Galois Counter Mode with Secure Short Tags (GCM-SST)

draft-mattsson-cfrg-aes-gcm-sst-02

Matthew Campagna
Amazon Web Services

John Preuß Mattsson
Ericsson

Alexander Maximov
Ericsson

AES with Galois Counter Mode (AES-GCM)

- AES-GCM is widely used due to its attractive performance and its provable security.
- During standardization, Ferguson pointed out two weaknesses in the GCM authentication function. The weaknesses are especially concerning when GCM is used with short tags:
  1. The first weakness significantly increases the probability of successful forgery.
  2. The second weakness reveals the subkey H if the attacker manages to create successful forgeries. With knowledge of the subkey H, the attacker always succeeds with subsequent forgeries. The probability of multiple successful forgeries is therefore significantly increased.
- As a comment to NIST, Nyberg, Gilbert, and Robshaw explained how small changes based on proven theoretical constructions mitigate the weaknesses.
- NIST did not follow the advice of Nyberg et al. and instead specified additional requirements for use with short tags in SP 800-38D Appendix C. Several cryptographers have criticized Appendix C and NIST has recently announced that they will remove Appendix C.
- While AES-CCM with short tags has forgery probabilities close to ideal, CCM has lower performance than GCM.

Every byte matters: the need for short tags

- 32-bit tags are standard in most radio link layers including 5G, 64-bit tags are very common in IoT transport and application layers, and 32-, 64-, and 80-bit tags are common in media-encryption applications.
- Audio packets are small, numerous, and ephemeral, so on the one hand, they are very sensitive in percentage terms to crypto overhead, and on the other hand, forgery of individual packets is not a big concern.
- Due to its weaknesses, GCM is typically not used with short tags. The result is either decreased performance from larger than needed tags, or decreased performance from using much slower constructions such as AES-CTR combined with HMAC.
- Short tags are also useful to protect packets transporting a signed payload such as a firmware and software updates.

Galois Counter Mode with Secure Short Tags (GCM-SST)

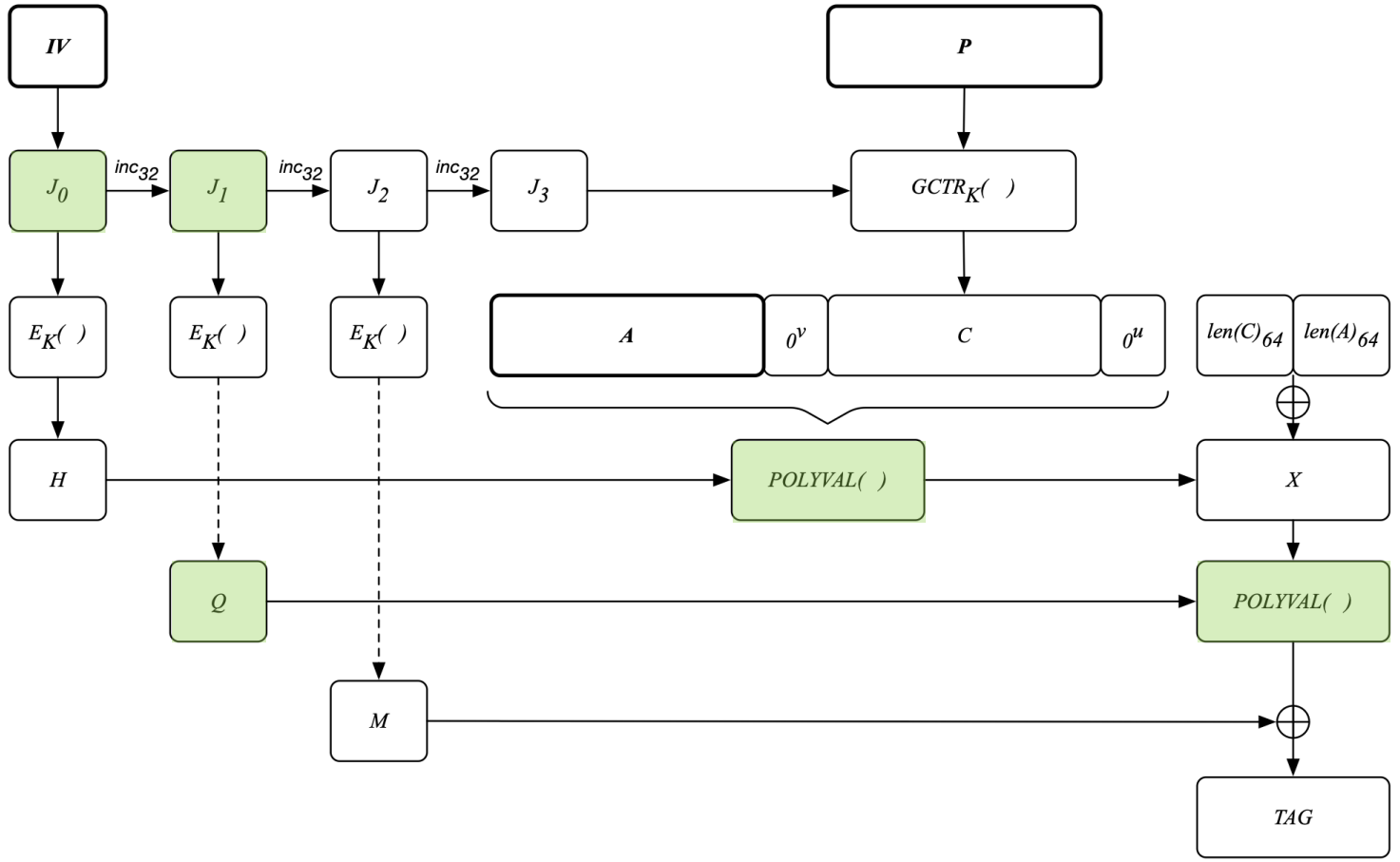
- Galois Counter Mode with Secure Short Tags (GCM-SST) is an AEAD algorithm following the recommendations from Nyberg et al.
- GCM-SST is defined with a general interface so that it can be used with any keystream generator, not just a 128-bit block cipher. AES-GCM-SST is a mode of operation of AES.
- The differences compared to GCM are that:
  1. GCM-SST uses an additional subkey Q. This enables short tags with forgery probabilities close to ideal.
  2. Fresh subkeys H and Q are derived for each nonce. This significantly decreases the probability of multiple successful forgeries.
  3. The POLYVAL function from AES-GCM-SIV is used instead of GHASH. POLYVAL is the "little-endian version" of GHASH and is more efficient in software implementations on little-endian architectures. GHASH and POLYVAL can be defined in terms of one another.
- ETSI SAGE and 3GPP have specified GCM-SST as the mode for future mobile networks. 5G Advance and 6G will use AES-256 and SNOW 5G in GCM-SST mode for "256-bit security" (requested by government customers).
  - Provides 10x higher performance on x86 in cloud-native deployments. 32–128-bit integrity tags.
- Strong interest in IETF for solutions like GCM-SST for use in media-encryption applications.

Authenticated encryption function

Steps:

1. If the lengths of K, N, A, or P are not supported return error and abort
2. Initiate keystream generator with K and N
3. Let $H = Z[0]$, $Q = Z[1]$, $M = Z[2]$
4. Let $ct = P \oplus \text{truncate}(Z[3: n + 2], \text{len}(P))$
5. Let $S = \text{zeropad}(A) \,||\, \text{zeropad}(ct)$
6. Let $L = \text{LE64}(\text{len}(ct)) \,||\, \text{LE64}(\text{len}(A))$
7. Let $X = \text{POLYVAL}(H, S[0], S[1], \ldots)$
8. Let $full\_tag = \text{POLYVAL}(Q, X \oplus L) \oplus M$
9. Let $tag = \text{truncate}(full\_tag, tag\_length)$
10. Return (ct, tag)

For AES, $Z[i] = \text{AES-ENC}(K, N \,||\, \text{BE32}(i))$

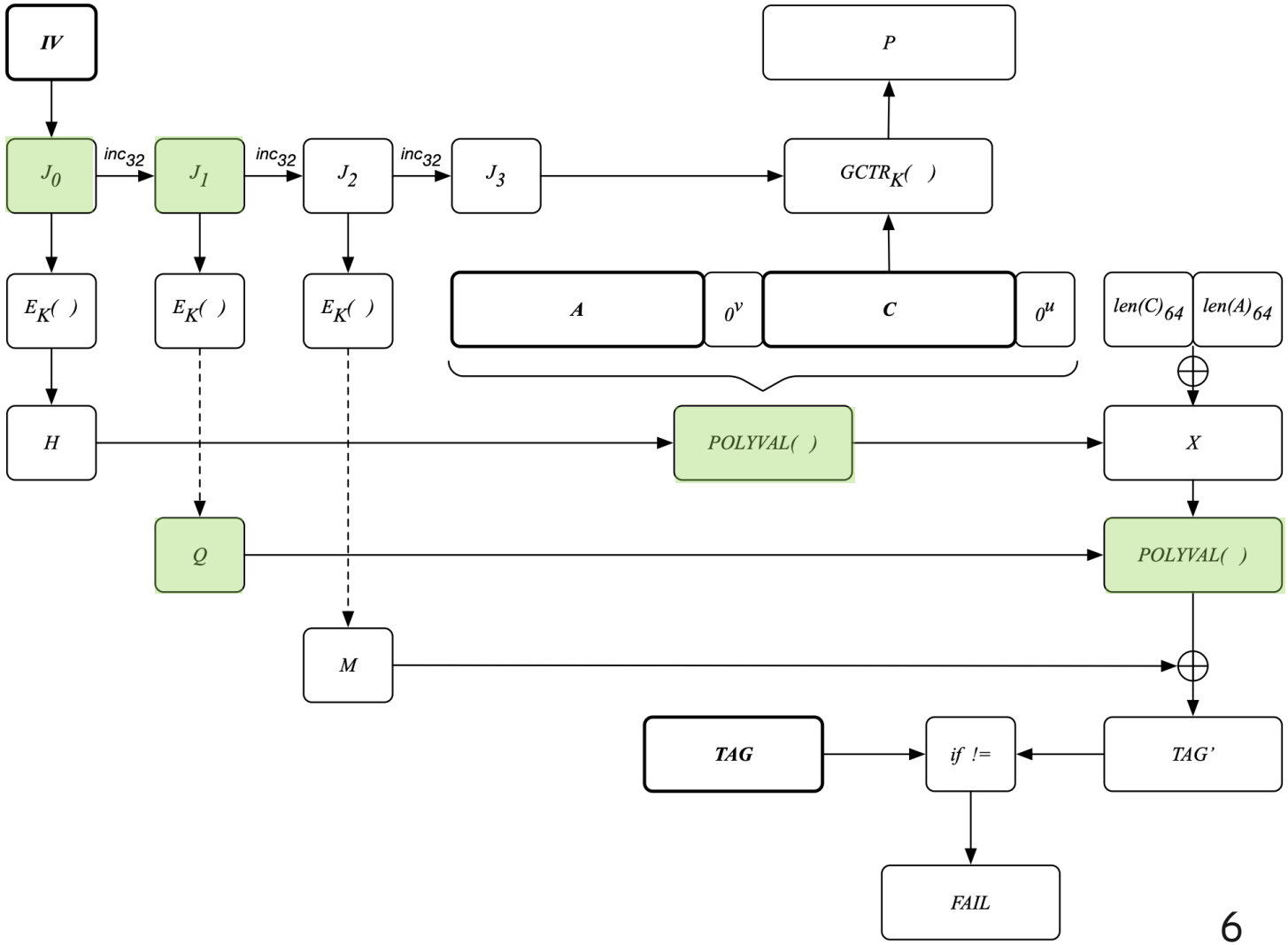


Authenticated decryption function

Steps:

1. If the lengths of K, N, A, or ct are not supported, or if len(tag) ≠ tag_length return error and abort
2. Initiate keystream generator with K and N
3. Let H = Z[0], Q = Z[1], M = Z[2]
4. Let S = zeropad(A) || zeropad(ct)
5. Let L = LE64(len(ct)) || LE64(len(A))
6. Let X = POLYVAL(H, S[0], S[1], . . .)
7. Let $full\_tag$ = POLYVAL(Q, $X \oplus L$) $\oplus M$
8. Let $expected\_tag$ = truncate($full\_tag$, tag_length)
9. If $tag \neq expected\_tag$, return error and abort
10. Let P = $ct \oplus$ truncate(Z[3: n + 2], len(ct))
11. Return P

For AES, $Z[i]$ = AES-ENC(K, N || BE32(i))



GCM-SST constrains and properties

- Performance is very similar to GCM. Two extra AES invocations are compensated by the faster POLYVAL.
- Tag size t ranges from 32 to 128 bits.
- For short tags of length $t < 128 - \log_2(n + m + 1)$ bits, the worst-case forgery probability is bounded by $\approx 2^{-t}$.
  - This is significantly better than GCM where the security level is only $t - \log_2(n + m + 1)$ bits.
- N_MIN and N_MAX (minimum and maximum size of the nonce) are both 12 octets, i.e., 96-bits.
- P_MAX (maximum size of the plaintext) is 2^{36} - 48 octets $\Rightarrow n \leq 2^{32} - 3$.
  - Adjusted as there are now three subkeys instead of two.
- A_MAX (maximum size of the associated data) is 2^{36} octets $\Rightarrow m \leq 2^{32}$.
  - Lowered to enable a forgery probability close to ideal for larger tags, even with maximum size P and A.
- With these constraints, $n + m + 1 < 2^{33}$ 128-bit blocks, and tags of length up to 95 bits have an almost perfect security level for all allowed plaintext and associated data lengths, i.e., the worst-case forgery probability is bounded by $\approx 2^{-t}$ where t is the tag length in bits.
- For a given key, the nonce must not be reused. Nonce reuse reveals the subkeys.

Summary

- GCM-SST is a small modification of GCM enabling short tags with forgery probabilities close to ideal.
- The changes are based on proven theoretical constructions and also work for stream ciphers.
- Performance-wise, it closely resembles GCM.
- Strong industry interest in a fast AES encryption mode with secure short tags.
- **CFRG Adoption?**

Summary by Nick Youngson CC BY-SA 3.0 Alpha Stock Images