Generic Attacks on Duplex-based AEAD modes

Small cycles and large components

Henri Gilbert, Rachelle Heim Boissier, Louiza Khati, Yann Rotella

ANSSI, Université de Versailles Saint Quentin en Yvelines

Frisiacrypt 2022, Terschelling, The Netherlands

UNIVERSITÉ DE VERSAILLES ST-QUENTIN-EN-YVELINES

université PARIS-SACLAY

Graph of function

$f : \mathcal{S} \rightarrow \mathcal{S}$ where $|\mathcal{S}| = n = 2^c$

Graph of function

$$f : \mathcal{S} \to \mathcal{S} \text{ where } |\mathcal{S}| = n = 2^c$$

- A collection of :
- a collection of trees,
- linked by cycles (components)

Graph of function

$$f : \mathcal{S} \rightarrow \mathcal{S} \text{ where } |\mathcal{S}| = n = 2^c$$

- A collection of :
- a collection of trees,
- linked by cycles (components)

We call $\mu(x)$ and $\lambda(x)$ the cycle length and tail length respectively

RELEVANT VALUES

DEFINITION (ν-COMPONENT)

let $0 < \nu < \frac{1}{2}$. A ν-component is a component that has a cycle of size at most $n^{\frac{1}{2}-\nu}$.

RELEVANT VALUES

DEFINITION (ν-COMPONENT)

let $0 < \nu < \frac{1}{2}$. A ν-component is a component that has a cycle of size at most $n^{\frac{1}{2}-\nu}$.

DEFINITION ((s, ν)-COMPONENT)

let $0 < \nu < \frac{1}{2}$ and $0 < s < 1$. A (s, ν)-component is a component whose size is greater or equal to ns and whose cycle is of size at most $n^{\frac{1}{2}-\nu}$.

Previous works

- It is known that $\mu(x)$ and $\lambda(x)$ are both on average $\sqrt{\pi n/8}$. See famous "Random mapping statistics, Flajolet and Odlyzko" in 1989

Previous works

- It is known that $\mu(x)$ and $\lambda(x)$ are both on average $\sqrt{\pi n/8}$. See famous "Random mapping statistics, Flajolet and Odlyzko" in 1989
- But, the probability that $\mu(x) < n^{\frac{1}{2}-\nu}$ is roughly

$$\frac{\sqrt{2\pi}}{2n^{\nu}}$$

Previous works

- It is known that $\mu(x)$ and $\lambda(x)$ are both on average $\sqrt{\pi n/8}$. See famous "Random mapping statistics, Flajolet and Odlyzko" in 1989
- But, the probability that $\mu(x) < n^{\frac{1}{2}-\nu}$ is roughly

$$\frac{\sqrt{2\pi}}{2n^{\nu}}$$

Harris 1960 : "Probability Distributions Related to Random Mappings"

Previous works

- It is known that $\mu(x)$ and $\lambda(x)$ are both on average $\sqrt{\pi n/8}$. See famous "Random mapping statistics, Flajolet and Odlyzko" in 1989
- But, the probability that $\mu(x) < n^{\frac{1}{2}-\nu}$ is roughly

  $$\frac{\sqrt{2\pi}}{2n^{\nu}}$$

  Harris 1960 : "Probability Distributions Related to Random Mappings"
- Also, the probability that a graph has a (s, ν)-component is roughly

  $$\sqrt{\frac{2(1-s)}{\pi s}}n^{-\nu}$$

Previous works

- It is known that $\mu(x)$ and $\lambda(x)$ are both on average $\sqrt{\pi n/8}$. See famous "Random mapping statistics, Flajolet and Odlyzko" in 1989
- But, the probability that $\mu(x) < n^{\frac{1}{2}-\nu}$ is roughly

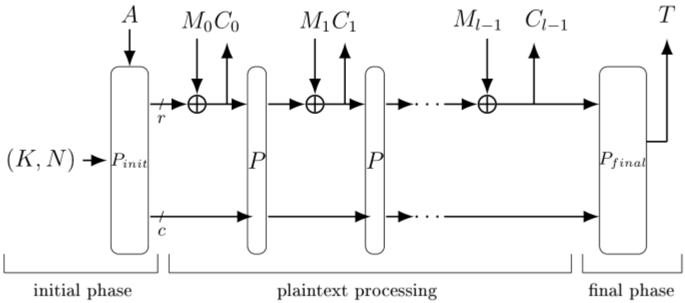
$$\frac{\sqrt{2\pi}}{2n^{\nu}}$$

  Harris 1960 : "Probability Distributions Related to Random Mappings"
- Also, the probability that a graph has a (s, ν)-component is roughly

$$\sqrt{\frac{2(1-s)}{\pi s}}\, n^{-\nu}$$

  De Laurentis, Crypto 1987, "Components and Cycles of a random function"

DUPLEX AEAD



A
$M_0 C_0$
$M_1 C_1$
M_{l-1}
C_{l-1}
T
(K, N)
P_{init}
r
c
P
P
P_{final}
initial phase
plaintext processing
final phase

SECURITY OF DUPLEX

Simplified Beyond conventional security in sponge-based authenticated encryption modes [Jovanovic, Luykx, Mennink, Sasaki, Yasuda, JoC 2019]

$$\mathcal{T} \ll \min\{2^{\frac{b}{2}}, \frac{2^c}{\alpha}, 2^\kappa\} \text{ and } q_d \ll 2^\tau$$

where, $\alpha < r$, where q_d is the number of forgery attempts.

Security of Duplex

Simplified Beyond conventional security in sponge-based authenticated encryption modes [Jovanovic, Luykx, Mennink, Sasaki, Yasuda, JoC 2019]

$$\mathcal{T} \ll \min\{2^{\frac{b}{2}}, \frac{2^c}{\alpha}, 2^{\kappa}\} \text{ and } q_d \ll 2^{\tau}$$

where, $\alpha < r$, where q_d is the number of forgery attempts.
So duplex construction is proven for $2^{\frac{c}{2}}$, and known generic attacks are in $\frac{2^c}{\alpha}$

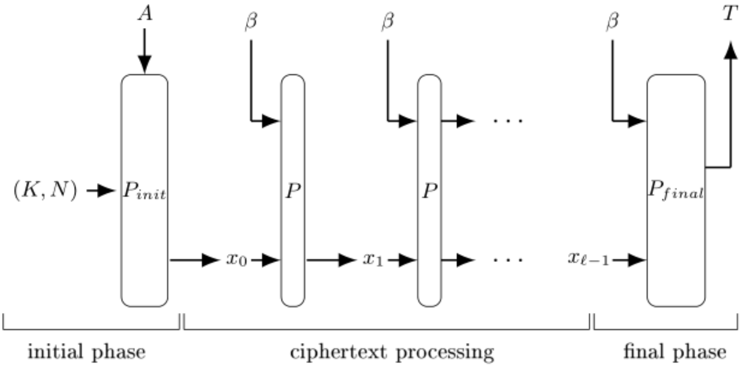
OBSERVATION IN DECRYPTION MODE

Let $C_{\beta}^{\ell} = \beta_{\ell} = \underbrace{\beta || \cdots || \beta}_{\ell}$.

Observation in decryption mode

Let $C^{\ell}_{\beta} = \beta_{\ell} = \underbrace{\beta || \cdots || \beta}_{\ell}$. Then the decryption of C^{ℓ}_{β} corresponds to the iteration of

$$\begin{array}{rcrcl} f_{\beta} & : & \mathbb{F}_2^c & \longrightarrow & \mathbb{F}_2^c \\ & & x & \longmapsto & \lfloor P(\beta || x) \rfloor_c . \end{array}$$



The attack

The attack is a forgery in $O(2^{\frac{3c}{4}})$ and there is no release of unverified plaintexts.

THE ATTACK

The attack is a forgery in $\mathcal{O}(2^{\frac{3c}{4}})$ and there is no release of unverified plaintexts.

Precomputation : find a β such that f_β has a (s, ν) component.

THE ATTACK

The attack is a forgery in $\mathcal{O}(2^{\frac{3c}{4}})$ and there is no release of unverified plaintexts.

Precomputation : find a β such that f_β has a (s, ν) component.
Online : input (N, A, C, T) with N, A possibly different and $C = C_\beta^\ell$ with $\ell = \gamma 2^{\frac{c}{2}}$.

THE ATTACK

The attack is a forgery in $\mathcal{O}(2^{\frac{3c}{4}})$ and there is no release of unverified plaintexts.

Precomputation : find a β such that f_β has a (s, ν) component.
Online : input (N, A, C, T) with N, A possibly different and $C = C_\beta^\ell$ with $\ell = \gamma 2^{\frac{c}{2}}$. And T being derived from a value of the cycle of f_β ($n^{\frac{1}{2}-\nu}$ possibilities at most)

PRECOMPUTATION

- detecting ν-components : Brent's algorithm

PRECOMPUTATION

- detecting ν-components : Brent's algorithm
- (s, ν) costs too much, so we use an approximation (CLT)

ONLINE

- Input N, A, C_{β}^{ℓ} and a proportion of possible tags (with respect to cycle's values)

Online

- Input N, A, C_β^ℓ and a proportion of possible tags (with respect to cycle's values)
- Possibly for different nonces (you might be outside the s-component)

Online

- Input N, A, C_{β}^{ℓ} and a proportion of possible tags (with respect to cycle's values)
- Possibly for different nonces (you might be outside the s-component)

Complexity $\mathcal{O}\left(2^{\frac{3c}{4}}\right)$

Experimental verification

Statistics verified up to small c values.

Specific modes and padding

Key recovery is possible and attack applicable to several proposals :

Specific modes and padding

Key recovery is possible and attack applicable to several proposals :

- Cyclist (Xoodyak) : 2^{148}
- MonkeyDuplex : Ketje, KNOT and NORX v2

Specific modes and padding

Key recovery is possible and attack applicable to several proposals :

- Cyclist (Xoodyak) : 2^{148}
- MonkeyDuplex : Ketje, KNOT and NORX v2
- Motorist : Keyak

What frustrates the attack

- Adding key material in the final phase

What frustrates the attack

- Adding key material in the final phase
- Use a ρ-like application (Beetle, Subterranean)