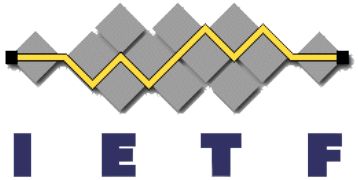


CGA-TSIG
a Possible Solution for Data Confidentiality

draft-rafiee-intarea-cga-tsig

Presenter: Erik Nordmark

Arista Networks

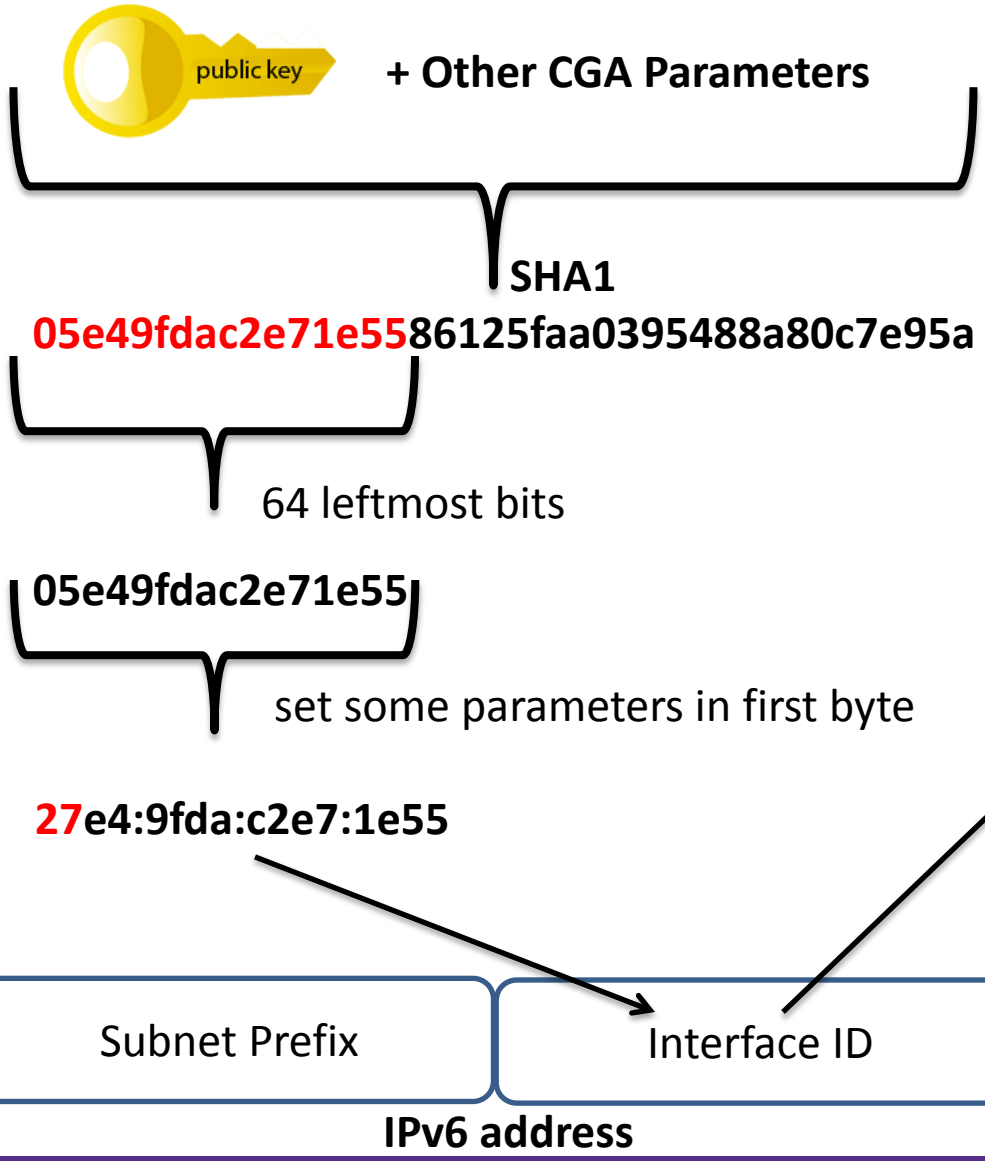
Authors: Hosnieh Rafiee
Ciber AG, Germany

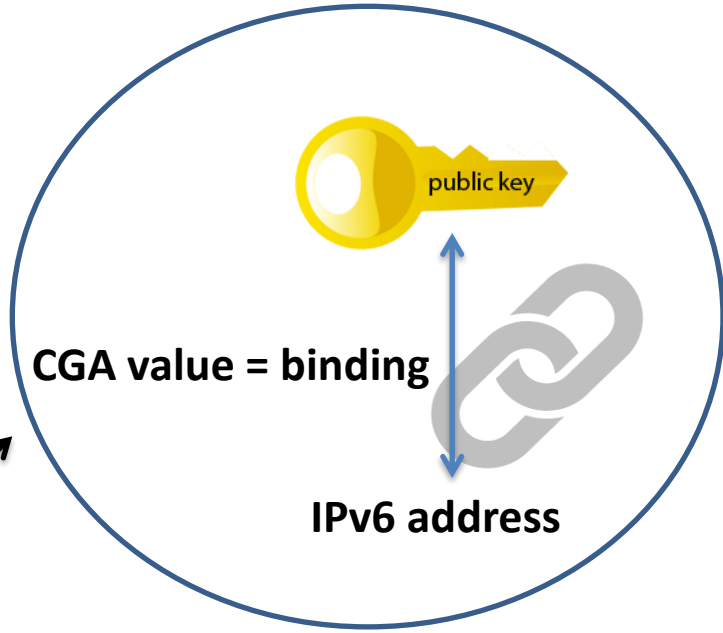
Martin v. Löwis, Christoph Meinel
Hasso Plattner Institute, Germany

IETF89
DNSOP WG
London
March 6, 2014

ciber®

CGA In a Simple Example (RFC 3972)





CGA-TSIGe in IPv6 Scenario - I

- Problem addressed:
  - Provide confidentiality while resolver must respond to anonymous queries

Step 1: Receiving the IP address of the resolver

Router authorization

- CGA verification
- Signature verification

Or

- Monitoring Node

Or

- Using FHS/SAVI or other mechanisms for router authorization

Or

- Manual configuration of IP address of the trusted resolver

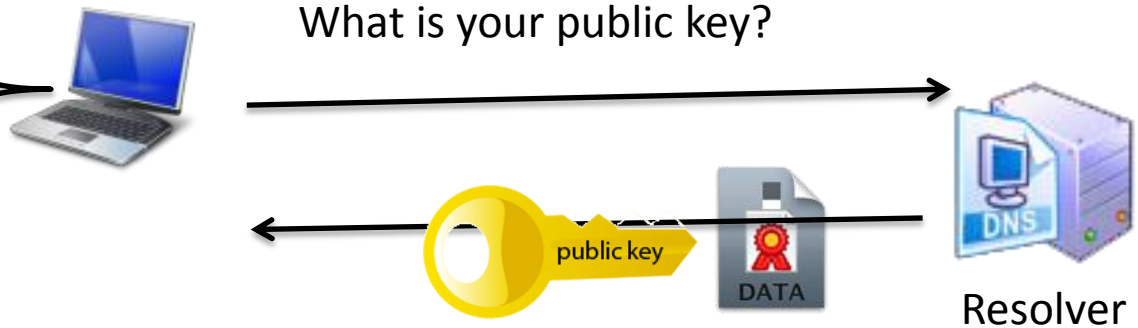
2010::**27e4:9fda:c2e7:1e55**

RA message with DNS option

CGA-TSIGe in IPv6 Scenario - II

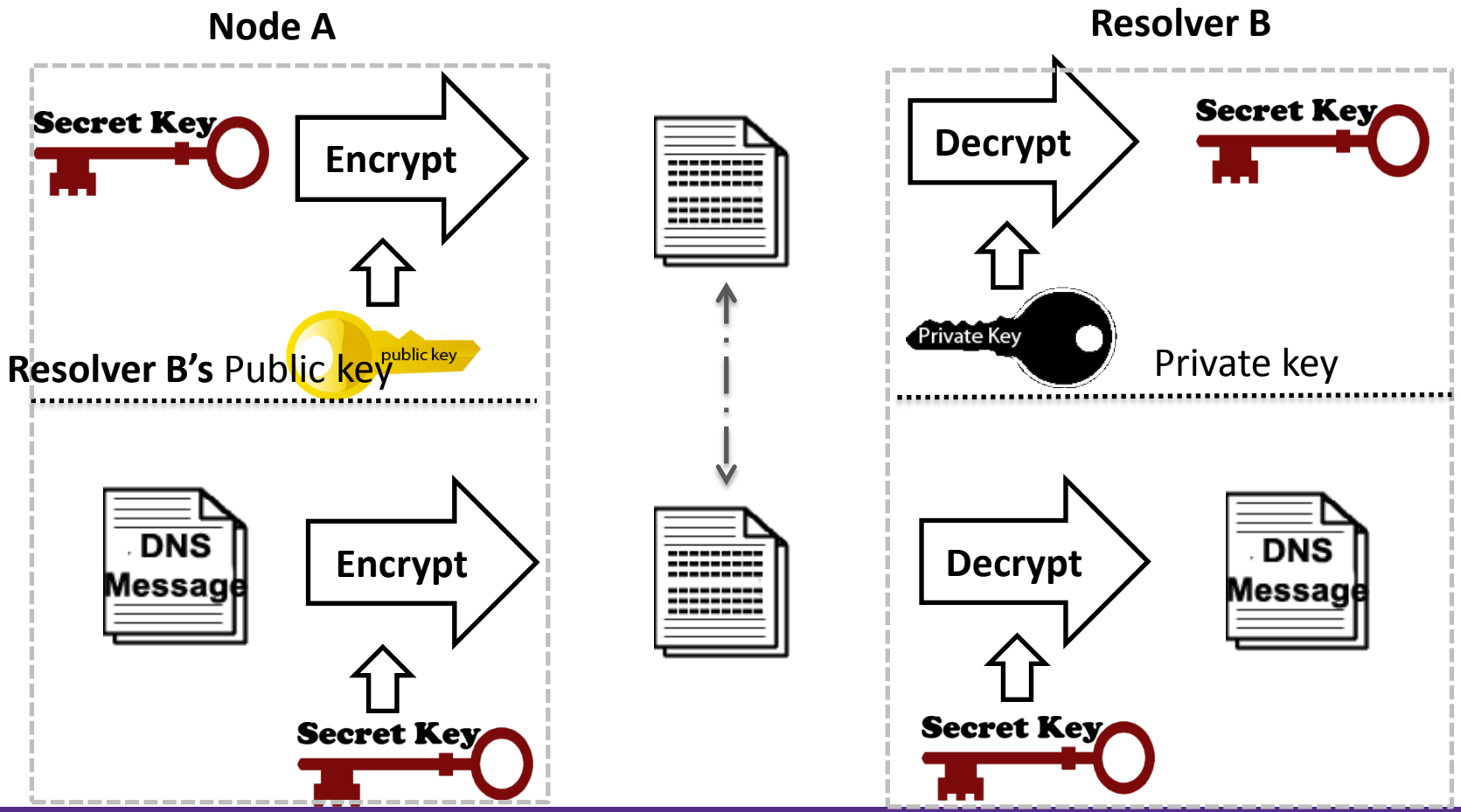
- Step 2: receive public key of the resolver
  - Resolver includes its public key in CGA-TSIG data structure
  - No need to repeat this step several times
    - Caching the public key of the resolver for further communication

Resolver verification
- CGA verification
- Signature verification
- Include the public key to his cache



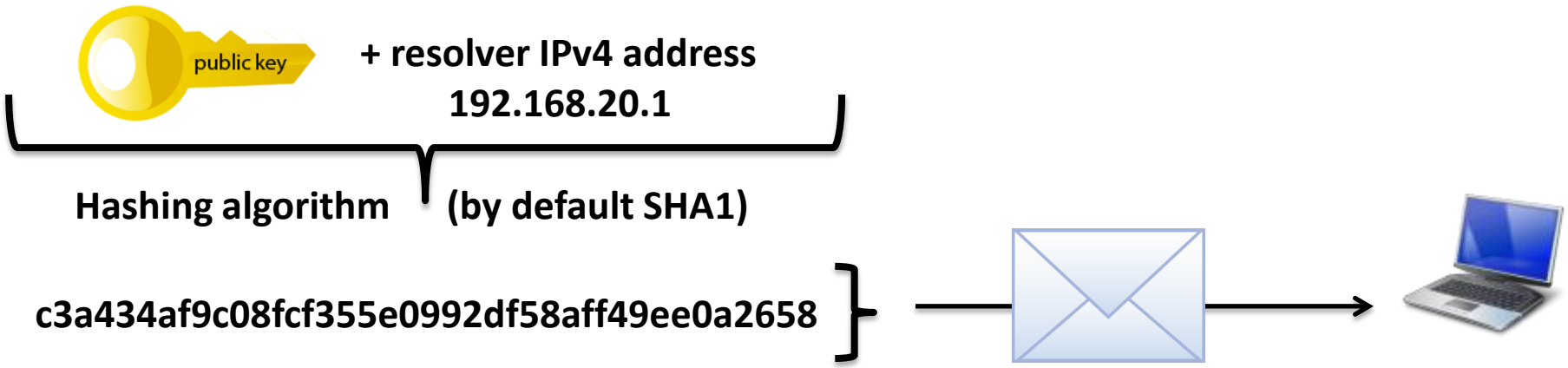
CGA-TSIGe in IPv6 Scenario - III

- Node A generates a 16 bytes random number and calls it a secret key
- Node A encrypts different section of DNS message and sets it to relevant sections of DNS message (prerequisite, query, etc)



CGA-TSIGe in IPv4 Scenario - I

- Retrieving the hash of {IP address + public key} and the IP address of the resolver from DHCPv4 (an option on DHCP packet)
  - Use monitoring nodes for security purpose
  - In unsecure environment, use the default home resolver

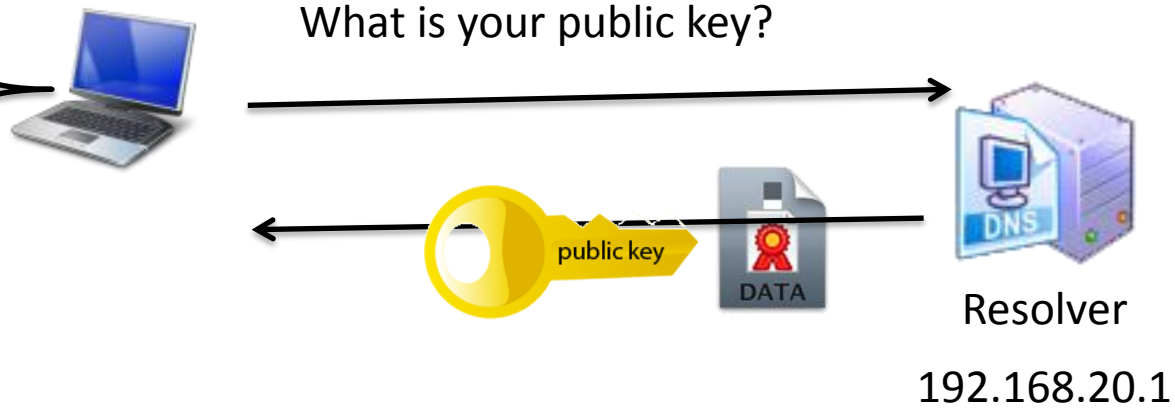


CGA-TSIGe in IPv4 Scenario - II

- Step 2: receive public key of the resolver
  - Resolver includes its public key in CGA-TSIG data structure

Resolver verification

- Is hash of public key+ IP address the same as available in node's cache? Yes/No
- Signature verification



- Step 3: symmetric encryption is in the same way as IPv6

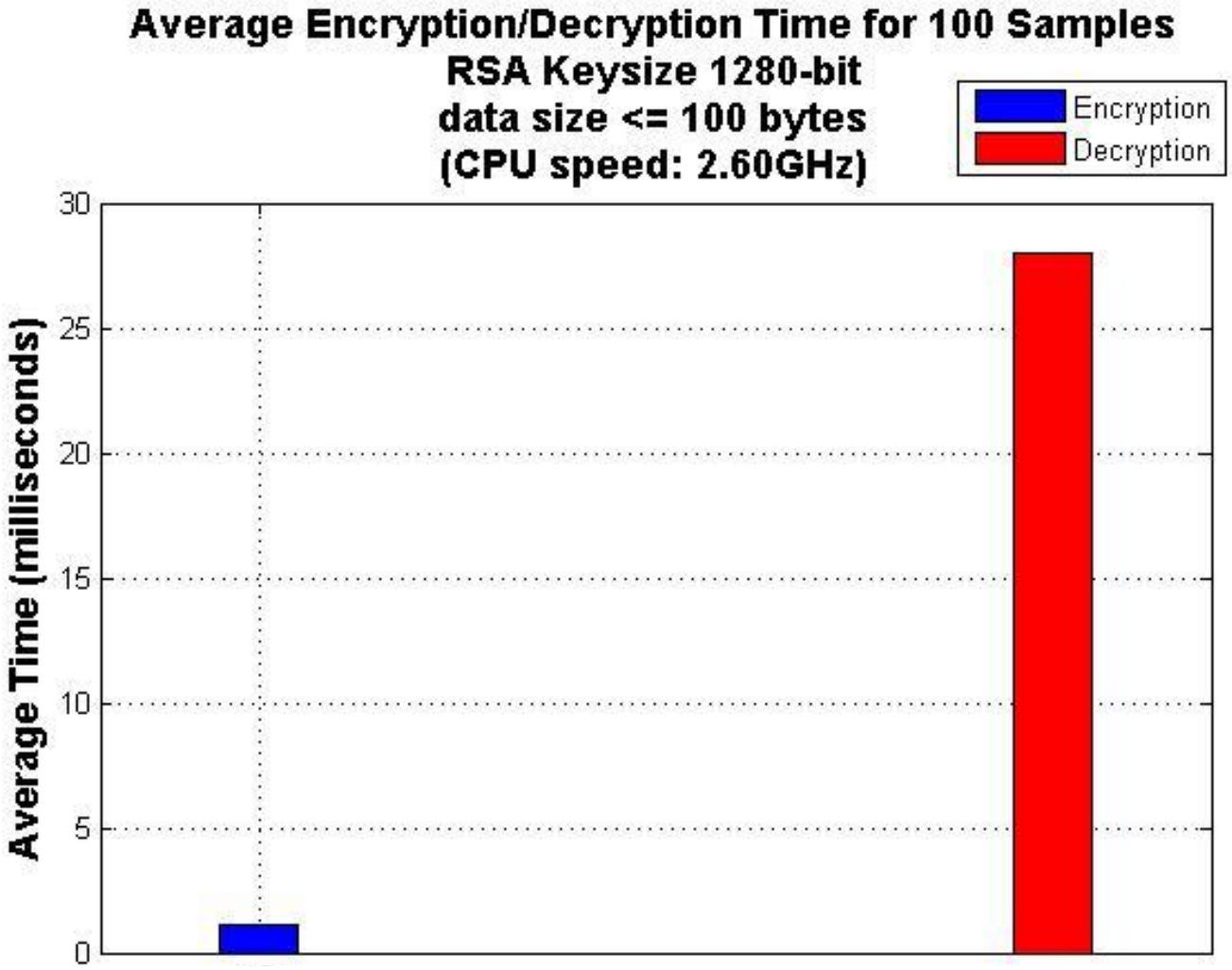
Thank you and changes to upcoming draft

- Question: Is this approach change DNS protocol?
- Answer: No, TSIG allows the definition of a new algorithm after the registration of this algorithm with IANA

- Including the IPv4 mapping section
- Applying the comments received on the mailing list during IETF
- Previous presentation of this draft

http://tools.ietf.org/agenda/89/slides/slides-89-intarea-5.pdf

Average Encryption/Decryption Time - RSA



Average Signature Generation/Verification Time - RSA