УДК 004.056.55:512.6

S-ФУНКЦІЇ ІЗ ЗАБУВАННЯМ ТА ЇХ СТІЙКІСТЬ ДО ОБЕРТАЛЬНОГО КРИПТОАНАЛІЗУ

С. В. Яковлєв[1,а], І. В. Волошин[1,б]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У даній роботі розглядається новий клас ARX-примітивів: S-функції із забуванням, головною особливістю яких є відсутність залежності між станами обчислень. Для S-функцій із забуванням у загальному випадку було знайдено вирази для імовірностей пар обертання, які характеризують стійкість до обертального криптоаналізу. Розглянуто два класи спеціального виду S-функцій із забуванням, для яких знайдено чисельні значення імовірностей усіх пар обертання.

Ключові слова: симетрична криптографія, ARX-криптосистема, обертальний криптоаналіз, S-функція

Вступ

Застосування ARX-криптосистем набуло популярності в останні роки, в першу чергу, через їх швидкість та простоту реалізації. Такі криптосистеми можуть бути легко адаптовані під будь-яку архітектуру апаратного забезпечення. ARX-криптосистеми широко використовуються у шифруванні даних на хмарних платформах, організації захищених інтернет-з'єднань, захисті даних банківських карток, забезпеченні швидкої криптографії у VPN.

Обертальний криптоаналіз ARX-систем [1, 2] досліджує зміни, які відбуваються із даними, що відрізняються циклічними зсувами, під час обчислення ARX-перетворень. Хоча обертальний криптоаналіз з усіх симетричних криптопримітивів практично застосовний тільки до ARX-систем, стійкість до нього є необхідною умовою для усіх сучасних легких шифрів.

У роботі [3] була запропонована концепція S-функції — представлення ARX-перетворення як скінченного автомату спеціального виду. S-функції дозволяють будувати обчислювально ефективні алгоритми для знаходження розподілів та статистик ARX-перетворень.

У даній роботі розглядається спеціальний клас S-функцій — S-функції із забуванням. Буде знайдено вирази для обчислення імовірностей пар обертання, які характеризують стійкість таких S-функцій до обертального криптоаналізу.

1. Терміни та означення

Введемо позначення, необхідні для подальшого викладення матеріалу.

$V_n = \{0,1\}^n$ — множина двійкових векторів довжини n.

$x \in V_n$ — довільний вектор, біти якого пронумеровані в такому порядку : $x = (x_{n-1}, \dots, x_0)$;

$x \lll r$ або x^r — циклічний зсув (обертання) вектора x вліво на r позицій;

$x \ll r$ — нециклічний зсув вектора x вліво на r позицій;

$x \oplus y$ — операція побітового додавання;

$x \wedge y$ — кон'юкція; $x \vee y$ — диз'юнкція;

$x \downarrow y$ — стрілка Пірса; $x \uparrow y$ — штрих Шеффера;

$x \to y$, $x \leftarrow y$ — імплікація та зворотна імплікація;

$x \nrightarrow y$, $x \nleftarrow y$ — заперечення імплікацій.

ARX–криптосистеми (від «Additon, Rotation, XOR») використовують в своїй будові тільки операції модульного додавання, побітового додавання та циклічного зсуву; іноді також використовуються інші операції, доступні на рівні інструкцій процесорів ($\vee$, $\wedge$, $\ll$ тощо).

Криптоаналіз на основі обертань (або *обертальний криптоаналіз*) — метод криптоаналізу ARX-криптосистем, який ґрунтується на вивченні властивостей так званих *пар обертання* — пар векторів (X, X^r), де r — довільне, але фіксоване значення.

Нехай $f : V_n \times V_n \to V_n$. Стійкість відображення f до обертального криптоаналізу визначається величиною $rp^f(r)$, де

$$rp^f(r) = \Pr_{x,y}\{f(x^r, y^r) = (f(x,y))^r\}.$$

Функція f виду $f : V_n \times V_n \to V_n$ називається *S-функцією* (*S-function*) [3] , якщо існують такий додатковий параметр $S = (S_0, S_1, \dots, S_{n-1}) \in Q^n$ і такі відображення φ та ψ, що обчислення вектору $z = f(x,y)$ можна представити як

$$z_i = \varphi(x_i, y_i, S_i),$$
$$S_{i+1} = \psi(x_i, y_i, S_i),$$

де множина Q є скінченною і не змінюється із збільшенням n, а початкове значення S_0 зафіксоване.

[а] yasv@rl.kiev.ua
[б] igovol-ipt25@lll.kpi.ua

Величини $S_i \in Q$ називають *станами обчислення* S-функції, φ — *функцією виходу*, ψ — *функцією переходу*.

2. S-функцій із забуванням та імовірності пар обертання

Розглянемо спеціальний клас S-функцій — *S-функції із забуванням* (*oblivious S-function*), у яких значення наступного стану визначається лише бітами входу:

$$\forall i > 0 : \; S_{i+1} = \psi(x_i, y_i).$$

Прикладами S-функцій із забуванням є досліджене у [4] сімейство відображень $f(x) = x \star (x \ll 1)$, де $\star$ позначає довільну побітову операцію, та функція $\mathsf{H}(x, y) = x \oplus y \oplus (xy \ll 1)$, запропонована розробниками шифру NORX [5] як апроксимація модульного додавання.

Для S-функцій із забуванням можна виразити усі імовірності пар обертання у загальному випадку. Сформулюємо цей результат у такій теоремі.

Теорема 1. Нехай $f(x, y)$ є S-функцією із забуванням з функцією виходу φ, функцією переходу ψ та початковим станом S_0. Для векторів $x, y \in V_n$ та $i \geq 1$ позначимо $S_i = \psi(x_{i-1}, y_{i-1})$. Тоді

$$rp^f(r) = \Pr\{\varphi(x_0, y_0, S_0) = \varphi(x_0, y_0, S_n), \\ \varphi(x_{n-r}, y_{n-r}, S_0) = \varphi(x_{n-r}, y_{n-r}, S_{n-r})\}.$$

Доведення. Позначимо $u = f(x^r, y^r)$; маємо:

$$\begin{aligned} i = 0 :&\; u_0 = \varphi(x_{n-r}, y_{n-r}, S_0), \\ 0 < i < r :&\; u_i = \varphi(x_{n-r+i}, y_{n-r+i}, S_{n-r+i}), \\ i = r :&\; u_r = \varphi(x_0, y_0, S_n), \\ r < i < n :&\; u_i = \varphi(x_{i-r}, y_{i-r}, S_{i-r}); \end{aligned}$$

аналогічно для $v = (f(x, y))^r$ маємо:

$$\begin{aligned} i = 0 :&\; v_0 = \varphi(x_{n-r}, y_{n-r}, S_{n-r}), \\ 0 < i < r :&\; v_i = \varphi(x_{n-r+i}, y_{n-r+i}, S_{n-r+i}), \\ i = r :&\; v_r = \varphi(x_0, y_0, S_0), \\ r < i < n :&\; v_i = \varphi(x_{i-r}, y_{i-r}, S_{i-r}). \end{aligned}$$

Отже, маємо $u_i = v_i$ для усіх $i \neq 0$, $i \neq r$; таким чином,

$$rp^f(r) = \Pr\{u = v\} = \\ = \Pr\{u_0 = v_0, u_r = v_r\},$$

звідки, підставляючи значення u_0, u_r, v_0, v_r, одержуємо твердження теореми. □

Зауважимо, що характерною особливістю імовірностей пар обертання S-функцій із забуванням є те, що вони не залежать від довжин векторів. Більш того, у випадку $2 \leq r \leq n-2$ рівності $u_0 = v_0$ та $u_r = v_r$ визначаються різними бітами векторів x, y, тобто є незалежними; відповідно, у даному випадку справедлива рівність

$$rp^f(r) = \left(\Pr\{\varphi(a, b, S_0) = \varphi(a, b, \psi(a', b'))\}\right)^2,$$

де $a, a', b, b' \in_R \{0, 1\}$; зокрема, значення $rp^f(r)$ будуть однакові для усіх $2 \leq r \leq n-2$.

Випадки $r = 1$ та $r = n-1$ треба розглядати окремо, оскільки у них рівняння $u_0 = v_0$ та $u_r = v_r$ є залежними.

3. Імовірності пар обертання S-функцій спеціального виду

У даній роботі буде розглянуто два типи ARX-перетворень:

$$f_\star(x, y) = x \oplus y \oplus (x \star (y \ll 1)) \oplus (y \star (x \ll 1));$$
$$g_\star(x, y) = x \oplus y \oplus (x \star (x \ll 1)) \oplus (y \star (y \ll 1)),$$

де $\star$ позначає деяку побітову операцію над двійковими векторами; у подальшому будуть розглядатись операції з множини $\mathbb{O} = \{\wedge, \vee, \downarrow, \uparrow, \to, \leftarrow, \nrightarrow, \nleftarrow\}$.

Твердження 1. Імовірності пар обертання функцій типу $f_\star(x, y)$, де $\star \in \mathbb{O}$, дорівнюють 3/8, 7/16 або 25/64; точні значення наведено у таблиці 1.

Таблиця 1. Імовірності пар обертання для $f_\star$

	$rp^{f_\star}(1)$, $rp^{f_\star}(n-1)$	$rp^{f_\star}(r)$, $2 \leq r \leq n-2$
$\wedge$	$\frac{7}{16}$	$\frac{25}{64}$
$\vee$	$\frac{3}{8}$	$\frac{25}{64}$
$\downarrow$	$\frac{3}{8}$	$\frac{25}{64}$
$\uparrow$	$\frac{7}{16}$	$\frac{25}{64}$
$\to$	$\frac{7}{16}$	$\frac{25}{64}$
$\leftarrow$	$\frac{3}{8}$	$\frac{25}{64}$
$\nrightarrow$	$\frac{7}{16}$	$\frac{25}{64}$
$\nleftarrow$	$\frac{3}{8}$	$\frac{25}{64}$

Доведення. Покажемо, що $f_\star$ є S-функцією із забуванням. Дійсно, можна побудувати таке представлення:

- множина станів: $Q = V_2$, стан $S_i = (a_i, b_i)$;
- початковий стан $S_0 = (0, 0)$;
- функція переходу

$$S_{i+1} = \psi(x_i, y_i) = (x_i, y_i);$$

- функція виходу

$$z_i = \varphi(x_i, y_i, S_i) = x_i \oplus y_i \oplus (x_i \star b_i) \oplus (y_i \star a_i).$$

Відповідно, за теоремою 1 імовірність $rp^{f_\star}(r)$ дорівнює імовірності виконання системи співвідношень

$$\begin{cases} \varphi(x_0, y_0, S_0) = \varphi(x_0, y_0, \psi(x_{n-1}, y_{n-1})), \\ \varphi(x_{n-r}, y_{n-r}, S_0) = \varphi(x_{n-r}, y_{n-r}, \psi(x_{n-r-1}, y_{n-r-1})). \end{cases}$$

Після підстановки виразів φ та ψ одержуємо таку систему співвідношень:

$$\begin{cases} (x_0 \star 0) \oplus (y_0 \star 0) \oplus \\ \qquad \oplus (x_0 \star y_{n-1}) \oplus (y_0 \star x_{n-1}) = 0, \\ (x_{n-r} \star 0) \oplus (y_{n-r} \star 0) \oplus \\ \qquad \oplus (x_{n-r} \star y_{n-r-1}) \oplus (y_{n-r} \star x_{n-r-1}) = 0. \end{cases}$$

Імовірність виконання даної системи для кожної операції $\star \in \mathbb{O}$ та кожного значення r знаходиться безпосередньо шляхом побудови відповідних таблиць істинності. □

Твердження 2. Імовірності пар обертання функцій типу $g_\star(x, y)$, де $\star \in \mathbb{O}$, дорівнюють 3/8, 7/16 або 25/64; точні значення наведено у таблиці 2.

Таблиця 2. Імовірності пар обертання для $g_\star$

	$rp^{g\star}(1)$, $rp^{g\star}(n-1)$	$rp^{g\star}(r)$, $2 \le r \le n-2$
$\wedge$	$\frac{7}{16}$	$\frac{25}{64}$
$\vee$	$\frac{3}{8}$	$\frac{25}{64}$
$\downarrow$	$\frac{3}{8}$	$\frac{25}{64}$
$\uparrow$	$\frac{7}{16}$	$\frac{25}{64}$
$\rightarrow$	$\frac{7}{16}$	$\frac{25}{64}$
$\leftarrow$	$\frac{3}{8}$	$\frac{25}{64}$
$\nrightarrow$	$\frac{7}{16}$	$\frac{25}{64}$
$\nleftarrow$	$\frac{3}{8}$	$\frac{25}{64}$

Доведення. Аналогічно до доведення твердження 1, спочатку покажемо, що $g_\star$ є S-функцією із забуванням. Дійсно, можна побудувати таке представлення:

- множина станів: $Q = V_2$, стан $S_i = (a_i, b_i)$;
- початковий стан $S_0 = (0, 0)$;
- функція переходу

$$S_{i+1} = \psi(x_i, y_i) = (x_i, y_i);$$

- функція виходу

$$z_i = \varphi(x_i, y_i, S_i) = x_i \oplus y_i \oplus (x_i \star a_i) \oplus (y_i \star b_i).$$

Відповідно, за теоремою 1 імовірність $rp^{g\star}(r)$ дорівнює імовірності виконання системи співвідношень

$$\begin{cases} \varphi(x_0, y_0, S_0) = \varphi(x_0, y_0, \psi(x_{n-1}, y_{n-1})), \\ \varphi(x_{n-r}, y_{n-r}, S_0) = \varphi(x_{n-r}, y_{n-r}, \psi(x_{n-r-1}, y_{n-r-1})). \end{cases}$$

За теоремою 1, після підстановки виразів для φ та ψ, одержуємо таку систему співвідношень, яка визначає імовірність $rp^{g\star}(r)$:

$$\begin{cases} (x_0 \star 0) \oplus (y_0 \star 0) \oplus \\ \qquad \oplus (x_0 \star x_{n-1}) \oplus (y_0 \star y_{n-1}) = 0, \\ (x_{n-r} \star 0) \oplus (y_{n-r} \star 0) \oplus \\ \qquad \oplus (x_{n-r} \star x_{n-r-1}) \oplus (y_{n-r} \star y_{n-r-1}) = 0. \end{cases}$$

Після чого імовірність виконання даної системи для кожної операції $\star \in \mathbb{O}$ та кожного значення r знаходиться безпосередньо шляхом побудови відповідних таблиць істинності. □

Наведемо для ілюстрації обчислення імовірностей пар обертання для функції

$$g_{\nrightarrow}(x, y) = x \oplus y \oplus (x \nrightarrow (x \ll 1)) \oplus (y \nrightarrow (y \ll 1)).$$

Легко переконатись, що для $a \in \{0, 1\}$ виконується співвідношення $a \nrightarrow 0 \equiv a$. Відповідно, згідно доведення твердження 2, імовірності $rp^{g_{\nrightarrow}(r)}$ дорівнюють імовірності виконання такої системи рівнянь:

$$\begin{cases} x_0 \oplus y_0 \oplus (x_0 \nrightarrow x_{n-1}) \oplus (y_0 \nrightarrow y_{n-1}) = 0, \\ x_{n-r} \oplus y_{n-r} \oplus (x_{n-r} \nrightarrow x_{n-r-1}) \oplus \\ \qquad \oplus (y_{n-r} \nrightarrow y_{n-r-1}) = 0. \end{cases}$$

У випадку $2 \le r \le n-2$ маємо $rp^{g_{\nrightarrow}}(r) = p^2$, де

$$p = \Pr\{a \oplus b \oplus (a \nrightarrow c) \oplus (b \nrightarrow d) = 0\}. \qquad (1)$$

Таблиця істинності для обчислення імовірності (1) наведена у таблиці 3. З неї маємо, що

$$rp^{g_{\nrightarrow}}(r) = \left(\frac{10}{16}\right)^2 = \frac{25}{64}.$$

Таблиця 3. Таблиця істинності для обчислення імовірності (1); тут $B = a \nrightarrow c$, $C = b \nrightarrow d$, $A = a \oplus b \oplus B \oplus C$. Імовірність p обчислюється як $p = \Pr\{A = 0\}$

a	b	c	d	B	C	A
0	0	0	0	0	0	0
0	0	0	1	0	0	0
0	0	1	0	0	0	0
0	0	1	1	0	0	0
0	1	0	0	0	1	0
0	1	0	1	0	0	1
0	1	1	0	0	1	0
0	1	1	1	0	0	1
1	0	0	0	1	0	0
1	0	0	1	1	0	0
1	0	1	0	0	0	1
1	0	1	1	0	0	1
1	1	0	0	1	1	0
1	1	0	1	1	0	1
1	1	1	0	0	1	1
1	1	1	1	0	0	0

У випадку $r = 1$ маємо таку систему рівнянь для обчислення $rp^{g_{\nrightarrow}}(1)$:

$$\begin{cases} x_0 \oplus y_0 \oplus (x_0 \nrightarrow x_{n-1}) \oplus (y_0 \nrightarrow y_{n-1}) = 0, \\ x_{n-1} \oplus y_{n-1} \oplus (x_{n-1} \nrightarrow x_{n-2}) \oplus \\ \qquad \oplus (y_{n-1} \nrightarrow y_{n-2}) = 0. \end{cases}$$

Відповідно,

$$rp^{g_{\nrightarrow}}(r) = \Pr\{a \oplus b \oplus (a \nrightarrow c) \oplus (b \nrightarrow d) = 0, \quad c \oplus d \oplus (c \nrightarrow e) \oplus (d \nrightarrow f) = 0\}. \qquad (2)$$

Таблиця істинності для обчислення імовірності (1) наведена у таблиці 4. З неї маємо, що

$$rp^{g_{\nrightarrow}}(r) = \frac{28}{64} = \frac{7}{16}.$$

Випадок $r = n-1$ розглядається аналогічно випадку $r = 1$.

Таблиця 4. Таблиця істинності для обчислення імовірності (2); тут $C = a \nrightarrow c$, $D = b \nrightarrow d$, $E = c \nrightarrow e$, $F = d \nrightarrow f$, $A = a \oplus b \oplus C \oplus D$, $B = c \oplus d \oplus E \oplus F$. Жирним шрифтом позначено рядки, які визначають імовірність $\Pr\{A = 0, B = 0\}$.

a	b	c	d	e	f	C	D	E	F	A	B
0	0	0	0	0	0	0	0	0	0	**0**	**0**
0	0	0	0	0	1	0	0	0	0	**0**	**0**
0	0	0	0	1	0	0	0	0	0	**0**	**0**
0	0	0	0	1	1	0	0	0	0	**0**	**0**
0	0	0	1	0	0	0	0	0	1	**0**	**0**
0	0	0	1	0	1	0	0	0	0	0	1
0	0	0	1	1	0	0	0	0	1	**0**	**0**
0	0	0	1	1	1	0	0	0	0	0	1
0	0	1	0	0	0	0	0	1	0	**0**	**0**
0	0	1	0	0	1	0	0	1	0	**0**	**0**
0	0	1	0	1	0	0	0	0	0	0	1
0	0	1	0	1	1	0	0	0	0	0	1
0	0	1	1	0	0	0	0	1	1	**0**	**0**
0	0	1	1	0	1	0	0	1	0	0	1
0	0	1	1	1	0	0	0	0	1	0	1
0	0	1	1	1	1	0	0	0	0	**0**	**0**
0	1	0	0	0	0	0	1	0	0	**0**	**0**
0	1	0	0	0	1	0	1	0	0	**0**	**0**
0	1	0	0	1	0	0	1	0	0	**0**	**0**
0	1	0	0	1	1	0	1	0	0	**0**	**0**
0	1	0	1	0	0	0	0	0	1	1	1
0	1	0	1	0	1	0	0	0	0	1	0
0	1	0	1	1	0	0	0	0	1	1	1
0	1	0	1	1	1	0	0	0	0	1	0
0	1	1	0	0	0	0	1	1	0	**0**	**0**
0	1	1	0	0	1	0	1	1	0	**0**	**0**
0	1	1	0	1	0	0	1	0	0	0	1
0	1	1	0	1	1	0	1	0	0	0	1
0	1	1	1	0	0	0	0	1	1	1	0
0	1	1	1	0	1	0	0	1	0	1	1
0	1	1	1	1	0	0	0	0	1	1	1
0	1	1	1	1	1	0	0	0	0	1	0
1	0	0	0	0	0	1	0	0	0	**0**	**0**
1	0	0	0	0	1	1	0	0	0	**0**	**0**
1	0	0	0	1	0	1	0	0	0	**0**	**0**
1	0	0	0	1	1	1	0	0	0	**0**	**0**
1	0	0	1	0	0	1	0	0	1	**0**	**0**
1	0	0	1	0	1	1	0	0	0	0	1
1	0	0	1	1	0	1	0	0	1	**0**	**0**
1	0	0	1	1	1	1	0	0	0	0	1
1	0	1	0	0	0	0	0	1	0	1	0
1	0	1	0	0	1	0	0	1	0	1	0
1	0	1	0	1	0	0	0	0	0	1	1
1	0	1	0	1	1	0	0	0	0	1	1
1	0	1	1	0	0	0	0	1	1	1	0
1	0	1	1	0	1	0	0	1	0	1	1
1	0	1	1	1	0	0	0	0	1	1	1
1	0	1	1	1	1	0	0	0	0	1	0
1	1	0	0	0	0	1	1	0	0	**0**	**0**
1	1	0	0	0	1	1	1	0	0	**0**	**0**
1	1	0	0	1	0	1	1	0	0	**0**	**0**
1	1	0	0	1	1	1	1	0	0	**0**	**0**
1	1	0	1	0	0	1	0	0	1	1	0
1	1	0	1	0	1	1	0	0	0	1	1
1	1	0	1	1	0	1	0	0	1	1	0
1	1	0	1	1	1	1	0	0	0	1	1
1	1	1	0	0	0	0	1	1	0	1	0
1	1	1	0	0	1	0	1	1	0	1	0
1	1	1	0	1	0	0	1	0	0	1	1
1	1	1	0	1	1	0	1	0	0	1	1
1	1	1	1	0	0	0	0	1	1	**0**	**0**
1	1	1	1	0	1	0	0	1	0	0	1
1	1	1	1	1	0	0	0	0	1	0	1
1	1	1	1	1	1	0	0	0	0	**0**	**0**

Висновки

У даній роботі введено новий ARX-примітив — S-функцію із забуванням. У таких S-функцій стани обчислення залежать тільки від вхідних аргументів і не залежать від попередніх станів, тому S-функції із забуванням відрізняються спрощеною схемою обчислення.

Для S-функцій із забуванням було одержано загальний вираз для імовірностей пар обертання — параметру, який характеризує стійкість до обертального криптоаналізу. Показано, що значення таких імовірностей не залежать від довжин вхідних векторів і приймають лише два різних значення, в залежності від величини обертання. Для двох класів S-функцій із забуванням вичерпно обчислені усі імовірності пар обертання.

Одержані результати можна використати для побудови нових ARX-криптосистем із оцінками гарантованої стійкості до обертального криптоаналізу.

Перелік використаних джерел

1. *Khovratovich D.*, *Nikolic I.* Rotational Cryptanalysis of ARX // Fast Software Encryption FSE 2010. — Springer, 2010. — С. 333—346. — (Lecture Notes in Computer Science, vol. 6147). — DOI: 10.1007/978-3-642-13858-4_19.
2. Rotational Cryptanalysis of ARX Revisited / D. Khovratovich, I. Nikolić, J. Pieprzyk, P. Sokołowski, R. Steinfeld // Fast Software Encryption. — Springer Berlin Heidelberg, 2015. — С. 519—536. — ISBN 9783662481165. — DOI: 10.1007/978-3-662-48116-5_25.
3. The Differential Analysis of S-Functions / N. Mouha, V. Velichkov, C. De Cannière, B. Preneel // Selected Areas in Cryptography / за ред. A. Biryukov, G. Gong, D. Stinson. — Springer, 2011. — С. 36—56. — ISBN 978-3-642-19574-7. — DOI: 10.1007/978-3-642-19574-7_3.
4. *Яковлєв С.*, *Кобець Д.* Обертальний криптоаналіз деяких функцій ускладнення ARX-криптосистем // Proceedings of International Conference on Innovative Solutions in Software Engineering (ICISSE 2023, Nov. 29–30, 2023, Ivano-Frankivsk, Ukraine). — Vasyl Stefanyk Precarpathian National University. 2023. — С. 101—104.
5. *Aumasson J.-P.*, *Jovanovic P.*, *Neves S.* Analysis of NORX: Investigating Differential and Rotational Properties // Progress in Cryptology – LATINCRYPT 2014 / за ред. D. F. Aranha, A. Menezes. — Springer International Publishing, 2015. — С. 306—324. — ISBN 978-3-319-16295-9.