(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 294 066**

(51) Int. Cl.:
G07F 17/32 (2006.01)
G07D 11/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **02013341 .9**
(86) Fecha de presentación : **19.06.2002**
(87) Número de publicación de la solicitud: **1274050**
(87) Fecha de publicación de la solicitud: **08.01.2003**

(54) Título: **Procedimiento para la encriptación de datos que se transmiten desde un módulo periférico a una unidad de control de una máquina accionada por monedas.**

(30) Prioridad: **05.07.2001 DE 101 32 052**
07.03.2002 DE 102 10 173

(45) Fecha de publicación de la mención BOPI:
01.04.2008

(45) Fecha de la publicación del folleto de la patente:
01.04.2008

(73) Titular/es: **adp Gauselmann GmbH**
Merkur-Allee 1-15
32339 Espelkamp, DE

(72) Inventor/es: **No consta**

(74) Agente: **Plaza Fernández-Villa, Luis**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

DESCRIPCIÓN

Procedimiento para la encriptación de datos que se transmiten desde un módulo periférico a una unidad de control de una máquina accionada por monedas.

La invención se refiere a un procedimiento para la encriptación de datos, transmitidos desde un módulo periférico a una unidad de control de una máquina accionada por monedas, según las reivindicaciones 1 o 2.

Del documento DE 199 47 421 se conoce una máquina de entretenimiento accionada por monedas con una unidad de control y una unidad de monedas, compuesta por un verificador de monedas electrónico con sus correspondientes tubos de apilamiento de monedas de monedas individuales, los cuales llevan asignado, respectivamente, en su parte inferior un dispensador de monedas. En la línea múltiple que une al verificador de monedas electrónico con la unidad de control va instalado un convertidor, cuyo fin es adaptar las señales de salida emitidas por el verificador de monedas a una nueva secuencia. Mediante la utilización del convertidor se posibilita, durante el cambio de moneda de MARCOS ALEMANES a EUROS, el poder seguir usando ininterrumpidamente las máquinas de entretenimiento existentes accionadas por monedas, cuando se introduzcan las monedas de Euro, a pesar de que las máquinas de entretenimiento accionadas por monedas estaban concebidas para la aceptación de monedas en marcos alemanes.

El documento US 5 737 418 describe un procedimiento para la validación de los medios de pago, en donde los datos de validación son transmitidos de forma encriptada. Los datos de validación comprenden el valor del billete de banco y el país de origen del billete de banco. La encriptación se realiza a través de una palabra clave, la cual se elige de una lista, en base a un índice. Después de un proceso de encriptación, el índice se desplaza con la ayuda de un sumando, de modo que el índice muestra otra palabra clave para el siguiente proceso de encriptación. El sumando se genera tras el proceso de encriptación a partir de un valor que contiene el número de las transacciones realizadas hasta ese momento, es decir, el número de billetes de banco aceptados, y de los datos de validación.

El objetivo de la presente invención es proteger el flujo de datos entre un módulo periférico y una unidad de control de una máquina de entretenimiento accionada por monedas frente a una posible manipulación.

Este objetivo se cumple, conforme a la invención, mediante las características de las reivindicaciones 1 o 2.

Otras realizaciones ventajosas se pueden deducir de las reivindicaciones subordinadas.

El procedimiento, conforme a la invención, presenta la ventaja de que, en base a la transferencia segura de datos entre un módulo periférico, por ejemplo, un verificador electrónico de monedas, y una unidad de control de una máquina de entretenimiento accionada por monedas, un intento de fraude mecánico y/o electrónico en los puntos de contacto para la modificación de las señales no tiene éxito. Debido a que la clave de seguridad emitida por la unidad de control al verificador de monedas cambia constantemente, se dificulta el rastreo por parte de terceros del posible proceso y solamente podría ser reproducido mediante la utilización masiva de medios de medición. Un rastreo de los datos necesarios *in situ* en una máquina de entretenimiento accionada por monedas que se encuentre en funcionamiento es, por lo tanto, suficientemente difícil y evita una manipulación de los impulsos de los valores transmitidos por el verificador de monedas a la unidad de control, que originan la modificación en el contador del saldo de la máquina de entretenimiento accionada por monedas.

Por parte de la unidad de control de la máquina de entretenimiento accionada por monedas se transmite un número de transacción al control del módulo periférico, realizado como verificador de monedas. El control del módulo periférico, realizado como verificador de monedas, emite una respuesta sin un número real a la unidad de control, cuando no hay un valor monetario. Por parte de la unidad de control se reconoce que no hay un valor monetario y la unidad de control remite de nuevo el número de transacción enviado anteriormente al módulo periférico, realizado como verificador de monedas. Cuando existe un valor monetario en el módulo periférico, realizado como verificador de monedas, se forma un número real entre el número de transacción transmitido por la unidad del control al control del verificador de monedas con el valor calculado del medio de pago introducido y aceptado y al menos otra constante más, conocida por la unidad del control, de acuerdo con un algoritmo predeterminado por el control del módulo periférico, que contiene un microprocesador. Desde el control del módulo periférico, p.ej. el verificador de monedas, se transmite seguidamente a la unidad de control el número real y el valor del medio de pago introducido. La unidad de control comprueba si el valor transferido en el número real del medio de pago concuerda con el valor transmitido. Solamente en caso de concordancia entre al valor del medio de pago que fue transmitido, y del valor a calcular a partir del número real, la unidad de control incrementa el contador de saldo en cuanto a este valor transmitido del medio de pago aceptado, p.ej. monedas. La unidad de control conoce el algoritmo y también la constante aplicados para la formación del número real.

La constante aplicada se puede formar, por ejemplo, a partir de la fecha, la hora y/o el número de serie del módulo periférico, p.ej. el verificador de monedas, lector de tarjetas-chip, unidad de escritura o sistema de aceptación de billetes.

El número de transacción emitido por la unidad de control al módulo periférico se genera mediante un generador aleatorio. El número real utilizado tiene un volumen de 2 Bytes.

En otra de las realizaciones conforme a la invención se calcula por parte de la unidad de control periódicamente un número de transacción, formado por un generador seudoaleatorio, y se transmite al control que contiene un microprocesador del módulo periférico, p.ej. del verificador de monedas. Por parte del control del módulo periférico, p.ej. el verificador de monedas, se forma un número real a partir del número de transacción, del valor calculado y de al menos otra constante más. El número real, y adicionalmente el valor calculado del medio de pago aceptado, son transmitidos a la unidad de control. Por parte de la unidad de control se forma, en un lenguaje claro del medio de pago aceptado, el número real según el valor recibido, el número de transacción previamente calculado y transmitido a la unidad de control, la constante

y de acuerdo con el algoritmo conocido. El número real calculado por la unidad de control es comparado por la misma con el número real transmitido. En caso de concordancia, el valor del medio de pago transmitido en un lenguaje claro se acumula en el contador de saldo de la unidad de control.

REIVINDICACIONES

1. La invención se refiere a un procedimiento para la encriptación de datos, transmitidos desde un módulo periférico a una unidad de control de una máquina accionada por monedas, en donde la unidad de control contiene al menos un contador de saldo que lleva asignado medios de visualización, en donde la unidad de control transmite repetidamente al control un número de transacción generado por un generador aleatorio, el control forma una constante a partir del número de serie del módulo periférico o de la fecha o entre ambas, y el control forma un número real, cuando existe un valor monetario de un medio de pago introducido y aceptado por el módulo periférico, a partir del número de transacción, del valor de pago calculado y de la constante, de acuerdo con un algoritmo predeterminado, en donde el control transmite el número real y el valor del pago a la unidad de control, la unidad de control comprueba si el valor del pago transmitido en el número real es idéntico que el valor de pago transmitido, y la unidad de control acumula, en caso de concordancia de los valores de pago, el valor de pago transmitido en el contador de saldo de la máquina.

2. Procedimiento para la encriptación de datos, transmitidos desde un módulo periférico a una unidad de control de una máquina accionada por monedas, en donde la unidad de control contiene al menos un contador de saldo que lleva asignado medios de visualización, en donde la unidad de control calcula periódicamente un número de transacción formado por un generador seudoaleatorio y lo transmite al control, el control forma una constante a partir del número de serie del módulo periférico o de la fecha o entre ambas, y el control forma un número real, cuando existe un valor monetario de un medio de pago introducido y aceptado por el módulo periférico, a partir del número de transacción, del valor de pago calculado y de la constante, de acuerdo con un algoritmo predeterminado, en donde el control transmite el número real y el valor de pago a la unidad de control, la unidad de control calcula asimismo también el número real a partir del número de transacción, del valor de pago transmitido y de la constante, según el algoritmo predeterminado, y comprueba si el número real calculado es idéntico con el número real transmitido, y la unidad de control acumula, en caso de concordancia de los valores de pago, el valor de pago transmitido en el contador de saldo de la máquina.

3. Procedimiento según una de las reivindicaciones 1 y 2, **caracterizado** porque el número real es igual o superior a 1 Byte.

4. Procedimiento según una de las reivindicaciones 1 hasta 3, **caracterizado** porque la unidad de control transmite el número de transacción periódicamente al control.

5. Procedimiento según una de las reivindicaciones 1 hasta 4, **caracterizada** porque el control emite, cuando recibe un número de transacción, una respuesta sin número real a la unidad de control, cuando no existe un valor de pago.

6. Procedimiento según una de las reivindicaciones 1 hasta 5, **caracterizado** porque el valor de pago es un valor monetario.

7. Procedimiento según una de las reivindicaciones 1 hasta 6, **caracterizado** porque el módulo periférico es un verificador electrónico de monedas.

8. Procedimiento según una de las reivindicaciones 1 hasta 7, **caracterizado** porque el módulo periférico es un dispositivo para la aceptación y comprobación de la autenticidad y valencia de los billetes.

9. Procedimiento según una de las reivindicaciones 1 hasta 8, **caracterizado** porque el módulo periférico es un dispositivo para la aceptación y lectura de tarjetas con chip.

10. Procedimiento según una de las reivindicaciones 1 hasta 9, **caracterizado** porque el módulo periférico contiene un microprocesador.