FNV: A Non-Cryptographic Hash Algorithm

Glenn Fowler

AT&T Labs Research

gsf@research.att.com

Landon Curt Noll

Cisco Systems

fnv-rfc-mail@asthe.com

Kiem-Phong Vo

AT&T Labs Research

kpv@research.att.com

Donald Eastlake 3rd

Huawei Technologies

d3e3e3@gmail.com

FNV

- The FNV (Fowler/Noll/Vo) family of hash algorithms is based on some IEEE POSIX P1003.2 reviewer comments by Fowler and Vo with later improvement by Noll.
- FNV hashes are designed to be fast while maintaining a low collision rate. They provide high dispersion of results even when hashing nearly identical data and are thus suitable for hashing URLs, hostnames, filenames, text, IP addresses, etc.

FNV Flexibility

- Takes a sequence of octets as input.
- Multiple parameters can be hashed together by logically concatenating them.
  - If fixed or slowly changing value and input before more rapidly changing input, the state of the algorithm can be saved after processing the fixed or slowly changing input, and FNV restarted for different rapidly changing input.
- Specified means of producing outputs of various sizes/rangers.

FNV

- FNV is widely used in DNS servers, database indexing hashes, major web search / indexing engines, netnews history file Message-ID lookup functions, anti-spam filters, etc., etc.
- Web site with source code, etc.
  - http://www.isthe.com/chongo/tech/comp/fnv/index.html
- Current Internet Draft
  - http://tools.ietf.org/html/draft-eastlake-fnv-00

FNV-1a Code

```
○    hash = offset_basis
○    For each octet_of_data to be hashed
○            hash = hash xor octet_of_data
○            hash = hash * FNV_Prime
○    return hash
```

- Basic algorithm is specified for hash sizes of 2**n bits from 32 up to 1,024 bits.

FNV-1a Magic Primes

- FNV_Prime and offset_basis are the same size as hash.
- FNV_Prime will always have exactly 6 or 7 one bits. The low order bit, the 2**8 bit, exactly 3 or 4 bits between those in the low order 9 bits, and a single higher order one bit.
- Examples:
  - FNV32 Prime = 2**24 + 2**8 + 0x93
  - FNV64 Prime = 2**40 + 2**8 + 0xB3
  - FNV1024 Primve = 2**680 + 2**8 + 0x8D

FNV (non-)IPR

- The authors of FNV publicly disclosed the algorithm and source code shortly after inventing it years ago and have carefully refrained from taking any steps to patent it. Thus, it is safe to say that the authors have no patent claims to FNV.

Status of Document?

- Current Internet Draft says it is aimed at Informational.
- Could be a Standards Track document. This might be useful if people want a Standards Track RFC to reference.
- Current version does not actually have source code in it. It is intended that this be provided in the next version.

END

Glenn Fowler

AT&T Labs Research

gsf@research.att.com

Kiem-Phong Vo

AT&T Labs Research

kpv@research.att.com

Landon Curt Noll

Cisco Systems

fnv-rfc-mail@asthe.com

Donald Eastlake 3rd

Huawei Technologies

d3e3e3@gmail.com