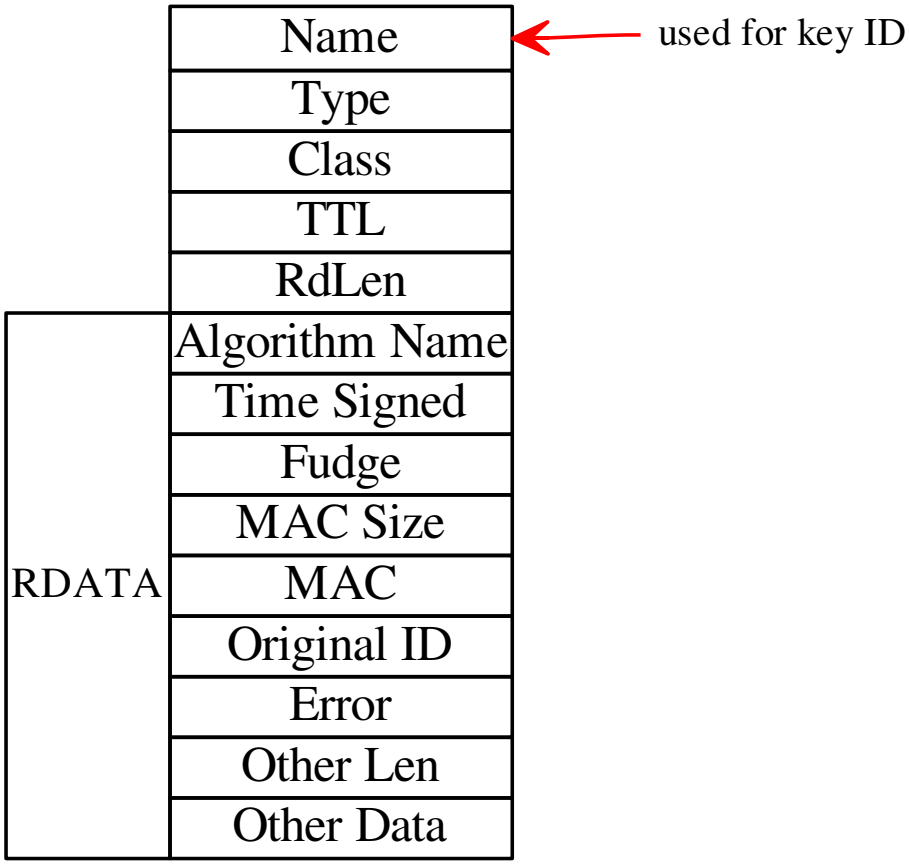
TSIG

Transaction Signature

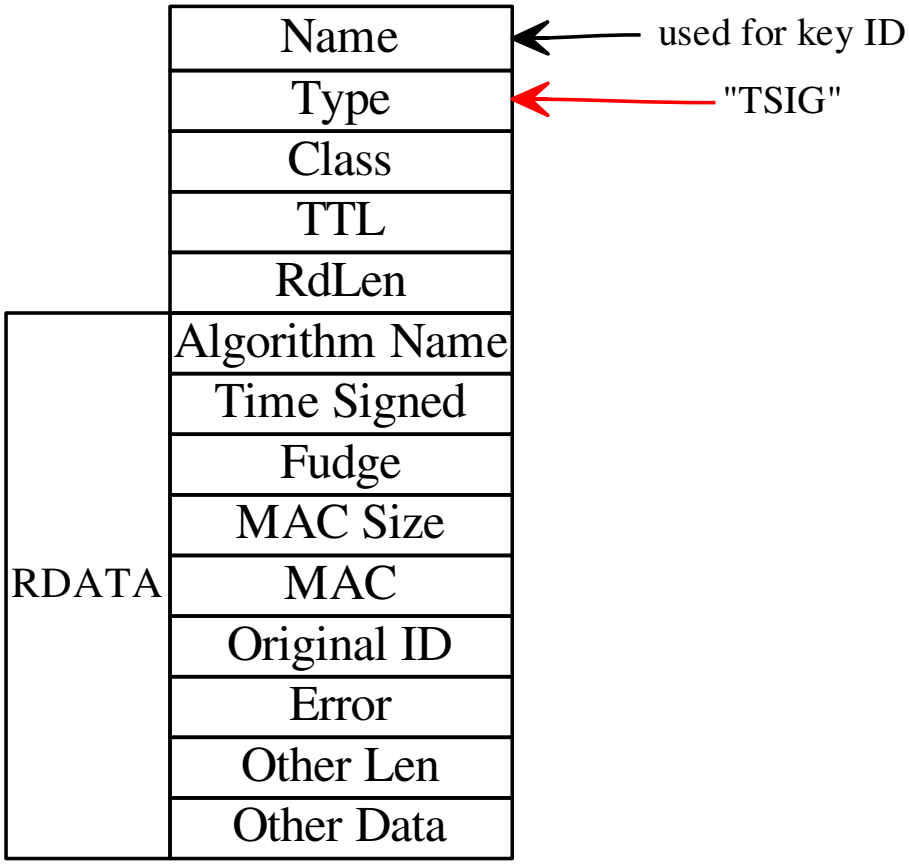
TSIG resource record



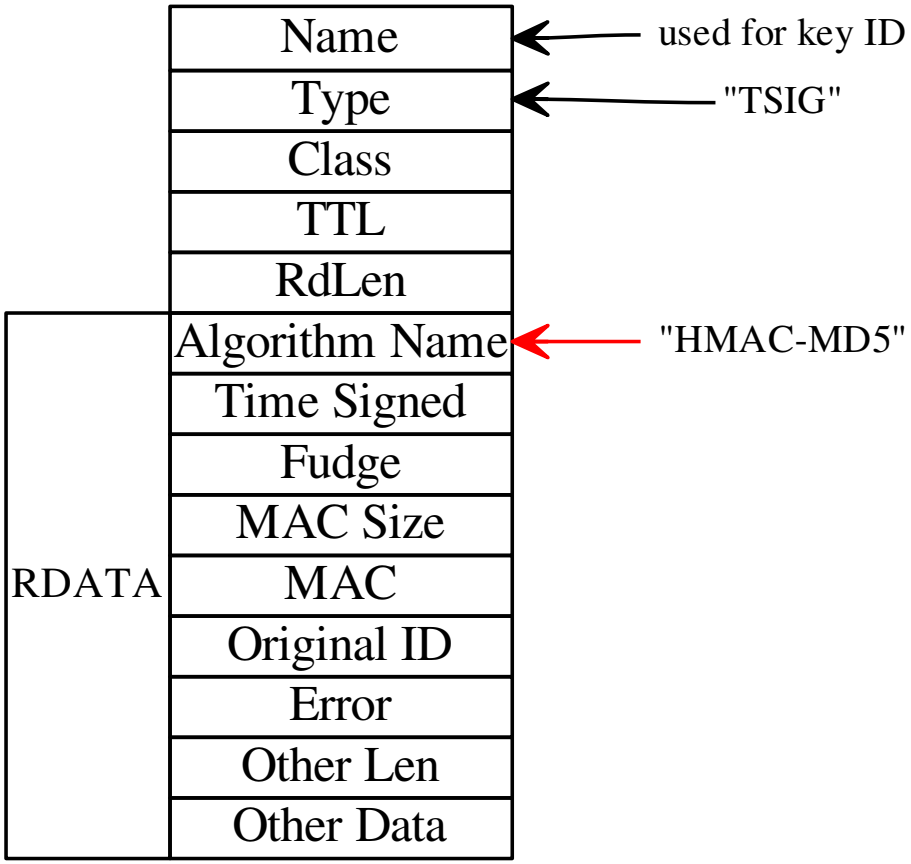
TSIG resource record



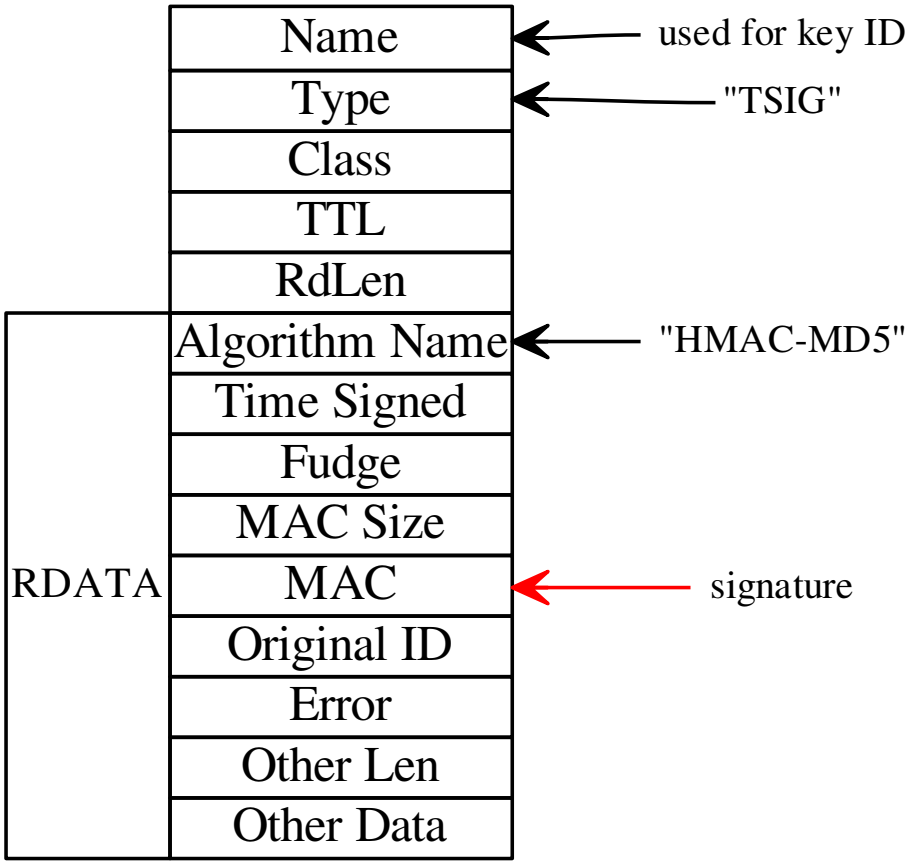
TSIG resource record



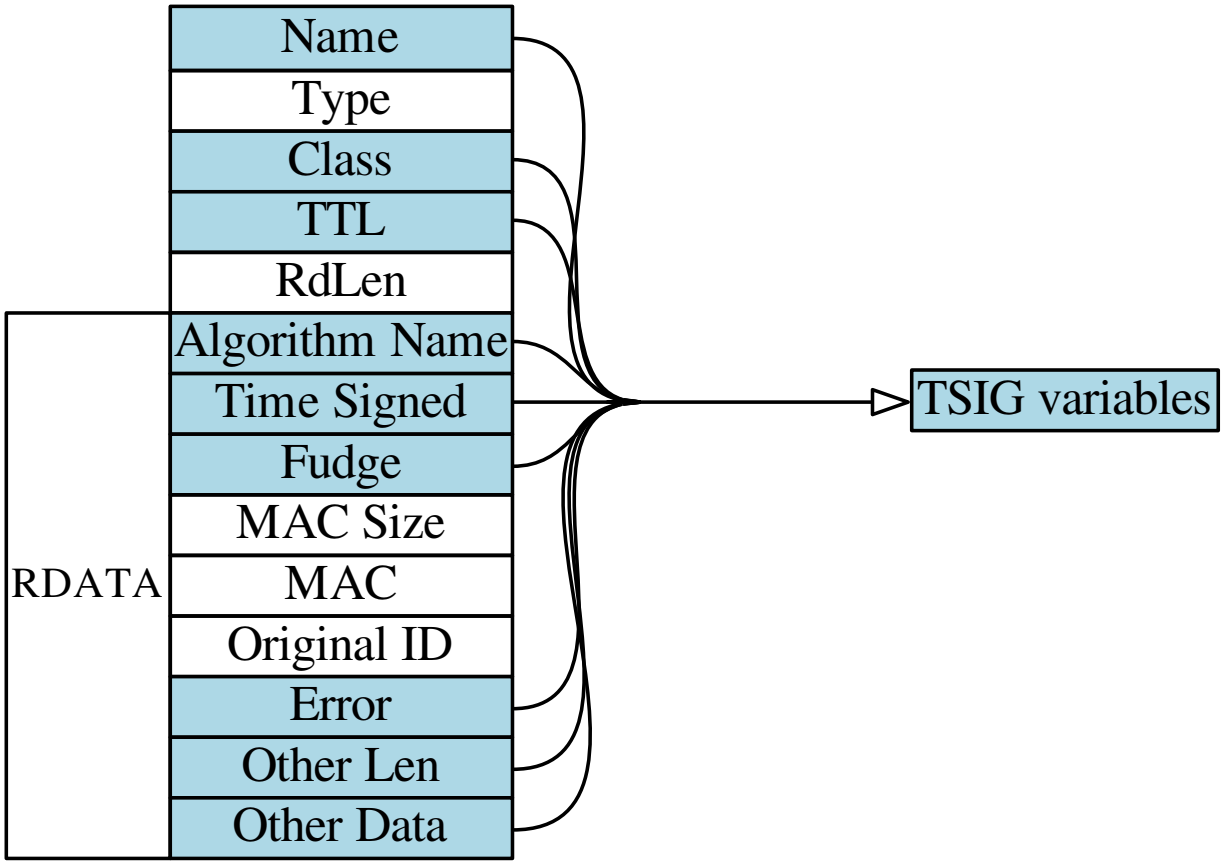
TSIG resource record



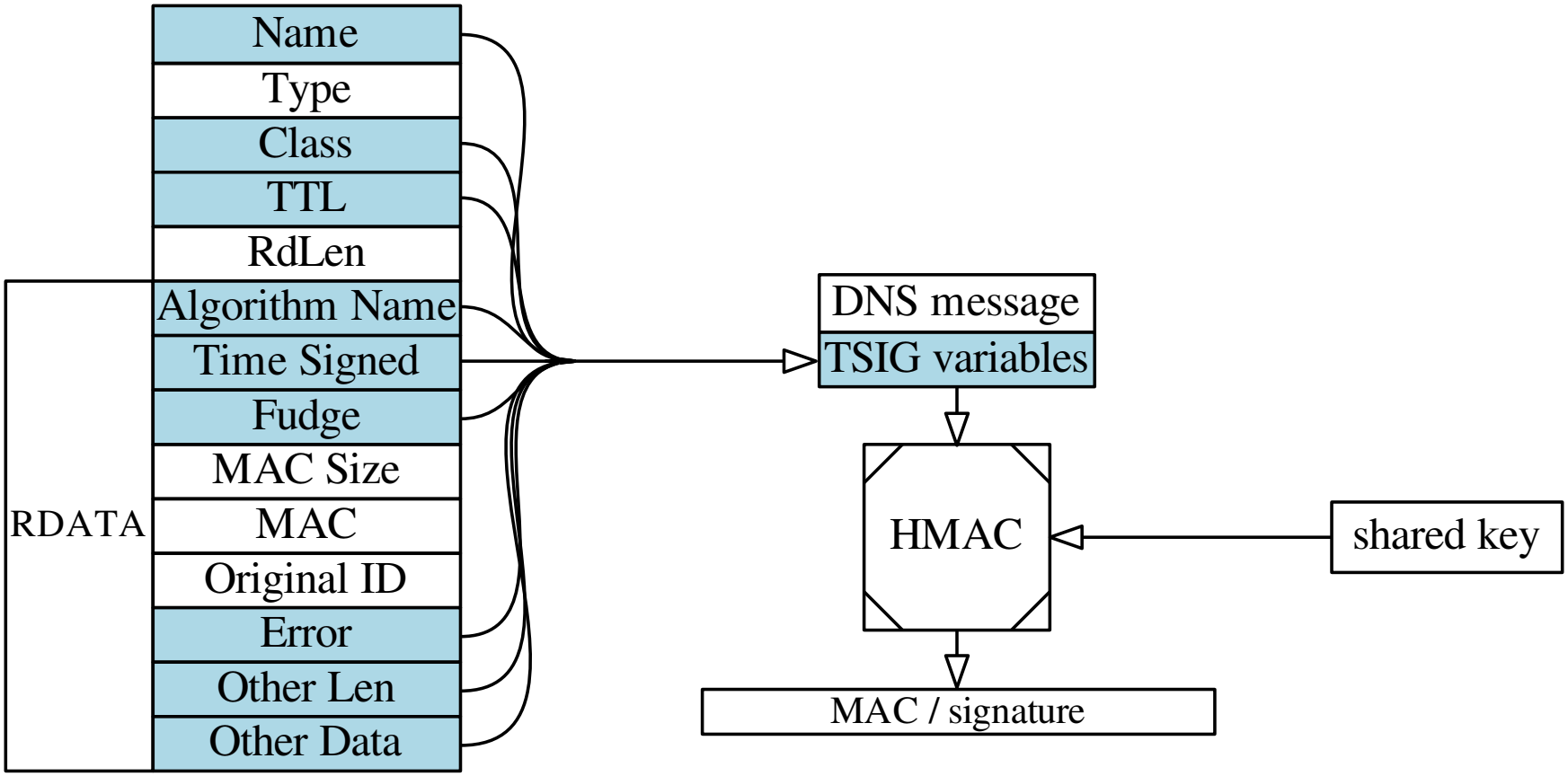
TSIG resource record



TSIG variables



TSIG signature



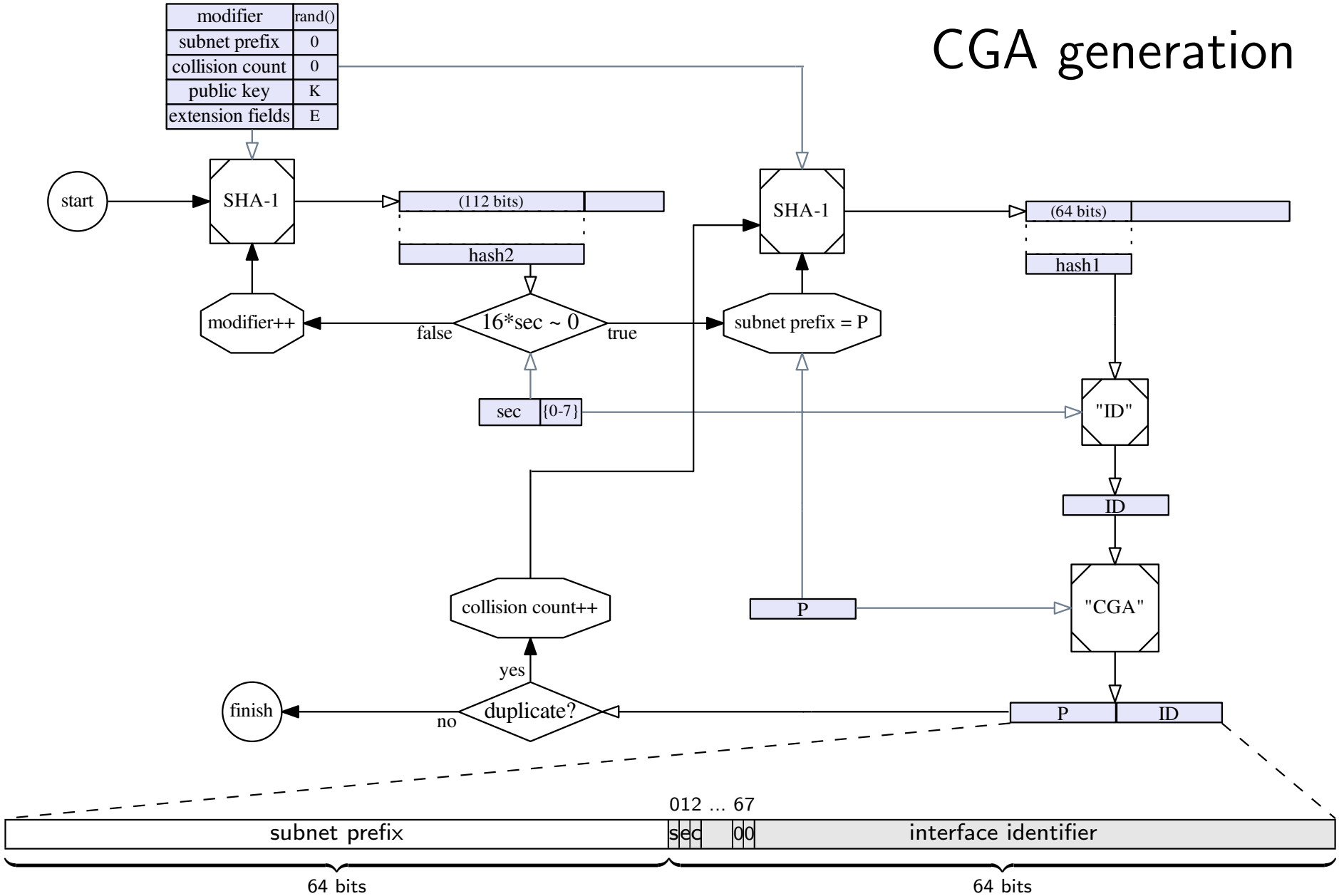
CGA

Cryptographically Generated Addresses

CGA

- public key authentication
- binds public key to IPv6 address
- comes signed message from that address?
- anyone can claim address

CGA generation

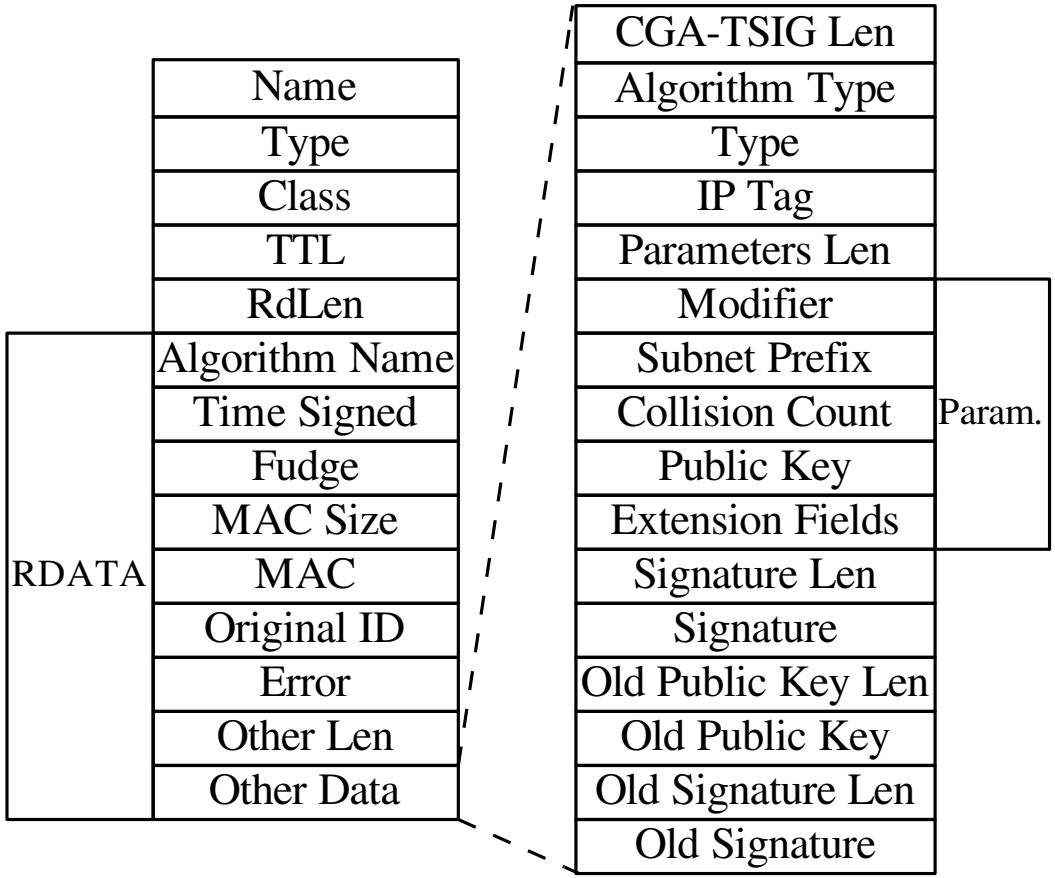


CGA-TSIG

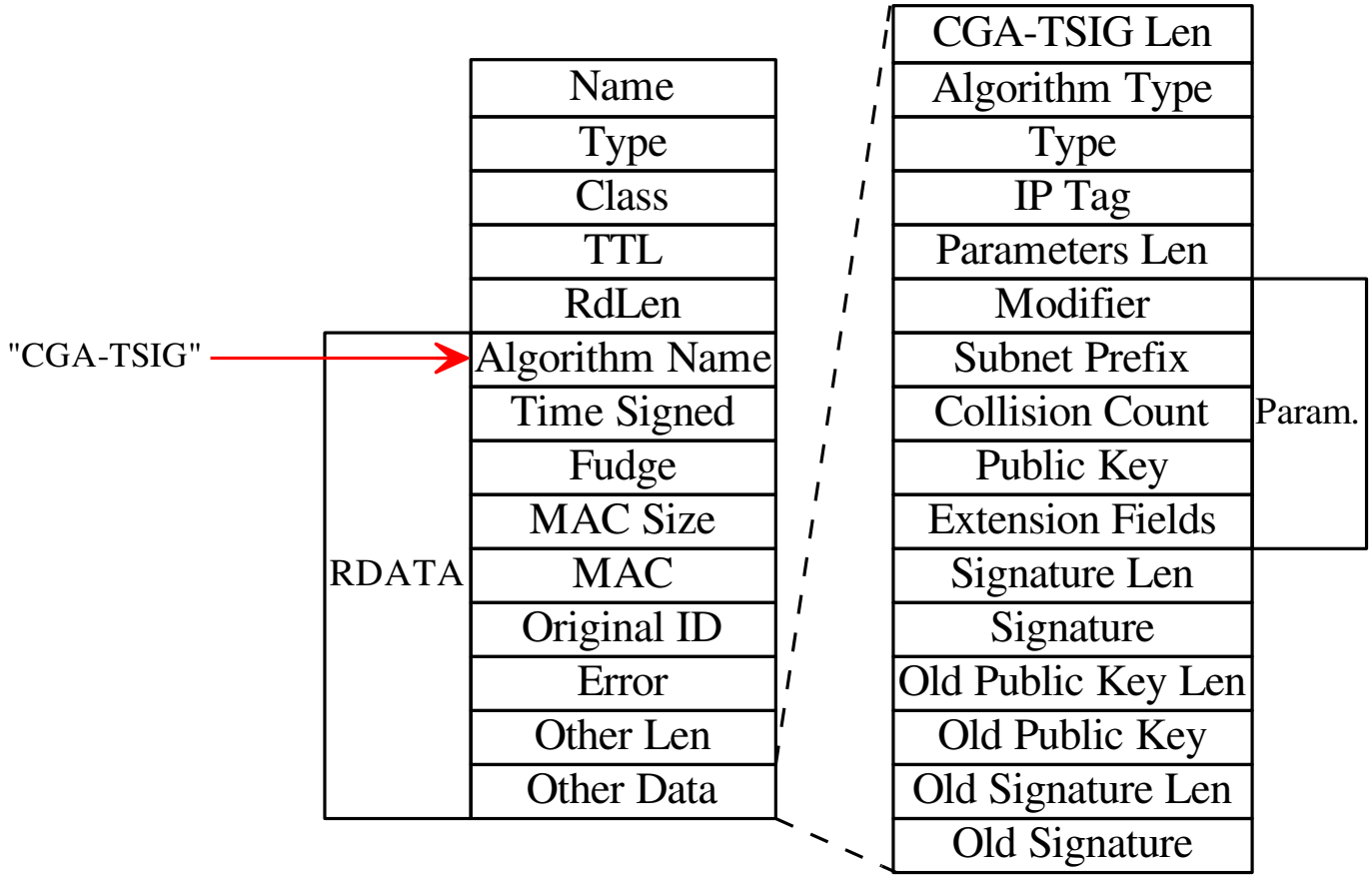
CGA-TSIG

- TSIG's individual message authentication...
- ...but with public-key crypto
  - scalable
  - CGA to authenticate public key
- recursive name server accepts anonymous queries
  - clients do not need CGA
- authenticated key/address changes
- initial address verification?
  - DHCP configuration maybe spoofed

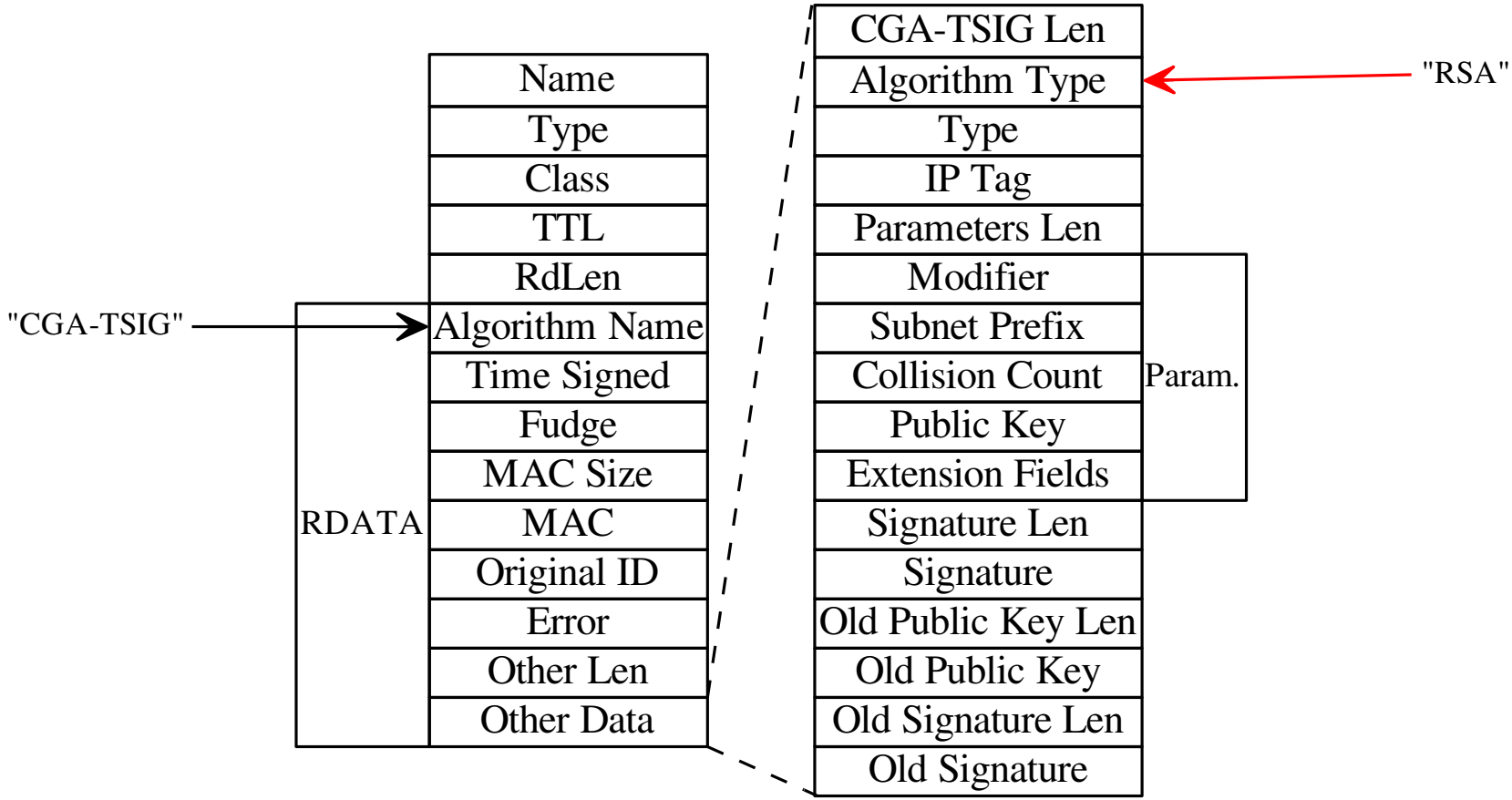
CGA-TSIG resource record



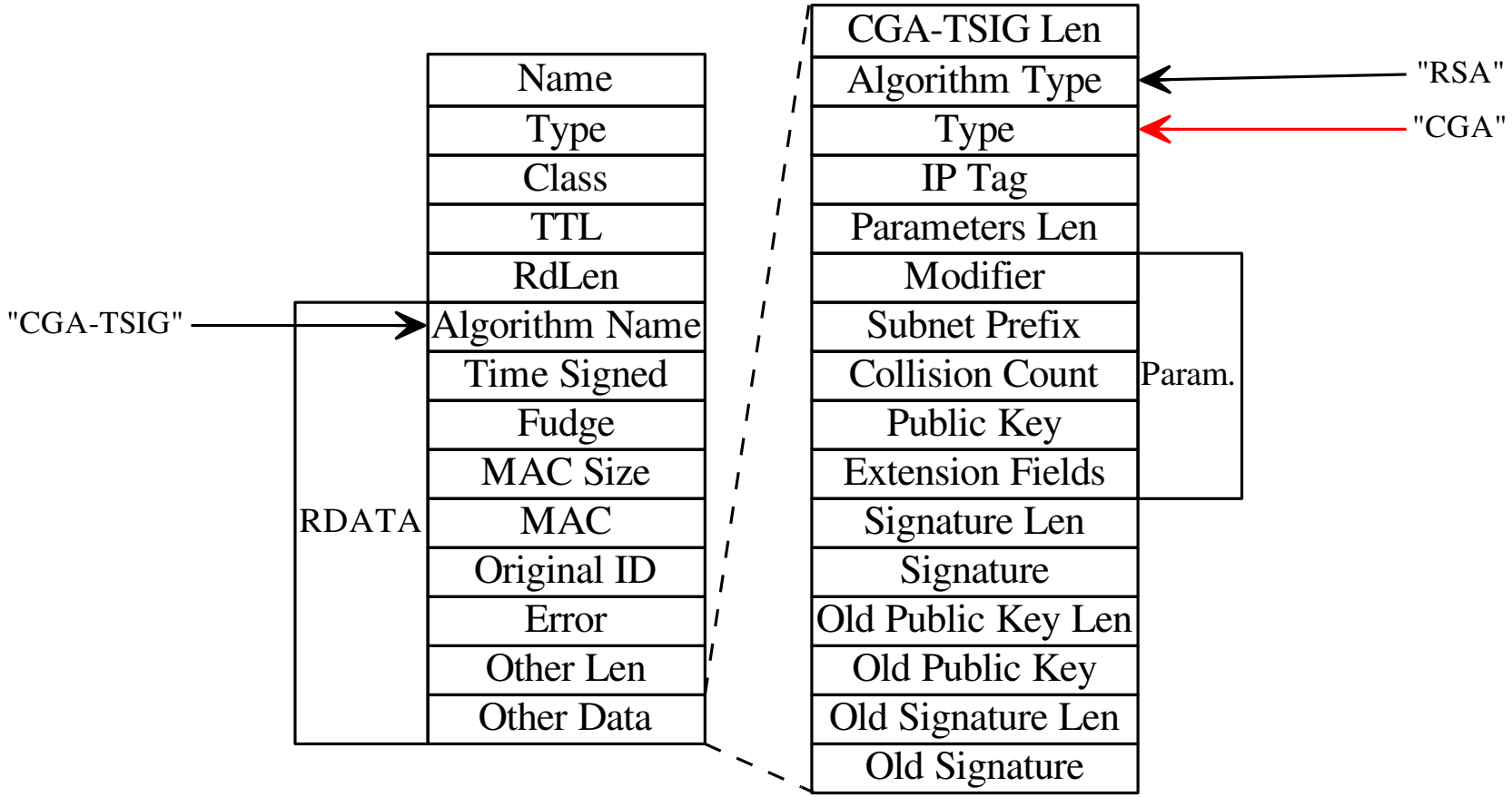
CGA-TSIG resource record



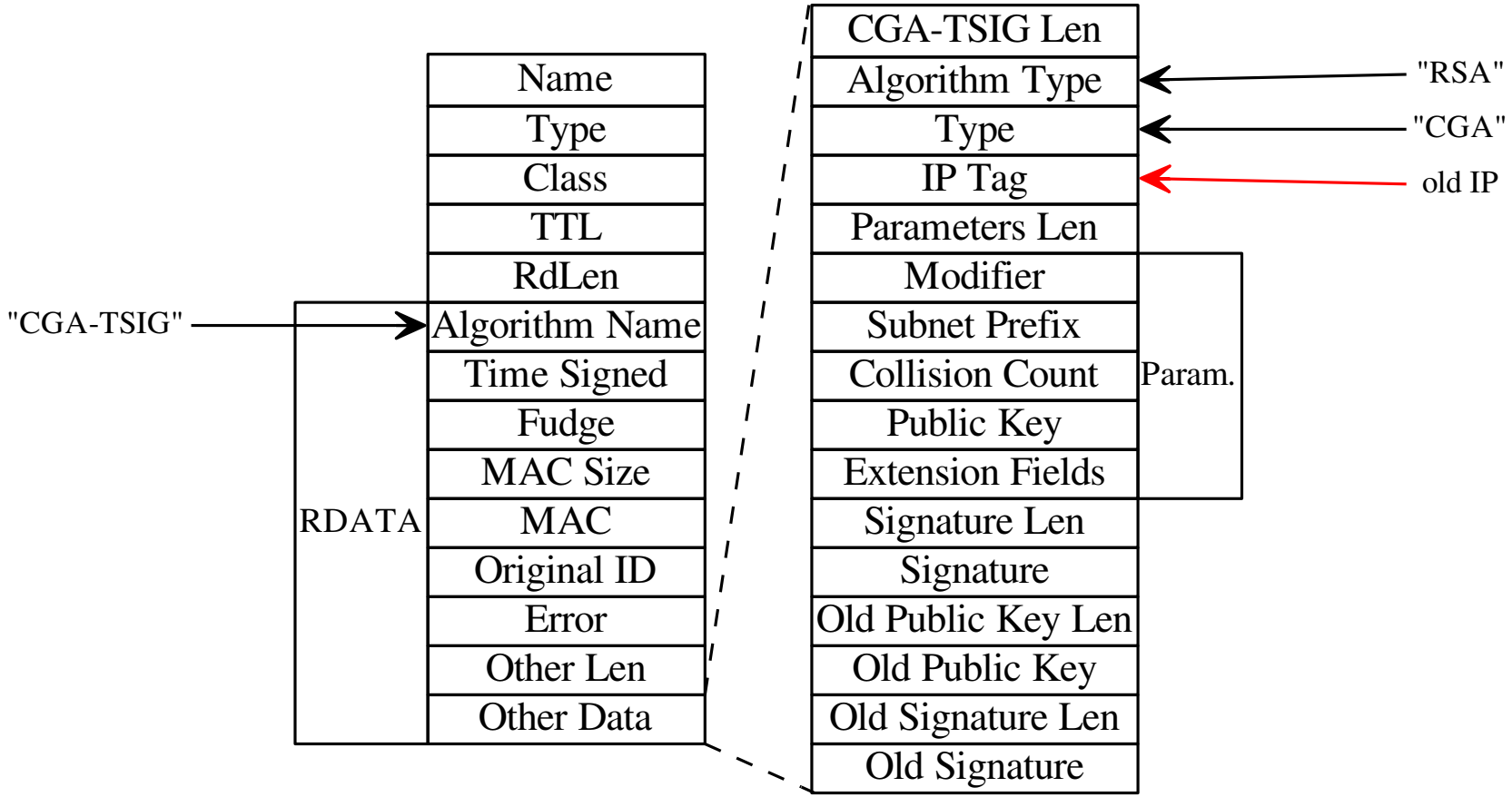
CGA-TSIG resource record



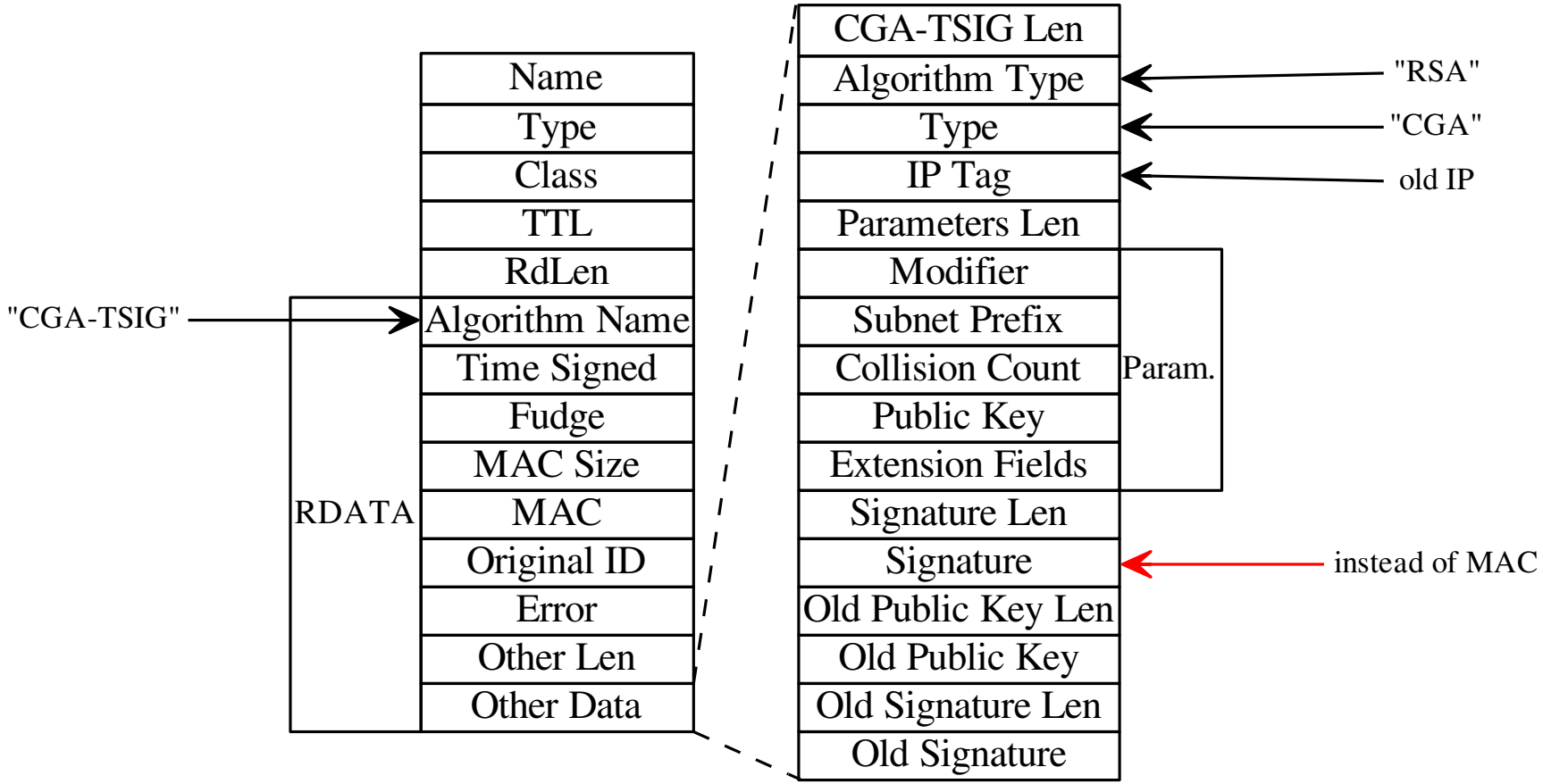
CGA-TSIG resource record



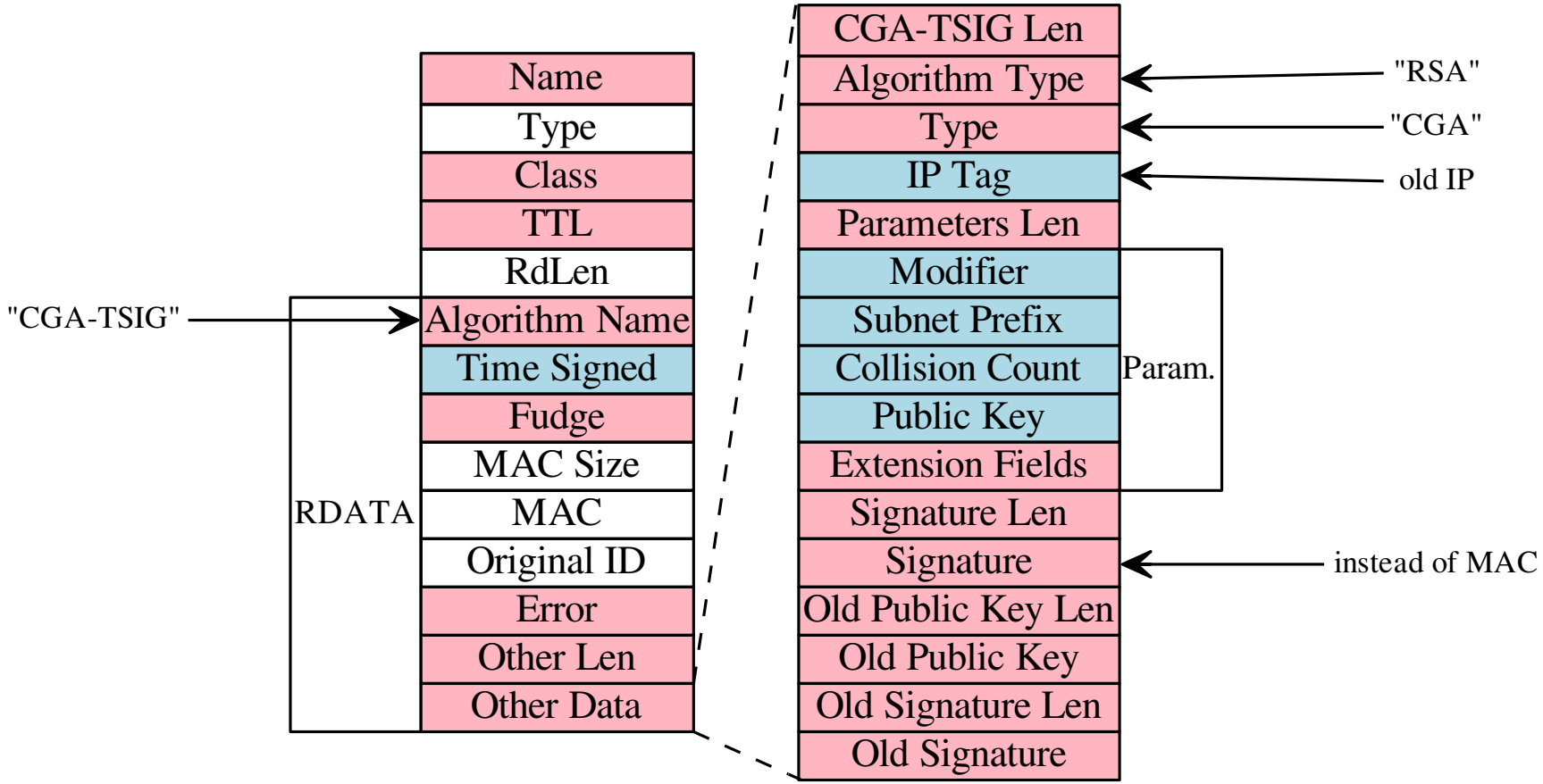
CGA-TSIG resource record



CGA-TSIG resource record



CGA-TSIG resource record



Proof of concept

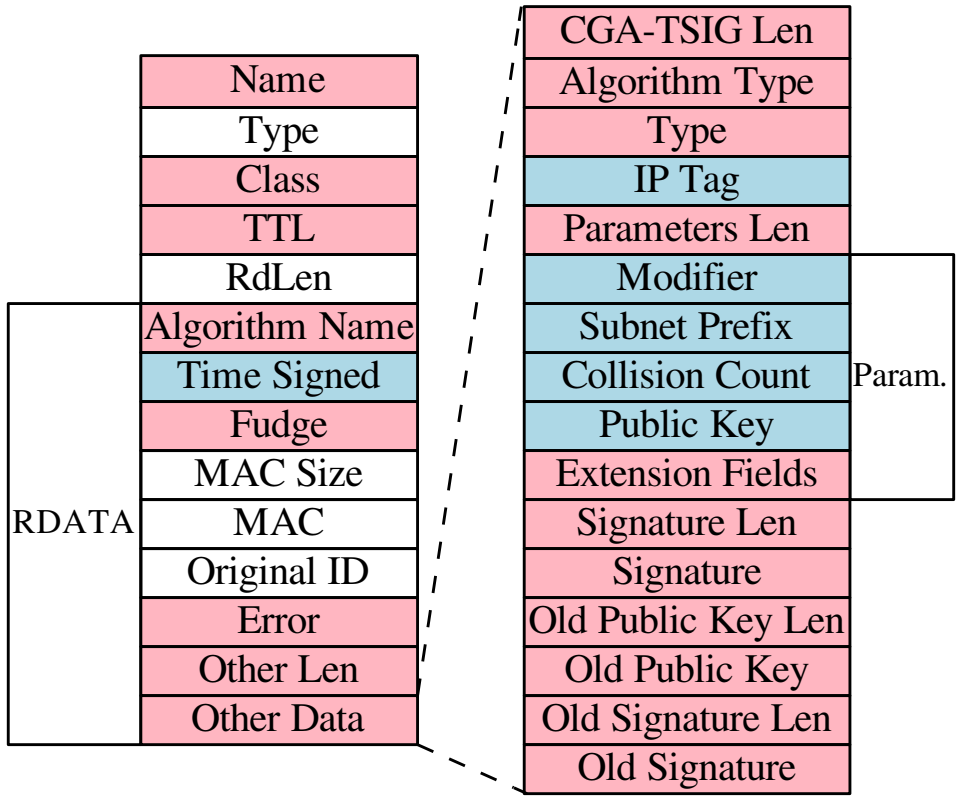
Proof of concept

- `ldns` library from NLnet Labs
  - written in C
  - already supports TSIG
- extended to support CGA-TSIG
  - CGA verification
  - public key signature generation/verification
- CGA generation tool
  - uses Scapy6
  - written in Python

Results

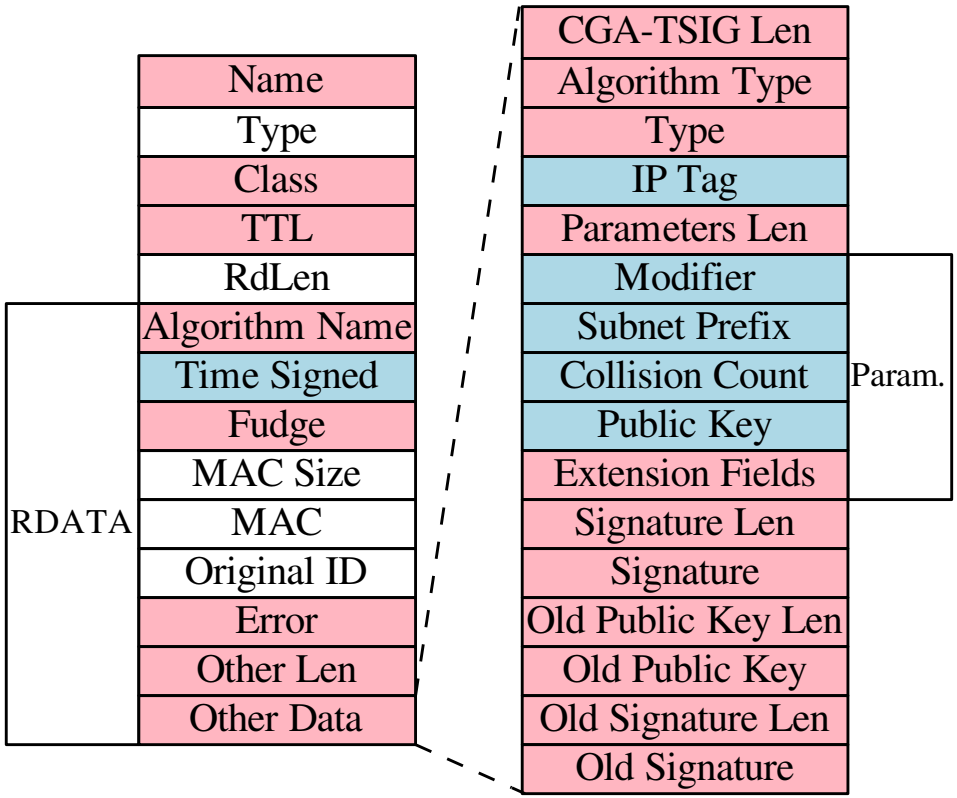
Results

- time signed is digested...
- ...but fudge is not
  - replay attacks
- nor other fields in red
- blue fields in arbitrary order
- does not adhere to TSIG
- signature fields left out



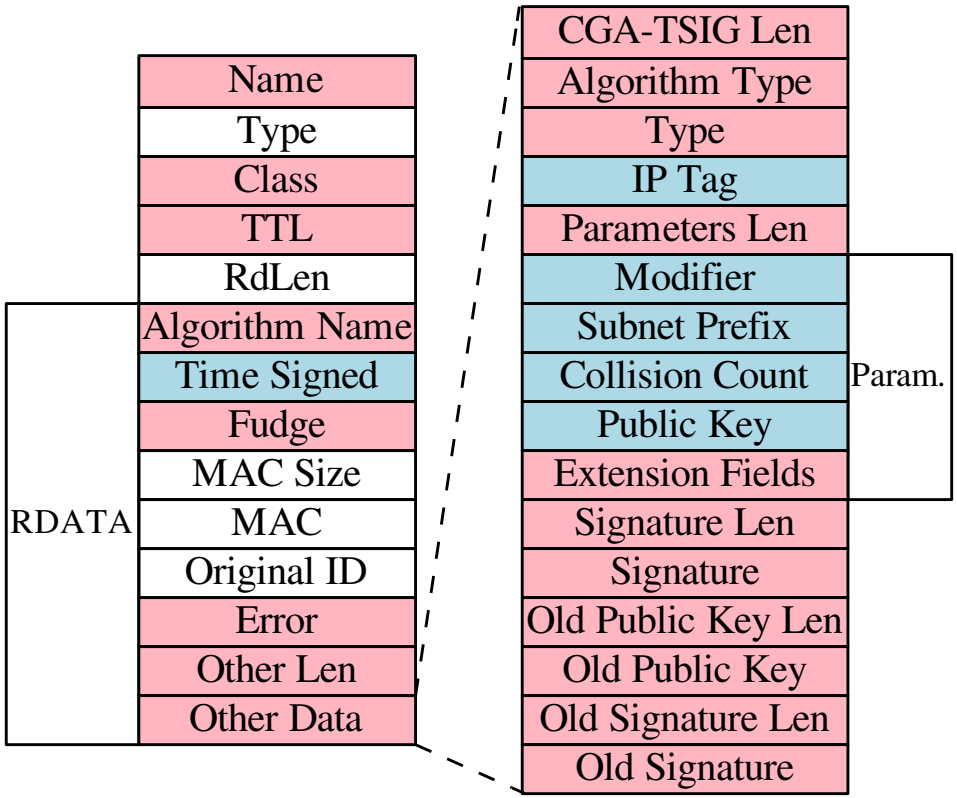
Results

- signature in new field
- MAC field left unused
- could save space if used



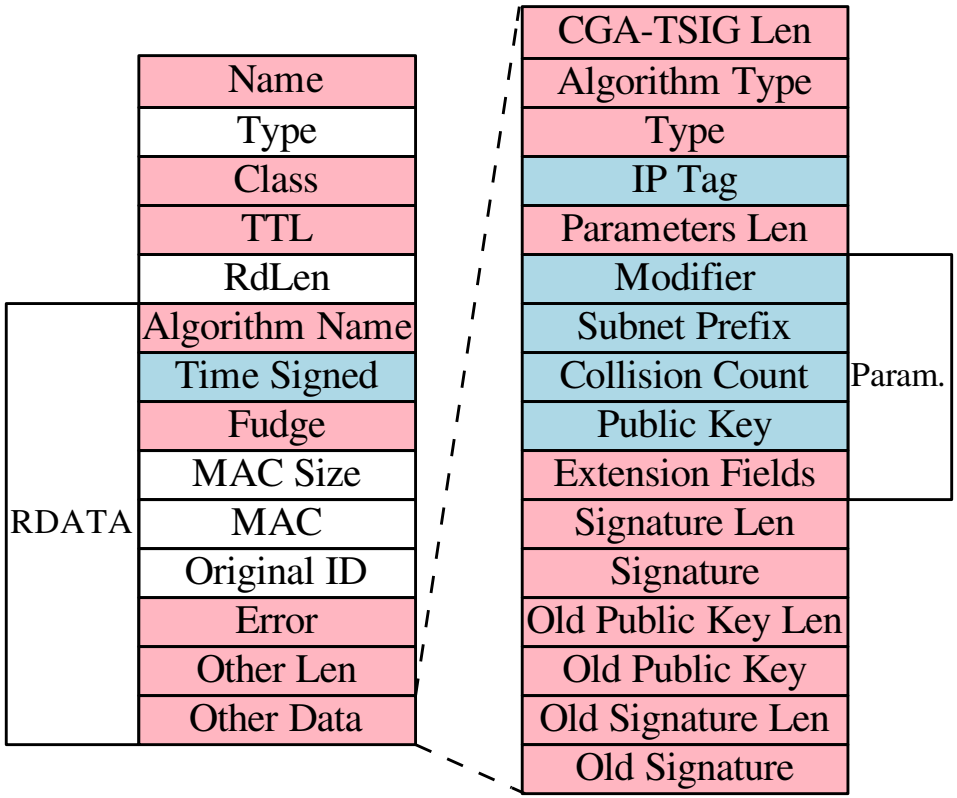
Results

- one-sided authentication
  - unlike TSIG
  - for last mile
- how to request CGA-TSIG?
  - set algorithm name
  - algorithm type too?
- time signed to 0
  - query is not signed



Results

- no CGA type tag defined
  - related protocol attacks
- what do do with name field?
- 1-octet length fields
- parameters length fields?
- other time signed check
- new CGA for server
  - how will clients know?
- old public key format not specified



Conclusion

Conclusion

- CGA-TSIG draft needs improvements
- can use any public key size
- CGA bit-strength up to 2^{171}
- only useful in IPv6
- TSIG implementations easy to extend
  - even though additions required
- clients still need to verify CGA somehow...

Is CGA-TSIG an adequate solution to the last mile problem?

CGA security

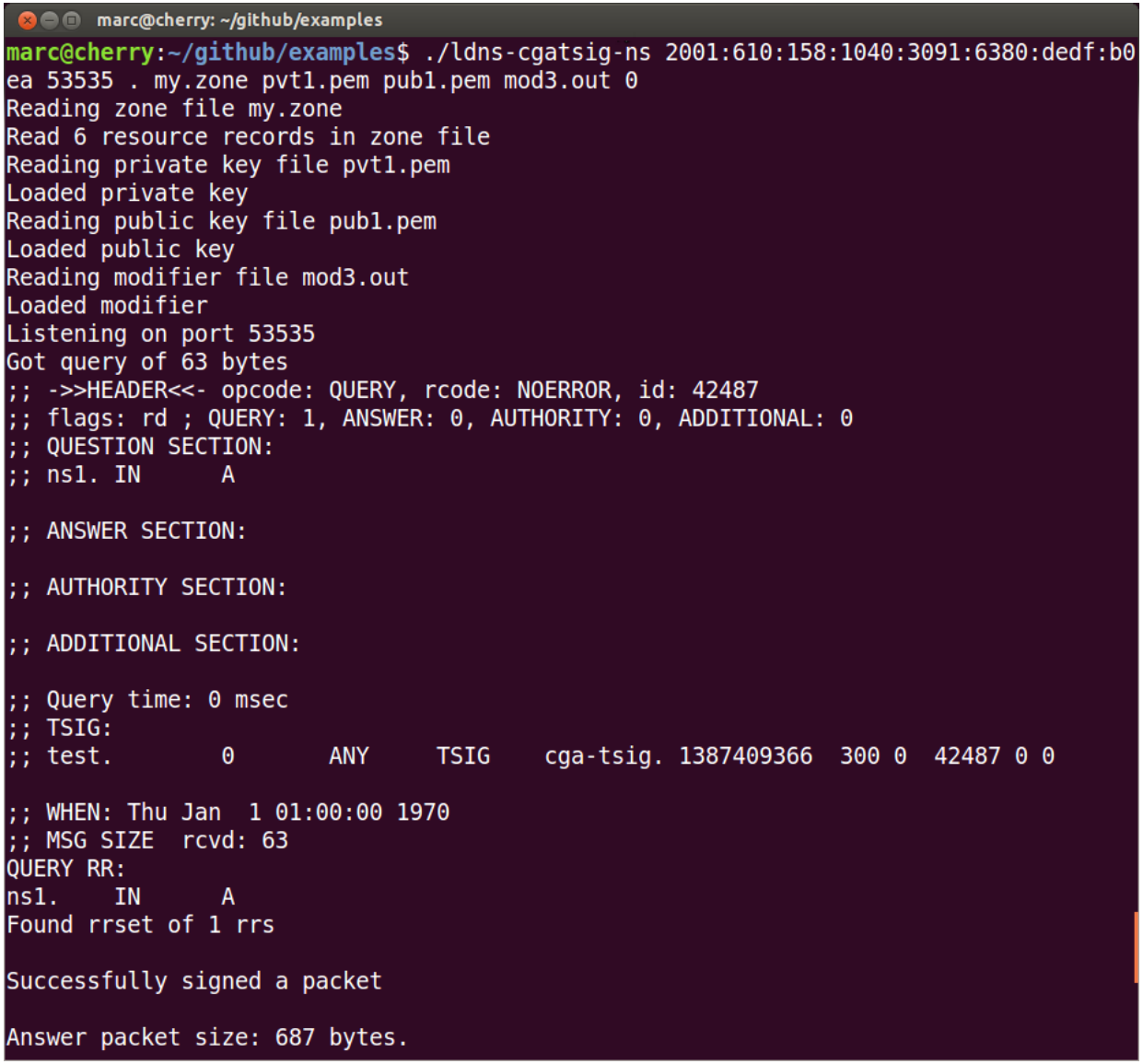
- cost to find *hash1* collision: $O(2^{59})$
- *sec* increases bit-strength
  - by factor $2^{16 \times sec}$
  - to find *hash2* collision
- total cost: $O(2^{59+16 \times sec})$
- *sec* cannot be spoofed

Demo~~lition~~ time!

Q&A

?

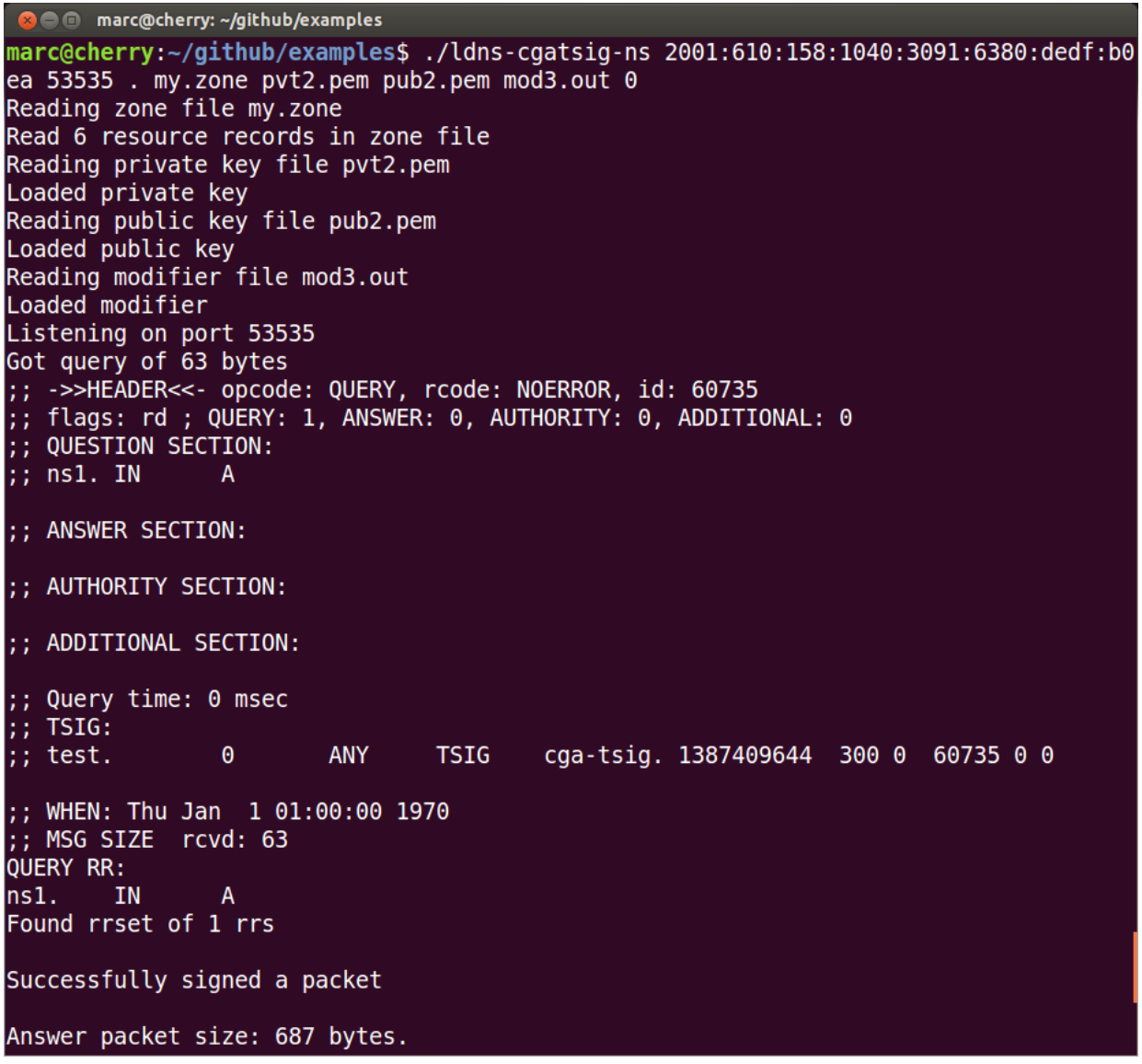
Demo


marc@cherry: ~/github/examples
marc@cherry:~/github/examples$ ./ldns-cgatsig-ns 2001:610:158:1040:3091:6380:dedf:b0
ea 53535 . my.zone pvt1.pem pub1.pem mod3.out 0
Reading zone file my.zone
Read 6 resource records in zone file
Reading private key file pvt1.pem
Loaded private key
Reading public key file pub1.pem
Loaded public key
Reading modifier file mod3.out
Loaded modifier
Listening on port 53535
Got query of 63 bytes
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 42487
;; flags: rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; ns1. IN A
;; ANSWER SECTION:
;; AUTHORITY SECTION:
;; ADDITIONAL SECTION:
;; Query time: 0 msec
;; TSIG:
;; test. 0 ANY TSIG cga-tsig. 1387409366 300 0 42487 0 0
;; WHEN: Thu Jan 1 01:00:00 1970
;; MSG SIZE rcvd: 63
QUERY RR:
ns1. IN A
Found rrset of 1 rrs
Successfully signed a packet
Answer packet size: 687 bytes.

Demo

```
marc@cherry: ~/github/examples
marc@cherry:~/github/examples$ ./ldns-cgatsig-query ns1 53535 0 resolv3.conf
0 0 4c b9 cd 52 bd d8 b7 65 6d 2b 87 22
sec = 1
enough zeros

;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 42487
;; flags: qr aa ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; ns1. IN      A

;; ANSWER SECTION:
ns1.    600     IN      A       145.100.104.28

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 5013 msec
;; TSIG:
;; test.        0       ANY     TSIG    cga-tsig. 1387409371  300 0  42487 0 605 Als
AAAABMJFjgN7fsOoAAAAAAAAAAAE/gHHggwxrpO/xMXcI6a8mLiABBhABWBBAADCCASIwDQYJKoZIhvcNAQE
BBQADggEPADCCAQoCggEBAMCZbq08v09XtboAlfqR4j7i7vApZo211R0s/TRjiPAf0r2VNTqNilwKZBojpQU
U0sxMr8glZQHWvQ5/623tzNCV3+yMqVElwHQR6Hwi+j+hzBWfATRd++juNpQJFVgM/3Avkfw33WHuP7fWlYN
zX4Redbg77GqiODB4AWRhQGpchpzO8qLa2asybt3xGwRqTc4n7SSOlf2dozllUeWUaDFYMFSBbIYGlg077vI
HurYu8fsWNkeQRyzyz1xzxmyG2FcpqwfdYNN6J9JpBlvBDBuCoZM2ZwJfjfQbQtly7EsEX+zryv5F1o5l3lo
yjBGvSYRKzktI1lXs69aW0O69CFkCAwEAAQEAfGU/oNNOVShS9n5SNeWwGQCopS56lHtMDNNDfXIVUBaxkwV
3MTrZO6qmnyQZYpuBqKhnsaZNp/iM5s/bVRdLpzdYmT2h7javma7Us3JJoRwsKUIaTEbNfJdgctjXt7bX1Jf
RhqFDnbtnYir6x3DN+eIkzJZuax5rto8+D/tah7FOC9QIgwdkpZ3gdMmzShgvCcA4yfY+3TELoy9KefIqTCl
FVfwHkpEAAppet9TpFm4PcIxHNvfznm5nVhgX/Ez/PhnsAwvV7eV2rjrVS7HtXAXeLAbTApYjKIS5TF74qxx
XOZQUcfcGp74wKnCFoAilvlFEGFRV7dTnwbbUQ82Z7gAAAAA=

;; SERVER: 2001:610:158:1040:3091:6380:dedf:b0ea
;; WHEN: Thu Dec 19 00:29:26 2013
;; MSG SIZE  rcvd: 687

Status after TSIG verification: All OK
```

Demo


marc@cherry: ~/github/examples
marc@cherry:~/github/examples$ ./ldns-cgatsig-ns 2001:610:158:1040:3091:6380:dedf:b0
ea 53535 . my.zone pvt2.pem pub2.pem mod3.out 0
Reading zone file my.zone
Read 6 resource records in zone file
Reading private key file pvt2.pem
Loaded private key
Reading public key file pub2.pem
Loaded public key
Reading modifier file mod3.out
Loaded modifier
Listening on port 53535
Got query of 63 bytes
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 60735
;; flags: rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; ns1. IN A
;; ANSWER SECTION:
;; AUTHORITY SECTION:
;; ADDITIONAL SECTION:
;; Query time: 0 msec
;; TSIG:
;; test. 0 ANY TSIG cga-tsig. 1387409644 300 0 60735 0 0
;; WHEN: Thu Jan 1 01:00:00 1970
;; MSG SIZE rcvd: 63
QUERY RR:
ns1. IN A
Found rrset of 1 rrs
Successfully signed a packet
Answer packet size: 687 bytes.

Demo


marc@cherry: ~/github/examples
marc@cherry:~/github/examples$ ./ldns-cgatsig-query ns1 53535 0 resolv3.conf
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 60735
;; flags: qr aa ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; ns1. IN A
;; ANSWER SECTION:
ns1. 600 IN A 145.100.104.28
;; AUTHORITY SECTION:
;; ADDITIONAL SECTION:
;; Query time: 5012 msec
;; TSIG:
;; test. 0 ANY TSIG cga-tsig. 1387409649 300 0 60735 0 605 Als
AAAABMJFjgN7fsOoAAAAAAAAAAAE/gHHggwxrpO/xMXcI6a8mLiABBhABWBBAADCCASIwDQYJKoZIhvcNAQE
BBQADggEPADCCAQoCggEBAOjgcZju7xsIvnBAYw9hAoPZ3Cc5+OCjJGyLCOrJcprPPCyBGHi77d/Ne54AqjZ
5GRU+xIy/WgrbTvu5A+JJePr+2sFS0Uw81iz7V+aKIjahqO/S13eGMwa2isxLVf0scKyp79oqhNhRfrgHlTk
71C0vTdcZvjSo7z8PN/9gaNM13zoWY3yFXYTKuX5zqcKxZIggylURW6YZe8p4cj/0xWEa6oKP+a+K6oYRCGW
KMAsuf1DUQO6UQQeNQuDWnjAYvqToTNwQCCrZNSgPYzijO7pqlMBO+rn+FaDIvQZgEBMiPr+KJ7uNf4ev6tT
U2neCMa7oN04Roo+YA/2gElWbCe0CAwEAAQEArq4FMqbO2ZKT+JuBu2YNIf205xVZC+fx5QhREkyJHB7r2zK
p0/m1rj+ToCtZh4G3ceQynsDwz2ZtHGbus2xh3bFuEYa+Y0Axh6up+fIvro/A98CeovkaEGJ/0quXR1xAum7
O/GthMpD6EY/EDl1P2jZXkW+toFs93wMcJH/7PANDAxQEkh+QOXKQHGtbx5p3x1boDJ2SSuHRfGU/88s5yyb
VdjxNKztY1eOrvdXAW2b92MvrOoll7yeoPMfNmU57VfL3yQAxAuEH9+phpkoafSrFgXBLGJrjAC/+qH29O5D
efZQ/62lflCEdNhRR50338RkddwCh62qwbqRLK3uYWQAAAAA=
;; SERVER: 2001:610:158:1040:3091:6380:dedf:b0ea
;; WHEN: Thu Dec 19 00:34:04 2013
;; MSG SIZE rcvd: 687
Status after TSIG verification: Bogus TSIG signature