Constants in GCM Security Bounds Are at Least . . .

Yuichi Niwa, Nagoya University
Keisuke Ohashi, Nagoya University
Kazuhiko Minematsu, NEC Corporation
Tetsu Iwata, Nagoya University

Rum(p) Session, FSE 2014
March 4, 2014, London, UK

GCM, Galois/Counter Mode

- NIST SP 800-38D, the benchmark for the CAESAR competition
- If |N| = 96 is not guaranteed, then GCM security bounds have a constant ($3{,}524{,}578 \leq 2^{22}$) [IOM12]
  - Do we really need the constant? Can it be smaller?

$$\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{GCM}[\mathrm{Perm}(n),\tau]}(\mathcal{A}) \leq \frac{0.5(\sigma+q+1)^2}{2^n} + \frac{2^{22}q(\sigma+q)(\ell_N+1)}{2^n}$$

$$\mathbf{Adv}^{\mathrm{auth}}_{\mathrm{GCM}[\mathrm{Perm}(n),\tau]}(\mathcal{A}) \leq \frac{0.5(\sigma+q+q'+1)^2}{2^n} + \frac{2^{22}(q+q'+1)(\sigma+q)(\ell_N+1)}{2^n} + \frac{q'(\ell_A+1)}{2^\tau}$$

[IOM12] Tetsu Iwata, Keisuke Ohashi, Kazuhiko Minematsu: Breaking and Repairing GCM Security Proofs. CRYPTO 2012: 31-49

GCM, Galois/Counter Mode

- NIST SP 800-38D, the benchmark for the CAESAR competition
- If |N| = 96 is not guaranteed, then GCM security bounds have a constant ($3{,}524{,}578 \leq 2^{22}$) [IOM12]
  - Do we really need the constant? Can it be smaller?

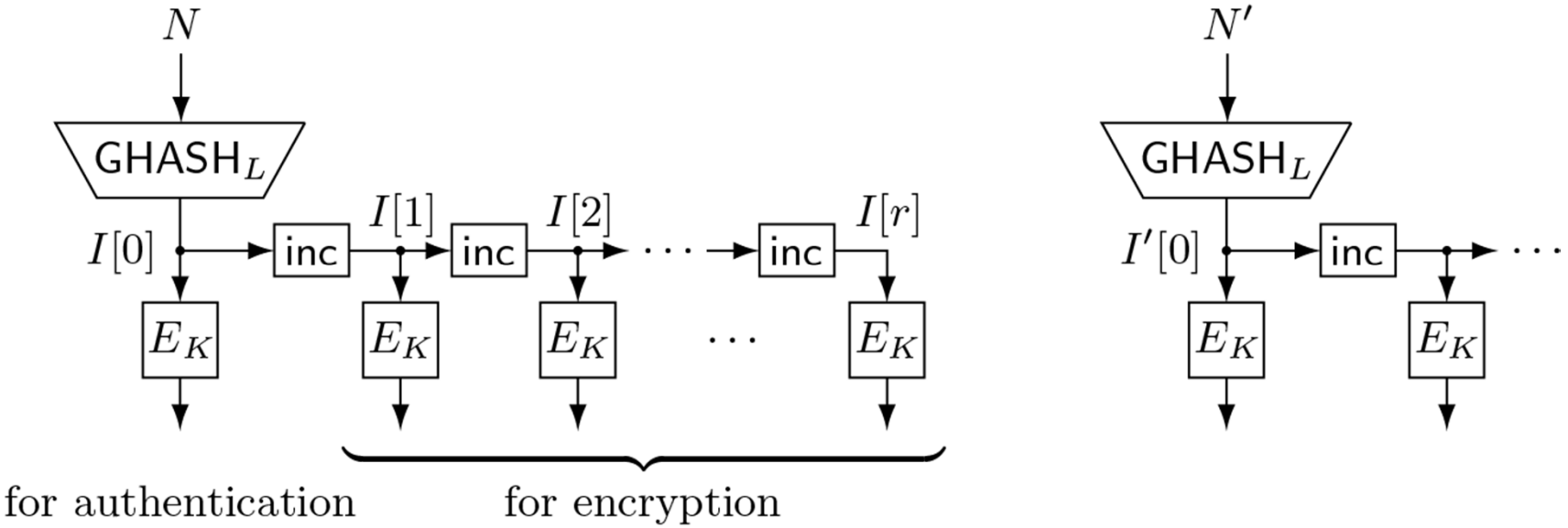
$$\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{GCM}[\mathrm{Perm}(n),\tau]}(\mathcal{A}) \leq \frac{0.5(\sigma+q+1)^2}{2^n} + \frac{2^{22}\ell(\sigma+q)(\ell_N+1)}{2^n}$$

$$\mathbf{Adv}^{\mathrm{auth}}_{\mathrm{GCM}[\mathrm{Perm}(n),\tau]}(\mathcal{A}) \leq \frac{0.5(\sigma+q+q'+1)^2}{2^n} + \frac{2^{22}(q+q'+1)(\sigma+q)(\ell_N+1)}{2^n} + \frac{q'(\ell_A+1)}{2^\tau}$$

[IOM12] Tetsu Iwata, Keisuke Ohashi, Kazuhiko Minematsu: Breaking and Repairing GCM Security Proofs. CRYPTO 2012: 31-49

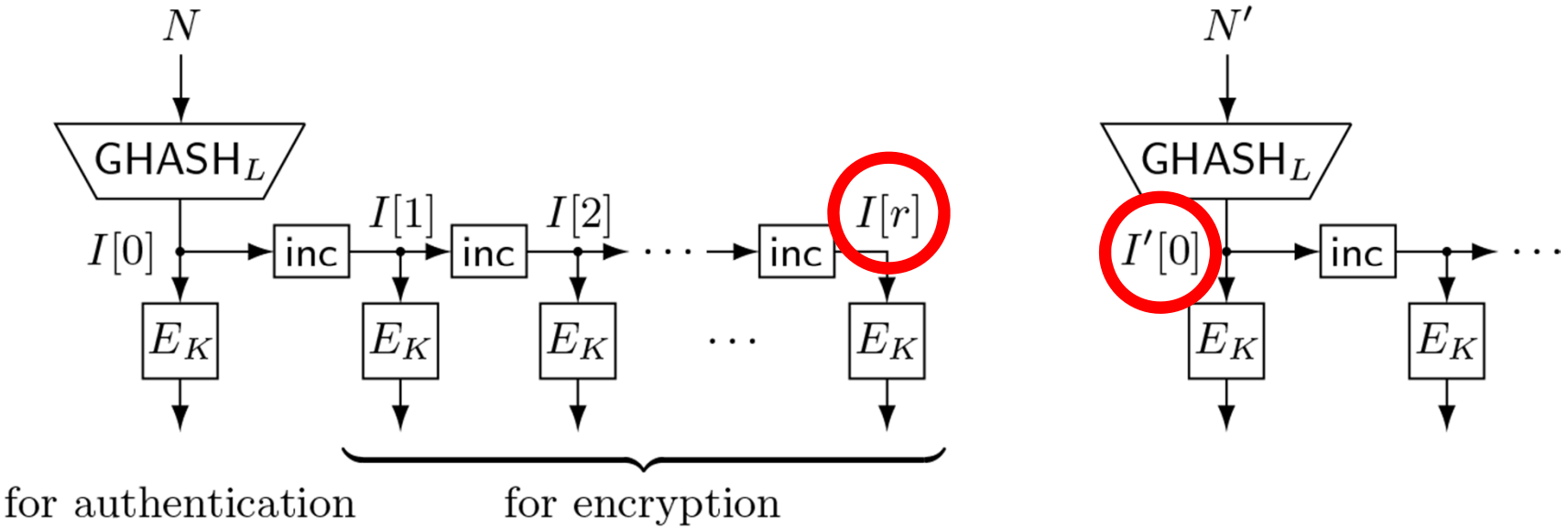
Counter Collision

- $|N|, |N'| \neq 96$
- $\mathrm{Coll}_L(r, N, N') \Leftrightarrow \mathrm{inc}^r(\mathrm{GHASH}_L(N)) = \mathrm{GHASH}_L(N')$



Counter Collision

- $|N|, |N'| \neq 96$
- $\text{Coll}_L(r, N, N') \Leftrightarrow \text{inc}^r(\text{GHASH}_L(N)) = \text{GHASH}_L(N')$



Counter Collision Probability

- [Lemma 2, IOM12] For any r, N, and N',

  $Pr_L[\ Coll_L(r, N, N')\ ] \leq 3{,}524{,}578 \times d / 2^{128}$

  - $d = \max\{\ \deg(\ GHASH_L(N)\ ), \deg(\ GHASH_L(N')\ )\ \}$

Counter Collision Probability

- [Lemma 2, IOM12] For any r, N, and N',
  $\Pr_L[\ \mathrm{Coll}_L(r, N, N')\ ] \leq 3{,}524{,}578 \times d / 2^{128}$
  - $d = \max\{\ \deg(\ \mathrm{GHASH}_L(N)\ ), \deg(\ \mathrm{GHASH}_L(N')\ )\ \}$

- Source of the constant in the security bounds
- $\Pr_L[\ \mathrm{Coll}_L(r, N, N')\ ] \geq$???

Result

- r = 0x55555555
- N = 0x8d44009c, dc550100, 00000000, 00000000
- N'= 0x5b6dbdd9, f3b151d9, d1bc4145, ecb396ef
- |N| = |N’| = 128
- $Pr_L[\ Coll_L(r, N, N')\ ] = 1{,}762{,}290 / 2^{128}$
- Anyone can verify the result (programming is needed)

Implication

- There exist r, N, and N’ such that

  $\Pr_L[\ \mathsf{Coll}_L(r, N, N')\ ] = 1{,}762{,}290 / 2^{128}$

  $= 881{,}145 \times 2 / 2^{128}$

  $\geq 2^{19.74} \times 2 / 2^{128}$

- To prove the security of GCM, [IOM12] uses “the sum bound”

$$\Pr_L[\mathsf{Coll}_L(r, N, N') \text{ for some } r] \leq \sum_r \Pr_L[\mathsf{Coll}_L(r, N, N')]$$

- If we follow the proof strategy, then the constant cannot be less than $881{,}145 \geq 2^{19.74}$

How?

- $Coll_L(r, N, N') <=> inc^r(GHASH_L(N)) = GHASH_L(N')$
- when $|N| = |N'| = 128$

  $inc^r(N \cdot L^2 \text{ xor } |N| \cdot L) = N' \cdot L^2 \text{ xor } |N'| \cdot L$ (1)
- r = 0x55555555, rewrite (1) in bits using 256 variables
- find the values of the 256 variables where (1) has as many solutions as possible
  - $Pr_L[\ Coll_L(r, N, N')\ ]$ = # solutions of (1) / 2^{128}
  - designed a greedy algorithm to select equations, used linearization to obtain linear equations, Gaussian elimination, . . .

Conclusion

- [Lemma 2, IOM12] For any r, N, and N',
  $\Pr_L[\ \mathrm{Coll}_L(r, N, N')\ ] \leq 3{,}524{,}578 \times d / 2^{128} \leq 2^{21.75} \times d / 2^{128}$
- There exist r, N, and N' such that
  $\Pr_L[\ \mathrm{Coll}_L(r, N, N')\ ] = 881{,}145 \times 2 / 2^{128} \geq 2^{19.74} \times 2 / 2^{128}$
- If we use "the sum bound," then the constant in GCM security bounds is at least

$$2^{19.74}$$