Для расширения линейности характеристики ВТГ прямого измерения, необходимо формировать сигнал об измеряемой угловой скорости, как отношение амплитуды узла к амплитуде пучности:

$$\frac{x_{20}^{\text{уст}}}{x_{10}^{\text{уст}}} = TK\Omega. \qquad (4)$$

Отношение амплитуд линейно зависит от угловой скорости основания, что подтверждается результатами экспериментов на рис. 4.

Структурная схема ВТГ. На рис. 5 приведена структурная схема ВТГ прямого измерения по огибающим амплитуд колебаний пучности и узла.

Структурная схема соответствует случаю постоянной угловой скорости основания и резонансной настройке контуров пучности (узла) и позволяет моделировать ВТГ без учета высокочастотной несущей колебаний резонатора [2]. Кроме того, схема позволяет исследовать ВТГ в компенсационном режиме путем формирования соответствующих обратных связей и включения в цепи корректирующих звеньев.

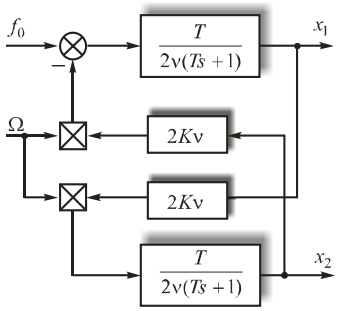

Рисунок 5 – Структурная схема КВГ для огибающих колебаний резонатора

Литература

1. Lynch, D. D. Coriolis vibratory gyroscope. IEEE standard specification format guide and test procedure for Coriolis vibratory gyros / D. D. Lynch, IEEE std.1431 annex B. – P. 56–66.

2. Информационные характеристики микромеханических гироскопов на основе кремниевой технологии микроэлектромеханических систем / Л. А. Северов, [и др.] // Изв. вузов «Приборостроение»/ – 2011. – № 8. – С. 12–22.

УДК 519.7

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ ПРИМЕНИТЕЛЬНО К ПРИБОРОСТРОЕНИЮ

Лебедев А.Н.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

Аннотация. Предложены новые методы решения трех главных задач в области защиты информации как при ее передаче по каналам связи, в частности, через интернет, так и при ее хранении на носителях и в процессе обработки на процессорах вычислительных и управляющих устройств. Это, во-первых, задача построения стойких и эффективных алгоритмов защитного кодирования данных, во-вторых, задача построения стойких и практически реализуемых алгоритмов выработки общего секрета (ключа) парой удаленных пользователей сети при помощи обмена только открытыми сообщениями и, в-третьих, задача надежной цифровой аутентификации передаваемых сообщений и хранимой информации.
Ключевые слова: защитное кодирование данных, обобщенный протокол Диффи-Хеллмана, цифровая аутентификация, легковесные алгоритмы, массовые микроконтроллеры общего назначения.

CONTEMPORARY INFORMATION SECURITY TECHNOLOGIES TO INSTRUMENT ENGINEERING

Lebedev A.

Bauman State Technical University
Moscow, Russia

Abstract. New methods of solving three main tasks in the field of information security are proposed, both when it is transmitted via public communication channels, in particular, via the Internet, and when it is stored on various types of media and directly during processing on processors of modern computing and control devices. This is, firstly, the task of building persistent and effective algorithms for data security encoding, secondly, the task of building persistent and practically implementable algorithms for generating a common secret (key) by a pair of remote network users using the exchange of only open messages, and, thirdly, the task of reliable digital authentication of transmitted messages and stored information.We have proposed some new one way functions for generalization of the Diffie-Hellman protocol.
Key words: security data encoding, generalized Diffie-Hellman protocol, digital authentication, lightweight algorithms, general-purpose mass microcontrollers.

Адрес для переписки: Лебедев А.Н., 2-я Бауманская ул. 5, стр 1, г. Москва 105005, Российская Федерация
lebedevan@bmstu.ru

Введение. Алгоритм защитного кодирования NASH (рис. 1) [1].

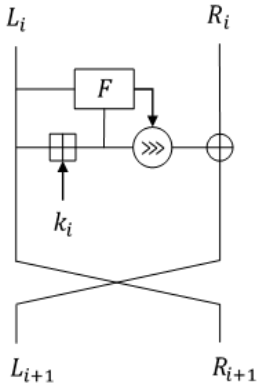

Рисунок 1 – Схема раунда *i* алгоритма NASH

Символами L_i и R_i обозначены левая и правая половинки блока данных, символом k_i обозначен раундовый ключ.

Формулы преобразования блока данных:

$$R_{i+1} = L_i,$$

$$L_{i+1} = \left(L_i \boxplus k_i \ggg F(L_i, L_i \boxplus k_i)\right) \oplus R_i.$$

В последнем раунде половинки выходного блока L_{i+1}, R_{i+1} не меняются местами, то есть:

$$L_{i+1} = L_i,$$

$$R_{i+1} = \left(L_i \boxplus k_i \ggg F(L_i, L_i \boxplus k_i)\right) \oplus R_i.$$

В работах [2–4] предложен новый общий метод формирования общего секрета (ключа, кода, аутентификатора) парой пользователей информационной системы (в частности, сети интернет), радикально расширяющий известные варианты протокола Диффи-Хеллмана и его обобщений, как его оригинального варианта, так и его модификаций с взаимной аутентификацией сторон или с аутентификацией только одной из них.

Оригинальный протокол Диффи-Хеллмана и его модификации [2, 3], что применяются для формирования общего секрета (ключа взаимной аутентификации) парой пользователей информационной системы (например, сети интернет), использующих для обмена сообщениями общедоступный канал передачи данных, состоят в следующем:

– пользователи, обозначаемые как *Алиса* и *Боб,* умеют вычислять значения конечных однонаправленных функций $f(x)$, $g(x, y)$;

– функция $f(x)$ определена на некотором конечном множестве X большой мощности и принимает значения из большого конечного множества Y, то есть $f(x) : X \to Y$;

– функция $g(x, y)$ определена на декартовом произведении этих множеств $X \times Y$ и принимает значения из третьего большого конечного множества Z, то есть $g(x, y) : X \times Y \to Z$;

– стороны независимо выбирают случайные элементы $x1$, $x2$ множества X, вычисляют значения $f(x1)$, $f(x2)$ и обмениваются ими по доступному им каналу связи, например, по сети интернет, то есть передают $f(x1) \leftrightarrow f(x2)$,

– затем они вычисляют общий секрет (ключ, аутентификатор) пары (*Алиса, Боб*) по формулам

$$K = g(x1, f(x2)) = g(x2, f(x1)).$$

Протокол DHFL

Шаг	Информация *Алисы*	Информация *Боба*
1	Случайно выбирает $x1$ $x1 \in X$	Случайно выбирает $x2$ $x2 \in X$
2	Вычисляет элемент $Q1 = g \otimes g \otimes \ \otimes g$ *«умножая его»* $x1$ раз	Вычисляет элемент $Q2 = g \otimes g \otimes \ \otimes g$ *«умножая его»* $x2$ раз
3	Получает от партнера $Q2 = g \otimes g \otimes \ \otimes g$ *«умноженный»* $x2$ раз	Получает от партнера $Q1 = g \otimes g \otimes \ \otimes g$ *«умноженный»* $x1$ раз
4	Вычисляет элемент $K1 = Q2 \otimes Q2 \otimes \otimes Q2$ *«умножая его»* $x1$ раз	Вычисляет элемент $K2 = Q1 \otimes Q1 \otimes \otimes Q1$ *«умножая его»* $x2$ раз

Предлагаются функции $f(x)$, $g(x, y)$ построенные на взаимно однозначном дробно-линейном преобразовании в показателях дискретной экспоненты над большим простым полем $\mathbb{Z}_p$, или взаимно однозначном дробно-линейном преобразовании в показателе кратности некоторой заданной заранее точки $P \in E_{a,b}(\mathbb{F})$ в группе точек эллиптической кривой над большим конечным полем

$$\mathbb{F}, E_{a,b}(p) = \{(x, y) | \, x, y \in \mathbb{F}, y^2 = x^3 + ax + b \ (\mathbb{F})\}.$$

Идея использования дробно-линейного взаимно однозначного преобразования именно для этой цели была впервые высказана в работах автора настоящего доклада [2, 3].

Поскольку новая операция умножения $\otimes$ ассоциативна, то возможна перестановка скобок, а перестановкой скобок доказывается равенство:

$$K = K1 = Q2 \otimes Q2 \otimes \ \otimes Q2 = K2 = Q1 \otimes Q1 \otimes \ \otimes Q1.$$

Таким образом, получившийся алгоритм корректен.

В работе [5] предложен новый метод защиты от манипулирования ценами в ходе электронных биржевых торгов. Алгоритмическая база метода построена на современных алгоритмах защиты данных и аутентификации трейдеров. Он может быть реализован в виде множества конкретных опций.

Литература

1. Лебедев, А. Н. Легковесный алгоритм защитного кодирования – NASH / А. Н. Лебедев, А. М. Карондеев, А. А. Козлов // Электронные информационные системы. – 2021. – Т. 31, № 4. – С. 56–64.
2. Лебедев, А. Н. Обобщенный протокол Диффи-Хеллмана с аутентификацией сторон / А. Н. Лебедев // Международная алгебраическая конференция, посвященная 110-летию со дня рождения профессора А. Г. Куроша. : тезисы докладов. – М.: Издательство МГУ, 2018. – С. 123–127.
3. Лебедев, А. Н. Новая арифметика конечного коммутативного кольца и ее использование в криптографии / А. Н. Лебедев // Электронные информационные системы. – 2021. – Т. 30, № 3. – С. 49–63.
4. Лебедев, А. Н. Новый протокол выработки общего секрета / А. Н. Лебедев, А. О. Кокорин // Электронные информационные системы. – 2021. – Т. 30, № 3. – С. 97–104.
5. Лебедев, А. Н. Методы защитного кодирования и аутентификации данных в организации биржевых торгов / А. Н. Лебедев // Электронные информационные системы. – 2021. – Т. 31, № 4. – С. 65–89.

УДК 534-16; 534-8:621.9.048.6

ФИЗИКО-МАТЕМАТИЧЕСКИЕ И ИНЖЕНЕРНЫЕ АСПЕКТЫ РАЗРАБОТКИ НОВЫХ ТИПОВ УЛЬТРАЗВУКОВЫХ КОЛЕБАТЕЛЬНЫХ СИСТЕМ ДЛЯ ПРИМЕНЕНИЯ В ТЕХНИКЕ И МЕДИЦИНЕ

Степаненко Д.А.[1], Бунчук К.А.[2]

[1]Белорусский национальный технический университет
[2]РИУП «Научно-технологический парк БНТУ «Политехник»
Минск, Республика Беларусь

Аннотация. Представлены результаты работ по исследованию и практической реализации новых типов ультразвуковых колебательных систем на основе кольцевых упругих элементов. Описаны механико-математические и компьютерные методы моделирования колебаний и методика экспериментального определения эксплуатационных характеристик кольцевых волноводов-концентраторов, обеспечивающих усиление ультразвуковых колебаний по амплитуде. Рассмотрены перспективные направления их применения в технике и медицине и преимущества по сравнению с традиционно применяемыми стержневыми концентраторами.
Ключевые слова: ультразвуковые концентраторы, кольцевые волноводы, усиление колебаний.

PHYSICAL, MATHEMATICAL AND ENGINEERING ASPECTS OF THE DEVELOPMENT OF NOVEL ULTRASONIC VIBRATORY SYSTEMS FOR APPLICATION IN ENGINEERING AND MEDICINE

Stepanenko D.[1], Bunchuk K.[2]

[1]Belarusian National Technical University
[2]State Unitary Innovative Enterprise "Science and Technology Park of BNTU "Polytechnic"
Minsk, Belarus

Abstract. The article presents results of the works on the study and practical implementation of novel ultrasonic vibratory systems based on application of ring-shaped elastic elements. It describes mechanical-mathematical and computer methods used for modelling of vibrations and methodology used for experimental determination of operational characteristics of ring-shaped waveguides ensuring amplification of ultrasonic vibrations amplitude. Potential applications of ring-shaped waveguides in engineering and medicine and their advantages over traditionally used bar waveguides (horns) are considered.
Key words: ultrasonic horns, ring-shaped waveguides, amplification of vibrations.

Адрес для переписки: Степаненко Д.А., пр. Независимости, 65, г. Минск 220113, Республика Беларусь
e-mail: dstepanenko@bntu.by

Низкочастотные ультразвуковые колебания высокой интенсивности с частотой от 20 до 100 кГц и интенсивностью более 1 Вт/см^2 являются эффективным средством повышения производительности и точности выполнения многих технологических операций, таких как обработка металлов давлением и резанием, размерная обработка хрупких материалов, очистка деталей от загрязнений, сварка и пайка. Ультразвуковые аппараты и инструменты также находят широкое применение в медицине, в частности в общей и сердечно-сосудистой хирургии используются хирургические инструменты, рабочим окончаниям которых сообщаются ультразвуковые колебания, что позволяет снизить травматичность хирургических операций за счет обеспечения гемостатического эффекта и селективности разрушения патологических тканей. С учетом широкого спектра практических применений ультразвука значительный интерес со стороны инженерного сообщества вызывают проблемы разработки и внедрения новых типов ультразвуковых колебательных систем (УЗКС), в частности, в БНТУ проводятся работы по ис-