NSA Patents SHA-256-SHA-512 Hashes (EN)

- Informatique - Sécurité Informatique -

Date de mise en ligne : mercredi 18 mai 2005

You probably already know this, but I studied that NSA hashing patent link you posted May 11, and it looks just like SHA-256/SHA-512 to me. I ve not seen it publicized anywhere that the NSA has patented the methods utilized by SHA-256/SHA-512 hashes (and possibly other variants).

- Original Link : http://patft.uspto.gov/netacgi/nph-Parser?patentnumber=6829355

- Readable flow/computation details : http://www.uspto.gov/web/patents/patog/week49/OG/html/1289-1/US06829355-20041207.html

- FIPS 180-2 (SHA2 family additions to SHS) :

http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf