Reconsidering the Security Bound of AES-GCM-SIV

Tetsu Iwata[1] and Yannick Seurin[2]

[1]Nagoya University, Japan

[2]ANSSI, France

March 7, 2018 — FSE 2018

Summary of the contribution

- we reconsider the security of the AEAD scheme AES-GCM-SIV designed by Gueron, Langley, and Lindell
- we identify flaws in the designers' security analysis and propose a new security proof
- our findings leads to significantly reduced security claims, especially for long messages
- we propose a simple modification to the scheme (key derivation function) improving security without efficiency loss

Summary of the contribution

- we reconsider the security of the AEAD scheme AES-GCM-SIV designed by Gueron, Langley, and Lindell
- we identify flaws in the designers' security analysis and propose a new security proof
- our findings leads to significantly reduced security claims, especially for long messages
- we propose a simple modification to the scheme (key derivation function) improving security without efficiency loss

Summary of the contribution

- we reconsider the security of the AEAD scheme AES-GCM-SIV designed by Gueron, Langley, and Lindell
- we identify flaws in the designers' security analysis and propose a new security proof
- our findings leads to significantly reduced security claims, especially for long messages
- we propose a simple modification to the scheme (key derivation function) improving security without efficiency loss

Summary of the contribution

- we reconsider the security of the AEAD scheme AES-GCM-SIV designed by Gueron, Langley, and Lindell
- we identify flaws in the designers' security analysis and propose a new security proof
- our findings leads to significantly reduced security claims, especially for long messages
- we propose a simple modification to the scheme (key derivation function) improving security without efficiency loss

Outline

Outline

History of (AES)-GCM-(SIV) AEAD schemes

- GCM [MV04]
  - CTR encryption + Wegman-Carter MAC
  - Encrypt-then-MAC composition
  - widely deployed, not nonce-misuse resistant [Jou06, BZD+16]
- GCM-SIV [GL15]
  - same components as GCM
  - Synthetic IV (SIV) composition [RS06]
  - nonce-misuse resistant
- AES-GCM-SIV [GLL16, GLL17]
  - ≠ GCM-SIV instantiated with AES
  - similar to GCM-SIV but three modifications:
    - universal hash function (POLYVAL instead of GHASH)
    - full-block counter
    - nonce-based key derivation $(K, N) \mapsto (K_{auth}, K_{enc})$
  - proposed for standardization at IETF CFRG

History of (AES)-GCM-(SIV) AEAD schemes

- GCM [MV04]
  - CTR encryption + Wegman-Carter MAC
  - Encrypt-then-MAC composition
  - widely deployed, not nonce-misuse resistant [Jou06, BZD+16]
- GCM-SIV [GL15]
  - same components as GCM
  - Synthetic IV (SIV) composition [RS06]
  - nonce-misuse resistant
- AES-GCM-SIV [GLL16, GLL17]
  - $\neq$ GCM-SIV instantiated with AES
  - similar to GCM-SIV but three modifications:
    - universal hash function (POLYVAL instead of GHASH)
    - full-block counter
    - nonce-based key derivation $(K, N) \mapsto (K_{auth}, K_{enc})$
  - proposed for standardization at IETF CFRG

History of (AES)-GCM-(SIV) AEAD schemes

- GCM [MV04]
  - CTR encryption + Wegman-Carter MAC
  - Encrypt-then-MAC composition
  - widely deployed, not nonce-misuse resistant [Jou06, BZD+16]
- GCM-SIV [GL15]
  - same components as GCM
  - Synthetic IV (SIV) composition [RS06]
  - nonce-misuse resistant
- AES-GCM-SIV [GLL16, GLL17]
  - $\neq$ GCM-SIV instantiated with AES
  - similar to GCM-SIV but three modifications:
    - universal hash function (POLYVAL instead of GHASH)
    - full-block counter
    - nonce-based key derivation
  - proposed for standardization at IETF CFRG

History of (AES)-GCM-(SIV) AEAD schemes

- GCM [MV04]
  - CTR encryption + Wegman-Carter MAC
  - Encrypt-then-MAC composition
  - widely deployed, not nonce-misuse resistant [Jou06, BZD+16]
- GCM-SIV [GL15]
  - same components as GCM
  - Synthetic IV (SIV) composition [RS06]
  - nonce-misuse resistant
- AES-GCM-SIV [GLL16, GLL17]
  - $\neq$ GCM-SIV instantiated with AES
  - similar to GCM-SIV but three modifications:
    - universal hash function (POLYVAL instead of GHASH)
    - full-block counter
    - nonce-based key derivation $(K, N) \mapsto (K_{polyval}, K_{ae})$
  - proposed for standardization at IETF CFRG

History of (AES)-GCM-(SIV) AEAD schemes

- GCM [MV04]
  - CTR encryption + Wegman-Carter MAC
  - Encrypt-then-MAC composition
  - widely deployed, not nonce-misuse resistant [Jou06, BZD+16]
- GCM-SIV [GL15]
  - same components as GCM
  - Synthetic IV (SIV) composition [RS06]
  - nonce-misuse resistant
- AES-GCM-SIV [GLL16, GLL17]
  - $\neq$ GCM-SIV instantiated with AES
  - similar to GCM-SIV but three modifications:
    - universal hash function (POLYVAL instead of GHASH)
    - full-block counter
    - nonce-based key derivation $(K, N) \mapsto (K_{\text{polyval}}, K_{\text{BC}})$
  - proposed for standardization at IETF CFRG

History of (AES)-GCM-(SIV) AEAD schemes

- GCM [MV04]
  - CTR encryption + Wegman-Carter MAC
  - Encrypt-then-MAC composition
  - widely deployed, not nonce-misuse resistant [Jou06, BZD+16]
- GCM-SIV [GL15]
  - same components as GCM
  - Synthetic IV (SIV) composition [RS06]
  - nonce-misuse resistant
- AES-GCM-SIV [GLL16, GLL17]
  - $\neq$ GCM-SIV instantiated with AES
  - similar to GCM-SIV but three modifications:
    - universal hash function (POLYVAL instead of GHASH)
    - full-block counter
    - nonce-based key derivation (K, N)
  - proposed for standardization at IETF CFRG

History of (AES)-GCM-(SIV) AEAD schemes

- GCM [MV04]
  - CTR encryption + Wegman-Carter MAC
  - Encrypt-then-MAC composition
  - widely deployed, not nonce-misuse resistant [Jou06, BZD$^+$16]
- GCM-SIV [GL15]
  - same components as GCM
  - Synthetic IV (SIV) composition [RS06]
  - nonce-misuse resistant
- AES-GCM-SIV [GLL16, GLL17]
  - $\neq$ GCM-SIV instantiated with AES
  - similar to GCM-SIV but three modifications:
    - universal hash function (POLYVAL instead of GHASH)
    - full-block counter
    - nonce-based key derivation $(K, N) \mapsto (K_{polyval}, K_{AES})$
  - proposed for standardization at IETF CFRG

History of (AES)-GCM-(SIV) AEAD schemes

- GCM [MV04]
  - CTR encryption + Wegman-Carter MAC
  - Encrypt-then-MAC composition
  - widely deployed, not nonce-misuse resistant [Jou06, BZD+16]
- GCM-SIV [GL15]
  - same components as GCM
  - Synthetic IV (SIV) composition [RS06]
  - nonce-misuse resistant
- AES-GCM-SIV [GLL16, GLL17]
  - ≠ GCM-SIV instantiated with AES
  - similar to GCM-SIV but three modifications:
    - universal hash function (POLYVAL instead of GHASH)
    - full-block counter
    - nonce-based key derivation $(K, N) \mapsto (K_{auth}, K_{enc})$
  - proposed for standardization at IETF CFRG

History of (AES)-GCM-(SIV) AEAD schemes

- GCM [MV04]
  - CTR encryption + Wegman-Carter MAC
  - Encrypt-then-MAC composition
  - widely deployed, not nonce-misuse resistant [Jou06, BZD+16]
- GCM-SIV [GL15]
  - same components as GCM
  - Synthetic IV (SIV) composition [RS06]
  - nonce-misuse resistant
- AES-GCM-SIV [GLL16, GLL17]
  - $\neq$ GCM-SIV instantiated with AES
  - similar to GCM-SIV but three modifications:
    - universal hash function (POLYVAL instead of GHASH)
    - full-block counter
    - nonce-based key derivation $(K, N) \mapsto (K_{\text{polyval}}, K_{\text{BC}})$
  - proposed for standardization at IETF CFRG

History of (AES)-GCM-(SIV) AEAD schemes

- GCM [MV04]
  - CTR encryption + Wegman-Carter MAC
  - Encrypt-then-MAC composition
  - widely deployed, not nonce-misuse resistant [Jou06, BZD+16]
- GCM-SIV [GL15]
  - same components as GCM
  - Synthetic IV (SIV) composition [RS06]
  - nonce-misuse resistant
- AES-GCM-SIV [GLL16, GLL17]
  - $\neq$ GCM-SIV instantiated with AES
  - similar to GCM-SIV but three modifications:
    - universal hash function (POLYVAL instead of GHASH)
    - full-block counter
    - nonce-based key derivation $(K, N) \mapsto (K_{\text{polyval}}, K_{\text{BC}})$
  - proposed for standardization at IETF CFRG

History of (AES)-GCM-(SIV) AEAD schemes

- GCM [MV04]
  - CTR encryption + Wegman-Carter MAC
  - Encrypt-then-MAC composition
  - widely deployed, not nonce-misuse resistant [Jou06, BZD+16]
- GCM-SIV [GL15]
  - same components as GCM
  - Synthetic IV (SIV) composition [RS06]
  - nonce-misuse resistant
- AES-GCM-SIV [GLL16, GLL17]
  - $\neq$ GCM-SIV instantiated with AES
  - similar to GCM-SIV but three modifications:
    - universal hash function (POLYVAL instead of GHASH)
    - full-block counter
    - nonce-based key derivation $(K, N) \mapsto (K_{\mathrm{polyval}}, K_{\mathrm{BC}})$
  - proposed for standardization at IETF CFRG

History of (AES)-GCM-(SIV) AEAD schemes

- GCM [MV04]
  - CTR encryption + Wegman-Carter MAC
  - Encrypt-then-MAC composition
  - widely deployed, not nonce-misuse resistant [Jou06, BZD+16]
- GCM-SIV [GL15]
  - same components as GCM
  - Synthetic IV (SIV) composition [RS06]
  - nonce-misuse resistant
- AES-GCM-SIV [GLL16, GLL17]
  - $\neq$ GCM-SIV instantiated with AES
  - similar to GCM-SIV but three modifications:
    - universal hash function (POLYVAL instead of GHASH)
    - full-block counter
    - nonce-based key derivation $(K, N) \mapsto (K_{\text{polyval}}, K_{\text{BC}})$
  - proposed for standardization at IETF CFRG

History of (AES)-GCM-(SIV) AEAD schemes

- GCM [MV04]
  - CTR encryption + Wegman-Carter MAC
  - Encrypt-then-MAC composition
  - widely deployed, not nonce-misuse resistant [Jou06, BZD+16]
- GCM-SIV [GL15]
  - same components as GCM
  - Synthetic IV (SIV) composition [RS06]
  - nonce-misuse resistant
- AES-GCM-SIV [GLL16, GLL17]
  - $\neq$ GCM-SIV instantiated with AES
  - similar to GCM-SIV but three modifications:
    - universal hash function (POLYVAL instead of GHASH)
    - full-block counter
    - nonce-based key derivation $(K, N) \mapsto (K_{\text{polyval}}, K_{\text{BC}})$
  - proposed for standardization at IETF CFRG

History of (AES)-GCM-(SIV) AEAD schemes

- GCM [MV04]
  - CTR encryption + Wegman-Carter MAC
  - Encrypt-then-MAC composition
  - widely deployed, not nonce-misuse resistant [Jou06, BZD+16]
- GCM-SIV [GL15]
  - same components as GCM
  - Synthetic IV (SIV) composition [RS06]
  - nonce-misuse resistant
- AES-GCM-SIV [GLL16, GLL17]
  - $\neq$ GCM-SIV instantiated with AES
  - similar to GCM-SIV but three modifications:
    - universal hash function (POLYVAL instead of GHASH)
    - full-block counter
    - nonce-based key derivation $(K, N) \mapsto (K_{\text{polyval}}, K_{\text{BC}})$
  - proposed for standardization at IETF CFRG

History of (AES)-GCM-(SIV) AEAD schemes

- GCM [MV04]
  - CTR encryption + Wegman-Carter MAC
  - Encrypt-then-MAC composition
  - widely deployed, not nonce-misuse resistant [Jou06, BZD+16]
- GCM-SIV [GL15]
  - same components as GCM
  - Synthetic IV (SIV) composition [RS06]
  - nonce-misuse resistant
- AES-GCM-SIV [GLL16, GLL17]
  - $\neq$ GCM-SIV instantiated with AES
  - similar to GCM-SIV but three modifications:
    - universal hash function (POLYVAL instead of GHASH)
    - full-block counter
    - nonce-based key derivation $(K, N) \mapsto (K_{\text{polyval}}, K_{\text{BC}})$
  - proposed for standardization at IETF CFRG

Nonce-Based Authenticated Encryption (nAE)

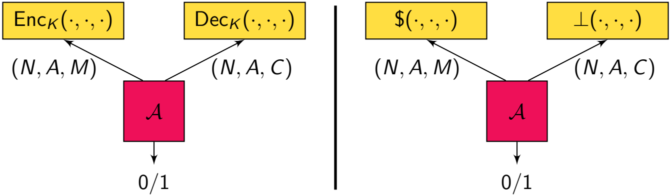
Syntax

A nAE scheme Π is a pair of algorithms $(\Pi.\mathrm{Enc}, \Pi.\mathrm{Dec})$ where

- algorithm $\Pi.\mathrm{Enc}$ takes
  - (a key K)
  - a nonce N
  - associated data A
  - a message M

  and returns a ciphertext C.
- algorithm $\Pi.\mathrm{Dec}$ takes K and (N, A, C) and returns M or $\perp$.

Nonce-Based Authenticated Encryption (nAE)



Security (all-in-one definition)

- The scheme Π is secure if adversary $\mathcal{A}$ cannot distinguish $(\mathrm{Enc}_K, \mathrm{Dec}_K)$ and $(\$, \perp)$.
- $\mathcal{A}$ cannot ask a decryption query (N, A, C) if it received C from an encryption query (N, A, M)
- $\mathcal{A}$ is said nonce-respecting if it never repeats a nonce in encryption queries.

Misuse-Resistant AE (MRAE)

Nonce-misuse resistance (informal) [RS06]

A nAE scheme is said nonce-misuse resistant if repeating a nonce in encryption queries:

- does not harm authenticity
- hurts confidentiality only insofar as repetitions of triplets (N, A, M) are detectable

- $\simeq$ deterministic authenticated encryption
- MRAE schemes *cannot* be online (each ciphertext bit must depend on each input bit)

Misuse-Resistant AE (MRAE)

Nonce-misuse resistance (informal) [RS06]

A nAE scheme is said nonce-misuse resistant if repeating a nonce in encryption queries:

- does not harm authenticity
- hurts confidentiality only insofar as repetitions of triplets (N, A, M) are detectable

- $\simeq$ deterministic authenticated encryption
- MRAE schemes *cannot* be online (each ciphertext bit must depend on each input bit)

Misuse-Resistant AE (MRAE)

Nonce-misuse resistance (informal) [RS06]

A nAE scheme is said nonce-misuse resistant if repeating a nonce in encryption queries:

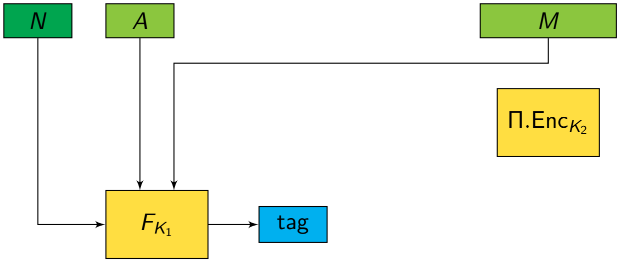
- does not harm authenticity
- hurts confidentiality only insofar as repetitions of triplets (N, A, M) are detectable

- $\simeq$ deterministic authenticated encryption
- MRAE schemes *cannot* be online (each ciphertext bit must depend on each input bit)

SIV composition method

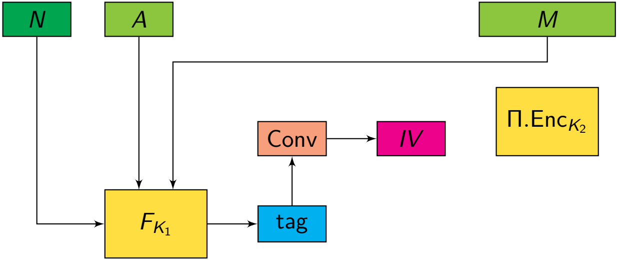
- SIV (*Synthetic IV*) [RS06] combines a PRF $F_{K_1}(N, A, M)$ and an IV-based encryption scheme $\Pi.\mathrm{Enc}_{K_2}(IV, M)$
- provides nonce-misuse resistance: any change to N, A, or M randomly modifies the tag and C

SIV composition method



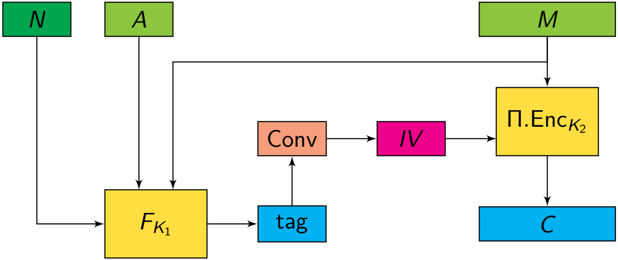
- SIV (*Synthetic IV*) [RS06] combines a PRF $F_{K_1}(N, A, M)$ and an IV-based encryption scheme $\Pi.\mathrm{Enc}_{K_2}(IV, M)$
- provides nonce-misuse resistance: any change to N, A, or M randomly modifies the tag and C

SIV composition method



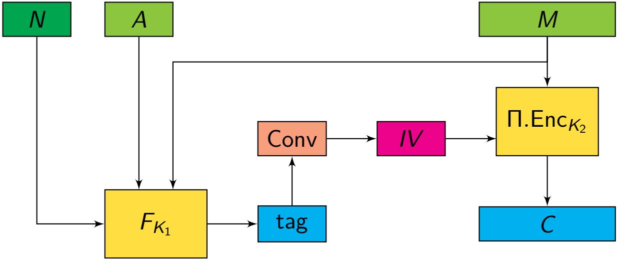
- SIV (*Synthetic IV*) [RS06] combines a PRF $F_{K_1}(N, A, M)$ and an IV-based encryption scheme $\Pi.\mathsf{Enc}_{K_2}(IV, M)$
- provides nonce-misuse resistance: any change to N, A, or M randomly modifies the tag and C

SIV composition method



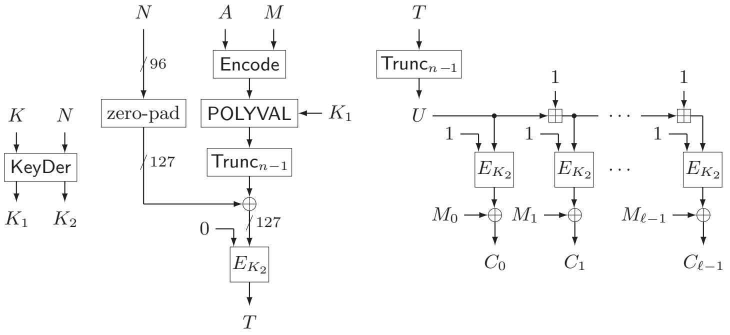
- SIV (*Synthetic IV*) [RS06] combines a PRF $F_{K_1}(N, A, M)$ and an IV-based encryption scheme $\Pi.\mathrm{Enc}_{K_2}(IV, M)$
- provides nonce-misuse resistance: any change to N, A, or M randomly modifies the tag and C

SIV composition method



- SIV (*Synthetic IV*) [RS06] combines a PRF $F_{K_1}(N, A, M)$ and an IV-based encryption scheme $\Pi.\mathrm{Enc}_{K_2}(IV, M)$
- provides nonce-misuse resistance: any change to N, A, or M randomly modifies the tag and C

Details of AES-GCM-SIV



- AES-GCM-SIV = KeyDer + GCM-SIV$^+$
- same BC key K_2 used in MAC and encryption
  $\Rightarrow$ 0/1 domain separation

Outline

Background on AES-GCM-SIV

Fixing the Security Bound

Improving Key Derivation

Final Remarks

Designers' claims ([GLL17], Theorem 6)

$$\mathbf{Adv}^{\text{mrae}}_{\text{AES-GCM-SIV}}(\mathcal{A}) \leq \underbrace{\mathbf{Adv}^{\text{prp}}_{\text{AES}}(\mathcal{A}'') + \min\left\{\frac{36Q^2}{2^{129}}, \frac{6Q}{2^{96}}\right\}}_{\text{KeyDer PRF-security}}$$

$$+ Q \underbrace{\left(2\mathbf{Adv}^{\text{prf}}_{\text{AES}}(\mathcal{A}') + \frac{R^2 \ell_M}{2^{126}} + \frac{R^2 + 2q_D}{2^{127}}\right)}_{\text{GCM-SIV}^+ \text{ MRAE-security}},$$

- ℓ_M = maximal message length of encryption queries
- Q = maximal number of distinct nonces in encryption queries
- R = maximal number of nonce repetitions in encryption queries
- q_D = number of decryption queries per nonce, σ_D = total length
- $\mathcal{A}'$ makes at most $Q(2R + 2q_D + \sigma_D)$ queries
- $\mathcal{A}''$ makes at most $6Q$ queries

Designers' claims ([GLL17], Theorem 6)

$$\mathbf{Adv}^{\text{mrae}}_{\text{AES-GCM-SIV}}(\mathcal{A}) \le \underbrace{\mathbf{Adv}^{\text{prp}}_{\text{AES}}(\mathcal{A}'') + \min\left\{\frac{36Q^2}{2^{129}}, \frac{6Q}{2^{96}}\right\}}_{\text{KeyDer PRF-security}}$$

$$+ Q \underbrace{\left(2\mathbf{Adv}^{\text{prf}}_{\text{AES}}(\mathcal{A}') + \frac{R^2 \ell_M}{2^{126}} + \frac{R^2 + 2q_D}{2^{127}}\right)}_{\text{GCM-SIV}^+ \text{ MRAE-security}},$$

- $\ell_M =$ maximal message length of encryption queries
- $Q =$ maximal number of distinct nonces in encryption queries
- $R =$ maximal number of nonce repetitions in encryption queries
- $q_D =$ number of decryption queries per nonce, $\sigma_D =$ total length
- $\mathcal{A}'$ makes at most $Q(2R + 2q_D + \sigma_D)$ queries
- $\mathcal{A}''$ makes at most $6Q$ queries

Designers' claims ([GLL17], Theorem 6)

$$\mathbf{Adv}^{\mathrm{mrae}}_{\text{AES-GCM-SIV}}(\mathcal{A}) \leq \underbrace{\mathbf{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(\mathcal{A}'') + \min\left\{\frac{36Q^2}{2^{129}}, \frac{6Q}{2^{96}}\right\}}_{\text{KeyDer PRF-security}}$$

$$+ Q\underbrace{\left(2\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{AES}}(\mathcal{A}') + \frac{R^2\ell_M}{2^{126}} + \frac{R^2 + 2q_D}{2^{127}}\right)}_{\text{GCM-SIV}^+ \text{ MRAE-security}},$$

- ℓ_M = maximal message length of encryption queries
- Q = maximal number of distinct nonces in encryption queries
- R = maximal number of nonce repetitions in encryption queries
- q_D = number of decryption queries per nonce, σ_D = total length
- $\mathcal{A}'$ makes at most $Q(2R + 2q_D + \sigma_D)$ queries
- $\mathcal{A}''$ makes at most $6Q$ queries

Problems in designers' bound

$$\mathbf{Adv}^{\mathrm{mrae}}_{\text{AES-GCM-SIV}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(\mathcal{A}'') + \min\left\{\frac{36Q^2}{2^{129}}, \frac{6Q}{2^{96}}\right\}$$
$$+ Q\left(2\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{AES}}(\mathcal{A}') + \frac{R^2\ell_M}{2^{126}} + \frac{R^2 + 2q_D}{2^{127}}\right)$$

- mixes PRP- and PRF-security of the underlying BC
- AD's length not taken into account
- number of queries $Q(2R + 2q_D + \sigma_D)$ of $\mathcal{A}'$ is flawed
- $Q = 0$ (no encryption queries), $q_D > 0 \Rightarrow \mathbf{Adv}^{\mathrm{mrae}}_{\text{AES-GCM-SIV}}(\mathcal{A}) = 0$
  $\rightarrow$ impossible for MRAE security definition
  (non-zero probability to forge a tag randomly)

Problems in designers' bound

$$\mathbf{Adv}^{\mathrm{mrae}}_{\text{AES-GCM-SIV}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(\mathcal{A}'') + \min\left\{\frac{36Q^2}{2^{129}}, \frac{6Q}{2^{96}}\right\} + Q\left(2\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{AES}}(\mathcal{A}') + \frac{R^2\ell_M}{2^{126}} + \frac{R^2 + 2q_D}{2^{127}}\right)$$

- mixes PRP- and PRF-security of the underlying BC
- AD's length not taken into account
- number of queries $Q(2R + 2q_D + \sigma_D)$ of $\mathcal{A}'$ is flawed
- $Q = 0$ (no encryption queries), $q_D > 0 \Rightarrow \mathbf{Adv}^{\mathrm{mrae}}_{\text{AES-GCM-SIV}}(\mathcal{A}) = 0$
  $\rightarrow$ impossible for MRAE security definition
  (non-zero probability to forge a tag randomly)

Problems in designers' bound

$$\mathbf{Adv}^{\mathrm{mrae}}_{\mathrm{AES\text{-}GCM\text{-}SIV}}(\mathcal{A}) \le \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(\mathcal{A}'') + \min\left\{\frac{36Q^2}{2^{129}}, \frac{6Q}{2^{96}}\right\} + Q\left(2\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{AES}}(\mathcal{A}') + \frac{R^2\ell_M}{2^{126}} + \frac{R^2+2q_D}{2^{127}}\right)$$

- mixes PRP- and PRF-security of the underlying BC
- AD's length not taken into account
- number of queries $Q(2R+2q_D+\sigma_D)$ of $\mathcal{A}'$ is flawed
- $Q=0$ (no encryption queries), $q_D>0 \Rightarrow \mathbf{Adv}^{\mathrm{mrae}}_{\mathrm{AES\text{-}GCM\text{-}SIV}}(\mathcal{A})=0$
  $\to$ impossible for MRAE security definition
  (non-zero probability to forge a tag randomly)

Problems in designers' bound

$$\mathbf{Adv}^{\mathrm{mrae}}_{\text{AES-GCM-SIV}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(\mathcal{A}'') + \min\left\{\frac{36Q^2}{2^{129}}, \frac{6Q}{2^{96}}\right\} + Q\left(2\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{AES}}(\mathcal{A}') + \frac{R^2\ell_M}{2^{126}} + \frac{R^2 + 2q_D}{2^{127}}\right)$$

- mixes PRP- and PRF-security of the underlying BC
- AD's length not taken into account
- number of queries $Q(2R + 2q_D + \sigma_D)$ of $\mathcal{A}'$ is flawed
- $Q = 0$ (no encryption queries), $q_D > 0 \Rightarrow \mathbf{Adv}^{\mathrm{mrae}}_{\text{AES-GCM-SIV}}(\mathcal{A}) = 0$
  $\rightarrow$ impossible for MRAE security definition
  (non-zero probability to forge a tag randomly)

Corrected security bound (privacy only)

If $q_D = 0$ (no decryption queries), then

$$\mathbf{Adv}^{\mathrm{mrae}}_{\text{AES-GCM-SIV}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(\mathcal{A}'') + \min\left\{\frac{36Q^2}{2^{129}}, \frac{6Q}{2^{96}}\right\} + Q\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{AES}}(\mathcal{A}') + \frac{QR^2\ell_M}{2^{126}} + \frac{QR^2\ell_A}{2^{128}}$$

Main changes:

- takes into account ℓ_A = maximal length of AD
- $\mathcal{A}'$ makes $R\ell_M$ queries versus $2QR$ in [GLL17]

Corrected security bound (privacy only)

If $q_D = 0$ (no decryption queries), then

$$\mathbf{Adv}^{\mathrm{mrae}}_{\text{AES-GCM-SIV}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(\mathcal{A}'') + \min\left\{\frac{36Q^2}{2^{129}}, \frac{6Q}{2^{96}}\right\} + Q\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{AES}}(\mathcal{A}') + \frac{QR^2\ell_M}{2^{126}} + \frac{QR^2\ell_A}{2^{128}}$$

Main changes:

- takes into account ℓ_A = maximal length of AD
- $\mathcal{A}'$ makes $R\ell_M$ queries versus $2QR$ in [GLL17]

Dominating term

$$\mathbf{Adv}^{\mathsf{mrae}}_{\mathsf{AES\text{-}GCM\text{-}SIV}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathsf{prp}}_{\mathsf{AES}}(\mathcal{A}'') + \min\left\{\frac{36Q^2}{2^{129}}, \frac{6Q}{2^{96}}\right\} + Q\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{AES}}(\mathcal{A}') + \frac{QR^2\ell_M}{2^{126}} + \frac{QR^2\ell_A}{2^{128}},$$

- [GLL17] claimed the security bound is dominated by $\frac{QR^2\ell_M}{2^{126}}$ (accounts for counter collision)
- but in fact the PRF term is $\sim \ell_M$ larger ($\mathcal{A}'$ makes $R\ell_M$ queries)

$$Q\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{AES}}(\mathcal{A}') \simeq Q\mathbf{Adv}^{\mathsf{prp}}_{\mathsf{AES}}(\mathcal{A}') + \frac{QR^2\ell_M^2}{2^{129}}$$

- the bound is tight and matched by a simple distinguishing attack

Dominating term

$$\mathbf{Adv}^{\mathsf{mrae}}_{\mathsf{AES\text{-}GCM\text{-}SIV}}(\mathcal{A}) \le \mathbf{Adv}^{\mathsf{prp}}_{\mathsf{AES}}(\mathcal{A}'') + \min\left\{\frac{36Q^2}{2^{129}}, \frac{6Q}{2^{96}}\right\} + Q\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{AES}}(\mathcal{A}') + \frac{QR^2\ell_M}{2^{126}} + \frac{QR^2\ell_A}{2^{128}},$$

- [GLL17] claimed the security bound is dominated by $\frac{QR^2\ell_M}{2^{126}}$ (accounts for counter collision)
- but in fact the PRF term is $\sim \ell_M$ larger ($\mathcal{A}'$ makes $R\ell_M$ queries)

$$Q\mathbf{Adv}^{\mathsf{prf}}_{\mathsf{AES}}(\mathcal{A}') \simeq Q\mathbf{Adv}^{\mathsf{prp}}_{\mathsf{AES}}(\mathcal{A}') + \frac{QR^2\ell_M^2}{2^{129}}$$

- the bound is tight and matched by a simple distinguishing attack

Dominating term

$$\mathbf{Adv}^{\mathrm{mrae}}_{\mathrm{AES\text{-}GCM\text{-}SIV}}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(\mathcal{A}'') + \min\left\{\frac{36Q^2}{2^{129}}, \frac{6Q}{2^{96}}\right\} + Q\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{AES}}(\mathcal{A}') + \frac{QR^2\ell_M}{2^{126}} + \frac{QR^2\ell_A}{2^{128}},$$

- [GLL17] claimed the security bound is dominated by $\frac{QR^2\ell_M}{2^{126}}$ (accounts for counter collision)
- but in fact the PRF term is $\sim \ell_M$ larger ($\mathcal{A}'$ makes $R\ell_M$ queries)

$$Q\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{AES}}(\mathcal{A}') \simeq Q\mathbf{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(\mathcal{A}') + \frac{QR^2\ell_M^2}{2^{129}}$$

- the bound is tight and matched by a simple distinguishing attack

Concrete security claims

Scheme	N_E	Q	R	ℓ_M	our bound	[GLL17] claim
AES-GCM-SIV (nonce based)	2^{32}	2^{32}	1	2^{32}	2^{-33}	2^{-61}
	2^{64}	2^{64}	1	2^{32}	2^{-1}	2^{-29}
	2^{31}	1	2^{31}	2^{32}	2^{-3}	2^{-32}
	2^{31}	1	2^{31}	2^{16}	2^{-35}	2^{-48}
	2^{39}	1	2^{39}	2^{16}	2^{-19}	2^{-32}
	2^{42}	1	2^{42}	2^{10}	2^{-25}	2^{-32}
	2^{50}	2^{42}	2^{8}	2^{32}	2^{-7}	2^{-36}
	2^{50}	2^{42}	2^{8}	2^{16}	2^{-39}	2^{-51}
	2^{50}	2^{46}	2^{4}	2^{32}	2^{-11}	2^{-40}
AES-GCM-SIV (random IV)	2^{48}	—	—	2^{32}	2^{-14}	2^{-44}
	2^{63}	—	—	2^{16}	2^{-31}	2^{-32}

$N_E = QR =$ total number of encryption queries

Taking decryption queries into account

- the adversary can choose nonces freely in decryption queries (it could reuse the same nonce q_D times)
- naive bound ($Q + q_D$ distinct nonces)

$$\mathbf{Adv}^{\mathrm{mrae}}_{\text{AES-GCM-SIV}}(\mathcal{A}) \leq (Q + q_D) \underbrace{\left((\cdots) + \frac{(R + q_D)^2(\ell_M + \ell_A)}{2^n} \right)}_{\text{GCM-SIV}^+ \text{ security}}$$

- loose bound (cubic in q_D)
- with a more careful multi-user analysis we recover a bound quadratic in q_D

Taking decryption queries into account

- the adversary can choose nonces freely in decryption queries (it could reuse the same nonce q_D times)
- naive bound ($Q + q_D$ distinct nonces)

$$\mathbf{Adv}^{\mathrm{mrae}}_{\text{AES-GCM-SIV}}(\mathcal{A}) \leq (Q + q_D) \underbrace{\left((\cdots) + \frac{(R + q_D)^2(\ell_M + \ell_A)}{2^n} \right)}_{\text{GCM-SIV}^+ \text{ security}}$$

- loose bound (cubic in q_D)
- with a more careful multi-user analysis we recover a bound quadratic in q_D

Taking decryption queries into account

- the adversary can choose nonces freely in decryption queries (it could reuse the same nonce q_D times)
- naive bound ($Q + q_D$ distinct nonces)

$$\mathbf{Adv}^{\mathrm{mrae}}_{\text{AES-GCM-SIV}}(\mathcal{A}) \leq (Q + q_D) \underbrace{\left((\cdots) + \frac{(R + q_D)^2(\ell_M + \ell_A)}{2^n} \right)}_{\text{GCM-SIV}^+ \text{ security}}$$

- loose bound (cubic in q_D)
- with a more careful multi-user analysis we recover a bound quadratic in q_D

Taking decryption queries into account

- the adversary can choose nonces freely in decryption queries (it could reuse the same nonce q_D times)
- naive bound ($Q + q_D$ distinct nonces)

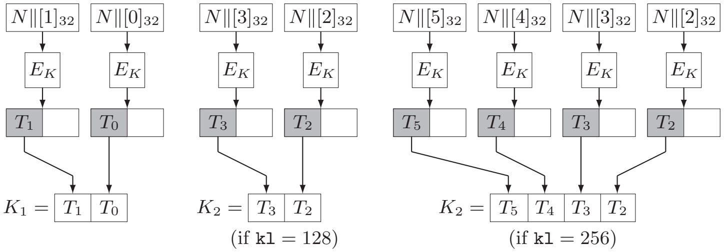
$$\mathbf{Adv}^{\text{mrae}}_{\text{AES-GCM-SIV}}(\mathcal{A}) \leq (Q + q_D) \underbrace{\left((\cdots) + \frac{(R + q_D)^2(\ell_M + \ell_A)}{2^n} \right)}_{\text{GCM-SIV}^+ \text{ security}}$$

- loose bound (cubic in q_D)
- with a more careful multi-user analysis we recover a bound quadratic in q_D

Outline

Key Derivation Function

- $(K, N) \xrightarrow{\text{KeyDer}} (K_1, K_2)$ constructed from E
- standard PRP-to-PRF conversion problem
- based on truncation [HWKS98, GGM18]



A Better Key Derivation Function

- security of truncation when dropping m bits: for q large enough,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{Trunc}_{n-m}[P]}(q) \leq \frac{q}{2^{(m+n)/2}}$$

- when dropping $m = n/2$ bits:
  - two BC calls to obtain an n-bit key
  - security up to $2^{3n/4}$ queries
- better construction: XOR of permutations

$$K_1 = E_K(N \| [0]_{32}) \oplus E_K(N \| [1]_{32})$$

  - two BC calls to obtain an n-bit key
  - security up to 2^n queries [Pat08, DHT17]

A Better Key Derivation Function

- security of truncation when dropping m bits: for q large enough,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathsf{Trunc}_{n-m}[P]}(q) \leq \frac{q}{2^{(m+n)/2}}$$

- when dropping $m = n/2$ bits:
  - two BC calls to obtain an n-bit key
  - security up to $2^{3n/4}$ queries
- better construction: XOR of permutations

$$K_1 = E_K(N \| [0]_{32}) \oplus E_K(N \| [1]_{32})$$

  - two BC calls to obtain an n-bit key
  - security up to 2^n queries [Pat08, DHT17]

A Better Key Derivation Function

- security of truncation when dropping m bits: for q large enough,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{Trunc}_{n-m}[P]}(q) \leq \frac{q}{2^{(m+n)/2}}$$

- when dropping $m = n/2$ bits:
  - two BC calls to obtain an n-bit key
  - security up to $2^{3n/4}$ queries
- better construction: XOR of permutations

$$K_1 = E_K(N \| [0]_{32}) \oplus E_K(N \| [1]_{32})$$

  - two BC calls to obtain an n-bit key
  - security up to 2^n queries [Pat08, DHT17]

A Better Key Derivation Function

- security of truncation when dropping m bits: for q large enough,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{Trunc}_{n-m}[P]}(q) \leq \frac{q}{2^{(m+n)/2}}$$

- when dropping $m = n/2$ bits:
  - two BC calls to obtain an n-bit key
  - security up to $2^{3n/4}$ queries
- better construction: XOR of permutations

$$K_1 = E_K(N \| [0]_{32}) \oplus E_K(N \| [1]_{32})$$

  - two BC calls to obtain an n-bit key
  - security up to 2^n queries [Pat08, DHT17]

A Better Key Derivation Function

- security of truncation when dropping m bits: for q large enough,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{Trunc}_{n-m}[P]}(q) \leq \frac{q}{2^{(m+n)/2}}$$

- when dropping $m = n/2$ bits:
  - two BC calls to obtain an n-bit key
  - security up to $2^{3n/4}$ queries
- better construction: XOR of permutations

$$K_1 = E_K(N \| [0]_{32}) \oplus E_K(N \| [1]_{32})$$

  - two BC calls to obtain an n-bit key
  - security up to 2^n queries [Pat08, DHT17]

A Better Key Derivation Function

- security of truncation when dropping m bits: for q large enough,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{Trunc}_{n-m}[P]}(q) \leq \frac{q}{2^{(m+n)/2}}$$

- when dropping $m = n/2$ bits:
  - two BC calls to obtain an n-bit key
  - security up to $2^{3n/4}$ queries
- better construction: XOR of permutations

$$K_1 = E_K(N \| [0]_{32}) \oplus E_K(N \| [1]_{32})$$

  - two BC calls to obtain an n-bit key
  - security up to 2^n queries [Pat08, DHT17]

A Better Key Derivation Function

- security of truncation when dropping m bits: for q large enough,

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{Trunc}_{n-m}[P]}(q) \leq \frac{q}{2^{(m+n)/2}}$$

- when dropping $m = n/2$ bits:
  - two BC calls to obtain an n-bit key
  - security up to $2^{3n/4}$ queries
- better construction: XOR of permutations

$$K_1 = E_K(N \| [0]_{32}) \oplus E_K(N \| [1]_{32})$$

  - two BC calls to obtain an n-bit key
  - security up to 2^n queries [Pat08, DHT17]

Outline

Concurrent/Subsequent work

- Gueron and Lindell, *Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation*, CCS 2017
  - security definition puts an upper bound on the number of decryption queries per nonce
    → complicated to enforce in practice (stateful decryption)
  - Theorem 6.2 still has problems and can be falsified
- Bose, Hoang, and Tessaro, *Revisiting AES-GCM-SIV: Multi-user Security, Faster Key Derivation, and Better Bounds*, EUROCRYPT 2018
  - shows that the security of AES-GCM-SIV does not degrade in the multi-user setting

Concurrent/Subsequent work

- Gueron and Lindell, *Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation*, CCS 2017
  - security definition puts an upper bound on the number of decryption queries per nonce
    $\rightarrow$ complicated to enforce in practice (stateful decryption)
  - Theorem 6.2 still has problems and can be falsified
- Bose, Hoang, and Tessaro, *Revisiting AES-GCM-SIV: Multi-user Security, Faster Key Derivation, and Better Bounds*, EUROCRYPT 2018
  - shows that the security of AES-GCM-SIV does not degrade in the multi-user setting

Concurrent/Subsequent work

- Gueron and Lindell, *Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation*, CCS 2017
  - security definition puts an upper bound on the number of decryption queries per nonce
    $\rightarrow$ complicated to enforce in practice (stateful decryption)
  - Theorem 6.2 still has problems and can be falsified
- Bose, Hoang, and Tessaro, *Revisiting AES-GCM-SIV: Multi-user Security, Faster Key Derivation, and Better Bounds*, EUROCRYPT 2018
  - shows that the security of AES-GCM-SIV does not degrade in the multi-user setting

Concurrent/Subsequent work

- Gueron and Lindell, *Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation*, CCS 2017
  - security definition puts an upper bound on the number of decryption queries per nonce
    $\rightarrow$ complicated to enforce in practice (stateful decryption)
  - Theorem 6.2 still has problems and can be falsified
- Bose, Hoang, and Tessaro, *Revisiting AES-GCM-SIV: Multi-user Security, Faster Key Derivation, and Better Bounds*, EUROCRYPT 2018
  - shows that the security of AES-GCM-SIV does not degrade in the multi-user setting

Concurrent/Subsequent work

- Gueron and Lindell, *Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation*, CCS 2017
  - security definition puts an upper bound on the number of decryption queries per nonce
    → complicated to enforce in practice (stateful decryption)
  - Theorem 6.2 still has problems and can be falsified
- Bose, Hoang, and Tessaro, *Revisiting AES-GCM-SIV: Multi-user Security, Faster Key Derivation, and Better Bounds*, EUROCRYPT 2018
  - shows that the security of AES-GCM-SIV does not degrade in the multi-user setting

The end...

Thanks for your attention!

Comments or questions?

References I

- Hanno Böck, Aaron Zauner, Sean Devlin, Juraj Somorovsky, and Philipp Jovanovic. Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS. In *USENIX Workshop on Offensive Technologies, WOOT 2016*. USENIX Association, 2016.

- Wei Dai, Viet Tung Hoang, and Stefano Tessaro. Information-theoretic Indistinguishability via the Chi-squared Method. In *Advances in Cryptology - CRYPTO 2017 (Proceedings, Part III)*, volume 10403 of *LNCS*, pages 497–523. Springer, 2017.

- Shoni Gilboa, Shay Gueron, and Ben Morris. How Many Queries are Needed to Distinguish a Truncated Random Permutation from a Random Function? *J. Cryptology*, 31(1):162–171, 2018.

- Shay Gueron and Yehuda Lindell. GCM-SIV: Full Nonce Misuse-Resistant Authenticated Encryption at Under One Cycle per Byte. In *ACM Conference on Computer and Communications Security - CCS 2015*, pages 109–119. ACM, 2015.

References II

- Shay Gueron, Adam Langley, and Yehuda Lindell. AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption. CFGR Draft, 2016. Available at https://tools.ietf.org/html/draft-irtf-cfrg-gcmsiv-05.
- Shay Gueron, Adam Langley, and Yehuda Lindell. AES-GCM-SIV: Specification and Analysis. IACR Cryptology ePrint Archive, Report 2017/168, 2017. Available at http://eprint.iacr.org/2017/168.
- Chris Hall, David Wagner, John Kelsey, and Bruce Schneier. Building PRFs from PRPs. In *Advances in Cryptology - CRYPTO '98*, volume 1462 of *LNCS*, pages 370–389. Springer, 1998.
- Antoine Joux. Authentication Failures in NIST Version of GCM. Comments submitted to NIST Modes of Operation Process, 2006. Available at http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/800-38_Series-Drafts/GCM/Joux_comments.pdf.

References III

- David A. McGrew and John Viega. The Security and Performance of the Galois/Counter Mode (GCM) of Operation. In *Progress in Cryptology - INDOCRYPT 2004*, volume 3348 of *LNCS*, pages 343–355. Springer, 2004.
- Jacques Patarin. A Proof of Security in $O(2^n)$ for the Xor of Two Random Permutations. In *Information Theoretic Security - ICITS 2008*, volume 5155 of *LNCS*, pages 232–248. Springer, 2008.
- Phillip Rogaway and Thomas Shrimpton. A Provable-Security Treatment of the Key-Wrap Problem. In *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 373–390. Springer, 2006.