

On the Counter Collision Probability of GCM*

Keisuke Ohashi, Nagoya University

Yuichi Niwa, Nagoya University

Tetsu Iwata, Nagoya University

Early Symmetric Crypto (ESC) seminar

January 14--18, Mondorf-les-Bains, Luxembourg

*Work in Progress

GCM

- Galois/Counter Mode
- authenticated encryption mode of 128-bit blockciphers
- designed by McGrew and Viega in 2004 [MV04]
- selected as the NIST recommended authenticated encryption mode in 2007
- widely used in practice
 - ISO/IEC 19772, IEEE P1619.1, NSA Suite B, IETF IPsec, SSH, SSL,...

[MV04] David A. McGrew and John Viega: The Security and Performance of the Galois/Counter Mode (GCM) of Operation. INDOCRYPT 2004. Full version in Cryptology ePrint Archive: Report 2004/193

Overview

- $\text{Adv}_{\text{GCM}[\text{Perm}(n),\tau]}^{\text{priv}}(\mathcal{A}) \leq \frac{0.5(\sigma + q + 1)^2}{2^n} + \frac{2^{22}q(\sigma + q)(\ell_N + 1)}{2^n}$
- $\text{Adv}_{\text{GCM}[\text{Perm}(n),\tau]}^{\text{auth}}(\mathcal{A}) \leq \frac{0.5(\sigma + q + q' + 1)^2}{2^n} + \frac{2^{22}(q + q' + 1)(\sigma + q)(\ell_N + 1)}{2^n} + \frac{q'(\ell_A + 1)}{2^\tau}$
- “big constant”
- Joux at Dagstuhl Seminar (January 2012): Do you have an attack that matches the bound (exploiting the fact that there is a big constant)? --- I don't know
 - tightness of the bounds, possibility of improvement

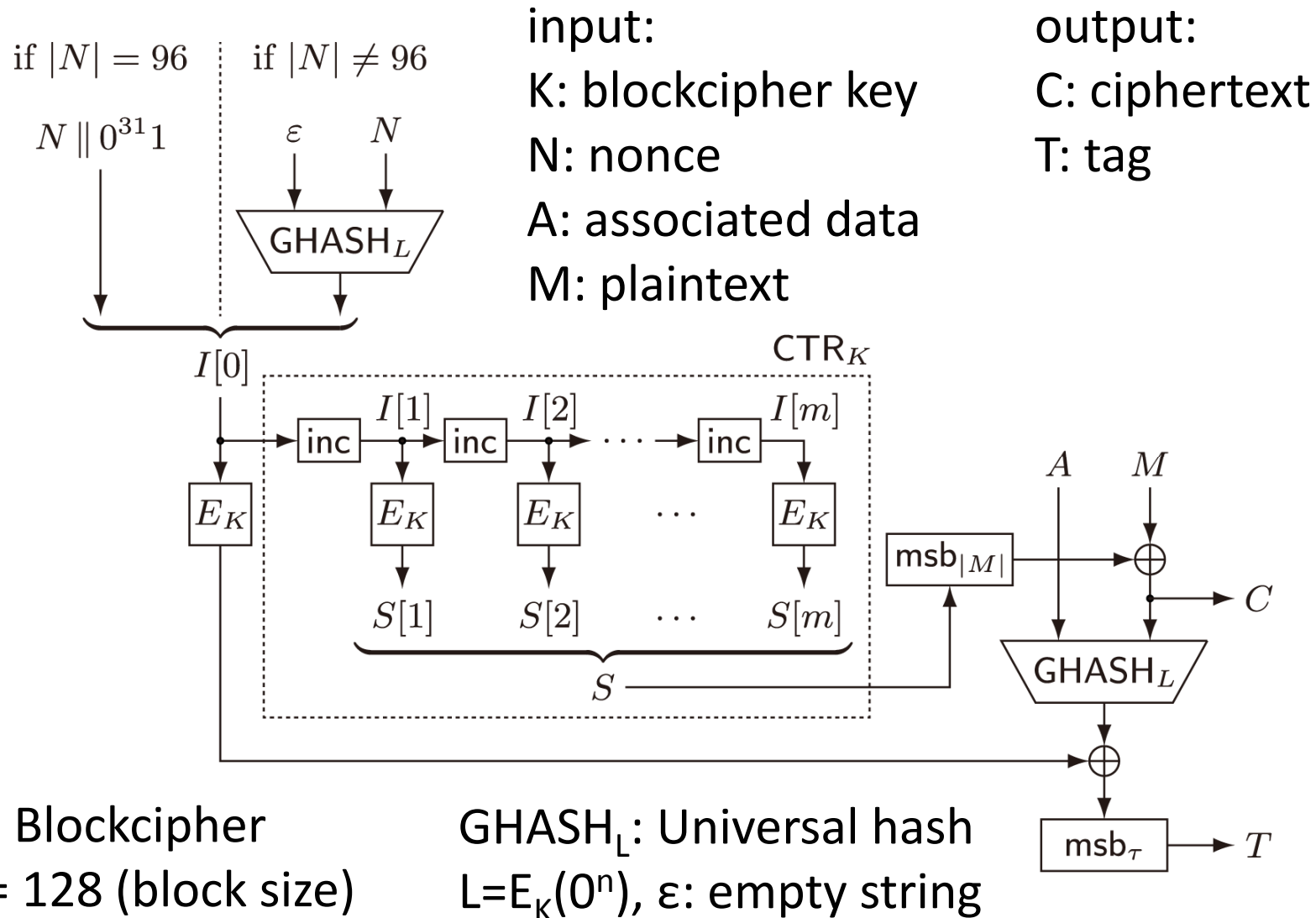
[IOM12] Tetsu Iwata, Keisuke Ohashi, and Kazuhiko Minematsu : Breaking and Repairing GCM Security Proofs. CRYPTO 2012. Full version in Cryptology ePrint Archive: Report 2012/438

Overview

- $\text{Adv}_{\text{GCM}[\text{Perm}(n),\tau]}^{\text{priv}}(\mathcal{A}) \leq \frac{0.5(\sigma + q + 1)^2}{2^n} + \frac{2^{22}q(\sigma + q)(\ell_N + 1)}{2^n}$
- $\text{Adv}_{\text{GCM}[\text{Perm}(n),\tau]}^{\text{auth}}(\mathcal{A}) \leq \frac{0.5(\sigma + q + q' + 1)^2}{2^n} + \frac{2^{22}(q + q' + 1)(\sigma + q)(\ell_N + 1)}{2^n} + \frac{q'(\ell_A + 1)}{2^\tau}$
- ESC (January 2013): I still don't know, but we have made some progress

[IOM12] Tetsu Iwata, Keisuke Ohashi, and Kazuhiko Minematsu : Breaking and Repairing GCM Security Proofs. CRYPTO 2012. Full version in Cryptology ePrint Archive: Report 2012/438

Encryption Algorithm of GCM



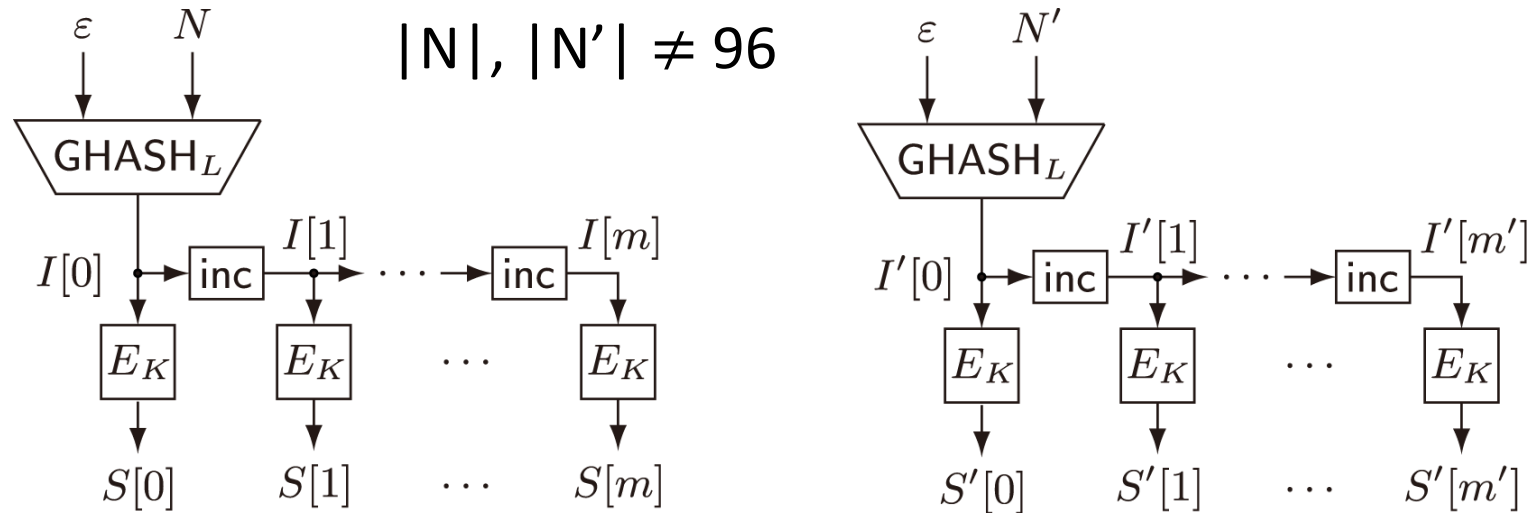
Increment Function in GCM

- $\text{inc}(X || Y) = X || (Y+1 \bmod 2^{32})$
 - $|X| = 96, |Y| = 32$
 - Example
 - $\text{inc}(0x0\dots01) = 0x0\dots02$
 - $\text{inc}(0x0\dots0\text{ffffffff}) = 0x0\dots0$
- $\text{inc}^r (Z)$: apply $\text{inc}(\cdot)$ on Z for r times
 - $|Z| = 128$

GHASH_L(ε, N)

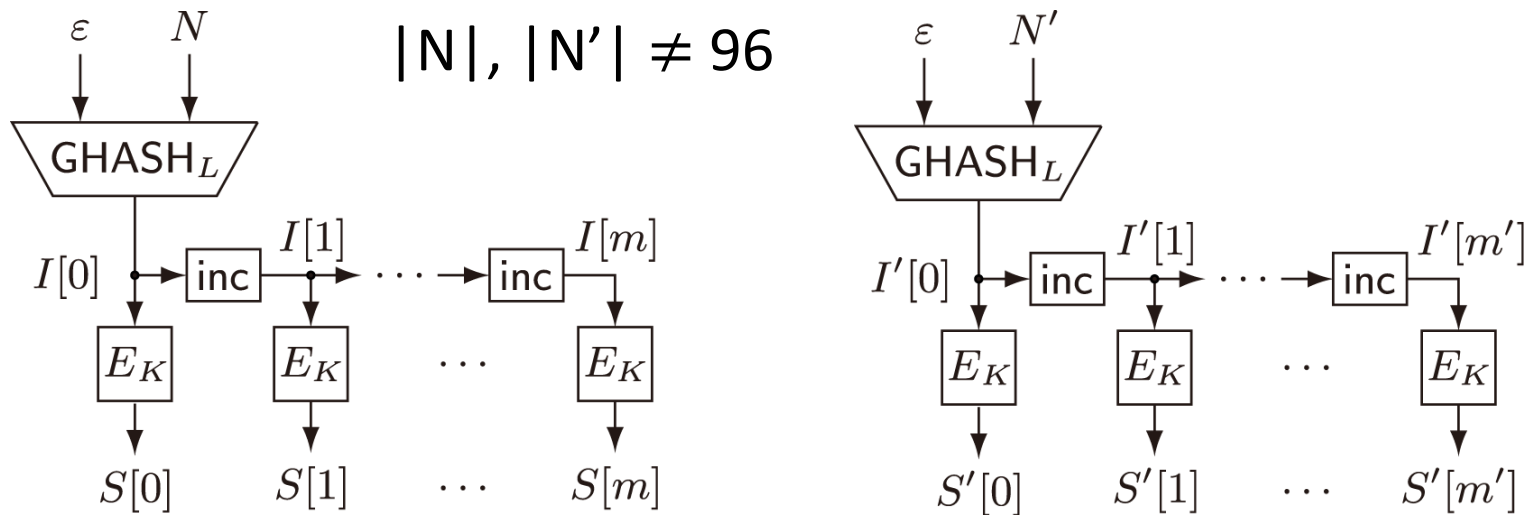
- A universal hash function defined over GF(2¹²⁸), which is defined by the irreducible polynomial $p(x) = 1+x+x^2+x^7+x^{128}$, where the multiplicative identity element is 0x80...0
- $N \parallel 0\dots0 \parallel |N|_{128} = (X[1], \dots, X[x])$
- $\text{GHASH}_L(\varepsilon, N) = X[1] \cdot L^x \oplus X[2] \cdot L^{x-1} \oplus \dots \oplus X[x] \cdot L$
- Example
 - $N = 0x00000000\ 00000000\ 02$ (72 bits)
 - $\text{GHASH}_L(\varepsilon, N)$
 - = $0x00000000\ 00000000\ 02000000\ 00000000 \cdot L^2$
 - $\oplus 0x00000000\ 00000000\ 00000000\ 00000048 \cdot L$
 - if $|N| \leq 128$ then $\deg(\text{GHASH}_L(\varepsilon, N)) \leq 2$

Counter Collision



- A counter collision: for some r ,
 - $I[r] = I'[0]$
 - $\text{inc}^r(\text{GHASH}_L(\epsilon, N)) = \text{GHASH}_L(\epsilon, N')$
 - $\text{Coll}_L(r, N, N')$

Counter Collision



- A counter collision is a bad event: $I[1] = I'[0], I[2] = I'[1], \dots$
 - xor of two ciphertexts = xor of two plaintexts
 - the information about plaintexts is leaked
- We need to show that $\Pr_L[\text{Coll}_L(r, N, N')]]$ is small

$\Pr_L[\text{Coll}_L(r, N, N')]$ Is Small

- [Lemma 3, MV04]

$$\Pr_L[\text{Coll}_L(r, N, N')] \leq \max\{ d, d' \} / 2^{128}$$

where $d = \deg(\text{GHASH}_L(\epsilon, N))$, $d' = \deg(\text{GHASH}_L(\epsilon, N'))$

- turns out to be wrong for some (r, N, N') [IOM12]
 - $r = 0x0\dots01$, $N = 0x0\dots02$ (72 bits), $N' = 0x0\dots06$ (72 bits)
 - [Lemma 3, MV04] says $\Pr_L[\text{Coll}_L(r, N, N')] \leq 2 / 2^{128}$
 - but $\Pr_L[\text{Coll}_L(r, N, N')] \geq 32 / 2^{128}$ (a lower bound)
 - a distinguishing attack with $\text{Adv}_{\text{GCM}[\text{Rand}(n), \tau]}^{\text{priv}}(A) \geq 32/2^{128}$

$\Pr_L[\text{Coll}_L(r, N, N')]$ Is Small

- [Lemma 2, IOM12] For each $0 \leq r \leq 2^{32}-1$
$$\Pr_L[\text{Coll}_L(r, N, N')] \leq \alpha_r \max\{ d, d' \} / 2^{128}$$
where $d = \deg(\text{GHASH}_L(\varepsilon, N))$, $d' = \deg(\text{GHASH}_L(\varepsilon, N'))$
- α_r can be large
 - $\alpha_r = 32$ when $r = 0x0\dots01$
 - $\alpha_r = 3524578$ when $r = 0x2aaaaaab, 0x55555555, 0xaaaaaaaaab, 0xd5555555$
 - 3524578 is about 2^{22}
 - “big constant” appears in the upper bound

Dagstuhl Seminar (January 2012)

- Joux: Do you have an attack that matches the bound (exploiting the fact that there is a big constant)?
 - finding (r, N, N') such that

$$\Pr_L[\text{Coll}_L(r, N, N')] \geq (\text{big constant}) / 2^{128}$$

Examples in [IOM12]

- $r = 0x0\dots01$, $N = 0x0^{17}2$, $N' = 0x0^{17}6$ (72 bits)
- $r = 0x0\dots01$, $N = 0x0^{15}20^{12}$, $N' = 0x0^{15}60^{12}$ (112 bits)
- $r = 0x0\dots01$, $N = 0x0^{17}20^{10}$, $N' = 0x0^{17}60^{10}$ (112 bits)
- $r = 0x0\dots01$, $N = 0x0^{14}40^3$, $N' = 0x0^{14}c0^3$ (72 bits)

- $\Pr_L[\text{Coll}_L(r, N, N')] \geq 32 / 2^{128}$

How We Found

- $|N|, |N'| \leq 128$
 - $\text{GHASH}_L(\varepsilon, N) = (N \parallel 0\dots 0) \cdot L^2 \oplus |N|_{128} \cdot L = U \cdot L^2 \oplus V \cdot L$
 - $\text{Pr}[\text{inc}^r(\text{GHASH}_L(\varepsilon, N)) = \text{GHASH}_L(\varepsilon, N')]$
 - $\text{inc}^1(U \cdot L^2 \oplus V \cdot L) = U' \cdot L^2 \oplus V' \cdot L$
 - started with random (U, V, U', V')
 - at some point we found that (U, V, U', V') of the form
 - $V = V'$
 - $U = 0^{8i} \parallel X \parallel 0^{120-8i}$
 - $U' = 0^{8i} \parallel X' \parallel 0^{120-8i}$
 - $|X|, |X'| = 8$
- has many solutions

Try the Same for $r = 0x55555555$

- $r = 0x55555555$
- for each (U, V, U', V') // $V=V'$
 counter = 0
 for 3524578 values of C
 solve $U \cdot L^2 \oplus V \cdot L \oplus C = U' \cdot L^2 \oplus V \cdot L$
 if $\text{incr}^r(U \cdot L^2 \oplus V \cdot L) = U' \cdot L^2 \oplus V \cdot L$ then counter++
 }
 output (U, U', V) if counter is large

Result

- $r = 0x55555555$
- counter = 8495 for the following values of (N, N') :
 - $(0x0...01d0000000000000, 0x0...02b0000000000000)$
 - $(0x0...02c0000000000000, 0x0...0640000000000000)$
 - $(0x0...0160000000000000, 0x0...0320000000000000)$
 - $(0x0...0270000000000000, 0x0...07d0000000000000)$
 - $|N| = |N'| = 112$

So?

- $\Pr_L[\text{Coll}_L(r, N, N')] \geq 8495 / 2^{128}$
 - $\text{Adv}_{\text{GCM}[\text{Rand}(n), \tau]}^{\text{priv}}(A) \geq 8495/2^{128}$
- $\Pr_L[\text{Coll}_L(r, N, N')] \geq 4247 \max\{d, d'\} / 2^{128} \geq 2^{12} \max\{d, d'\} / 2^{128}$
- Not as large as 2^{22} , but the gap is now smaller
 - 32 vs 2^{22} -> 2^{12} vs 2^{22}

Security Bounds [IOM12]

- $\text{Adv}_{\text{GCM}[\text{Perm}(n),\tau]}^{\text{priv}}(\mathcal{A}) \leq \frac{0.5(\sigma + q + 1)^2}{2^n} + \frac{2^{22}q(\sigma + q)(\ell_N + 1)}{2^n}$
- $\text{Adv}_{\text{GCM}[\text{Perm}(n),\tau]}^{\text{auth}}(\mathcal{A}) \leq \frac{0.5(\sigma + q + q' + 1)^2}{2^n} + \frac{2^{22}(q + q' + 1)(\sigma + q)(\ell_N + 1)}{2^n} + \frac{q'(\ell_A + 1)}{2^\tau}$
- The tightness is open
- There is a possibility to reduce 2^{22} to a smaller constant, but it cannot be less than 2^{12} (if we follow the proof strategy in [IOM12])

ASK 2012 (August 2012)

- Try to find (r, N, N') that gives a higher collision probability
 - (U, V, U', V') can take approximately $2^{128} 2^{128}$ values
- Yasuda: Try smaller GCM?

Small GCM with $n = 16$

- block size is $n = 16$ bits
- $\text{inc}(\cdot)$ operates on 4 bits
- GHASH is defined over $\text{GF}(2^{16})$ with the lexicographically first irreducible polynomial $p(x) = 1+x+x^4+x^5+x^{16}$

Small GCM with $n = 16$

- $\Pr_L[\text{Coll}_L(r, N, N')] \leq \alpha_r \max\{d, d'\} / 2^{16}$
 - $\alpha_r = 5$ (max) when $r = 0x3, 0x5, 0xb, 0xd$
- $|N|, |N'| \leq 16$
 - $\text{GHASH}_L(\varepsilon, N) = (N \parallel 0\dots 0) \cdot L^2 \oplus |N|_{16} \cdot L = U \cdot L^2 \oplus V \cdot L$
 - $\Pr[\text{inc}^r(\text{GHASH}_L(\varepsilon, N)) = \text{GHASH}_L(\varepsilon, N')] \leq 10 / 2^{16}$
- $\text{inc}^r(U \cdot L^2 \oplus V \cdot L) = U' \cdot L^2 \oplus V' \cdot L$
 - also consider $V \neq V'$
 - about 2^{33} values of (U, V, U', V')

Result

- $\Pr [\text{Coll}_L(r, N, N')] = 10 / 2^{16}$ holds
 - for 87,406 pairs of (N, N') when $r = 0x3, 0xd$
 - for 86,951 pairs of (N, N') when $r = 0x5, 0xb$
- For any (r, N, N') , $\Pr_L[\text{Coll}_L(r, N, N')] \leq \alpha_r \max\{ d, d' \} / 2^{16}$
- There exists (r, N, N') such that $\Pr_L[\text{Coll}_L(r, N, N')] = \alpha_r \max\{ d, d' \} / 2^{16}$
- There is an attack that matches the bound
- The “big constant” in security bounds cannot be replaced by a smaller one

Small GCM with $n = 20$

- block size is $n = 20$ bits
- $\text{inc}(\cdot)$ operates on 5 bits
- GHASH is defined over $\text{GF}(2^{20})$ with the lexicographically first irreducible polynomial $p(x) = 1+x^3+x^{20}$

Small GCM with $n = 20$

- $\Pr_L[\text{Coll}_L(r, N, N')] \leq \alpha_r \max\{d, d'\} / 2^{20}$
 - $\alpha_r = 8$ (max) when $r = 0x5, 0xb, 0x15, 0x1b$
- $|N|, |N'| \leq 20$
 - $\text{GHASH}_L(\varepsilon, N) = (N \parallel 0\dots 0) \cdot L^2 \oplus |N|_{20} \cdot L = U \cdot L^2 \oplus V \cdot L$
 - $\Pr[\text{inc}^r(\text{GHASH}_L(\varepsilon, N)) = \text{GHASH}_L(\varepsilon, N')] \leq 16 / 2^{20}$
- $\text{inc}^r(U \cdot L^2 \oplus V \cdot L) = U' \cdot L^2 \oplus V' \cdot L$
 - also consider $V \neq V'$
 - about 2^{41} values of (U, V, U', V')
- Result: $\Pr[\text{Coll}_L(r, N, N')] = 16 / 2^{20}$ holds
 - for 49,065 pairs of (N, N') when $r = 0x5$
 - There is an attack that matches the bound

Conclusions

- Joux: Do you have an attack that matches the bound?
- The tightness is still open for $n = 128$, but the gap is now smaller (2^{12} vs 2^{22})
- We have a matching attack for small versions of GCM ($n = 16, 20$)
- Plan: to investigate small versions of GCM for $n = 24, 28, 32, \dots$