IP-ЯДРО АЛГОРИТМА ХЕШИРОВАНИЯ СТБ 34.101.31

Гращенко А. И.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Станкевич А. В. – кандидат техн. наук

В работе представлен алгоритм хеширования СТБ 34.101.31 [1]. Данный алгоритм является симметричным блочным алгоритмом, который позволяет обеспечить защиту информации и данных от несанкционированного доступа, кибератак и нарушения целостности данных на территории Республики Беларусь.

Ключевые слова: криптографический алгоритм, шифрование, хеширование, тактовые ключи.

Криптографические алгоритмы являются фундаментальным инструментом в обеспечении защиты данных от несанкционированного доступа и вмешательства [2]. Они предоставляют не только средства для шифрования и защиты конфиденциальности, но и механизмы для контроля целостности данных, обеспечивая гарантии, что информация остается неизменной и недоступной для изменения без разрешения. Только путем постоянного развития и применения современных криптографических методов можно обеспечить надежную защиту информации.

Входными данными алгоритма хеширования является сообщение $X \in \{0, 1\}^*$.

Выходными данными является слово $Y \in \{0, 1\}^{256}$ — хеш-значение сообщения X. К входному сообщению X предварительно добавляется t нулевых символов, где t — минимальное неотрицательное целое число такое, что $|X|+t$ кратно 256. Полученное слово записывается в виде:

$$X \| 0\ t = X1 \| X2 \| \ldots \| Xn,\ |X1| = |X2| = \ldots = |Xn| = 256 \quad (1)$$

Хэширование сообщения X состоит в выполнении следующих шагов:

1 Установить $s \leftarrow 0^{128}$.

2 Установить $h \leftarrow$ B194BAC80A08F53B366D008E584A5DE48504FA9D1BB6C7AC252E72C202FD CE0D$_{16}$, где присваиваемое значение определяется последовательными (слева направо и сверху вниз) элементами первых двух строк таблицы 1.

3 Для $i = 1, 2, \ldots, n$ выполнить:

1) $s \leftarrow s \oplus \sigma1(Xi \| h)$,

2) $h \leftarrow \sigma2(Xi \| h)$.

4 Установить $Y \leftarrow \sigma2(\langle |X| \rangle_{128} \| s \| h)$.

5 Возвратить Y.

Таблица 1 – Подстановка H

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	B1	94	BA	C8	0A	08	F5	3B	36	6D	00	8E	58	4A	5D	E4
1	85	04	FA	9D	1B	B6	C7	AC	25	2E	72	C2	02	FD	CE	0D
2	5B	E3	D6	12	17	B9	61	81	FE	67	86	AD	71	6B	89	0B
3	5C	B0	C0	FF	33	C3	56	B8	35	C4	05	AE	D8	E0	7F	99
4	E1	2B	DC	1A	E2	92	57	EC	70	3F	CC	F0	95	EE	8D	F1
5	C1	AB	76	38	9F	E6	78	CA	F7	C6	F8	60	D5	BB	9C	4F
6	F3	3C	65	7B	63	7C	30	6A	DD	4E	A7	79	9E	B2	3D	31
7	3E	98	B5	6E	27	D3	BC	CF	59	1E	18	1F	4C	5A	B7	93
8	E9	DE	E7	2C	8F	0C	0F	A6	2D	DB	49	F4	6F	73	96	47
9	06	07	53	16	ED	24	7A	37	39	CB	A3	83	03	A9	8B	F6
A	92	BD	9B	1C	E5	D1	41	01	54	45	FB	C9	5E	4D	0E	F2
B	68	20	80	AA	22	7D	64	2F	26	87	F9	34	90	40	55	11
C	BE	32	97	13	43	FC	9A	48	A0	2A	88	5F	19	4B	09	A1
D	7E	CD	A4	D0	15	44	AF	8C	A5	84	50	BF	66	D2	E8	8A
E	A2	D7	46	52	42	A8	DF	B3	69	74	C5	51	EB	23	29	21
F	D4	EF	D9	B4	3A	62	28	75	91	14	10	EA	77	6C	DA	1D

На рисунке 1 представлена структурная схема алгоритма хеширования СТБ 34.101.31.

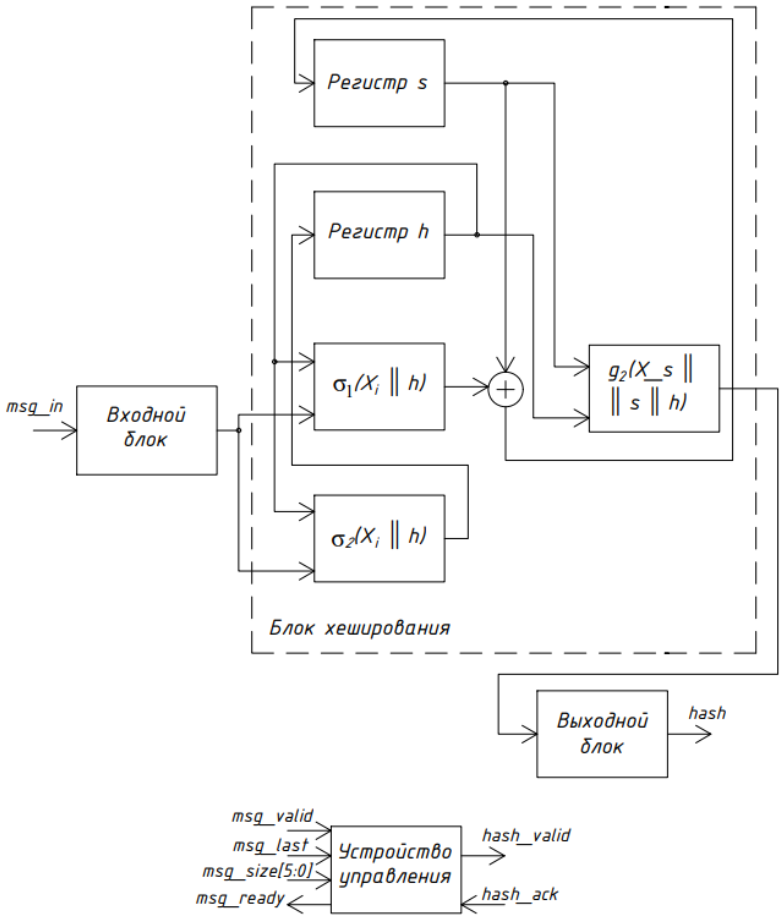

Рисунок 1 – структурная схема алгоритма хеширования СТБ 34.101.31

Рисунок 1 так же представляет собой интерфейс устройства. Где msg_in – входная 32-разрядная шина данных, msg_valid – входной сигнал доступности данных, msg_last – сигнал, сообщающий о последнем слове данных сообщения, msg_size – 6-разрядная информационная шина для идентификации числа актуальных бит в последнем слове сообщения, msg_ready – выходной сигнал, означающий готовность к приему данных следующего сообщения, hash_valid – выходной сигнал сообщающий о доступности хеш-значения, hash_ack – входной сигнал запроса хеш-значения, hash – выходная шина хеш-значения разрядностью 256.

В результате проекта были решены следующие задачи:

1 Изучен материал по теме проекта;

2 Написана программа на языке высокого уровня Python;

3 Разработан интерфейс устройства;

4 Сделана часть графического материала;

5 Поставлены задачи для успешного выполнения проекта.

Список использованных источников:

1. НИИ прикладных проблем математики и информатики БГУ [Электронный ресурс]. – Режим доступа : https://apmi.bsu.by/resources/std.

2. СТБ 34.101.31-2020[Электронный ресурс]. – Режим доступа : https://apmi.bsu.by/assets/files/std/belt-spec371.pdf.