(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 569 209**

(51) Int. CI.:

H04L 12/22 (2006.01)
H04L 29/06 (2006.01)
G06F 21/72 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.12.2006 E 06830777 (6)**

(97) Fecha y número de publicación de la concesión europea: **09.03.2016 EP 1964316**

(54) Título: **Sistema en chip seguro**

(30) Prioridad:

23.12.2005 EP 05112980

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
09.05.2016

(73) Titular/es:

NAGRAVISION S.A. (100.0%)
ROUTE DE GENÈVE 22-24
1033 CHESEAUX-SUR-LAUSANNE, CH

(72) Inventor/es:

KUDELSKI, ANDRÉ

(74) Agente/Representante:

TOMAS GIL, Tesifonte Enrique

DESCRIPCIÓN

Sistema en chip seguro.

Introducción

[0001] La presente invención concierne el campo de los sistemas en chip y en particular la seguridad relacionada con éstos.

Estado de la técnica

[0002] El sistema en chip o "System on Chip" (SoC o SOC) es una idea de integración de todos los componentes de un sistema informático u otro sistema electrónico en un único circuito integrado (chip).
Puede contener funciones digitales, análogas, de señal mixta, y frecuentemente de radiofrecuencia, todo en un chip.
Una aplicación típica es en el área de los sistemas embebidos.

[0003] Ya se han descrito entornos seguros para procesadores, en particular respecto a la arquitectura de multiprocesamiento.
Por ejemplo, una solución para limitar el acceso a una memoria segura fue descrito en el documento WO04015553.
Según esta solución, el procesador tiene dos modos de funcionamiento; en el primer modo, llamado el modo seguro, se permite el acceso a la memoria segura; y en el modo no seguro, el acceso a la memoria segura está prohibido.
El modo no seguro está destinado a fines de desarrollo, por ejemplo, a probar o depurar el circuito.
Durante la ejecución en modo no seguro, el acceso a la memoria segura es bloqueado físicamente , es decir, se genera una señal "desactivar".
Esta señal "desactivar" prohíbe cualquier intento de acceder la memoria segura.

[0004] Otra solución se describe en el documento PCT/EP2005/056145, donde un procesador de desaleatorización de un único chip procesa los datos de audio/vídeo aleatorizados para no dejar nunca el acceso a los datos libres.
Cuando la operación de desaleatorización se ha completado, la unidad de desaleatorización comprende un motor de encriptación para encriptar los datos desaleatorizados antes de que éstos sean almacenados temporalmente en una memoria externa.
Cuando el procesador finaliza la tarea de organización, los datos se descifran en el módulo de salida y se envían al dispositivo de visualización.

[0005] El documento US2005/182948 divulga un dispositivo de sistema en chip (SOC) que comprende salidas externas y entradas externas.
Una primera ubicación de almacenamiento seguro está operativamente desvinculada de todas las salidas externas del dispositivo SOC durante un modo normal de funcionamiento.
Al estar desvinculadas de todas las salidas externas, se evita que representaciones de los datos almacenados en el primer dispositivo seguro sean proporcionadas a las salidas externas.
El motor de desencriptación también está incluido en el sistema en chip, que comprende una primera entrada de datos, y una entrada de clave privada acoplada a una primera parte de la primera ubicación de almacenamiento seguro, y una salida acoplada a una segunda ubicación segura.
El motor de desencriptación es operable para determinar datos descifrados a partir de datos recibidos en la primera entrada de datos basándose en una clave privada recibida en la entrada de clave privada.
El motor de desencriptación es posteriormente operable para escribir los datos desencriptados sólo a la primera ubicación de memoria segura y a la segunda ubicación segura.

Breve descripción de la invención

[0006] El objetivo de la presente invención es el de proporcionar un sistema en chip seguro para el procesamiento de datos, sistema en chip que comprende al menos una unidad central de procesamiento, un canal de entrada y de salida, un motor de encriptación/desencriptación y una memoria, caracterizado por el hecho de que dicho canal de entrada comprende un módulo de encriptación de entrada para añadir una capa de encriptación interna a todos los datos entrantes, donde dicho canal de salida incluye un módulo de desencriptación de salida para eliminar la capa de encriptación interna de todos los datos salientes, donde dicha unidad central de procesamiento recibe los datos encriptados del módulo de encriptación de entrada y los almacena en la memoria y, mientras procesa los datos almacenados, dicha unidad central de procesamiento lee los datos almacenados de la memoria, solicita la eliminación de la capa de encriptación interna de los mismos en el motor de encriptación/desencriptación, procesa los datos y solicita la encriptación del resultado por el motor de encriptación/desencriptación para añadir la capa de encriptación interna y almacena el resultado encriptado, envía el resultado al módulo de desencriptación de salida para la eliminación de la capa de encriptación interna y hace salir el resultado a través del canal de salida.

[0007] La característica principal de la invención es la adición de una capa de encriptación en el sistema en chip.
Los datos que entran y salen del sistema en chip normalmente están encriptados.
Se aplica una capa de encriptación adicional a estos datos de modo que todos los datos almacenados en el sistema

en chip tengan al menos una capa de encriptación.
Una vez los datos se reciben en el sistema en chip, éstos normalmente son descifrados con la clave que pertenece al sistema de transmisión y el resultado se almacena en claro.
En la presente invención, una vez el mensaje encriptado es leído por el sistema en chip, se aplica una capa de encriptación interna sobre este mensaje y y se pasa a la unidad de procesamiento.
Dicha unidad puede memorizarla para otro uso o procesar inmediatamente el mensaje.
Durante el tratamiento del mensaje, el primer paso es eliminar la capa de encriptación interna de modo que los datos estén en el mismo estado en que fueron recibidos por el sistema en chip.
Después de que el mensaje sea procesado y el permiso (por ejemplo) extraído, este permiso es posteriormente encriptado para añadir la capa de encriptación interna antes de ser almacenado.

[0008] La eliminación de la capa de encriptación interna ocurre solo en la fase posterior cuando los datos son realmente usados por la unidad central, sin que los datos libres sean accesibles en ingñun momento en estado estático.
Cuando se han procesado, los datos se pueden almacenar en claro si son para uso interno o reencriptados (por ejemplo. añadiendo la capa de encriptación interna) si están destinados a ser emitidos desde el sistema en chip.

[0009] Una vez reencriptados, los datos son temporalmente almacenados en un búfer antes de ser enviados al canal de salida.

[0010] La clave para encriptar y desencriptar los datos es, en una forma de realización preferida, única para ese sistema en chip.
Esta clave se puede preprogramar en el paso de fabricación o puede ser generada de forma aleatoria en la fase de inicialización y no ser conocida por nadie en ningún momento.
Esta clave se usa sólo internamente.
El algoritmo usado se puede guardar en secreto, al igual que los parámetros de dicho algoritmo.
Por ejemplo, el algoritmo IdeaNxt se usa como motor de encriptación y los valores de la caja de sustitución son generados de forma aleatoria en el sistema en chip.

[0011] Según una forma de realización particular, el algoritmo de encriptación/desencriptación es asimétrico, de modo que un par de claves (pública/privada) se utiliza respectivamente para encriptar y desencriptar los datos.

[0012] Según una forma de realización alternativa, el módulo de encriptación de entrada se puede sustituir por un módulo de firma, donde los datos se firman mientras son introducidos en el sistema en chip y la firma se almacena junto con los datos.
Cuando la unidad central desea usar estos datos, el motor de encriptación/desencriptación que es ahora un motor de verificación de firma, verifica la firma y autoriza el uso de los datos si la firma es correcta.

[0013] Por datos se hace referencia a un único byte o un conjunto de bytes, por ejemplo para formar un mensaje o un mensaje de permiso en el sistema en chip.

Breve descripción de los dibujos

[0014] La invención se entenderá mejor gracias a las figuras adjuntas, donde:

- la figura 1 describe el sistema en chip y su distintos elementos en el modo de encriptación/desencriptación,
- las figuras 2A y 2B describen la fase de encriptación usando dos unidades,
- la figura 3 describe el sistema en chip y su distintos elementos en el modo de firma.

Descripción detallada de la invención

[0015] El sistema en chip seguro SOC se basa en una unidad central de procesamiento CPU.
El objetivo de esta unidad es ejecutar el código y ejecutar las tareas solicitadas.
El sistema en chip SOC comprende dos canales conectados al mundo exterior, es decir, los canales de entrada y de salida.
El canal de entrada RCV comprende un módulo de encriptación de entrada RCV-E que encripta todos los datos que vienen del mundo exterior para añadir una capa de encriptación interna.
De la misma manera, el canal de salida SND comprende un módulo de desencriptación de salida SND-D para desencriptar los datos recibidos de la unidad central CPU antes de enviarlos al mundo exterior para eliminar el capa de encriptación interna.

[0016] La unidad central CPU tiene acceso al motor de encriptación/desencriptación CR-EN.
Este motor tiene la misma función que el módulo de encriptación de entrada y el módulo de desencriptación de salida.
La clave K cargada en el módulo de encriptación de entrada es la misma en la parte de encriptación del motor de encriptación/desencriptación.

Lo mismo se aplica al módulo de desencriptación de salida y la parte de desencriptación del motor de encriptación/desencriptación, para las operaciones de desencriptación.
Cuando la unidad central CPU necesita algunos datos, o bien que vienen directamente del módulo de encriptación de entrada o bien extraídos de la memoria MEM, estos datos primero son pasados a través del motor de desencriptación para eliminar la capa de encriptación interna antes de que sean usados por la unidad central CPU.

[0017] De la misma manera, cuando la unidad central CPU ha completado una tarea y produce un resultado, el siguiente paso es memorizar el resultado (o enviar el resultado al canal de salida).
Este resultado es previamente pasado a través del motor de encriptación CR-EN para añadir la capa de encriptación interna antes de ser almacenado.
Este resultado encriptado después puede ser almacenado en una memoria o enviado al canal de salida.

[0018] La unidad central de procesamiento CPU puede decidir si el resultado debe ser reencriptado o dejado en claro.
En vez de dejar que el procesador decida, la ubicación de destino puede seleccionar comportamientos diferentes como se muestra en figura 2A.
En este caso, la capa de encriptación interna está hecha de dos unidades de encriptación ENC1, ENC2, que usan dos claves diferentes K1, K2, una clave permanente, y una clave generada de forma aleatoria.
Si el resultado debe ser almacenado en una memoria volátil V-MEM, ambas unidades de encriptación encriptarán los datos.
Por el contrario, si el almacenamiento es en una memoria no volátil NV-MEM (EEPROM), sólo se usa una unidad de encriptación, la de la clave permanente.
De la misma manera, al leer los datos de la memoria volátil, se aplica la desencriptación doble aunque, al leer datos de la memoria no volátil, sólo se aplica una unidad de desencriptación.

[0019] Según una forma de realización alternativa mostrada en la figura 3, el proceso de encriptación se sustituye por un proceso de firma.
Los datos no son encriptados, sino que se genera una firma y se asocia a los datos.
Para todos los datos que viene del mundo exterior, se calcula una firma en el módulo de firma de entrada RCV-S.
Los datos se almacenan luego con sus firmas.
Cuando la unidad central necesita acceder estos datos, el motor de verificación de firma S-VER primero verifica la firma antes de que la unidad central tenga permiso para usar los datos.
Antes de que los datos se emitan por el canal de salida, la firma es verificada en el módulo de firma de salida SDN-V.
Entonces, la firma es eliminada de los datos que se envían al canal de salida SND.

[0020] Según una forma de realización alternativa, el motor de encriptación/desencriptación está localizado directamente en la unidad central CPU.
Cuando se lee un dato de la memoria, por ejemplo cargando una variable en el acumulador de la CPU (por ejemplo LDAA #1200h para Motorola 68HC11), el dato leído en esa ubicación se pasa automáticamente al motor de desencriptación para eliminar la capa de encriptación interna antes de ser transferido al acumulador.
De la misma manera, la instrucción de almacenar el contenido del acumulador a la memoria (por ejemplo STAA #1200h) no se ejecuta directamente, sino que el dato del acumulador se pasa previamente a través del motor de encriptación (para añadir la capa de encriptación interna) antes de ser almacenado en la ubicación 1200h.

[0021] En una forma de realización particular, el motor de encriptación/desencriptación se comparte con el canal de entrada y de salida.
El módulo de encriptación de entrada es por lo tanto un módulo virtual y las operaciones de encriptación en el canal de entrada se consiguen por el motor de encriptación a través de un multiplexor de datos.
Los datos introducidos en el sistema en chip SOC, en particular a través del canal de entrada, se pasan a través del motor de encriptación antes de otras manipulaciones, por ejemplo para almacenar los datos en un búfer de entrada.
El módulo de encriptación de entrada es por lo tanto un módulo virtual que utiliza el recurso del motor de encriptación/desencriptación en el modo de encriptación.
Lo mismo se aplica al módulo de desencriptación de salida que usa el motor de encriptación/desencriptación en el modo de desencriptación.

[0022] El módulo de encriptación de entrada RCV-E puede comprender más de una unidad de encriptación.
Según una forma de realización particular mostrada en la figura 2A, dos unidades de encriptación (o más) se conectan en serie, cada una con una clave diferente.
La primera unidad de encriptación se carga con una clave K1 que pertenece al sistema en chip, es decir, es única y constante para un dispositivo específico.
Esta clave se carga o bien durante el paso de instalación o bien se genera internamente.
La segunda unidad ENC2 se carga con una clave K2 que se genera dinámicamente en el encendido del dispositivo.
Cuando el sistema en chip se reinicia, esta clave se pierde y se genera una nueva clave.
Los datos que tienen que ser permanentemente almacenados, una vez procesados por el procesador CPU, son sólo reencriptados con la primera unidad con la clave permanente K1.

[0023] El módulo de desencriptación de salida, así como el motor de encriptación/desencriptación, comprenden de la misma manera también dos o más unidades.

[0024] Alternativamente, si el procesador CPU reconoce que los datos recibidos, almacenados en un búfer de entrada, no necesitan ser procesados sino que sólo deben ser almacenados en una memoria permanente NV-MEM, el procesador puede solicitar del motor de encriptación/desencriptación la desencriptación por una sola unidad de desencriptación, por ejemplo la unidad con la clave volátil.
Los datos almacenados todavía siguen encriptados por la clave permanente para un uso posterior.

[0025] El sistema en chip SOC puede comprender adicionalmente un módulo de supervisión autónomo SM que puede de forma determinista controlar el sistema en chip SOC. Este módulo SM comprende unas definiciones de condiciones de trabajo normales del sistema en chip SOC, y medios de deshabilitación cuando las condiciones normales ya no se cumplen.
Este se consigue por diferentes medios.
Un primer medio incluye la medición de la cantidad de datos emitidos, por ejemplo el recuento del número de conjuntos de datos emitidos.
Esta operación será de aquí en adelante descrita como recuento de datos.
Un segundo medio incluye la definición de periodos de tiempo durante los cuales se permiten las operaciones de entrada o de salida.
Un bloque de datos es, por lo tanto permitido, si la longitud del mismo no excede el tiempo máximo definido para un bloque.
Un tercer medio incluye la detección del estado de la unidad central CPU y su duración respectiva, y la acción consiguiente como se ilustrará de aquí en adelante.
La unidad central CPU típicamente tiene diferentes estados posibles, tales como estado de adquisición, estado de procesamiento, estado de espera y estado de resultado de emisión.
Cuando un mensaje llega al sistema en chip, éste cambia del estado de espera al estado de adquisición.
Durante ese estado de adquisición, el canal de entrada es habilitado por el módulo de supervisión SM.
También durante el mismo estado de adquisición, el módulo de supervisión SM cuenta los datos que llegan y compara este número con un máximo predefinido.
Cualquier situación anormal lleva a un estado de advertencia en el que la unidad central CPU puede decidir cómo reaccionar.
El módulo de supervisión SM tiene la capacidad, especialmente en caso de un estado de advertencia, de bloquear los canales de entrada y de salida y/o el el motor de encriptación/desencriptación CR-EN.

[0026] Cuando el mensaje externo se recibe, el módulo de supervisión SM hace que la unidad central CPU se ponga en estado de procesamiento.
Durante este estado, los canales de entrada y de salida están deshabilitados.
El módulo de supervisión SM comprende un modelo temporal que corresponde con el tiempo de procesamiento mínimo de la unidad central CPU, y deshabilita los canales durante este tiempo.
La unidad central CPU puede informar al módulo de supervisión SM de que no se va a emitir ningún resultado.
Esto tiene como consecuencia que el módulo de supervisión SM sólo habilita el canal de entrada para esperar un mensaje nuevo.
Entonces, el canal de salida permanece deshabilitado.

[0027] En el caso de que la unidad central CPU desee enviar datos al mundo exterior, informa de ello al módulo de supervisión SM, que a su vez habilita el canal de salida.
El módulo de supervisión SM sigue controlando las actividades en el canal de salida mediante el recuento de los datos enviados y mediante la aplicación de un periodo de tiempo durante el cual el envío está autorizado.

[0028] En esta forma de realización de la invención, el módulo de supervisión SM es así capaz de trabajar con información recibida de la unidad central CPU, al igual que con modelos de trabajo preprogramado.

[0029] Este módulo puede también controlar el motor de encriptación/desencriptación al contar los datos encriptados o desencriptados.
De la misma manera, el modelo de trabajo del motor de encriptación/desencriptación CR-EN es supervisado en cuanto a la cantidad de datos procesados y tiempo.
El módulo de supervisión puede deshabilitar el motor de encriptación/desencriptación CR-EN si se detectan condiciones anormales.

[0030] Se debe tener en cuenta que el módulo de supervisión SM se puede implementar en un sistema en chip sin la encriptación/desencriptación en el canal de entrada/salida.
Los datos son procesados sin añadir un nivel de encriptación (o desencriptación) adicional y el canal de entrada/salida es controlado por el módulo de supervisión SM.

[0031] Este sistema en chip SOC se usa en el módulo de control de acceso seguro encargado de recibir mensajes

de gestión que incluyen permisos o claves.
Este módulo puede también comprender una unidad de desaleatorización de alta velocidad para recibir un flujo de datos de vídeo encriptados.

REIVINDICACIONES

1. Sistema en chip (SOC) seguro para el procesamiento de datos, sistema en chip que comprende al menos una unidad central de procesamiento (CPU), un canal de entrada (RCV) y de salida (SND), un motor de encriptación/desencriptación (CR-EN) y una memoria (MEM), **caracterizado por el hecho de que** dicho canal de entrada comprende un módulo de encriptación de entrada (RCV-E) para añadir una capa de encriptación interna a todos los datos entrantes, donde dicho canal de salida incluye un módulo de desencriptación de salida (SND-D) para eliminar la capa de encriptación interna de todos los datos salientes, donde dicha unidad central de procesamiento recibe los datos encriptados del módulo de encriptación de entrada y los almacena en la memoria y, mientras procesa los datos almacenados, dicha unidad central de procesamiento lee los datos almacenados de la memoria, solicita la eliminación de la capa de encriptación interna de los mismos en el motor de encriptación/desencriptación, procesa los datos y solicita la encriptación del resultado por el motor de encriptación/desencriptación para añadir la capa de encriptación interna y almacena el resultado encriptado, envía el resultado al módulo de desencriptación de salida para la eliminación de la capa de encriptación interna y hace salir el resultado a través del canal de salida.

2. Sistema en chip seguro según la reivindicación 1, **caracterizado por el hecho de que** el módulo de encriptación de entrada es un módulo virtual que pasa los datos que han de ser encriptados al motor de encriptación/desencriptación mientras añade la capa de encriptación interna.

3. Sistema en chip seguro según la reivindicación 1, **caracterizado por el hecho de que** el módulo de encriptación de entrada es un módulo virtual que pasa los datos que han de ser desencriptados al motor de encriptación/desencriptación mientras elimina la capa de encriptación interna.

4. Sistema en chip seguro según las reivindicaciones 1 a 3, **caracterizado por el hecho de que** el algoritmo para encriptar y desencriptar los datos es un algoritmo simétrico.

5. Sistema en chip seguro según la reivindicación 4, **caracterizado por el hecho de que** el algoritmo de encriptación/desencriptación usa un conjunto de constantes de inicialización y todas o parte de las constantes de inicialización son generadas de forma aleatoria en el sistema en chip.

6. Sistema en chip seguro según las reivindicaciones 1 a 3, **caracterizado por el hecho de que** el algoritmo para encriptar y desencriptar los datos es un algoritmo asimétrico.

7. Sistema en chip seguro según las reivindicaciones 1 o 6, **caracterizado por el hecho de que** comprende medios para generar de forma aleatoria la clave o el par de claves usadas para el motor de encriptación/desencriptación.

8. Sistema en chip seguro según las reivindicaciones 1 o 6**, caracterizado por el hecho de que** el módulo de encriptación de entrada, así como el módulo de desencriptación de salida, comprende varias unidades de encriptación o desencriptación respectivamente, al menos una de estas unidades se carga con una clave que es no volátil y al menos una de estas unidades se carga con una clave permanente.

9. Sistema en chip seguro según las reivindicaciones 1 o 8, **caracterizado por el hecho de que** comprende un módulo de supervisión autónoma (SM) que está preprogramado con definiciones de las condiciones de trabajo normales de al menos el flujo de datos de entrada y/o de salida, y medios para deshabilitar el canal de entrada y/o de salida si las condiciones actuales se salen de las definiciones de condiciones normales.

10. Sistema en chip seguro según la reivindicación 9, **caracterizado por el hecho de que** la definición de las condiciones de trabajo normales comprende una duración en la que el módulo de supervisión (SM) comprende medios para definir un periodo de tiempo durante el que el canal de entrada o de salida tiene permitido recibir o enviar datos.

11. Sistema en chip seguro según la reivindicación 9 o 10, **caracterizado por el hecho de que** la definición de las condiciones de trabajo normales comprende una duración en la que el módulo de supervisión deshabilita el canal de entrada y/o de salida después de la recepción de un bloque de datos.

12. Sistema en chip seguro según la reivindicación 9 a 11, **caracterizado por el hecho de que** el módulo de supervisión (SM) comprende medios para recibir la condición de estado de la unidad central de procesamiento (CPU), y medios para habilitar o deshabilitar el canal de salida según el estado de la unidad central de procesamiento (CPU).

13. Sistema en chip seguro según cualquiera de las reivindicaciones 1 a 12, **caracterizado por el hecho de que** las operaciones de encriptación/desencriptación se pueden ejecutar en un único dato o en un conjunto de datos a la vez.

Fig. 1

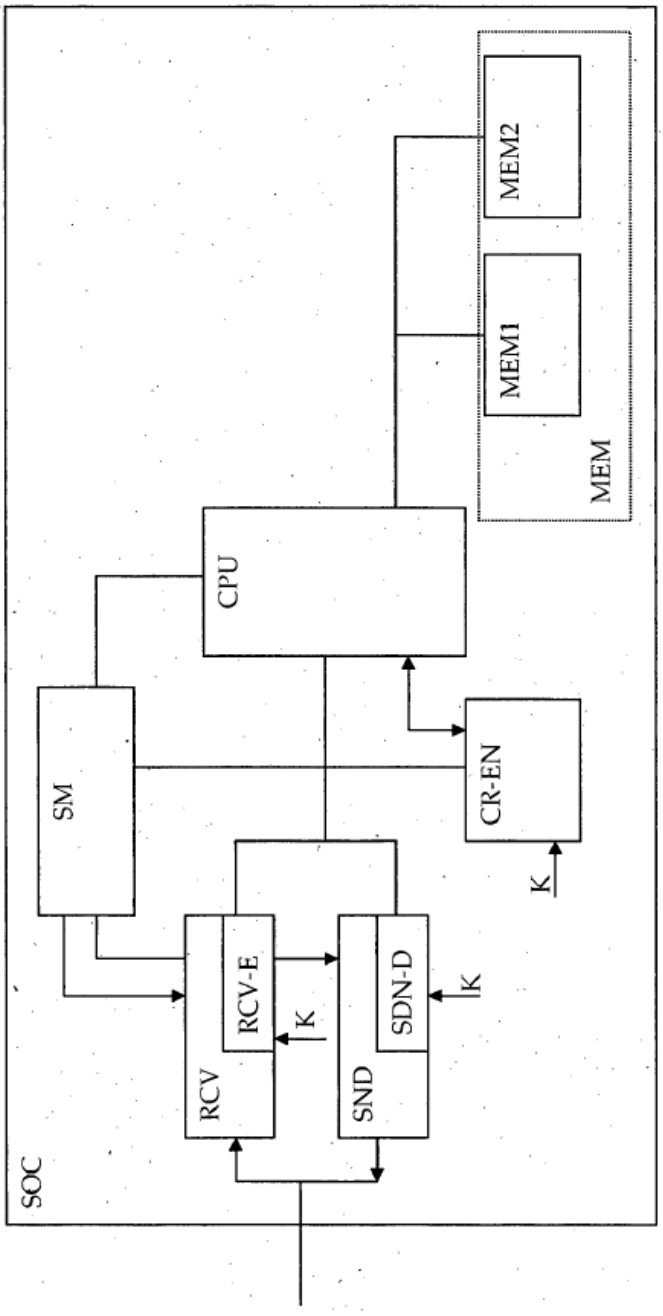


Fig. 2A

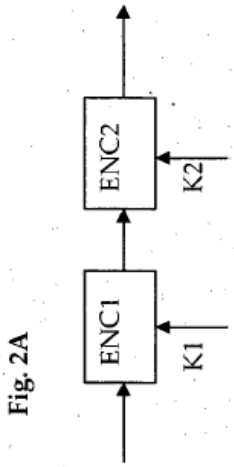
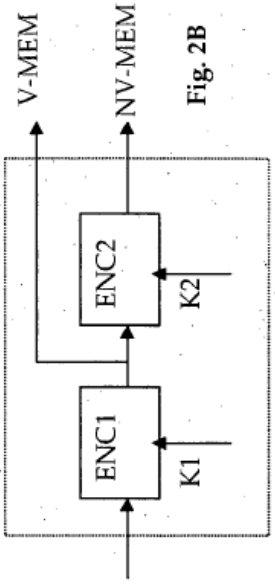


Fig. 2B



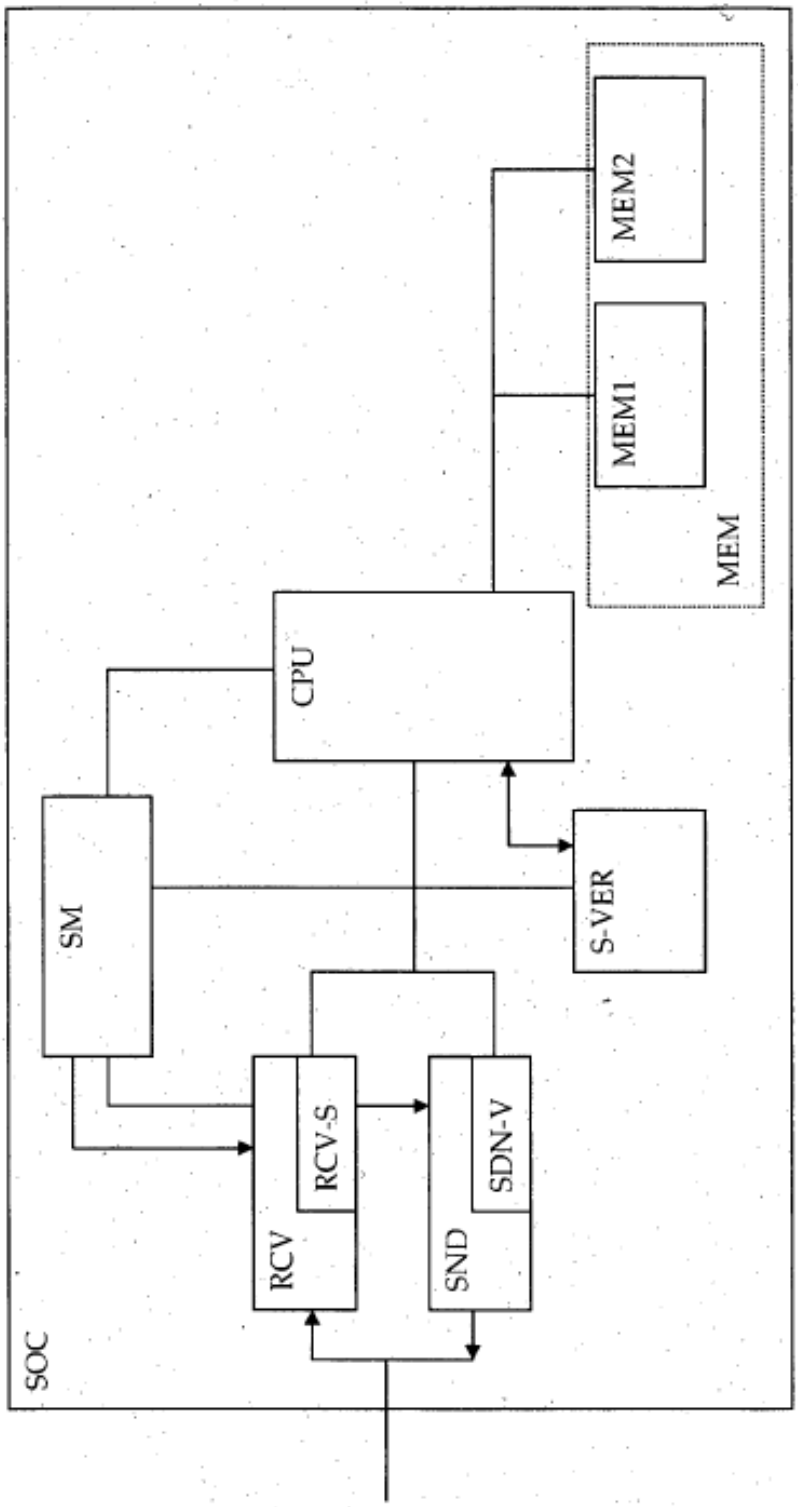


Fig. 3