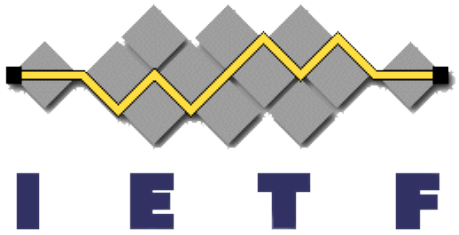


Hasso Plattner Institut

IT Systems Engineering | Universität Potsdam

A Simple Secure Addressing Scheme for IPv6 AutoConfiguration (SSAS)

http://tools.ietf.org/html/draft-rafiee-6man-ssas

Hosnieh Rafiee, Prof. Dr. Christoph Meinel

Hasso Plattner Institute, Germany

IETF87

6man WG

Berlin

July 29, 2013

What is SSAS?

- SSAS has two version:

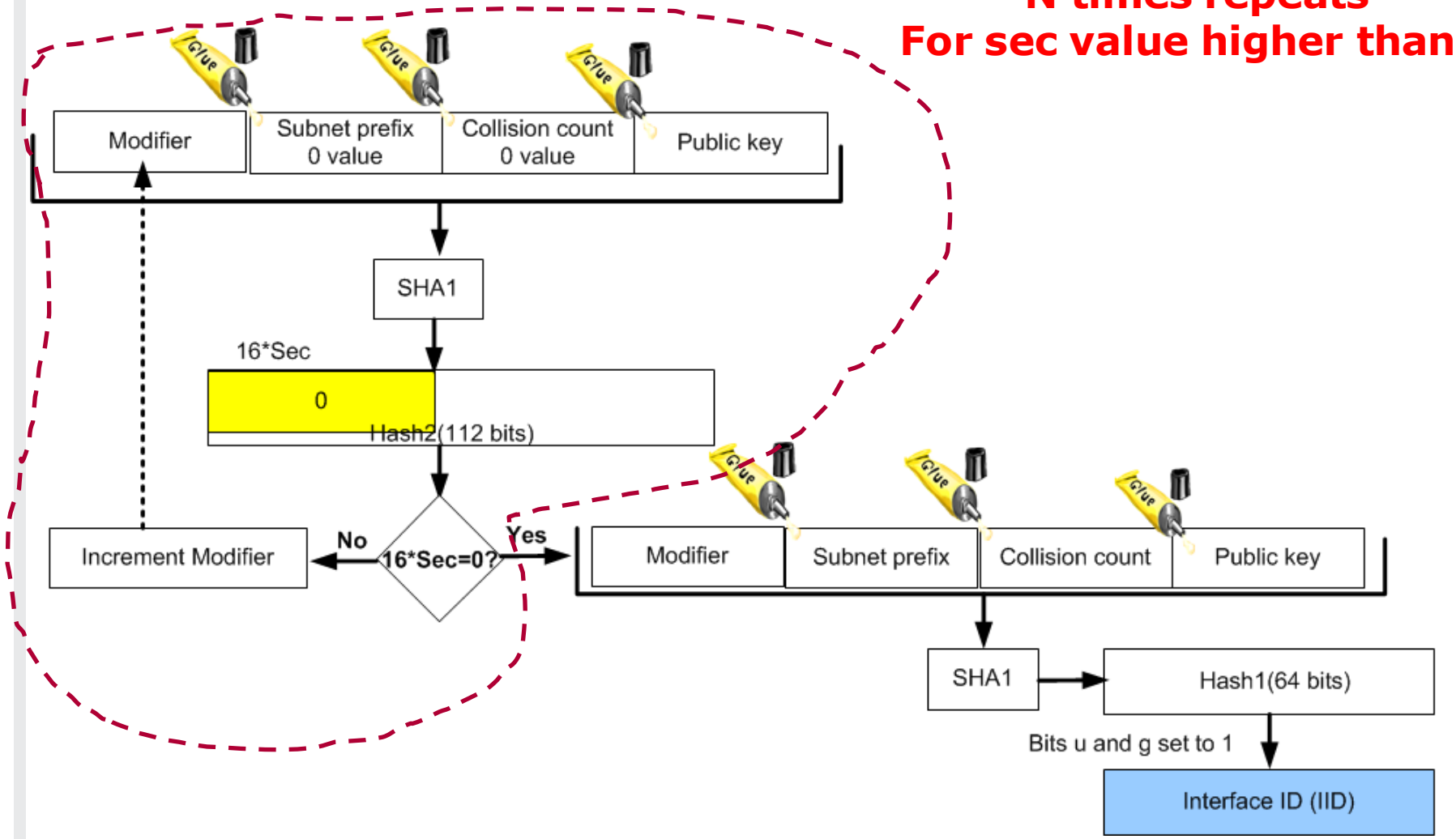
- SSAS v1:
  - The direct use of the public key in IID generation
  - The use of ECC (RFC 6090) rather than RSA in order to decrease the packet size by a factor of 5
  - Ideal for nodes with limited resources

- SSAS v2:
  - Execute a root function on the public key (Pk) where x is the value dependent on the size of Pk in order to make use the entire security of public key

$$R = \sqrt[x]{Pk}$$

Why SSAS?

- Faster and more secure than CGA



Why SSAS can use the whole security of public key? - I

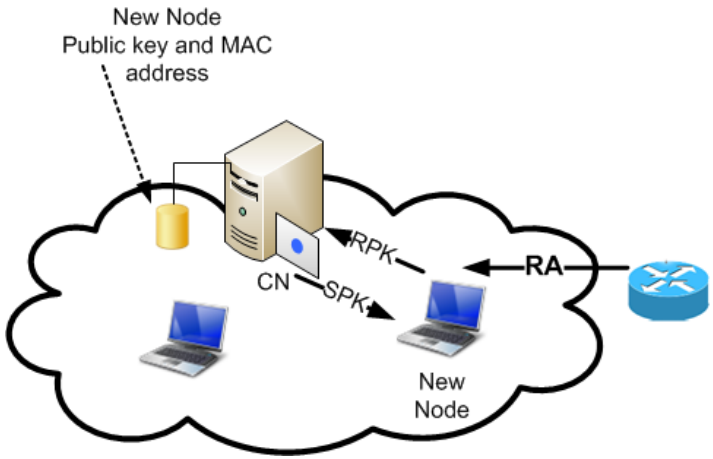
- For the **first time a node** joins a new network:
  - The attacker needs to do brute force attacks against **62 bits,** for CGA sec value 0 it is 59 bits.
- **After the first time:**
  - The whole security of the public key
- **Why?**
  - The node stores the public key of new node in its neighboring cache (After successful verification process)
  - Include the old public key when changes IP address and sign link layer address with old private key

Why SSAS can use the whole security of the public key? - II

- Proposed RPKI protect the routers
  - Controller Node (CN) in the network where the MAC address and public keys for new nodes are saved.
- According to the US National Security Agency, the ECC key size of 192 bits is equivalent to a RSA key size of 7680 bits.

http://www.nsa.gov/business/programs/elliptic_curve.shtml

- The whole security of the public key considered for SSAS v2



Thank you

Any Question 

Question for WG: Can we use the bits u and g?

- Does 6man wants to adopt this draft?

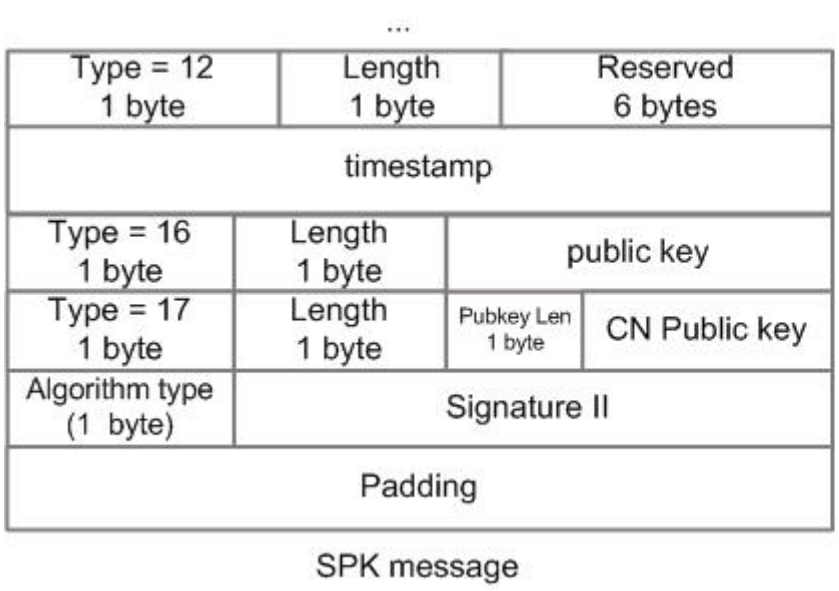
SSAS Second Algorithm (SSAS v2)

- SSAS v2 uses 5 bytes for real value of R and 5 parts for mantissa part

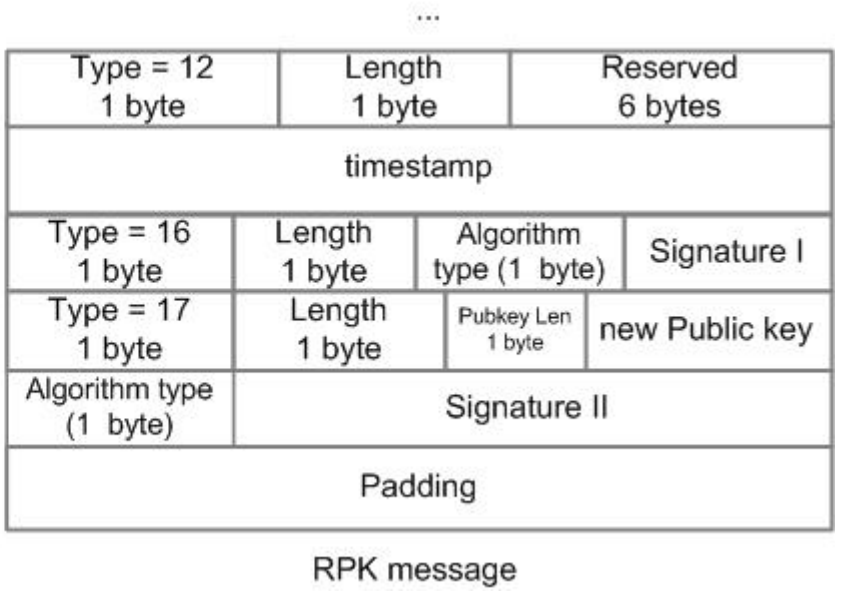
Number of bytes	Number of digits	Max number
3	8	16777215
5	13	1099511627775

- Time require to do division on a keysize of 192 bits is 100.01 microseconds

RPKI architecture with this approach



SPK message



RPK message

Controller Node (CN) in the network where the MAC address and public keys for new nodes are saved.

RPKI architecture with this approach - I

In this approach two new messages are used: Send Public Key (SPK) and Request Public Key (RPK). When a node joins a new network it generates its local IP address using SSAS and then sends a Router Solicitation message. This message need not include the SSAS signature. The router answers with an RA message that includes the SSAS signature. The node then sends an RPK asking the CN for the public key of this router. The CN responds with an SPK that includes the public key for the router and then it signs this message with its own public key. After a successful verification, the node will maintain the CN public key in a file.

When the CN node receives an RPK message, the MAC address and the public key are placed in its database. If a record already exists in the database, then the CN node answers by setting the length of the public key to zero indicating that there is already one public key in the database. If this node is the owner of that old public key, it signs the timestamp and the MAC address with its old public key, and then adds it to the RPK message, in signature II, before sending the packet to the CN node.