Кафедра 42
Криптология и дискретная математика
Тел. 324-7334; факс. 323-9137; e-mail: kaf42@mail.ru.
Факультет "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ"

Атака на основе коллизий на AES-подобные алгоритмы блочного шифрования

Машошин С.Н.

Использованные материалы

Спецификации алгоритмов блочного шифрования:

1. AES
2. Square
3. CRYPTON
4. Anubis
5. W

Статья “A collision attack on 7 rounds of Rijndael”

Henri Gilbert, Marine Minier

AES

- размер блока 128 бит
- размер ключа 128\192\256 бит
- количество раундов 10\12\14

Преобразования, используемые внутри раунда:

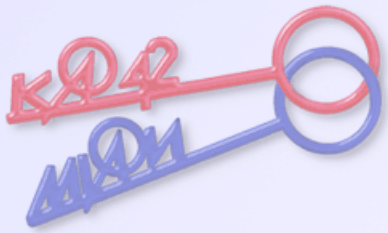
1) SubBytes(S – блок)
2) ShiftRows (Перестановка)
3) MixColumns (Линейное рассеивание)
4) AddRoundKey(Добавление ключа)

Square

- размер блока 128 бит
- размер ключа 128 бит
- количество раундов 8

Преобразования, используемые внутри раунда:

1) A Linear Transformation (Линейное рассеивание)
2) A Nonlinear Transformation(S – блок)
3) A Byte Permutation (Перестановка)
4) Bitwise Round Key Addition (Добавление ключа)



CRYPTON

- размер блока 128 бит
- размер ключа 128\192\256 бит
- количество раундов 12

Преобразования, используемые внутри раунда:

1) Byte Substitution (S – блок)
2) Bit Permutation (Линейное рассеивание)
3) Byte Transposition (Перестановка)
4) Key Addition (Добавление ключа)

Anubis

- размер блока 128 бит
- размер ключа 32*N* бит(*N* = 4, ..., 10)
- количество раундов 8+*N*

Преобразования, используемые внутри раунда:

1) The nonlinear layer (S – блок)
2) The transposition (Перестановка)
3) The linear diffusion layer (Линейное рассеивание)
4) The key addition (Добавление ключа)

W

- размер блока 512 бит
- размер ключа 512 бит
- количество раундов 10

Преобразования, используемые внутри раунда:

1) The nonlinear layer (S – блок)
2) The cyclical permutation (Перестановка)
3) The linear diffusion layer (Линейное рассеивание)
4) The key addition (Добавление ключа)

Коллизия в AES

y			
c_0			
c_1			
c_2			

z_0			
z_1			
z_2			
z_3			

r_0			
	r_1		
		r_2	
			r_3

s			

t_0			
t_1			
t_2			
t_3			

1) существует два различных набора (c_0, c_1, c_2), для которых s(y) равны при всех значениях y
2) $s=SB^{-1}(MC^{-1}(t_0,t_1,t_2,t_3)+k)$, где SB – SubBytes (S – блок), MC – MixColumns (линейное рассеивание)

Коллизия в Square

y			
c_0			
c_1			
c_2			

z_0			
z_1			
z_2			
z_3			

r_0	r_1	r_2	r_3

s			

t_0			
t_1			
t_2			
t_3			

1) существует два различных набора (c_0, c_1, c_2), для которых s(y) равны при всех значениях y
2) $s=NT^{-1}(LT^{-1}(t_0,t_1,t_2,t_3)+k)$, где NT - A Nonlinear Transformation (S – блок), LT - A Linear Transformation (линейное рассеивание)

Коллизия в CRYPTON

y	c_0	c_1	c_2

z_0	z_1	z_2	z_3

r_0			
r_1			
r_2			
r_3			

s			

t_0	t_1	t_2	t_3

1) существует два различных набора (c_0, c_1, c_2), для которых s(y) равны при всех значениях y
2) $s=BS^{-1}(BP^{-1}(t_0,t_1,t_2,t_3)+k)$, где BS - Byte Substitution(S – блок) , BP - Bit Permutation (линейное рассеивание)

Коллизия в Anubis

y	c_0	c_1	c_2

z_0	z_1	z_2	z_3

r_0			
r_1			
r_2			
r_3			

s			

t_0	t_1	t_2	t_3

1) существует два различных набора (c_0, c_1, c_2), для которых s(y) равны при всех значениях y
2) $s=NL^{-1}(MC^{-1}(t_0,t_1,t_2,t_3)+k)$, где NL - The nonlinear layer (S – блок), LD - The linear diffusion layer (линейное рассеивание)

Коллизия в W

- строится аналогично AES
- существует два различных набора (c_0, c_1, c_2), для которых s(y) равны при всех значениях y
- $s=NL^{-1}(LD^{-1}(t_0,t_1,t_2,t_3,t_4,t_5,t_6,t_7)+k)$, где NL - the nonlinear layer(S – блок), LD - The linear diffusion layer (линейное рассеивание)

Атака на основе коллизий на AES

x_0			
	x_1		
		x_2	
			x_3

y
c_0
c_1
c_2

z_0
z_1
z_2
z_3

r_0			
	r_1		
		r_2	
			r_3

s			

t_0
t_1
t_2
t_3

$u_{0,0}$	$u_{0,1}$	$u_{0,2}$	$u_{0,3}$
$u_{1,0}$	$u_{1,1}$	$u_{1,2}$	$u_{1,3}$
$u_{2,0}$	$u_{2,1}$	$u_{2,2}$	$u_{2,3}$
$u_{3,0}$	$u_{3,1}$	$u_{3,3}$	$u_{3,3}$

$v_{0,0}$	$v_{0,1}$	$v_{0,2}$	$v_{0,3}$
$v_{1,0}$	$v_{1,1}$	$v_{1,2}$	$v_{1,3}$
$v_{2,0}$	$v_{2,1}$	$v_{2,2}$	$v_{2,3}$
$v_{3,0}$	$v_{3,1}$	$v_{3,3}$	$v_{3,3}$

- Трудоемкость атаки на 5,5 раундов - 2^{101} шифрований при наличии 2^{32} открытых текстов.
- Трудоемкость атаки на 6 раундов - 2^{117} шифрований при наличии 2^{32} открытых текстов.
- Трудоемкость атаки на 6,5 раундов - 2^{133} шифрований при наличии 2^{32} открытых текстов.

Атака на основе коллизий на Square

x_0	x_1	x_2	x_3

y			
c_0			
c_1			
c_2			

z_0			
z_1			
z_2			
z_3			

r_0	r_1	r_2	r_3

s			

t_0			
t_1			
t_2			
t_3			

$u_{0,0}$	$u_{0,1}$	$u_{0,2}$	$u_{0,3}$
$u_{1,0}$	$u_{1,1}$	$u_{1,2}$	$u_{1,3}$
$u_{2,0}$	$u_{2,1}$	$u_{2,2}$	$u_{2,3}$
$u_{3,0}$	$u_{3,1}$	$u_{3,3}$	$u_{3,3}$

- Трудоемкость атаки на 6 раундов - 2^{117} шифрований при наличии 2^{32} открытых текстов.

Атака на основе коллизий на Crypton

x_0			
x_1			
x_2			
x_3			

y	c_0	c_1	c_2

z_0	z_1	z_2	z_3

r_0			
r_1			
r_2			
r_3			

s			

t_0	t_1	t_2	t_3

$u_{0,0}$	$u_{0,1}$	$u_{0,2}$	$u_{0,3}$
$u_{1,0}$	$u_{1,1}$	$u_{1,2}$	$u_{1,3}$
$u_{2,0}$	$u_{2,1}$	$u_{2,2}$	$u_{2,3}$
$u_{3,0}$	$u_{3,1}$	$u_{3,3}$	$u_{3,3}$

$v_{0,0}$	$v_{0,1}$	$v_{0,2}$	$v_{0,3}$
$v_{1,0}$	$v_{1,1}$	$v_{1,2}$	$v_{1,3}$
$v_{2,0}$	$v_{2,1}$	$v_{2,2}$	$v_{2,3}$
$v_{3,0}$	$v_{3,1}$	$v_{3,3}$	$v_{3,3}$

- Трудоемкость атаки на 5,5 раундов - 2^{101} шифрований при наличии 2^{32} открытых текстов.
- Трудоемкость атаки на 6 раундов - 2^{117} шифрований при наличии 2^{32} открытых текстов.
- Трудоемкость атаки на 6,5 раундов - 2^{133} шифрований при наличии 2^{32} открытых текстов.

Атака на основе коллизий на Anubis

x_0			
x_1			
x_2			
x_3			

y	c_0	c_1	c_2

z_0	z_1	z_2	z_3

r_0			
r_1			
r_2			
r_3			

s			

t_0	t_1	t_2	t_3

$u_{0,0}$	$u_{0,1}$	$u_{0,2}$	$u_{0,3}$
$u_{1,0}$	$u_{1,1}$	$u_{1,2}$	$u_{1,3}$
$u_{2,0}$	$u_{2,1}$	$u_{2,2}$	$u_{2,3}$
$u_{3,0}$	$u_{3,1}$	$u_{3,3}$	$u_{3,3}$

$v_{0,0}$	$v_{0,1}$	$v_{0,2}$	$v_{0,3}$
$v_{1,0}$	$v_{1,1}$	$v_{1,2}$	$v_{1,3}$
$v_{2,0}$	$v_{2,1}$	$v_{2,2}$	$v_{2,3}$
$v_{3,0}$	$v_{3,1}$	$v_{3,3}$	$v_{3,3}$

- Трудоемкость атаки на 5,5 раундов - 2^{101} шифрований при наличии 2^{32} открытых текстов.
- Трудоемкость атаки на 6 раундов - 2^{117} шифрований при наличии 2^{32} открытых текстов.
- Трудоемкость атаки на 6,5 раундов - 2^{133} шифрований при наличии 2^{32} открытых текстов.

Атака на основе коллизий на W

Строится аналогично атаке на AES

- Трудоемкость атаки на 5,5 раундов – 2^{325} шифрований при наличии 2^{64} открытых текстов.
- Трудоемкость атаки на 6 раундов - 2^{357} шифрований при наличии 2^{64} открытых текстов.
- Трудоемкость атаки на 6,5 раундов – 2^{389} шифрований при наличии 2^{64} открытых текстов.

Рассмотрение зависимостей раундовых ключей AES

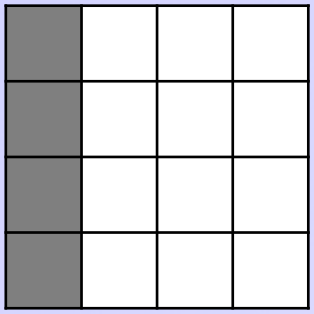
x_0			
	x_1		
		x_2	
			x_3

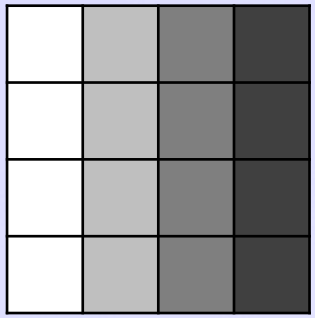
y			
c_0			
c_1			
c_2			

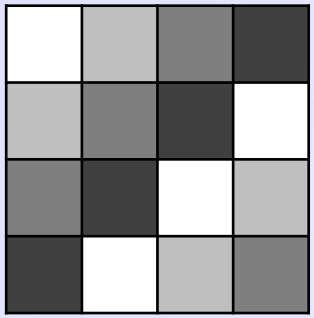
t_0			
t_1			
t_2			
t_3			

$u_{0,0}$	$u_{0,1}$	$u_{0,2}$	$u_{0,3}$
$u_{1,0}$	$u_{1,1}$	$u_{1,2}$	$u_{1,3}$
$u_{2,0}$	$u_{2,1}$	$u_{2,2}$	$u_{2,3}$
$u_{3,0}$	$u_{3,1}$	$u_{3,3}$	$u_{3,3}$

$v_{0,0}$	$v_{0,1}$	$v_{0,2}$	$v_{0,3}$
$v_{1,0}$	$v_{1,1}$	$v_{1,2}$	$v_{1,3}$
$v_{2,0}$	$v_{2,1}$	$v_{2,2}$	$v_{2,3}$
$v_{3,0}$	$v_{3,1}$	$v_{3,3}$	$v_{3,3}$







- Трудоёмкость атаки без рассмотрения алгоритма развертывания ключа равна 2^{133} шифрований при наличии 2^{32} открытых текстов.
- Количество вариантов разбиения ключа в последнем раунде равно 3.
- Существует класс алгоритмов развертывания ключа, при которых возможно снижение трудоёмкости данной атаки до 2^{117}.
- Для простейших алгоритмов развертывания ключа, трудоёмкость атаки, возможно, понизить до 2^{101}.

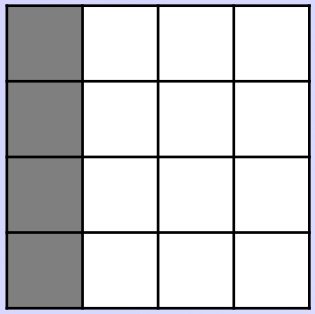
Рассмотрение зависимостей раундовых ключей Square

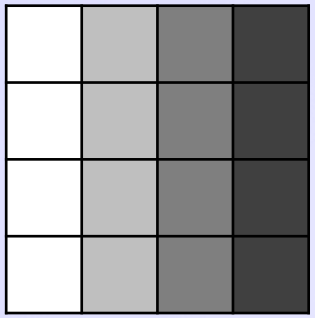
x_0	x_1	x_2	x_3

y			
c_0			
c_1			
c_2			

t_0			
t_1			
t_2			
t_3			

$u_{0,0}$	$u_{0,1}$	$u_{0,2}$	$u_{0,3}$
$u_{1,0}$	$u_{1,1}$	$u_{1,2}$	$u_{1,3}$
$u_{2,0}$	$u_{2,1}$	$u_{2,2}$	$u_{2,3}$
$u_{3,0}$	$u_{3,1}$	$u_{3,3}$	$u_{3,3}$





- Трудоёмкость атаки без рассмотрения алгоритма развертывания ключа равна 2^{117} шифрований при наличии 2^{32} открытых текстов.
- Количество вариантов разбиения ключа в последнем раунде равно 3.
- Для простейших алгоритмов развертывания ключа, трудоёмкость атаки, возможно, понизить до 2^{101}.

Рассмотрение зависимостей раундовых ключей CRYPTON

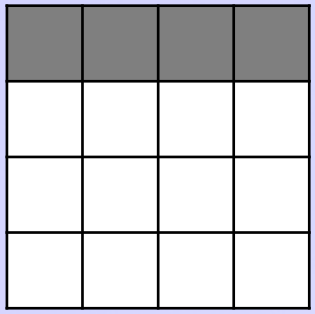
x_0			
x_1			
x_2			
x_3			

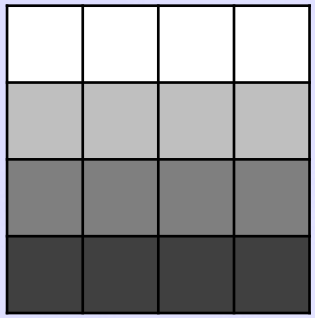
y	c_0	c_1	c_2

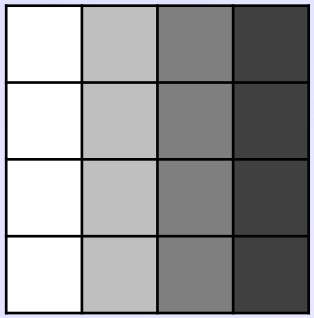
t_0	t_1	t_2	t_3

$u_{0,0}$	$u_{0,1}$	$u_{0,2}$	$u_{0,3}$
$u_{1,0}$	$u_{1,1}$	$u_{1,2}$	$u_{1,3}$
$u_{2,0}$	$u_{2,1}$	$u_{2,2}$	$u_{2,3}$
$u_{3,0}$	$u_{3,1}$	$u_{3,3}$	$u_{3,3}$

$v_{0,0}$	$v_{0,1}$	$v_{0,2}$	$v_{0,3}$
$v_{1,0}$	$v_{1,1}$	$v_{1,2}$	$v_{1,3}$
$v_{2,0}$	$v_{2,1}$	$v_{2,2}$	$v_{2,3}$
$v_{3,0}$	$v_{3,1}$	$v_{3,3}$	$v_{3,3}$







- Трудоёмкость атаки без рассмотрения алгоритма развертывания ключа равна 2^{133} шифрований при наличии 2^{32} открытых текстов.
- Количество вариантов разбиения ключа в последнем раунде равно 3.
- Существует класс алгоритмов развертывания ключа, при которых возможно снижение трудоёмкости данной атаки до 2^{117}.
- Для простейших алгоритмов развертывания ключа, трудоёмкость атаки, возможно, понизить до 2^{101}.

Рассмотрение зависимостей раундовых ключей Anubis

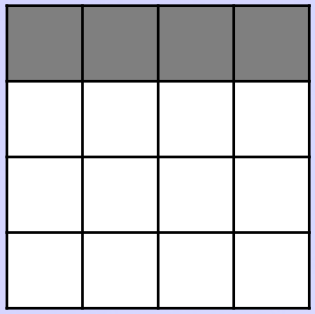
x_0			
x_1			
x_2			
x_3			

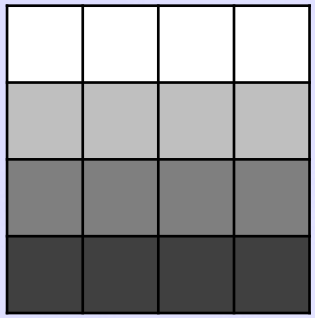
y	c_0	c_1	c_2

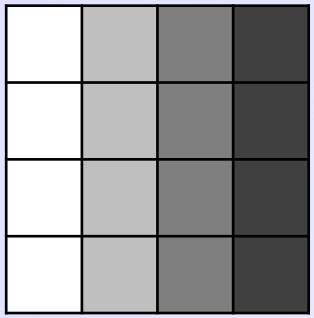
t_0	t_1	t_2	t_3

$u_{0,0}$	$u_{0,1}$	$u_{0,2}$	$u_{0,3}$
$u_{1,0}$	$u_{1,1}$	$u_{1,2}$	$u_{1,3}$
$u_{2,0}$	$u_{2,1}$	$u_{2,2}$	$u_{2,3}$
$u_{3,0}$	$u_{3,1}$	$u_{3,3}$	$u_{3,3}$

$v_{0,0}$	$v_{0,1}$	$v_{0,2}$	$v_{0,3}$
$v_{1,0}$	$v_{1,1}$	$v_{1,2}$	$v_{1,3}$
$v_{2,0}$	$v_{2,1}$	$v_{2,2}$	$v_{2,3}$
$v_{3,0}$	$v_{3,1}$	$v_{3,3}$	$v_{3,3}$







- Трудоёмкость атаки без рассмотрения алгоритма развертывания ключа равна 2^{133} шифрований при наличии 2^{32} открытых текстов.
- Количество вариантов разбиения ключа в последнем раунде равно 3.
- Существует класс алгоритмов развертывания ключа, при которых возможно снижение трудоёмкости данной атаки до 2^{117}.
- Для простейших алгоритмов развертывания ключа, трудоёмкость атаки, возможно, понизить до 2^{101}.

Рассмотрение зависимостей раундовых ключей W

Аналогично зависимостям алгоритма AES

- Трудоёмкость атаки без рассмотрения алгоритма развертывания ключа равна 2^{389} шифрований при наличии 2^{64} открытых текстов.
- Количество вариантов разбиения ключа в последнем раунде равно 35.
- Существует класс алгоритмов развертывания ключа, при которых возможно снижение трудоёмкости данной атаки до 2^{357}.
- Для простейших алгоритмов развертывания ключа, трудоёмкость атаки, возможно, понизить до 2^{325}.

Потенциальное применение атаки

Размер ключа, бит	Трудоемкость полного перебора ключа	Трудоемкость атаки
128	2^{128}	2^{133}
512	2^{512}	2^{389}
1024	2^{1024}	$\sim 2^{700}$

Спасибо за внимание.