Another Support for Multiple Hash Algorithms in Cryptographically Generated Addresses

(CGAs)

(draft-zhou-6man-mhash-cga-00)

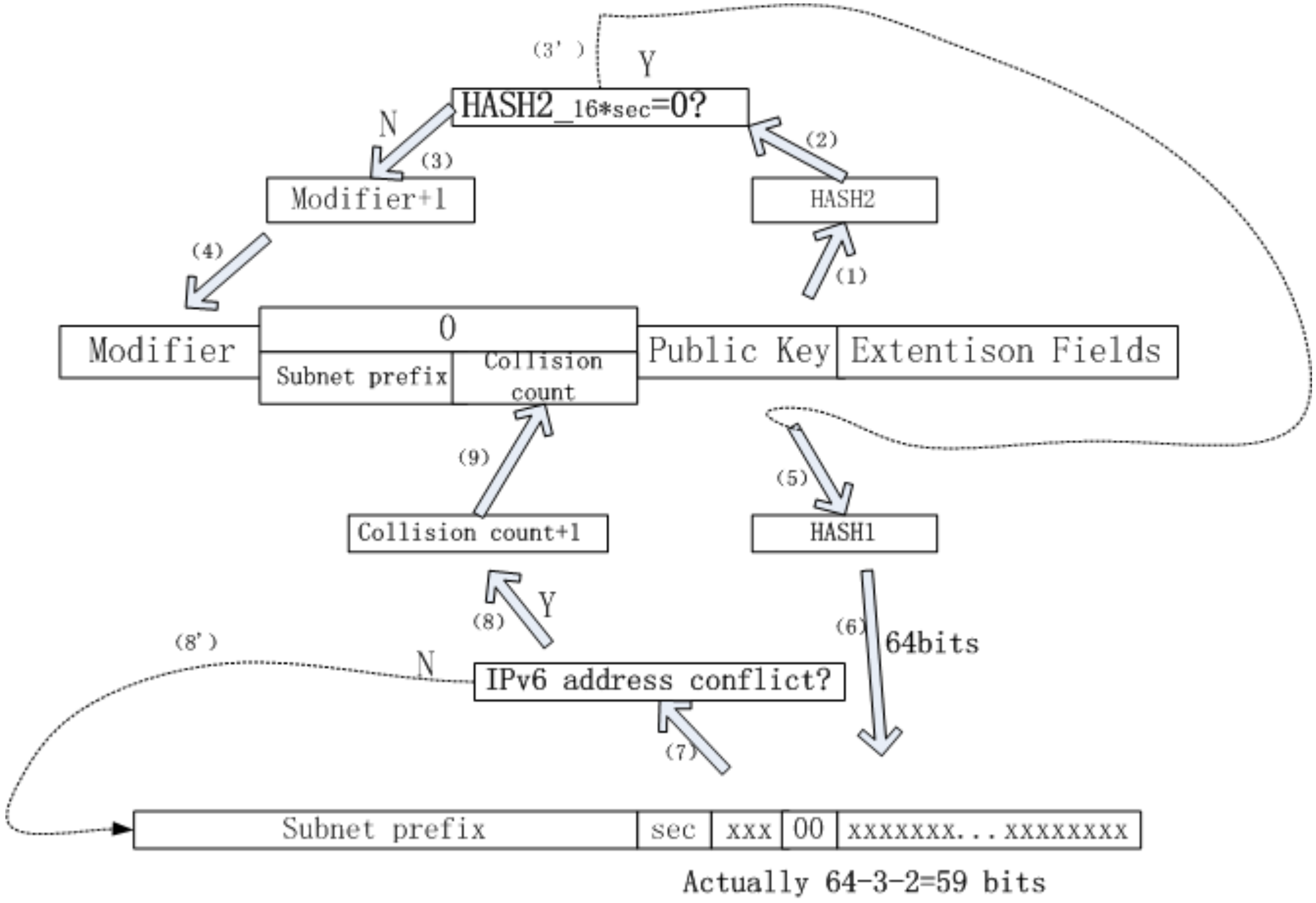
S. Zhou, R. Zhang, Z. Xie

IETF 83-6man, 2012-3

Motivation

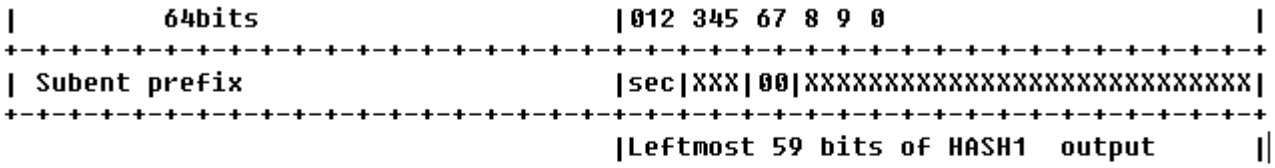
- Motivation：
  - SHA1 is hardcoded in Cryptographically Generated Addresses (CGAs) define in RFC 3972
  - At most 3 hash algorithms will be supported in RFC 4982
  - But support of 8 hash algorithms is reasonable
- Proposal
  - Trying to support more hash algorithms (8)
  - An improvement to RFC 4982

CGA generation in RFC3972



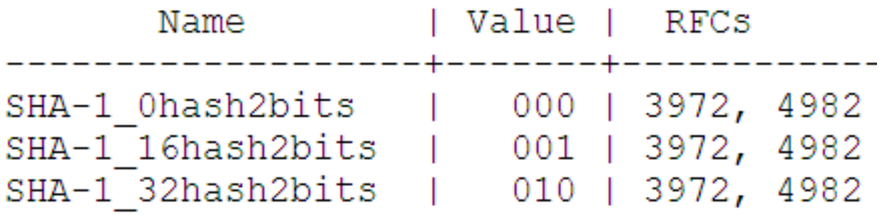
Solution in RFC 4982

- Hash indication must be in CGA to prevent down grading attack(RFC 4982)



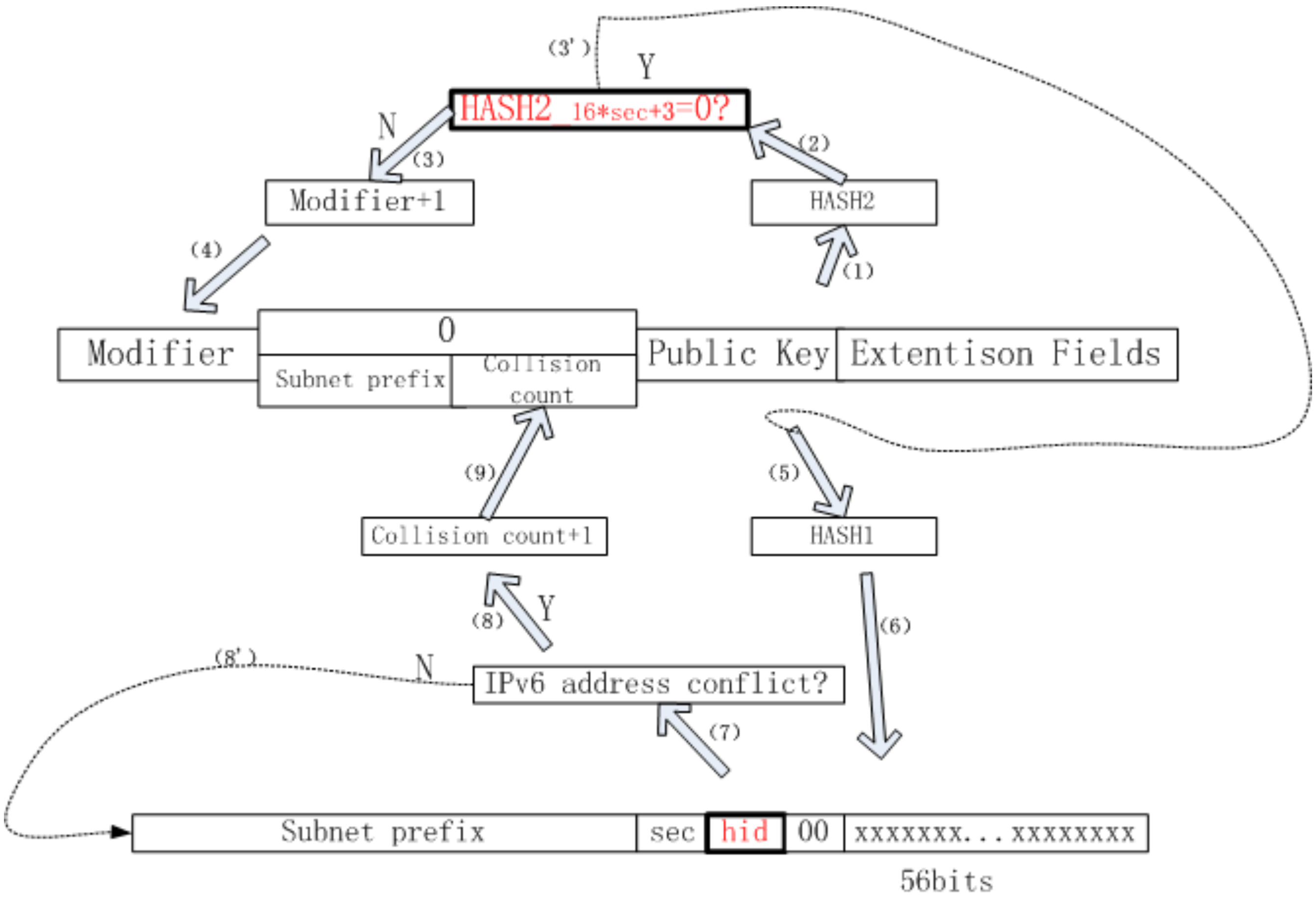
```
|         64bits                       |012 345 67 8 9 0                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Subent prefix                        |sec|XXX|00|XXXXXXXXXXXXXXXXXXXXXXXXXXXX|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                       |Leftmost 59 bits of HASH1  output      ||
```

- Shortened HASH1 output will weaken security level
- Redefinition of Sec in RFC 4982

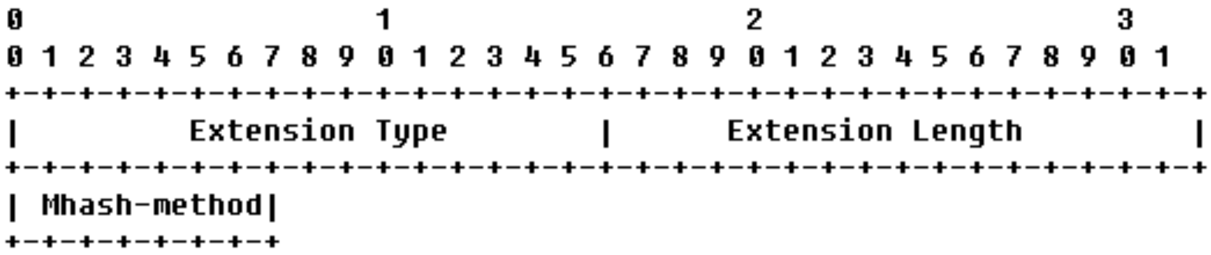


Name	Value	RFCs
SHA-1_0hash2bits	000	3972, 4982
SHA-1_16hash2bits	001	3972, 4982
SHA-1_32hash2bits	010	3972, 4982

Our proposal (figure)



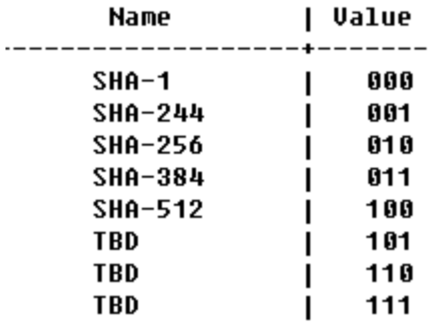
Our proposal

- 

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Extension Type        |       Extension Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Mhash-method|
+-+-+-+-+-+-+-+
```

mhash-method	Value
4982	0
this draft	1

- New parameter “hid”



Name	Value
SHA-1	000
SHA-244	001
SHA-256	010
SHA-384	011
SHA-512	100
TBD	101
TBD	110
TBD	111

Security Consideration

- Overall security in RFC3972

  O(2^(16*sec)+59).

- Overall security in this draft

  O(2^(16*sec)+3+56).

Next Steps

- Improvements based on comments
- Ask for adoption as WG item

Thanks!