Устройства состоит из блока автоматического контроля продвижения хлеба и управления процессом измерения его влажности (БАКУПИ), кювета (К), блока генератора (БГ), блока обработки информации (БОИ), дисплея (ДИС) и блока звуковой сигнализации (БЗС), а также блока стабилизированного источника питания (БСИП).

Блок автоматического контроля продвижения хлеба и управления процессом измерения его влажности (БАКУПИ) состоит из таймера, фотоэлектрического датчика, логического элемента, усилителя мощности, выполненный на базе полевого транзистора и электромагнитного клапана с подвижным сердечником. Фотоэлектрический датчик предназначен для обнаружения хлеба до точки проведения контроля влажности и формирования управляющего сигнала для запуск таймера и электромагнитного клапана. Выходной сигнал фотоэлектрического датчика одновременно служит запускающим сигналом таймера и электромагнитного клапана. Электромагнитный клапан предназначен для автоматического удержания (на 1–2 s)-останова хлеба, с целью проведения измерения его влажности в этом интервале времени. Таймер предназначен для управления работой электромагнитного клапана (ЭМК), управляющий продвижением или остановом хлеба, а также поступления выделенной серии импульсов (частоты) на вход микропроцессорного блока обработки информации.

Блок обработки информации проводит обработки поступающей серии частот (импульсов), соответствующей влажности хлеба и выдача обработанных данных на дисплей в удобном виде оператору. После проведение измерения влажности хлеба таймер выдает управляющий сигнал электромагнитному клапану о продолжении продвижении остановленного хлеба по транспортерной ленте. Размеры обкладок конденсатора (кюветы) приведены на рис. 4.

Литература

1. Берлинер, М. А. Измерения влажности / М. А. Берлинер. – М. : Энергия, 1973. – 400 с.

2. Пономарев С. В. Теоретические и практические аспекты теплофизических измерений: монография. В 2 кн. / С. В. Пономарев, С. В. Мищенко, А. Г. Дивин. – Тамбов : Тамб. гос. техн. ун-т, 2006. – Кн. 1. – 204 с.

3. Афонин, В. С. Разработка прибора контроля влажности зерновой продукции на основе многоэлектродных емкостных преобразователей : дис. … на соискание ученой степени канд. техн. наук / В. С. Афонин. – Барнаул, 2007. – 134 с.

4. ГОСТ 21094-75 Хлеб и хлебобулочные изделия. Метод определения влажности.

УДК 519.7

ЗАЩИТНОЕ КОДИРОВАНИЕ ДАННЫХ ДЛЯ ЭЛЕКТРОННЫХ БИРЖЕВЫХ ТОРГОВ

Лебедев А.Н., Завадская Т.Е.

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

Аннотация. Предложен новый метод защиты от манипулирования ценами в ходе электронных биржевых торгов. Алгоритмическая база метода построена на современных алгоритмах защиты данных и аутентификации трейдеров. Предложеный метод может быть реализован в виде множества конкретных опций, в зависимости от конкретных алгоритмов, составляющих его основу. Описана общая идеология построения конкретных реализаций и приведены их конкретные примеры. Дальнейшее развитие этого метода значительно расширит сферу его возможного применения.

Ключевые слова: биржевые спекуляции, манипуляции ценами, защитное кодирование, однонаправленные функции, электронная подпись, хэширование, аутентификация.

PROTECTIVE DATA ENCODING FOR ELECTRONIC EXCHANGE TRADING

Lebedev A., Zavadskaya T.

Bauman Moscow State Technical University
Moscow, Russia

Abstract. A new method of protection against price manipulation during electronic exchange trading is proposed. The algorithm base of the method consisits of the modern algorithms for data protection and authentication of traders. The proposed method can be implemented in the form of many specific options, depending on the specific algorithms that make up its basis. The general ideology of constructing specific implementations is described and their specific examples are given. Further development of this method will significantly expand the scope of its possible application.

Key words: stock speculation, price manipulation, protective data encoding, one-way functions, electronic digital signature, hashing, authentication.

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

Введение. Мы начнем с краткого описания современной техники биржевых торгов.

Спекулятивная составляющая. Спекуляции можно разделить на два основных вида – информационные и технические.

Информационные спекуляции возможны когда у кого-то из участников торгов есть информация, которой нет у других.

Математическая постановка задачи. Пусть $A = \{a_i, |i = \overline{1, \dots, N}\}$ – множество из N участников торгов на бирже, каждому соответствует идентификатор a_i. Пусть $T = \{0, 1, 2, 3, 4\}$ – множество типов биржевых ордеров.

Участник может выставить ордер в виде сообщения вида $M_i = \big(a_i, t, p, E(v, K)\big)$, где a_i – перс. идентификатор участника; $t \in T$ – тип ордера; $p \in P = \{Step * n \mid n \in \mathbb{N}\}$ – цена сделки, которая зависит от спецификации финансового инструмента. Цена имеет Step – дискретный шаг изменения, минимальное значение, на которое может изменяться цена; $E(v, K)$ – значение однонаправленной функции, которая вычисляется от объема заявки v с использованием ключа К: $v < MAX$ макс. объем заявки.

Ордеру, прошедшему проверку на корректность, присваивается номер $n \in I = \{1, \dots, N\} \subset \mathbb{N}$, строго в порядке поступления заявки на Биржу.

Ордер типа (Sell Limit)/(Buy Limit) помещается в очередь с параметром Limit ценового уровня. Значению цены $p \in P$ соответствует массив номеров $a\left[\frac{p}{Step}\right][n] \in I,\ n < N_i \in I$, где N_i – количество ордеров на указанном уровне цены $\frac{p}{Step}$. В результате формируется «стакан цен».

Ордер типа (Sell Market)/(Buy Market) также помещается в очередь на исполнение. Как только очередь оказывается не пустой, происходит исполнение заявки из стакана цен с соответствующими параметрами для сделки.

Множество сделок $D = \{d_i, |i = \overline{0, \dots, M}\}$, при наличии полной истории сделок, экспертной оценкой можно разделить множество на два подмножества: D_0 – сделки спекулятивного характера, D_1 – сделки не спекулятивного характера.

Первый вакиант кодированных торгов. Вид любого асимметричного защитного кодирования данных заявки подходит для этой цели. Владелец только открытого ключа может только закодировать сообщение, а владелец закрытого ключа пары «открытый ключ – закрытый ключ» – единственный может декодировать сообщения, закодированные открытым ключом.

Участник генерирует пары «закрытый ключ – открытый ключ» для кодирующего преобразования, может отправить кодированную заявку на биржу, а закрытый ключ для ее раскрытия отправить по защищенному каналу в некоторый доверенный орган (удостоверяющий центр). УЦ хранит закрытые ключи всех ордеров всех участников торгов, но он не знает сами ордера [1–4].

До совершения сделки информация об объеме сделки и ключ, с помощью которого объем заявки может быть декодирован, будут в разных местах. Только в ходе исполнения заявки биржа будет отправлять в УЦ заявки, которые надо свести, а в ответ будет получать подтверждение сделки с точным указанием исполненного объема и новый кодированный ордер с не исполненным объемом. Тикет частично исполненного ордера можно не менять. Рассмотрим формирование стакана цен и процедуру сведения заявок в рамках данного способа.

Стакан цен Crypto Darkpool. Объемы заявок храним в кодированном виде с помощью асимметричного алгоритма [1]. Этот алгоритм обозначим *E*. Рассмотрим обмен информацией в данном случае. Когда *A* хочет зарегистрироваться как участник, он формирует две пары ключей («закрытый ключ – открытый ключ») системы защиты данных с открытым ключом. По защищенному каналу отправляет по закрытому ключу каждой пары на биржу и в УЦ.,

Участник A_i соединеняется с сервером биржи и сервером УЦ. После его аутентификации на УЦ, УЦ генерирует пару открытый ключ – закрытый ключ (e_i, d_i) и отправляет открытый ключ e_i участнику A_i . На выданном открытом ключе будет происходить кодирование объема заявки.

Участник A_i формирует ордер O_{ij} с номером Ord_{ij}.

Кодируется объем заявки: $Sh(V_{ij}) = E(V_{ij}, e_i)$.

A_i отправляет ордер O_{ij} объема $Sh(V_{ij})$ и идентификатором Ord_{ij} на биржу. Отправляет идентификатор Ord_{ij} в УЦ.

Бирже передается заявка $(Sh(V_{ij}), Ord_{ij})$, а в УЦ передается идентификатор ордера. Ордер проходит проверку биржей, помещается в очередь. A_i получает ответ «ордер принят» и биржевой тикет $Ticket(O_{ij})$. УЦ получает от биржи пару $(Ticket(O_{ij}), Ord_{ij})$. На бирже хранятся ордера O_{ij} с кодированным объемом заявок и двумя идентификаторами $(Ticket(O_{ij}),\ Ord_{ij})$, а в УЦ паре $(Ticket(O_{ij}), Ord_{ij})$ ставится в соответствие пара открытый/закрытый ключ, чтобы УЦ мог раскрыть соответствующий ордер или кодировать его снова и отправить на биржу с тем же уникальным идентификатором Ord_{ij}, новым тикетом $Ticket(OS_{ij})$, который отправляется участнику A_i.

Безопасность обмена данными. Участник формирует пару открытый/закрытый ключ, открытый ключ отправляет на биржу с надежным подтверждением его подлинности. Например, по технологии аутентификации FIDO [8]. При помощи защитного кодирования с открытым ключом можно от биржи передавать клиентам создаваемые сервером биржи ключи кодирования при помощи любого стойкого симметричного алгоритма защитного кодирования данных [1, 4, 6, 7].

Обмен информацией клиентов с УЦ может быть защищен также с помощью симметричного алгоритма защитного кодирования.

Формирование сеансовых ключей – по протоколу Диффи-Хеллмана (DH, ECDH) [1, 5] или его современным обобщениям DHL, DHFL [3, 4, 6, 7].

Литература

1. Шнайер, Б. Прикладная криптография. – Изд. 3-е / Б. Шнайер. – Москва: «Триумф», 2018. – 610 с.

2. Лебедев, Г. А. Новые однонаправленные функции / Г.А. Лебедев // Флеровские чтения : сборник тезисов четвертой школы-конференции молодых исследователей. – ОИЯИ, Дубна, 2011. – С. 5–7,

3. Лебедев Г. А. Применение знаково-цифровых систем счисления для вычисления однонаправленных функций / Г. А. Лебедев // Тезисы «XI Школьные Харитоновские чтения». – РФЯЦ-ВНИИЭФ, Саров, 2011. – С. 16–18.

4. 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. – М.: Издательство МГУ, 2018. – С. 123–127.

5. Diffie, W. New Directions in Cryptography / W. Diffie, M. E. Hellman // IEEE Trans. Inform. Theory, 1976. – Vol. IT-22, №. 6. – P. 644–654.

6. Лебедев А. Н. Новая арифметика конечного коммутативного кольца и ее использование в аутентификации / А. Н. Лебедев // Электронные информационные системы. – 2021. – Т. 30, № 3. – С. 49–63.

7. Лебедев А.Н. Обобщение протокола Диффи-Хеллмана с использованием дробно-линейного преобразования / А. Н. Лебедев, А. О. Кокорин // Электронные информационные системы. – 2021. – Т. 30, № 3. – С. 64–71.

8. FIDO Alliance, Fast IDentification Online [Электронный ресурс]. Режим доступа: https://fidoalliance.org. – Дата доступа: 01.10.2021.

УДК 519.7

ЛЕГКОВЕСНЫЙ АЛГОРИТМ ЗАЩИТНОГО КОДИРОВАНИЯ – NASH

Лебедев А.Н., Карондеев А.М., Козлов А.А.

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

Аннотация. В работе описывается новый легковесный блочный алгоритм защитного кодирования NASH, названный в память выдающегося математика Джона Нэша (John Nash), который кроме работы по экономике, удостоенной нобелевской премии, и работ по чистой математике, удостоенных премии Абеля, занимался также и проблемами защиты информации. Алгоритм NASH при высоком уровне стойкости защитного кодирования показывает также и высокий уровень эффективности при реализации на современных микроконтроллерах.

Ключевые слова. защитное кодирование, блочный алгоритм защитного кодирования, легковесный блочный алгоритм защитного кодирования.

LIGHTWEIGHT SECURE ENCODING ALGORITHM – NASH

Lebedev A., Karondeev A, Kozlov A.

Bauman Moscow State Technical University
Moscow, Russia

Abstract. The paper describes a new lightweight block secure encoding algorithm NASH, which is named in memory of the outstanding mathematician John Nash, who, in addition to his work on economics, awarded the Nobel Prize, and works on pure mathematics, awarded the Abel Prize, was also engaged in the information security. The algorithm NASH having a high security is also a very adaptive to contemporary microcontrollers.

Key words: secure encoding, block secure encoding, lightweight secure encoding, lightweight block secure encoding algorithm.

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

Введение. Термин «кодирование» или «кодирование информации» имеет в современных энциклопедиях, технических словарях и специальных монографиях очень широкую трактовку.

Математическая Энциклопедия, изданная в СССР в 1977–1985 гг. определяет его следующим образом: «Кодирование – процесс представления *информации* в определенной стандартной форме и обратный процесс восстановления информации по ее такому представлению. В математической литературе кодированием называется отображение произвольного множества А в множество конечных последовательностей (слов) в некотором алфавите *B,* а декодированием – обратное отображение» [1].

Из этого общего определения кодирования естественно следует представление, что среди всех возможных кодов (понимаемых как алгорит-