Списание „Математика, компютърни науки и образование“ Том 9, кн. 1, 2026
Journal of Mathematics, Computer Science and Education Vol. 9, No. 1, 2026

DOI: 10.54664/AOJS8646

КРИПТОГРАФСКИ СВОЙСТВА НА БУЛЕВИТЕ ФУНКЦИИ

Теодора Тодорова

CRYPTOGRAPHIC PROPERTIES OF BOOLEAN FUNCTIONS

Teodora Todorova

Abstract: *This paper presents the main cryptographic properties of Boolean functions, which play a crucial role in the design of modern cryptographic algorithms. The study includes representations such as truth tables and algebraic normal forms. Special focus is given to analyzing essential properties including balancedness, nonlinearity, correlation immunity, resiliency, and the avalanche effect. A detailed case analysis of a sample Boolean function illustrates the impact of these properties on resistance to cryptanalytic attacks. The results highlight the importance of achieving a balance between different properties in the construction of secure Boolean functions.*

Keywords: *Boolean functions, cryptographic properties, nonlinearity, balancedness, resiliency, avalanche effect, correlation immunity.*

1 Въведение

Булевите функции са основен математически инструмент, използван в областта на дискретната математика и компютърните науки. Формално, булева функция на n променливи е функция $f : \{0,1\}^n \to \{0,1\}$, като всяка комбинация от входни стойности се изобразява в единствен изход — 0 или 1. Заради своята опростена структура и двоичен характер, булевите функции се използват широко в логически схеми, цифрови системи и имат особено значима роля в криптографията.

В съвременната криптография булевите функции играят ключова роля при проектирането на криптографски примитиви като поточни шифри, хеш функции и блокови шифри. При тези примитиви именно булевите функции изграждат нелинейните преобразувания, които осигуряват устойчивост срещу различни видове криптоаналитични атаки. Например, в блоковите шифри AES (Advanced Encryption Standard) и DES (Data Encryption Standard) S-кутии (substitution boxes) се реализират чрез сложни булеви функции, които придават нелинейност и лавинен ефект. В поточни шифри като Grain и Trivium булевите функции изграждат нелинейни обратни връзки в LFSR и NLFSR регистри. При хеш алгоритмите от семействата SHA-2 и SHA-3 булеви операции (XOR, AND, OR, NOT) и по-сложни комбинации от тях гарантират равномерност и непредсказуемост на изхода.

За да се гарантира сигурността на криптографските алгоритми, булевите функции, които ги изграждат, трябва да притежават определени свойства, които ги правят устойчиви

на различни видове атаки. Сред най-важните криптографски свойства са нелинейността, балансираността, устойчивостта (resiliency), пропагиращото свойство (avalanche effect) и корелационната имунност. Липсата на подходяща стойност на някое от тези свойства може да доведе до компрометиране на криптографската система.

Изследването на криптографските свойства на булеви функции е от съществено значение за осигуряване на високо ниво на сигурност в комуникационните и информационните системи. Чрез анализа и конструирането на булеви функции с добри криптографски характеристики, се изграждат по-надеждни алгоритми, способни да устоят на съвременните криптоаналитични методи. Затова темата за криптографските свойства на булевите функции представлява важна и актуална насока както в теоретичните, така и в приложните аспекти на криптографията.

2 Начини на представяне на булеви функции

Булевите функции могат да бъдат представени по различни начини, като всеки от тях има своето приложение в анализа и синтеза на логически схеми и криптографски алгоритми. Двата най-разпространени метода за представяне са таблицата на истинност (*True Table - TT*) и алгебричната нормална форма (*Algebraic Normal Form - ANF*).

2.1 Таблица на истинност

Таблицата на истинност е най-интуитивният начин за описание на булева функция. Тя представя изходите при всички възможни стойности на входа. За булева функция на n променливи съществуват 2^n различни входни комбинации [2, 5].

Този вид представяне е особено полезно за визуализиране на пълното поведение на функцията и за директна проверка на нейните свойства, като балансираност или симетрия.

Пример 1. *Нека разгледаме булева функция на две променливи $f(x_1, x_2)$. В Таблица 1 е изобразена таблицата на истинност за такава функция:*

Таблица 1: Таблица на истинност за булевата функция $f(x_1, x_2)$

x_1	x_2	$f(x_1, x_2)$
0	0	1
0	1	1
1	0	0
1	1	1

2.2 Алгебрична нормална форма

В алгебричната нормална форма булевата функция се записва като полином над крайното поле $\mathbb{F}_2$, използвайки операцията AND (умножение) и XOR (сума по модул 2). Двете операции са представени в Таблица 2:

Таблица 2: Операции умножение и сума по модул 2

$\cdot$	0	1
0	0	0
1	0	1

$\oplus$	0	1
0	0	1
1	1	0

В ANF булевата функция се изразява като сума (по модул 2) от произведения на променливи. Формално:

$$f(x_1, x_2, \cdots, x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus a_{1,2} x_1 x_2 \oplus \cdots \oplus a_{1,2,\cdots,n} x_1 x_2 \cdots x_n, \tag{1}$$

където коефициентите a_i принадлежат на полето F_2.

Пример 2. *Алгебричната нормална форма за функцията от Таблица 1:*

$$f(x_1, x_2) = 1 \oplus x_1 \oplus x_1 x_2$$

Алгебричната нормална форма е особено важна в криптографията, тъй като степента на полинома в ANF определя алгебричната степен на функцията — един от основните параметри, които влияят на нейната устойчивост срещу определени видове атаки, като алгебрични атаки.

3 Криптографски свойства на булевите функции

3.1 Балансираност (Balancedness)

Булева функция е балансирана, ако за всички 2^n входни стойности тя връща 0 и 1 с еднаква честота, т.е. изходът 1 е в точно половината от случаите [1, 3, 4].

Определя се лесно от таблицата на истинност.

Пример 3. *Булева функция на 3 променливи (8 входа) е балансирана, ако изходът съдържа точно 4 единици и 4 нули. Таблица 3 представя функцията* $f(x_1, x_2, x_3) = x_3 \oplus x_1 x_2$, *която е балансирана:*

Таблица 3: Пример за балансирана функция на 3 променливи

x_1	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_3	0	1	0	1	0	1	0	1
TT_f	0	1	0	1	0	1	1	0

Ако функцията не е балансирана, тя има пристрастие — изходът по-често е 0 или 1. Това помага на атакуващия да прави статистически изводи и евентуално да възстанови входа или ключа. Балансираността гарантира, че всеки изход е еднакво вероятен, което е важно за непредсказуемостта.

3.2 Нелинейност (Nonlinearity)

Нелинейността на булева функция измерва колко силно се различава тя от всички линейни и афинни функции.

- Линейна функция има вида [5]:

$$a'(x_1, x_2, \cdots, x_n) = a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n, \tag{2}$$

  където $a_i \in \{0, 1\}$.

- Афинна функция включва и константа [5]:

$$a(x) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n \tag{3}$$

Това различие се измерва чрез разстоянието на Хеминг[1] между дадената функция f и всички възможни афинни функции $a(x)$ [1, 2, 3, 4, 5]. Множеството на всички афинни булеви функции означаваме с *Affine* :

$$NL(f) = \min_{a \in Affine} d_H(f, a) \tag{4}$$

Колкото по-голямо е това разстояние, толкова по-висока е нелинейността, и съответно функцията е по-сигурна.

Нелинейността може да се изрази и чрез Уолш спектъра на функцията. За всяка булева функция $f : \{0,1\}^n \to \{0,1\}$, Уолш коефициентът се дефинира като:

$$W_f(a') = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus a'.x}, \tag{5}$$

където $a'.x = a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n$ е скаларното произведение по модул 2. Тогава нелинейността се изчислява чрез следната формула:

$$NL(f) = 2^{n-1} - \frac{1}{2} \max_{a' \in \{0,1\}^n} |W_f(a')| \tag{6}$$

Тази формула показва, че колкото по-малки са абсолютните стойности на Уолш коефициентите, толкова по-далеч е функцията от всяка афинна функция и толкова по-висока е нейната нелинейност.

Линейният криптоанализ използва линейни апроксимации, за да предсказва поведението на шифри. Нелинейността пречи на атакуващия да направи такива приближения, като по този начин защитава шифъра.

3.3 Корелационен имунитет (Correlation Immunity)

Функцията е корелационно имунна от ред t, ако изходът е статистически независим от всяка комбинация на t или по-малко входни променливи [1, 4].

Атакуващите използват корелации между определени входове и изхода, за да отгатнат части от ключа (например в поточни шифри). Корелационният имунитет защитава срещу такива атаки, като елиминира статистическите връзки между изхода и входовете.

Пример 4. *Функция от* 6 *променливи е* 2*-корелационно имунна, ако знанието на която и да е комбинация от* 2 *входни променливи не дава информация за изхода.*

Корелационният имунитет на булева функция f може да бъде определен чрез нейния Уолш спектър $W_f(a)$. Функцията $f : \{0,1\}^n \to \{0,1\}$ е корелационно имунна от ред t, ако:

$$W_f(a) = 0 \tag{7}$$

за всяко $a \in \{0,1\}^n$ с $1 \leq wt(a) \leq t$, където $wt(a)$ е теглото на вектора a (брой ненулеви координати), Ненулева стойност на $W_f(a)$ за вектора a с тегло $\leq t$ означава наличие на корелация между изхода и съответното подмножество от входни променливи, което нарушава условието за имунитет от този ред.

3.4 Устойчивост (Resiliency)

Устойчивостта комбинира балансираност и корелационен имунитет [5]. Функцията е m-устойчива, ако е балансирана и остава балансирана, когато до m входни променливи са фиксирани (т.е. при частично известен вход) [1].

[1] Хеминговото разстояние е броят на различията между стойностите на две функции върху всички входове.

Пример 5. *Да разгледаме булева функция от* 5 *променливи. Ако е* 2*-устойчива, за всяка комбинация от* 2 *фиксирани променливи, функцията остава балансирана върху останалите* 3*. Това означава, че знанието на* 2 *входа не дава предимство при предсказване на изхода.*

В поточни шифри, ако атакуващият знае част от ключа (или входа), не трябва да може да предвиди нищо за изхода. Устойчивостта е комбинирано свойство – изисква и балансираност, и корелационен имунитет.

3.5 Пропагиращо свойство (Avalanche Effect)

Пропагиращото свойство, известно още като ефект на лавината (avalanche effect), е важно криптографско свойство, което описва чувствителността на булева функция (или на криптографски алгоритъм като цяло) към малки промени във входа. Ефектът на лавината гласи, че ако се промени само един бит във входа на функцията, изходът трябва да се промени значително — в идеалния случай, около половината от изходните битове трябва да се обърнат (променят стойността си) [4].

За булеви функции това означава, че ако $f : \{0,1\}^n \to \{0,1\}$, то функцията има добро пропагиращо свойство, ако всяка промяна на стойността на променлива x_i, причинява промяна в изхода на функцията с вероятност близка до 0.5.

Пропагиращото свойство (ефект на лавината) гарантира, че булевата функция реагира "хаотично"и непредвидимо на малки промени във входа, което я прави по-устойчива на криптоанализ и по-подходяща за използване в сигурни криптографски системи. Без лавинен ефект, криптоанализът може да отгатне структурата на алгоритъма, като анализира как малки промени във входа влияят на изхода.

3.6 Обобщение на криптографските свойства

Таблица 4 представя обобщение на разгледаните по-горе свойства на булевите функции:

Таблица 4: Обобщение на основни криптографски свойства на булевите функции

Свойство	**Защита от**	**Какво измерва**
Нелинейност	Линеен криптоанализ	Разстояние до афинни функции
Балансираност	Пристрастие в изхода	Равномерно разпределение на 0 и 1
Устойчивост	Атаки с частично известен вход	Балансираност при фиксирани променливи
Лавинен ефект	Диференциални атаки	Силна реакция на минимална промяна
Корелационен имунитет	Корелационен криптоанализ	Липса на статистическа зависимост

Въпреки че всяко от изброените свойства играе важна роля за осигуряване на криптографска устойчивост, на практика често се наблюдава компромис между тях. Например, увеличаването на нелинейността на булевата функция — ключов фактор за защита срещу линеен криптоанализ — може да доведе до намаляване на устойчивостта или корелационния имунитет. Също така, постигането на висока степен на устойчивост обикновено изисква определени ограничения върху броя на променливите, което може да ограничи лавинния ефект. Тези взаимни зависимости налагат търсене на баланс между свойствата, при който функцията не оптимизира едно свойство за сметка на пълна загуба на друго. В този контекст проектирането на булеви функции с добри криптографски качества представлява оптимизационна задача, при която се търси най-добрият възможен компромис в зависимост от конкретното приложение и заплахите, срещу които се цели защита.

4 Анализ на примерна булева функция

В този раздел ще направим анализ на примерна булева функция. Нека разгледаме функцията на 3 променливи: $f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1$. Представяме функцията чрез таблицата на истинност - изчисляваме $f(x_1, x_2, x_3)$ за всички $2^3 = 8$ входни комбинации, като резултатите са систематизирани в Таблица 5:

Таблица 5: Таблица на истинност за $f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1$

x_1	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_3	0	1	0	1	0	1	0	1
TT_f	0	0	0	1	1	1	0	1

Балансираност
Функция е балансирана, ако броят на нули и единици в изхода е равен. При $n = 3$ имаме 8 входа $\rightarrow$ търсим 4 нули и 4 единици.
Изходът на f: 4 нули, 4 единици. Следователно, функцията е балансирана.

Нелинейност
Нелинейността $NL(f)$ се дефинира като минималното Хемингово разстояние между функцията f и всяка афинна функция $a(x)$:

$$NL(f) = \min_{a \in Affine} d_H(f, a),$$

където $d_H(f, a)$ е броят позиции, в които f и a се различават.

Всички афинни функции с 3 променливи са от вида:

$$a(x_1, x_2, x_3) = a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3$$

Общо има $2^4 = 16$ такива.

Изчисляваме Хеминговото разстояние между f и всяка афинна функция - резултатите са систематизирани в Таблица 6. Най-малкото от тези разстояния е нелинейността.

Таблица 6: Разстояние на Хеминг между f и афинните функции

вход	000	001	010	011	100	101	110	111	Разлика
$a_{0000}(x) = 0$	0	0	0	0	0	0	0	0	$d_H(f, a_{0000}) = 4$
$a_{1000}(x) = 1$	1	1	1	1	1	1	1	1	$d_H(f, a_{1000}) = 4$
$a_{0100}(x) = x_1$	0	0	0	0	1	1	1	1	$d_H(f, a_{0100}) = 2$
$a_{1100}(x) = 1 \oplus x_1$	1	1	1	1	0	0	0	0	$d_H(f, a_{1100}) = 6$
$a_{0010}(x) = x_2$	0	0	1	1	0	0	1	1	$d_H(f, a_{0010}) = 4$
$a_{1010}(x) = 1 \oplus x_2$	1	1	0	0	1	1	0	0	$d_H(f, a_{1010}) = 4$
$a_{0110}(x) = x_1 \oplus x_2$	0	0	1	1	1	1	0	0	$d_H(f, a_{0110}) = 2$
$a_{1110}(x) = 1 \oplus x_1 \oplus x_2$	1	1	0	0	0	0	1	1	$d_H(f, a_{1110}) = 6$
$a_{0001}(x) = x_3$	0	1	0	1	0	1	0	1	$d_H(f, a_{0001}) = 2$
$a_{1001}(x) = 1 \oplus x_3$	1	0	1	0	1	0	1	0	$d_H(f, a_{1001}) = 6$
$a_{0101}(x) = x_1 \oplus x_3$	0	1	0	1	1	0	1	0	$d_H(f, a_{0101}) = 4$
$a_{1101}(x) = 1 \oplus x_1 \oplus x_3$	1	0	1	0	0	1	0	1	$d_H(f, a_{1101}) = 4$
$a_{0011}(x) = x_2 \oplus x_3$	0	1	1	0	0	1	1	0	$d_H(f, a_{0011}) = 6$
$a_{1011}(x) = 1 \oplus x_2 \oplus x_3$	1	0	0	1	1	0	0	1	$d_H(f, a_{1011}) = 2$
$a_{0111}(x) = x_1 \oplus x_2 \oplus x_3$	0	1	1	0	1	0	0	1	$d_H(f, a_{0111}) = 4$
$a_{1111}(x) = 1 \oplus x_1 \oplus x_2 \oplus x_3$	1	0	0	1	0	1	1	0	$d_H(f, a_{1111}) = 4$
$f(x) = x_1x_2 \oplus x_2x_3 \oplus x_1$	0	0	0	1	1	1	0	1	

Изчислявайки за всички афинни функции, намираме: $NL(f) = 2$.

Корелационен имунитет

Една булева функция $f : \{0,1\}^n \to \{0,1\}$ е от корелационна степен t, ако стойността на f е статистически независима от всяко непразно подмножество от максимум t входни променливи. Корелационният имунитет се проверява чрез коефициента на Уолш за вектор $a \in \{0,1\}^n$ с тегло $\leq t$:

$$W_f(a) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus a.x},$$

където $a.x = a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n$

Ще проверим дали $f(x)$ има корелационен имунитет от ред 1 като изчислим коефициента на Уолш за вектори $a \in \{0,1\}^3$ с тегло $wt(a) = 1$. Ако коефициентът на Уолш е нулев, следователно функцията е независима и има корелационен имунитет от ред 1.

Таблица 7: Таблица на истинност за $f(x) \oplus a.x$ и $W_f(a)$

$x_1x_2x_3$	$f(x) \oplus x_1$	$f(x) \oplus x_2$	$f(x) \oplus x_3$	$(-1)^{f(x) \oplus x_1}$	$(-1)^{f(x) \oplus x_2}$	$(-1)^{f(x) \oplus x_3}$
000	0	0	0	1	1	1
001	0	0	1	1	1	-1
010	0	1	0	1	-1	1
011	1	0	0	-1	1	1
100	0	1	1	1	-1	-1
101	0	1	0	1	-1	1
110	1	1	0	-1	-1	1
111	0	0	0	1	1	1
				$W_f(100) = 4$	$W_f(010) = 0$	$W_f(001) = 4$

Резултатите от изчисленията на коефициента на Уолш, представени в Таблица 7, показват, че

- $W_f(100) \neq 0$, следователно функцията f зависи от x_1;
- $W_f(001) \neq 0$, следователно функцията f зависи от x_3

Функцията f има корелационен имунитет от ред 0, т.е. не е статистически независима от никоя единична променлива.

Устойчивост

Булева функция е t-устойчива, ако е балансирана и статистически независима от всяка комбинация от $\leq t$ променливи.

Проверяваме дали функцията f е устойчива като фиксираме една променлива (1-устойчивост). Фиксираме $x_1 = 0$, както е показано на Таблица 8:

Таблица 8: Таблица на истинност за $f(x)$ при фиксирана променлива $x_1 = 0$

x_2	x_3	$f(0, x_2, x_3) = x_2 x_3$
0	0	0
0	1	0
1	0	0
1	1	1

Изходът се състои от 3 нули и 1 единица, следователно функцията f не е балансирана при фиксиране на една променлива (не е 1-устойчива). Оттук следва, че функцията не е t-устойчива за всяко t: $1 \leq t \leq 3$.“

Пропагиращо свойство
Булева функция f удовлетворява свойството, ако при промяна на всяка една отделна променлива на входа, стойността на функцията се променя с вероятност 0.5, т.е. за половината от входовете резултатът се променя. Нека извършим ръчна проверка на пропагиращото свойство за функцията $f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_1$. За целта конструираме таблица на истинност с всички 8 възможни входни комбинации. За всяка от тях изчисляваме стойността на функцията. След това, за всяка от трите променливи поотделно, обръщаме стойността (от 0 на 1 или от 1 на 0), като останалите две променливи остават непроменени, и пресмятаме отново стойността на функцията. Сравняваме двете стойности – преди и след промяната – и отбелязваме дали се е променила.

Таблица 9: Таблица на истинност за $f(x)$ при промяна на входна променлива x_i

$x_1x_2x_3$	$f(x)$	$f_1 : x_1' = x_1 \oplus 1$	$f_2 : x_2' = x_2 \oplus 1$	$f_3 : x_3' = x_3 \oplus 1$
000	0	$f(100) = 1$	$f(010) = 0$	$f(001) = 0$
001	0	$f(101) = 1$	$f(011) = 1$	$f(000) = 0$
010	0	$f(110) = 0$	$f(000) = 0$	$f(011) = 1$
011	1	$f(111) = 1$	$f(001) = 0$	$f(010) = 0$
100	1	$f(000) = 0$	$f(110) = 0$	$f(101) = 1$
101	1	$f(001) = 0$	$f(111) = 1$	$f(100) = 1$
110	0	$f(010) = 0$	$f(100) = 1$	$f(111) = 1$
111	1	$f(011) = 1$	$f(101) = 1$	$f(110) = 0$

Данните в Таблица 9 показват, че:

- промяна на x_1 води до промяна на изхода в 4 от 8 случая (50%);
- промяна на x_2 води до промяна на изхода в 4 от 8 случая (50%);
- промяна на x_3 води до промяна на изхода в 4 от 8 случая (50%)

Функцията удовлетворява пропагиращото свойство.

5 Заключение и бъдеща работа

Изучаването на булевите функции и техните криптографски свойства е от съществено значение за изграждането на надеждни криптографски механизми. Всеки от анализираните показатели – нелинейност, устойчивост, корелационен имунитет и т.н. – има пряко отражение върху устойчивостта на шифри срещу специфични видове атаки. Балансирането между тези свойства изисква прецизно проектиране и често води до компромиси. С нарастващите изисквания към сигурността в цифровия свят, разработването на нови булеви функции с оптимални характеристики остава активна и предизвикателна научна област, с широко практическо приложение в съвременните криптографски протоколи и хардуерни решения.

В бъдеща работа може да се разгледа проектирането на булеви функции с оптимизиран баланс между криптографските свойства, като се използват еволюционни алгоритми или методи от машинното обучение. Също така би било полезно да се изследват по-сложни булеви функции с повече променливи и тяхното поведение при реални криптографски

атаки. Друга възможна насока е автоматизираната оценка на устойчивостта чрез симулация и статистически анализ на големи множества функции. Такива изследвания биха допринесли за разработването на още по-сигурни криптографски системи в практиката.

Литература

[1] Claude Carlet. 2020. *Boolean Functions for Cryptography and Coding Theory.* Cambridge University Press

[2] Augustine Musukwa. 2019. Some cryptographic properties of Boolean functions. Retrieved June 3, 2025 from https://iris.unitn.it/retrieve/handle/11572/246824/290226/Musukwa-Aug-PhD-Thesis-Final.pdf

[3] Isaac López-López, Guillermo Sosa-Gómez, Carlos Segura, Diego Oliva and Omar Rojas. 2020. Metaheuristics in the Optimization of Cryptographic Boolean Functions. Entropy

[4] Chuan-Kun Wu, Dengguo Feng. 2016. Boolean Functions and Their Applications in Cryptography. Springer

[5] Душан Биков. 2017. Криптографски свойства на някои векторни булеви функции и паралелни алгоритми с CUDA

ИНФОРМАЦИЯ ЗА АВТОРА

Теодора Стоянова Тодорова, студент, магистърска програма „Математически структури в информационната сигурност“, Факултет „Математика и информатика“, Великотърновски университет „Св. св. Кирил и Методий“, E-mail: tedi100yanova@gmail.com

ABOUT THE AUTHOR

Teodora Stoyanova Todorova, student, Master Program Mathematical Structures in Information Security, Faculty of Mathematics and Informatics, St. Cyril and St. Methodius University of Veliko Tarnovo, E-mail: tedi100yanova@gmail.com