GCM Counter Collision Probability for Short Plaintext*

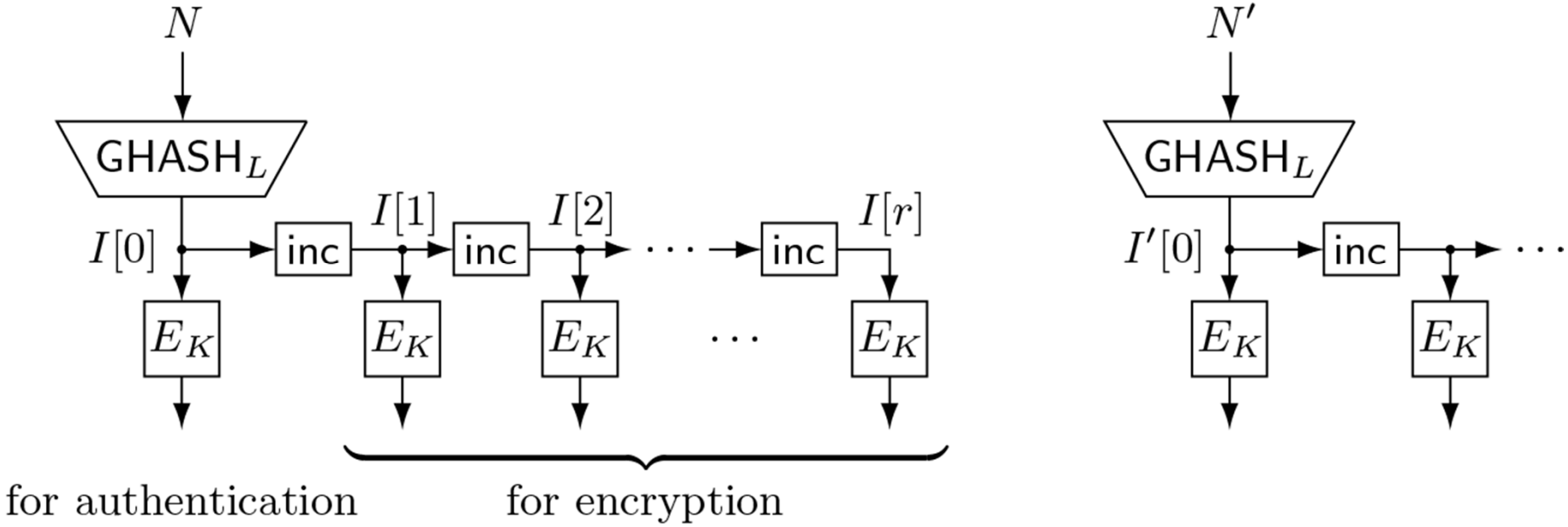
Shohei Ando, Yuichi Niwa, and Tetsu Iwata
Nagoya University

FSE 2015, Rump Session
March 10, 2015, Istanbul, Turkey

* Thanks to Keisuke Ohashi for discussions at the initial stage of the work

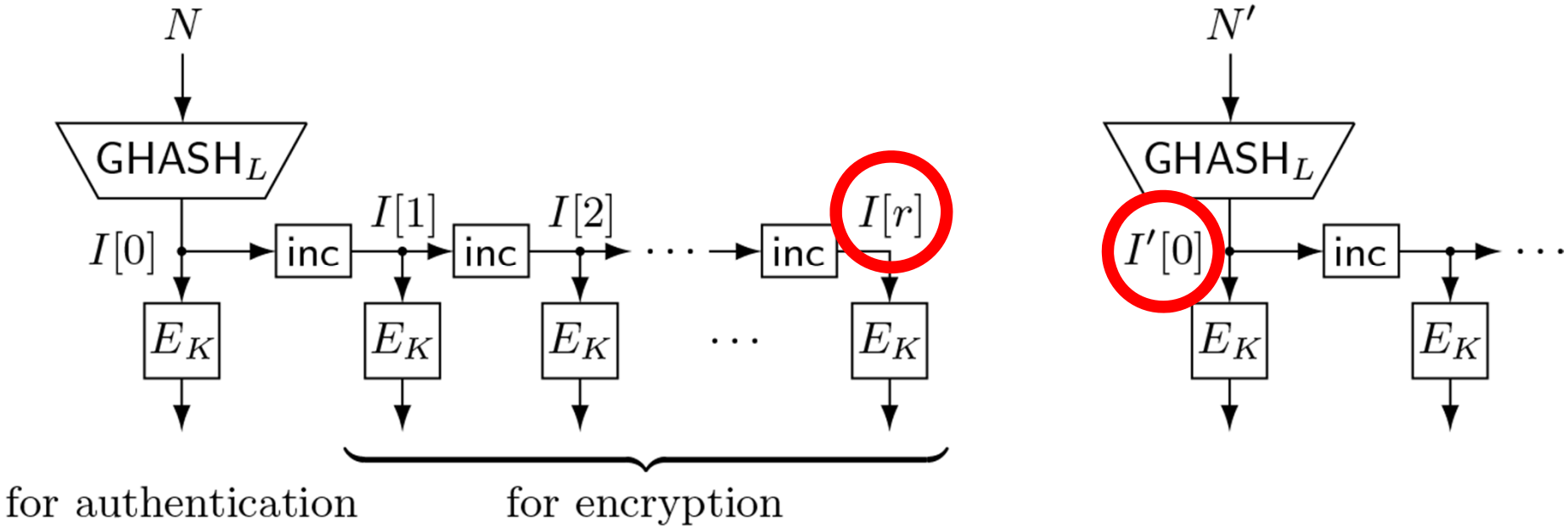
Counter Collision

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



Counter Collision

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



Counter Collision Probability

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

$$\Pr_L[\mathrm{Coll}(r, N, N')] \leq \alpha_r \times d \,/\, 2^{128},$$

where α_r is a constant and
$d = \max\{\deg(\mathrm{GHASH}_L(N)), \deg(\mathrm{GHASH}_L(N'))\}$

[IOM12] Iwata, Ohashi, and Minematsu: Breaking and Repairing GCM Security Proofs. CRYPTO 2012.

Counter Collision Probability

- [IOM12] For $r = \texttt{0x55555555}$, $\alpha_r \leq 2^{22}$

$$\Pr_L[\mathrm{Coll}(r, N, N')] \leq 2^{22} \times d \,/\, 2^{128}$$

- [NOMI15] For $r = \texttt{0x55555555}$,

$N = \texttt{0x8d44009c dc550100 00000000 00000000}$,

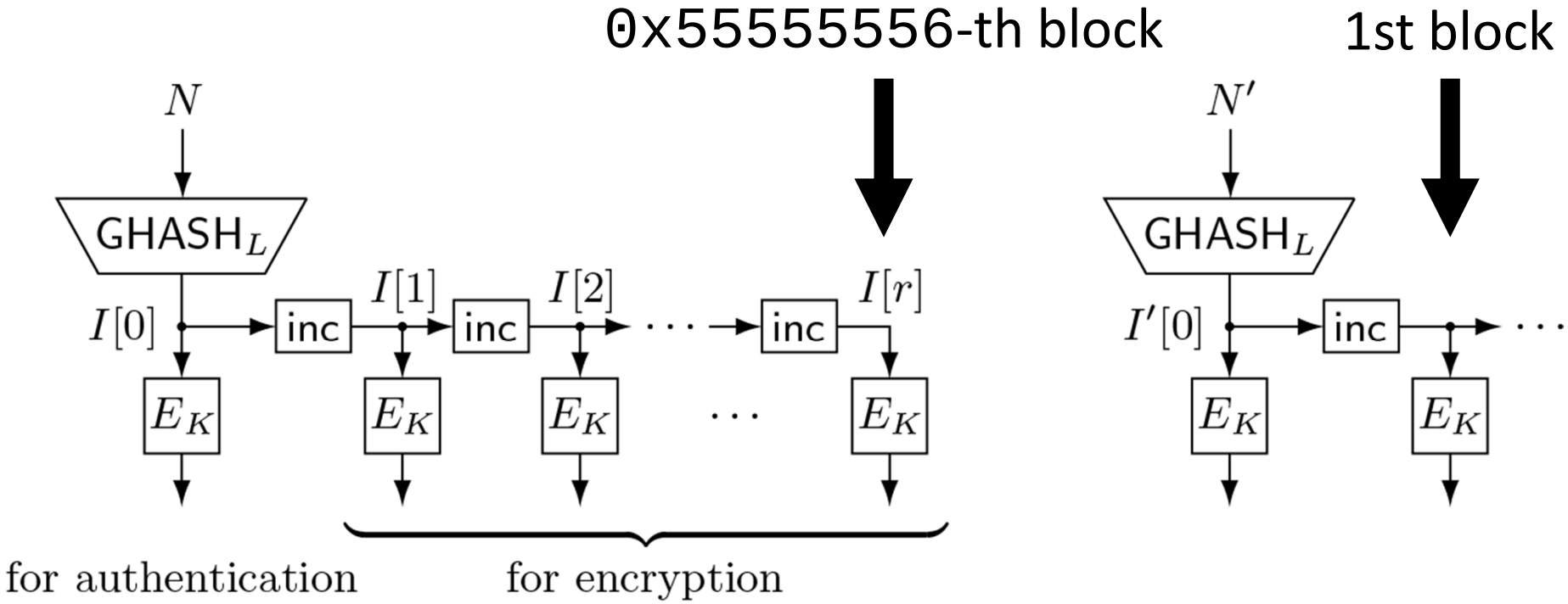
$N' = \texttt{0x5b6dbdd9 f3b151d9 00000000 00000000}$,

$$\Pr_L[\mathrm{Coll}(r, N, N')] \geq 2^{19.74} \times d \,/\, 2^{128},$$

where $d = 2$

[NOMI15] Niwa, Ohashi, Minematsu, and Iwata: GCM Security Bounds Reconsidered. FSE 2015.

Turning into Attack



- We need a long plaintext

Short Plaintexts?

- [IOM12] For $r = \texttt{0x00000001}$, $\alpha_r = 32$

$$\Pr_L[\mathrm{Coll}(r, N, N')] \leq 32 \times d \,/\, 2^{128}$$

- For $r = \texttt{0x00000001}$,

$$\Pr_L[\mathrm{Coll}(r, N, N')] \geq ? \,/\, 2^{128}$$

- [IOM12] For $r = \texttt{0x00000001}$,

$N = \texttt{0x00000000 00000000 02}$ (72 bits),

$N' = \texttt{0x00000000 00000000 06}$ (72 bits),

$$\Pr_L[\mathrm{Coll}(r, N, N')] \geq 16 \times d \,/\, 2^{128},$$

where $d = 2$

Short Plaintexts?

- [IOM12] For $r = \texttt{0x00000001}$, $\alpha_r = 32$

$$\Pr_L[\mathrm{Coll}(r, N, N')] \leq 32 \times d \,/\, 2^{128}$$

- For $r = \texttt{0x00000001}$,

$$\Pr_L[\mathrm{Coll}(r, N, N')] \geq ? \,/\, 2^{128}$$

a gap

- [IOM12] For $r = \texttt{0x00000001}$,

$N = \texttt{0x00000000 00000000 02}$ (72 bits),

$N' = \texttt{0x00000000 00000000 06}$ (72 bits),

$$\Pr_L[\mathrm{Coll}(r, N, N')] \geq 16 \times d \,/\, 2^{128},$$

where $d = 2$

New Result

- [IOM12] For $r = \texttt{0x00000001}$, $\alpha_r = 32$

$$\Pr_L[\mathrm{Coll}(r, N, N')] \leq 32 \times d \,/\, 2^{128}$$

- For $r = \texttt{0x00000001}$,

  $N = \texttt{0x00000000 400080}$ (56 bits),

  $N' = \texttt{0x00000000 c0018000 00}$ (72 bits),

$$\Pr_L[\mathrm{Coll}(r, N, N')] \geq 32 \times d \,/\, 2^{128},$$

  where $d = 2$

New Result

- [IOM12] For $r = \texttt{0x00000001}$, $\alpha_r = 32$

$$\Pr_L[\mathrm{Coll}(r, N, N')] \leq 32 \times d \,/\, 2^{128}$$

- For $r = \texttt{0x00000001}$,

  $N = \texttt{0x00000000 400080}$ (56 bits),

  $N' = \texttt{0x00000000 c0018000 00}$ (72 bits),

$$\Pr_L[\mathrm{Coll}(r, N, N')] \geq 32 \times d \,/\, 2^{128},$$

  where $d = 2$

tight

- The **first** example that matches the upper bound

How?

- Experimentally figured out $N = \texttt{0x8001}$ is a “good” nonce
- Shift this N in various ways with different lengths of (N, N')
- tested various nonce lengths to follow the length encoding rule of GCM
- The result was obtained experimentally
  - Mathematical explanation of the result is not clear at present

Conclusions

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

$$\Pr_{L}[\mathrm{Coll}(r, N, N')] \leq \alpha_r \times d \,/\, 2^{128},$$

where α_r is a constant and
$d = \max\{\deg(\mathrm{GHASH}_L(N)), \deg(\mathrm{GHASH}_L(N'))\}$

- The lemma is tight when $r = \texttt{0x00000001}$