



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ(21)(22) Заявка: **2009122336/08**, **10.06.2009**(24) Дата начала отсчета срока действия патента:
10.06.2009

Приоритет(ы):

(22) Дата подачи заявки: **10.06.2009**(43) Дата публикации заявки: **20.12.2010** Бюл. № 35(45) Опубликовано: **20.05.2011** Бюл. № 14(56) Список документов, цитированных в отчете о поиске: **WO 2007129935 A2**, **15.11.2007**. **RU 2289886 C2**, **27.10.2005**. **RU 2250124 C1**, **20.04.2005**. **KR 20020066053 A**, **14.08.2002**. **US 2009017893 A1**, **15.01.2005**. **RU 2295773 C2**, **20.03.2007**. **RU 82358 U1**, **20.04.2009**.

Адрес для переписки:

420138, Республика Татарстан, г.Казань, ул. Гарифьянова, 28А, ООО "МОМОЛОТ"

(72) Автор(ы):

**Макаров Игорь Игоревич (RU),
Насыров Ильдар Заурович (RU)**

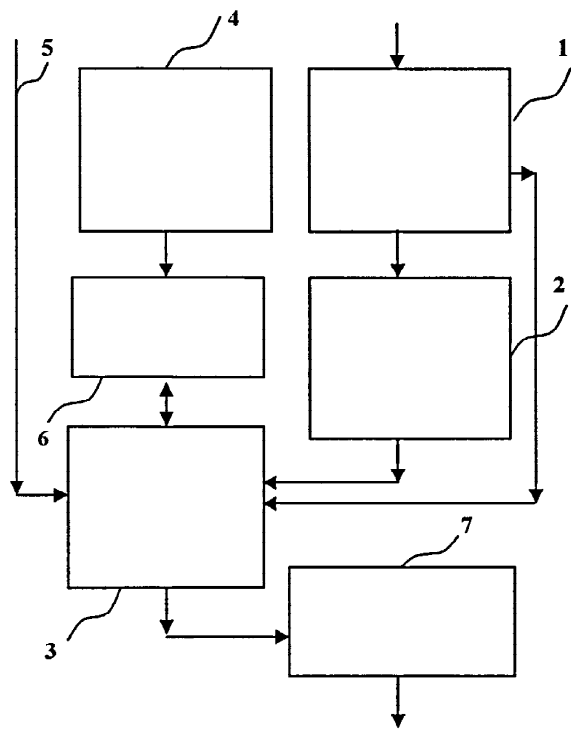
(73) Патентообладатель(и):

**Общество с ограниченной
ответственностью "МОМОЛОТ" (RU)****(54) СИСТЕМА И СПОСОБ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ ЛОТЕРЕИ**

(57) Реферат:

Изобретение предназначено для проведения лотерей при помощи электронных лотерейных билетов. Техническим результатом является повышение защиты электронных лотерейных билетов. Изобретение может быть использовано для всех видов лотерей, включая и «мгновенные» лотереи различного вида. Для приема электронного лотерейного билета могут использоваться мобильные устройства, например сотовые телефоны и персональные

компьютеры. Известны различного рода электронные мгновенные лотереи, в которых выигрышный вариант сообщается игроку только после того, как он передал свой выигрышный вариант организатору такой лотереи. Настоящее изобретение позволяет реализовывать мгновенные лотереи с электронными лотерейными билетами в точности так, как это происходит при использовании бумажного лотерейного билета мгновенной лотереи. 2 н. и 25 з.п. ф-лы, 4 ил.



Фиг. 1



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2009122336/08, 10.06.2009**

(24) Effective date for property rights:
10.06.2009

Priority:

(22) Date of filing: **10.06.2009**

(43) Application published: **20.12.2010 Bull. 35**

(45) Date of publication: **20.05.2011 Bull. 14**

Mail address:

**420138, Respublika Tatarstan, g.Kazan', ul.
Garif'janova, 28A, OOO" MOMOLOT"**

(72) Inventor(s):

**Makarov Igor' Igorevich (RU),
Nasyrov Il'dar Zaurovich (RU)**

(73) Proprietor(s):

**Obshchestvo s ogranichennoj otvetstvenost'ju
"MOMOLOT" (RU)**

(54) SYSTEM AND METHOD TO ORGANISE AND DRAW LOTTERY

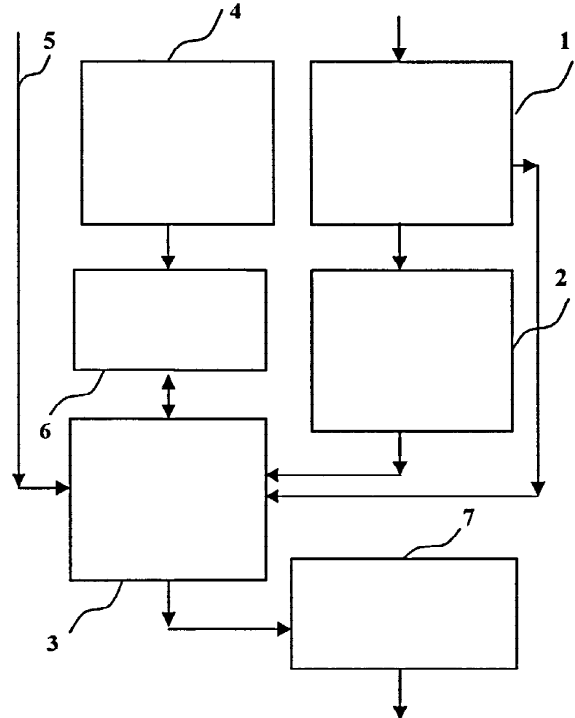
(57) Abstract:

FIELD: information technologies.

SUBSTANCE: mobile devices, such as cellular phones and personal computers, may be used to receive an electronic lottery ticket. Various electronic instantaneous lotteries are available, where the winning version is provided to a player only after he or she has submitted his or her winning version to the organiser of such lottery. This invention makes it possible to realise instantaneous lotteries with electronic lottery tickets, exactly as it happens when using a paper lottery ticket of the instantaneous lottery.

EFFECT: improved protection of electronic lottery tickets.

27 cl, 4 dwg



Фиг. 1

RU 2 4 1 9 1 5 6 C 2

RU 2 4 1 9 1 5 6 C 2

Изобретение относится к области организации и проведения лотерей в безбумажной форме.

Наиболее близко к предлагаемому изобретению относится патент США 7,303,468 «Off-line remote system for lotteries and games of skill». В нем для приема электронного лотерейного билета используются мобильные устройства и персональные компьютеры, так называемые «hand-held ticket viewers» (HTV). Множество лотерейных билетов с распределенными выигрышами генерируется на центральном компьютере, а затем распределяется по локальным HTV. Система полностью имитирует моментальную лотерею, так как его локальные HTV могут работать при отсутствии связи с центральным компьютером. Недостатком этой системы является невозможность использования HTV конечным пользователем (игроком лотереи).

Настоящее изобретение предназначено для проведения лотерей при помощи так называемых электронных лотерейных билетов в режиме «off-line». Заявляемой задачей (и основным отличительным признаком) изобретения является внедрение электронных лотерейных билетов в режиме «off-line» на основе технологии электронной цифровой подписи (ЭЦП). Оно может быть использовано для всех видов лотерей, включая и «мгновенные» лотереи сложного вида. Например, игровое поле лотерейного билета содержит 49 подполей. Семь подполей окрашены в красный цвет, а все остальные - в белый. На игровое поле нанесено непрозрачное покрытие, которое может отдельно удаляться для каждого подполя. Условия «мгновенной» лотереи состоят в выборе 7 из 49 подполей и удалении непрозрачного покрытия только для этих подполей. Фиксированная заранее, до начала лотереи, величина выигрыша определяется количеством открытых красных подполей (например, для двух - 20 рублей, для трех - 50 рублей, для четырех - 1000 рублей, для пяти - 10000 рублей, для шести - 100000 рублей, а для семи - 1000000 рублей). Настоящее изобретение позволяет реализовать проведение такой лотереи в электронном виде. Игрок покупает электронный лотерейный билет. Номера шести подполей, окрашенных в красный цвет, в зашифрованном виде включены в этот электронный лотерейный билет. Предлагаемый (для данного изобретения) метод шифрования имеет, с одной стороны, наивысший уровень безопасности (для расшифровки необходимы миллиарды миллиардов лет, поэтому игрок не имеет никаких физических возможностей для раскрытия выигрышного варианта), а с другой стороны, имеется простой способ проверить соответствие конкретного выигрышного варианта конкретному электронному лотерейному билету. Этот способ объявляется организаторами лотерей заранее, до начала действия лотереи. Предлагаемый (для данного изобретения) метод шифрования является однозначным, т.е. один и только один выигрышный вариант соответствует конкретному электронному лотерейному билету. Поэтому игрок (после предъявления своего варианта и получения от организаторов лотереи выигрышного варианта) может абсолютно надежно и независимо ни от кого проверить соответствие полученного выигрышного варианта электронному лотерейному билету, купленному им. Предлагаемый (для данного изобретения) метод шифрования обеспечивает абсолютную невозможность подделки злоумышленниками правильного электронного лотерейного билета (для расшифровки злоумышленникам потребуются миллиарды миллиардов лет). Предлагаемый способ проведения лотерей можно применять для перевода всех видов существующих лотерей бумажного типа в безбумажный (электронный вид). При этом надежность и безопасность как для игрока, так и для организаторов повысится в сотни тысяч раз, а значительные расходы на печать бумажных билетов и эксплуатацию пунктов продажи и регистрации бумажных

билетов нивелируются. Существенно, расширится круг участников лотерей. Они уже не будут зависеть от пунктов продажи и регистрации бумажных билетов, так как для этого можно будет использовать индивидуальные средства получения электронных лотерейных билетов (такие как ИВ, подключенные к Интернету, коммуникаторы, мобильные телефоны и т.п.).

ОПИСАНИЕ ЧЕРТЕЖЕЙ

Для более полного понимания сущности предлагаемого изобретения части описания представлены на следующих чертежах:

фиг.1 - блок-схема функционирования центрального сервера;

фиг.2 - блок-схема функционирования индивидуального устройства игрока;

фиг.3 показывает схемы взаимодействия между центральным сервером и индивидуальными устройствами игроков;

фиг.4 показывает схемы взаимодействия между центральным сервером и индивидуальными устройствами игроков через посредника.

Эти чертежи далее будут использованы для детального описания примера реализации предлагаемого изобретения.

На фиг.1 приведена блок-схема функционирования центрального сервера (ЦС), которая выполняет следующие функции. Устройство 1 принимает информацию (через различные коммуникационные сети) от индивидуальных устройств (ИУ) игроков лотерей. Принимаемая информация включает идентификационную информацию игрока, которую он использует для того, чтобы идентифицировать себя при покупке электронного лотерейного билета (ЭЛБ). Часть этой информации передается по умолчанию (например, номер мобильного телефона или дата и время покупки), а часть может вводиться непосредственно игроком в его ИУ (например, номер паспорта или водительского удостоверения и т.п.).

Принимаемая информация также включает выбранный игроком вариант для купленного ЭЛБ. Эта информация может передаваться как в зашифрованном, так и в открытом виде.

Устройство 2 определяет регистрационную информацию для ЭЛБ, которая может включать номер нового инициированного ЭЛБ. Устройство 3 формирует содержимое ЭЛБ как комбинацию регистрационной и идентификационной информации с выигрышным вариантом, который конкатенируется со случайным или псевдослучайным числом. Длина битового представления этой конкатенации должна быть не менее 64-х бит. Объяснение этого будет дано ниже. Случайное или псевдослучайное число генерируется устройством 4, а выигрышный вариант принимается по каналу 5. Для генерации выигрышных вариантов используются известные методы, которые в данном изобретении не рассматриваются. Устройство 6 используется для формирования электронной цифровой подписи для конкатенации выигрышного варианта и случайного или псевдослучайного числа. Здесь и везде далее используется электронная цифровая подпись, хотя вместо нее можно использовать любые функции, которые применяются в «Public-key cryptography». Для формирования электронной цифровой подписи используется ключ подписи, а для проверки электронной цифровой подписи используется ключ проверки. Эта электронная цифровая подпись объединяется с регистрационной информацией, полученной в устройстве 2, и идентификационной информацией об игроке, принятой устройством 1. Полученная, таким образом, информация и является ЭЛБ. Далее для этого ЭЛБ формируется электронная цифровая подпись и ЭЛБ с этой электронной цифровой подписью посылается на ИУ игрока устройством 7.

Последняя электронная цифровая подпись необходима для проверки подлинности ЭЛБ. Проверка подлинности выигрышного варианта, полученного игроком, может быть выполнена им после получения им этого выигрышного варианта. Для этого может использоваться один и тот же ключ проверки электронной цифровой подписи.

Для тиражных лотерей процесс создания ЭЛБ будет еще проще. ЭЛБ будет состоять из идентификационной информации, принятой с 1, регистрационной информации, принятой с 2, и выбранного варианта игрока. Если лотерея была безвыборная, то последний компонент отсутствует. Далее электронная цифровая подпись получается для ЭЛБ и все это через 7 посылается на ИУ игрока.

На фиг.2 приведена блок-схема функционирования ИУ игрока, которая выполняет следующие функции. Устройство 11 принимает информацию (через различные коммуникационные сети) от центрального сервера. Эта информация включает: ЭЛБ, его электронную цифровую подпись и элементы схем взаимодействия между ЦС и ИУ игроков, описанных ниже (фиг.3 и 4).

В качестве ИУ игроков могут использоваться различные устройства, такие как персональный компьютер, КПК, мобильный телефон и т.п.

Если это устройство - простой мобильный телефон, в котором нет возможности для формирования электронной цифровой подписи (отсутствует устройство 12), тогда информация о выбранном игроком варианте формируется посредством устройств 13-16 и не шифруется. Вместе с регистрационной информацией выбранный игроком вариант передается устройством 17 на ЦС.

Если ИУ игрока имеет устройство 12, то для шифрования ответа используется следующая процедура. Выбранный игроком вариант конкатенируется со случайным или псевдослучайным числом в битовую строку длиной не менее 64-х бит. Это ограничение будет пояснено ниже. Устройство 12 использует ключ подписи при формировании электронной цифровой подписи игрока этой битовой строки (ключ проверки электронной цифровой подписи игрока посылается на ЦС при регистрации). Далее эта информация объединяется с регистрационной или идентификационной информацией об игроке, подписывается электронной цифровой подписью игрока и посылается устройством 17 на ЦС.

Посылая только электронную цифровую подпись выбранного им варианта, игрок не позволяет ЦС определить его, но если игрок выиграет и предъявит его, то ЦС легко проверит подлинность этого варианта, используя ключ проверки электронной цифровой подписи игрока.

Конкатенация информации со случайным или псевдослучайным числом в битовую строку длиной не менее 64-х бит необходима для исключения прямого перебора всех возможных выигрышных вариантов за разумное (несколько сотен лет) время.

На фиг.3 показаны схемы взаимодействия между центральным сервером и индивидуальным устройством игрока. Используются следующие обозначения:

И - идентификационная информация об игроке,

Р - регистрационная информация,

В - выбранный игроком вариант,

К - конкатенация выбранного игроком варианта со случайным или псевдослучайным числом,

П - конкатенация выигрышного варианта со случайным или псевдослучайным числом,

Ц_И - электронная цифровая подпись игрока,

Ц_С - электронная цифровая подпись ЦС (организатора лотереи),

Ц_П - электронная цифровая подпись посредника.

Электронная цифровая подпись на фиг.3 и 4, помещенная в прямоугольник, относится к информации, расположенной в левом нижнем углу этого прямоугольника.

На фиг.3а и 3б показаны схемы взаимодействия между ЦС и ИУ игрока, имеющие устройство 12 для формирования электронной цифровой подписи игрока.

На фиг.3а показана однораундовая схема взаимодействия между ЦС и ИУ игрока.

1. Игрок Серверу: (И || Ц_И (К)) || Ц_И (И || Ц_И (К)),

2. Сервер Игроку: П || Ц_С (П || И || Ц_И (К)), где "||" - символ для конкатенации.

Игрок (1) посылает подписанное сообщение, содержащее конкатенацию идентификационной информации об игроке И и электронную цифровую подпись игрока конкатенации выбранного им варианта со случайным или псевдослучайным числом К.

Сервер (2) посылает сообщение, содержащее конкатенацию конкатенации выигрышного варианта со случайным или псевдослучайным числом П и электронную цифровую подпись ЦС конкатенации выигрышного варианта со случайным или псевдослучайным числом П, идентификационной информацией об игроке И и электронную цифровую подпись игрока конкатенации выбранного им варианта со случайным или псевдослучайным числом К.

Это самая простая и самая надежная схема взаимодействия между ЦС и ИУ игрока, в которой игрок посылает только свою электронную цифровую подпись выбранного им варианта. Оператор лотереи никак не может по электронной цифровой подписи определить выбранный игроком вариант, он только регистрирует ее и возвращает игроку выигрышный вариант. Игрок сравнивает полученный выигрышный вариант с выбранным им вариантом и сам определяет свой выигрыш в соответствии с правилами лотереи. Для получения выигрыша игроку надо представить посланную им информацию и документ, определяемый в идентификационной информации об игроке И.

На фиг.3а показана двухраундовая схема взаимодействия между ЦС и ИУ игрока.

1. Игрок Серверу: И,

2. Сервер Игроку: Р || И || Ц_С (П) || Ц_С (Р || И || Ц_С (П)),

3. Игрок Серверу: (Р || Ц_И (К)) || Ц_И (Р || Ц_И (К)),

4. Сервер Игроку: П || Ц_С (П || Р || Ц_И (К)).

В первом раунде игрок посылает только идентификационную информацию о себе И, а сервер возвращает регистрационную и идентификационную информацию Р и И и электронную цифровую подпись ЦС конкатенации выигрышного варианта со случайным или псевдослучайным числом П. Это все подписывается электронной цифровой подписью ЦС. В этом раунде игрок получает ЭЛБ.

Второй раунд такой же, как и первый раунд первой схемы взаимодействия между ЦС и ИУ игрока. Только И заменяется на Р. В этом протоколе игрок сначала получает «зашифрованный» выигрышный вариант и только затем посылает выбранный им вариант. Полное соответствие с моментальной лотереей.

В вышеприведенные схемы взаимодействия между ЦС и ИУ игрока игрок может добавить ключ проверки его (или посредника) электронной цифровой подписи.

В первую схему:

1. Игрок Серверу: (И || И_К || Ц_И (К)) || Ц_И (И || И_К || Ц_И (К)),

2. Сервер Игроку: П || Ц_С (П || И || И_К || Ц_И (К)), где И_К - ключ проверки игрока (или посредника) электронной цифровой подписи.

Во вторую схему:

3. Игрок Серверу: (P || И_К || Ц_И (К)) || Ц_И (P || И_К || Ц_И (К)),

4. Сервер Игроку: П || Ц_С (П || Р || И_К || Ц_И (К)).

На фиг.3в и 3г показаны схемы взаимодействия между ЦС и ИУ игрока, не имеющие устройства 12 для формирования электронной цифровой подписи игрока.

Например, простые модели сотовых телефонов.

На фиг.3в показана трехраундовая схема взаимодействия между ЦС и ИУ игрока.

1. Игрок Серверу: И,

2. Сервер Игроку: P || И || Ц_С (П) || Ц_С (P || И || Ц_С (П)),

3. Игрок Серверу: P || В,

4. Сервер Игроку: P || В || Ц_С (P || В),

5. Игрок Серверу: P || В || Ц_С (P || В),

6. Сервер Игроку: П || Ц_С (П).

Первый раунд такой же, как и во второй схеме взаимодействия между ЦС и ИУ игрока. Во втором раунде игрок посылает только P и В (выбранный им вариант без случайного числа). Сервер возвращает этот пакет, подписанный своей электронной цифровой подписью. В третьем раунде игрок переправляет все это обратно на сервер и получает от него выигрышный вариант, подписанный электронной цифровой подписью ЦС.

На фиг.3г показана схема взаимодействия между ЦС и ИУ игрока, которая является двухраундовым вариантом предыдущей схемы взаимодействия между ЦС и ИУ игрока. По сравнению с предыдущей она является менее безопасной. Во втором раунде ответ сервера P || В || Ц_С (P || В) заменяется на П || P || В || Ц_С (П || P || В), который включает ответ из третьего раунда предыдущей схемы взаимодействия между ЦС и ИУ игрока.

На фиг.4 показаны схемы взаимодействия между ЦС и ИУ игрока, не имеющие устройства 12 для формирования электронной цифровой подписи игрока, с участием независимого посредника. Эти схемы получаются из первых двух схем добавлением еще одного раунда между игроком и посредником. В этом раунде посредник подписывает своей электронной цифровой подписью информацию игрока. Посредник также конкатенирует В со случайным или псевдослучайным числом.

Формула изобретения

1. Метод для реализации лотереи, использующий индивидуальное устройство игрока и центральный сервер, для выполнения следующих действий:

- приема нешифрованной/шифрованной информации о выбранном игроком варианте от упомянутого индивидуального устройства игрока и/или приема идентификационной информации об игроке и определения регистрационной информации об игроке и отправки упомянутой регистрационной информации на упомянутое индивидуальное устройство игрока;

- отправки упомянутой нешифрованной/шифрованной информации о выбранном игроком варианте на упомянутый центральный сервер и приема упомянутой регистрационной информации от упомянутого центрального сервера;

отличающийся тем, что используется информация о выигрышном варианте при формировании верификационных данных, которые могут быть использованы игроком для проверки подлинности выигрышного варианта, при помощи ключа проверки электронной цифровой подписи, которая применяется при формировании упомянутых верификационных данных.

2. Метод по п.1, отличающийся тем, что упомянутое формирование

верификационных данных использует упомянутую информацию о выигрышном варианте и идентификационную/регистрационную информацию об игроке и верификационные данные, которые получаются при использовании упомянутой информации о выбранном игроком варианте.

5 3. Метод по п.1, отличающийся тем, что упомянутое формирование верификационных данных использует упомянутую информацию о выигрышном варианте и идентификационную/регистрационную информацию об игроке и упомянутую информацию о выбранном игроком варианте.

10 4. Метод по п.1, отличающийся тем, что упомянутое формирование верификационных данных использует упомянутую информацию о выигрышном варианте.

15 5. Метод по п.1, отличающийся тем, что упомянутое формирование верификационных данных использует идентификационную и регистрационную информацию об игроке и верификационные данные, которые получаются при использовании упомянутой информации о выигрышном варианте.

20 6. Метод по п.1, отличающийся тем, что упомянутое формирование верификационных данных использует упомянутую информацию о выбранном игроком варианте и/или идентификационную и регистрационную информацию об игроке.

25 7. Метод по п.1, отличающийся тем, что упомянутое индивидуальное устройство игрока использует формирование верификационных данных, которые получаются при использовании идентификационной/регистрационной информации об игроке, и верификационные данные, которые получаются при использовании упомянутой информации о выбранном игроком варианте.

30 8. Метод по любому из пп.2 - 6 и 7, отличающийся тем, что упомянутое формирование верификационных данных использует информацию, которая объединяется со случайным/псевдослучайным числом.

9. Метод по п.1, отличающийся тем, что упомянутое индивидуальное устройство игрока использует формирование верификационных данных и/или проверку верификационных данных.

35 10. Метод по п.1, отличающийся тем, что упомянутое индивидуальное устройство игрока есть персональный компьютер, или коммуникатор, или платежный терминал, которые связаны с упомянутым центральным сервером через коммуникационную сеть.

40 11. Метод по п.1, отличающийся тем, что упомянутое индивидуальное устройство игрока есть мобильный телефон или коммуникатор, которые используют сотовую связь для коммуникации с упомянутым центральным сервером, посредством SMS, или MMS, или WAP, или Интернет.

12. Система для реализации лотереи, использующая индивидуальное устройство игрока и центральный сервер, включает:

45 - центральный сервер, который содержит: устройство для приема нешифрованной/шифрованной информации о выбранном игроком варианте от упомянутого индивидуального устройства игрока и/или устройство для приема идентификационной информации об игроке, и устройство для определения регистрационной информации об игроке, и устройство для отправки упомянутой регистрационной информации на упомянутое индивидуальное устройство игрока;

50 - индивидуальное устройство игрока, которое содержит: устройство для отправки упомянутой нешифрованной/шифрованной информации о выбранном игроком варианте на упомянутый центральный сервер и устройство для приема упомянутой

регистрационной информации от упомянутого центрального сервера;

отличающаяся тем, что центральный сервер содержит: устройство, использующее информацию о выигрышном варианте, для формирования верификационных данных, которые могут быть использованы игроком для проверки подлинности выигрышного варианта, при помощи ключа проверки электронной цифровой подписи, которая применяется в упомянутом устройстве формирования верификационных данных, устройство формирования содержимого электронного лотерейного билета и устройство для отправки упомянутого электронного лотерейного билета на упомянутое индивидуальное устройство игрока, который может проверить подлинность выигрышного варианта при помощи упомянутого ключа.

13. Система по п.12, отличающаяся тем, что упомянутое устройство для формирования верификационных данных использует упомянутую информацию о выигрышном варианте и идентификационную/регистрационную информацию об игроке и верификационные данные, которые получаются при использовании упомянутой информации о выбранном игроком варианте.

14. Система по п.12, отличающаяся тем, что упомянутое устройство для формирования верификационных данных использует упомянутую информацию о выигрышном варианте и идентификационную/регистрационную информацию об игроке и упомянутую информацию о выбранном игроком варианте.

15. Система по п.12, отличающаяся тем, что упомянутое устройство для формирования верификационных данных использует упомянутую информацию о выигрышном варианте.

16. Система по п.12, отличающаяся тем, что упомянутое устройство для формирования верификационных данных использует идентификационную и регистрационную информацию об игроке и верификационные данные, которые получаются при использовании упомянутой информации о выигрышном варианте.

17. Система по п.12, отличающаяся тем, что упомянутое устройство для формирования верификационных данных использует упомянутую информацию о выбранном игроком варианте и/или идентификационную и регистрационную информацию об игроке.

18. Система по п.12, отличающаяся тем, что упомянутое индивидуальное устройство игрока содержит устройство для формирования верификационных данных, которые получаются при использовании идентификационной/регистрационной информации об игроке, и верификационные данные, которые получаются при использовании упомянутой информации о выбранном игроком варианте.

19. Система по любому из пп.2 - 6 и 7, отличающаяся тем, что упомянутое устройство для формирования верификационных данных использует информацию, которая объединяется со случайным/псевдослучайным числом.

20. Система по п.12, отличающаяся тем, что упомянутое индивидуальное устройство игрока включает устройство для формирования верификационных данных и/или устройство для проверки верификационных данных.

21. Система по п.12, отличающаяся тем, что упомянутое индивидуальное устройство игрока есть персональный компьютер, или коммуникатор, или платежный терминал, которые связаны с упомянутым центральным сервером через коммуникационную сеть.

22. Система по п.12, отличающаяся тем, что упомянутое индивидуальное устройство игрока есть мобильный телефон или коммуникатор, которые используют сотовую связь для коммуникации с упомянутым центральным сервером,

посредством SMS, или MMS, или WAP, или Интернет.

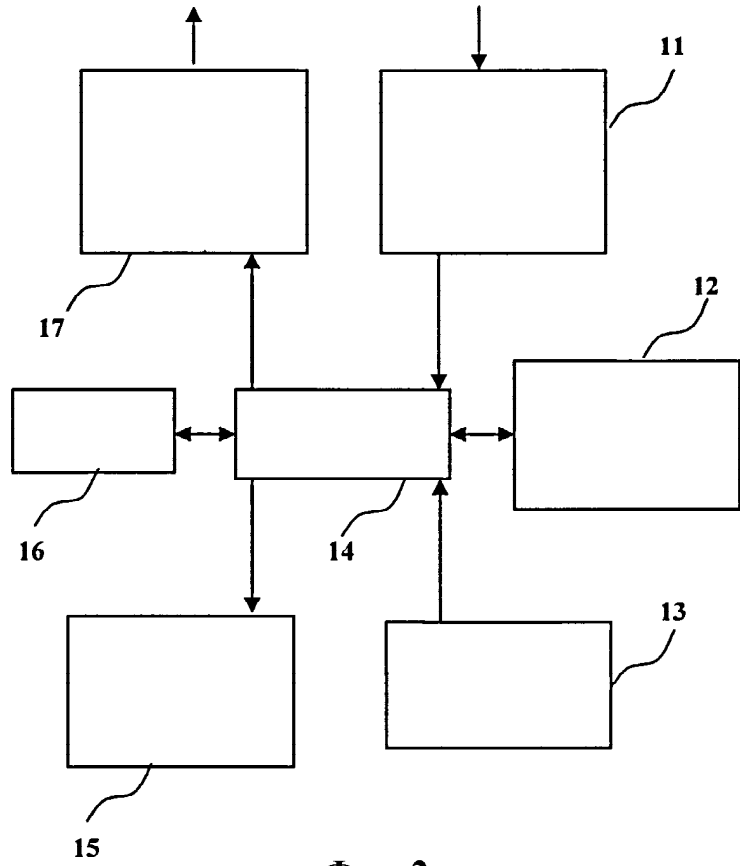
23. Метод по любому из пп.1 и 9, отличающийся тем, что упомянутое формирование верификационных данных и/или упомянутая проверка верификационных данных используют электронную цифровую подпись, или шифрование с открытыми ключами, или вычисление однонаправленной функции.

24. Метод по п.23, отличающийся тем, что упомянутое формирование верификационных данных использует упомянутую информацию о выигрышном варианте и идентификационную/регистрационную информацию об игроке, и верификационные данные, которые получаются при использовании упомянутой информации о выбранном игроком варианте, и ключ проверки для электронной цифровой подписи/шифрования с открытыми ключами.

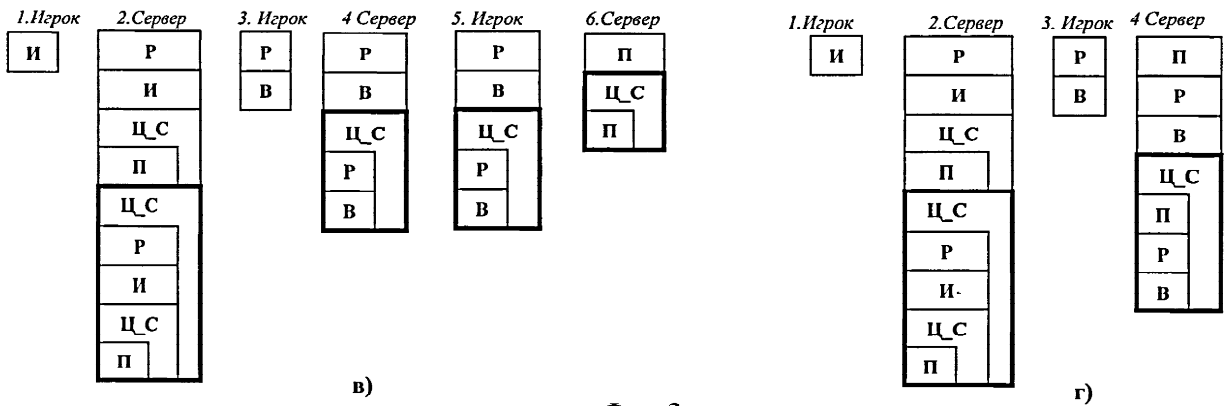
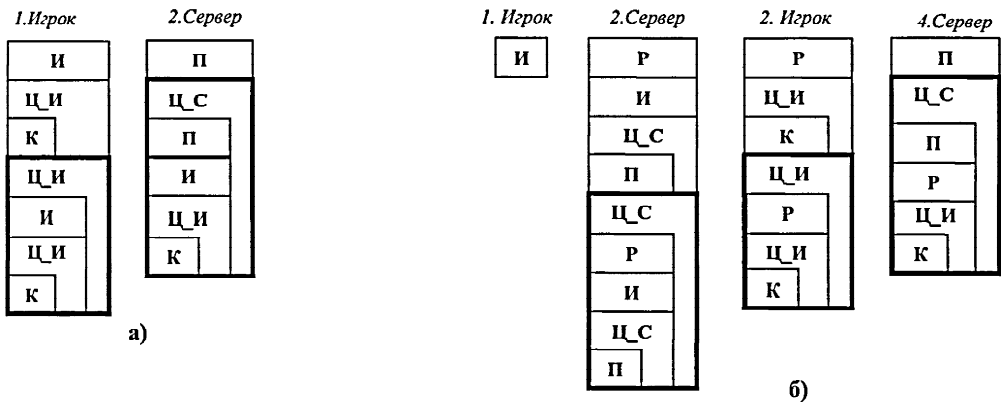
25. Метод по п.23, отличающийся тем, что упомянутое индивидуальное устройство игрока использует формирование верификационных данных, которые получаются при использовании идентификационной/регистрационной информации об игроке, и верификационные данные, которые получаются при использовании упомянутой информации о выбранном игроком варианте, и ключ проверки для электронной цифровой подписи/шифрования с открытыми ключами.

26. Система по п.23, отличающаяся тем, что упомянутое устройство для формирования верификационных данных использует упомянутую информацию о выигрышном варианте и идентификационную/регистрационную информацию об игроке, и верификационные данные, которые получаются при использовании упомянутой информации о выбранном игроком варианте, и ключ проверки для электронной цифровой подписи/шифрования с открытыми ключами.

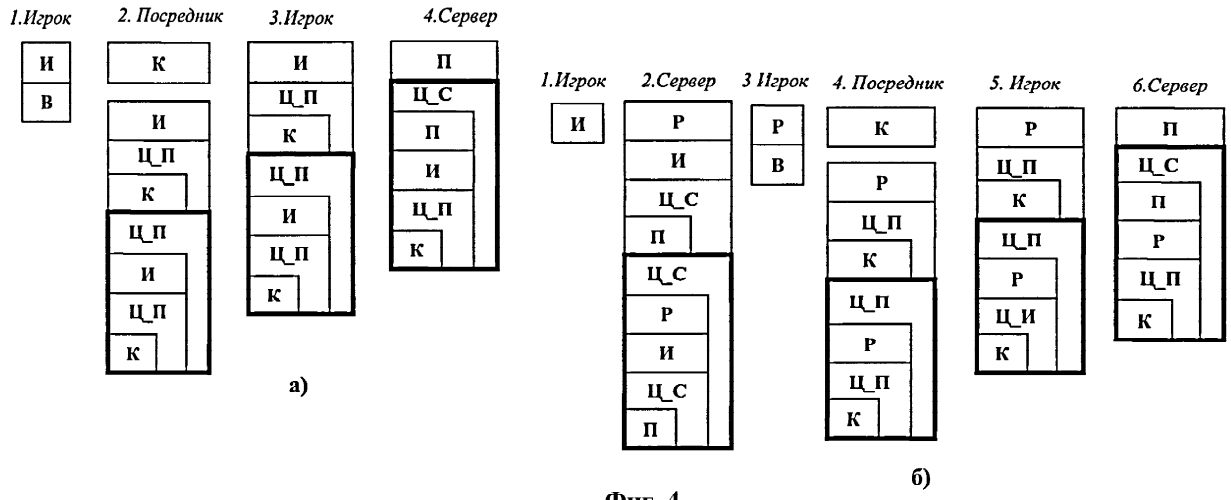
27. Система по п.23, отличающаяся тем, что упомянутое индивидуальное устройство игрока использует упомянутое устройство для формирования верификационных данных, которые получаются при использовании идентификационной или регистрационной информации об игроке, и верификационные данные, которые получаются при использовании упомянутой информации о выбранном игроком варианте, и ключ проверки для электронной цифровой подписи/шифрования с открытыми ключами.



Фиг. 2



Фиг. 3



Фиг. 4