Comments on CWC and GCM Modes for Authenticated Encryption

Dana Neustadter, Michael Bowler, Tom St. Denis, Mike Borza*

June 1, 2005

Carter-Wegman + Counter mode and Galois Counter Mode are authenticated encryption modes intended to provide secure scalable high-speed encryption and authentication functions. This commentary is made primarily from a hardware-centric point of view, which the authors feel is appropriate given the objective of achieving high speed operation. At the highest levels of performance, hardware implementations are required as they achieve orders of magnitude improvement in power and area efficiency compared with software. While the modes could conceivably make use of any 128-bit block cipher, this commentary is made specifically in the context of AES.

In current standard ASIC technologies, a single core implementation is capable of performance to beyond 50 Gbps. More aggressive fully custom implementations will be capable of higher performance still. This performance will continue to scale up as integrated circuit fabrication technology progresses. Owing to block-to-block independence in both modes it is possible to achieve linearly scalable performance gains by processing data in parallel across multiple identical blocks. As a result it is feasible to contemplate multi-hundreds gigabits per second implementations at this writing.

While both CWC and GCM modes achieve the same goals, if a single mode is to be preferred these authors favor adoption of GCM. There are a variety of commercial and technical reasons for this position as outlined below.

1. The authors of both modes assert no claims to IP rights through implementation and use of the respective modes and likewise know of no infringement of IP rights of others. These authors are similarly aware of no issues of IP rights infringement associated with the modes.
2. GCM-AES is the basis for security processing in emerging security standards such as IEEE 802.1AE and an extension to the IETF IPsec standard. The authors know of no such actual or planned adoption of CWC mode.
3. GCM computes a universal hash over GF(2^{128}) whereas CWC mode operates in the prime field GF(2^{127}-1). This makes hardware implementations of CWC mode larger due to the requirement for a hardware integer multiplier needing more gates than the binary Galois Field multiplier used in GCM. This may also translate into a speed advantage for GCM due to shorter critical path at the limit.
4. The 11 bytes length of the CWC nonce does not lend itself to a clean interface to other hardware, which will commonly be 32 bits in many modern systems. The GCM nonce is variable size, with a preferred 96 bits (12 bytes) length, making it compatible with 32 bits systems.

* The authors are employees of Elliptic Semiconductor Inc., 362 Terry Fox Drive Suite 220, Ottawa, Ontario, Canada. Questions or comments about this submission may be directed to mborza@ellipticsemi.com.

5. CWC mode requires one more AES encryption to compute the authentication tag if the hash key is not precomputed than does GCM. If the hash key is precomputed, CWC mode has the same number of AES cipher operations as GCM, but the precomputed powers of the hash subkeys must be maintained in expensive memory or registers.
6. The extra AES encryption required in CWC mode without precomputed hash key causes an undesirable stall in a pipelined implementation of CWC mode. This does not occur in GCM.
7. In CWC mode, multiplication is 96x128. As typically implemented in a hardware serial implementation, a shift register will store the multiplicand data. This shift register will be a problem in pipeline implementations as data would optimally be processed in 384 bit chunks to keep both multiplier and encryption unit optimally utilized. This will cause problems in real world protocol implementations which will typically not have this much buffered data present at one time. The result is that area is wasted on hardware which is not 100% utilized, and possibly requirements to provide buffer memory at points in a system where this is undesirable.

In conclusion, the authors are of the opinion that GCM represents an authenticated encryption solution that is more in tune with the architectural and design constraints of hardware based security processors than does CWC mode. As such we advocate for adoption of GCM as the preferred authenticated encryption mode.