



УКРАЇНА

(19) UA

(11) 46064

(13) C2

(51) 6 H04L9/00

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІОПИС
ДО ПАТЕНТУ НА ВІНАХІД

(54) МІКРОСХЕМА БЕЗПЕКИ ЗВ'ЯЗКУ

1

2

(21) 98042063

(22) 25 09 1996

(24) 15 05 2002

(86) PCT/DE96/01813, 25 09 1996

(31) 195 39 700 2

(32) 25 10 1995

(33) DE

(46) 15 05 2002, Бюл. № 5, 2002 р

(72) Еберхард Гюнтер, DE, Гесснер Юрген, DE,

Шефер Манфред, DE, Мьопер Вольф-Дітріх, DE

(73) ДАЙМЛЕР-БЕНЦ АКЦІОНГЕЗЕЛЬШАФТ, DE

(56) US 5355413 A, 11 10 1994

ELECTRONICS, Bd 54, Nr 12, p 161-165,
16 06 1981

IEEE MICRO, Bd 3, Nr 5, p 5-15, October 1983

(57) 1 Мікросхема безпеки зв'язку (SC), яка зв'язана з приєднуваними апаратними засобами (AHW) тільки через інтерфейс даних (DS) і через інтерфейс команд (BS), у якій передбачені процесор (P), набір (VZ) алгоритмічних модулів (AM_i, i=1 n), призначених для здійснення алгоритмів шифрування, причому незалежні алгоритмічні модулі (AM_i) зв'язані через власну внутрішню шину (IB) мікросхеми з процесором (P) та через власну внутрішню шину даних (DB) мікросхеми - з інтерфейсом даних (DS), запам'ятовуючий

пристрій (SP), зв'язаний з внутрішньою шиною (IB) мікросхеми

2 Мікросхема безпеки (SC) за п. 1, в якій передбачений щонайменше один алгоритмічний модуль (AM_i) для здійснення симетричних алгоритмів шифрування (SV)

3 Мікросхема безпеки (SC) за п. 1 або п. 2, в якій з набору (VZ) алгоритмічних модулів (AM_i) передбачений щонайменше один алгоритмічний модуль (AM_i) для здійснення асиметричних алгоритмів шифрування (AV)

4 Мікросхема безпеки (SC) за будь-яким з пп. 1-3, в якій передбачено таймер (ZM), що надійно формує і видає сигнали абсолютного часу і/або сигнали відносного часу

5 Мікросхема безпеки (SC) за будь-яким з пп. 1-4, в якій передбачено сенсорний модуль (SM) і/або виконавчий модуль (AKM) для виявлення спроб несанкціонованого підключення до мікросхеми безпеки (SC) і/або для здійснення заходів безпеки при наявності розпізнаних спроб несанкціонованого підключення до мікросхеми безпеки (SC)

6 Мікросхема безпеки (SC) за будь-яким з пп. 1-5, в якій алгоритмічні модулі (AM_i) виконані з можливістю підтримки керування криптографічним ключем безпосередньо в апаратних засобах

Для здійснення безпеки зв'язку, наприклад під час обміну даними або мовного зв'язку, використовують криптографічні алгоритми шифрування безпосередньо даних зв'язку. Різноманітні алгоритми застосовуються, наприклад, для забезпечення конфіденційності й автентичності переданих даних або партнерів по зв'язку.

Тому потрібні мікросхеми безпеки, що здійснюють криптографічне шифрування для різних інформаційно-технічних застосувань.

Вже існують модулі безпеки, орієнтовані на конкретні застосування, наприклад, модуль безпеки, призначений для здійснення безпечної передачі телефаксів (Сіменс, DSM-Fax, безпечна передача факсів, сфера діяльності Сіменс - "Техніка безпеки") або для шифрування телефонних розмов (Сіменс, DSM-Voice-Telephoning in Confidence,

сфера діяльності Сіменс - "Техніка безпеки", Luis Cypher, LC-1 Цифровий шифратор мовлення для захищеного від підслуховування телефонування).

Крім того існують спеціальні, розроблені для асиметричних криптоалгоритмів, чіп-картки і співпроцесори (IS-Aktuell, Produkte/Systeme, стор 7 - 17 до 7 - 18, квітень 1993) 7 - 17 до 7 - 18, квітень 1993).

Існують також інші мікросхеми безпеки, в яких здійснюється або симетричний криптоалгоритм - з апаратною підтримкою, або асиметричний криптоалгоритм - тільки з програмною підтримкою, або навпаки (L. Goldberg "Нова стратегія шифрування, що використовує апаратне і програмне забезпечення для захисту даних у суспільних мережах зв'язку" Electronic Design, стор 39 - 40, березень 1995, G. Eberhard "Два нових криптопродукти фір-

(13) C2

(11) 46064

(19) UA

ми Сіменс контролер для карт з умонтованою мікросхемою SLE44C200 і співпроцесор SLE44CP2, процесори для асиметричних алгоритмів", IS-Aktuell, стор 7 - 17 – 7 - 18, квітень 1993)

Недоліком цих відомих модулів безпеки є їх обмеженість тільки цілком конкретними застосуваннями. Насамперед - це лише асиметричний алгоритм шифрування даних на одній окремій мікросхемі безпеки, або лише симетричне шифрування даних на мікросхемі, в обох випадках - з прямою апаратною підтримкою

Це обмеження є причиною ще одного недоліку попередніх рішень - критична для безпеки інформація в обчислювальному блоці, що здійснює алгоритм шифрування, частково передається по незахищеній шині обчислювального блоку, наприклад, при керуванні криптографічними ключами і передаванні корисних даних, а тому може бути перехоплена

Завданням даного винаходу є створення мікросхеми безпеки, що не має вищеназаних недоліків

В даному винаході це завдання виконується за допомогою мікросхеми безпеки відповідно до пункту 1 формули винаходу

Згадана мікросхема безпеки повністю розв'язана від приєднаних апаратних засобів і може "запитуватися" тільки через інтерфейс даних і інтерфейс команд. Оскільки мікросхема безпеки містить в собі власний процесор, власну внутрішню шину мікросхеми, до якої під'єднані апаратні засоби не мають доступу, а також різні алгоритмічні модулі, що здійснюють різні засоби безпеки, за асиметричними і симетричними алгоритмами, мікросхема безпеки є універсально застосовною і не подає ніякої, суттєвої для безпеки, інформації на під'єднані апаратні засоби

Таким чином, приєднані апаратні засоби і прикладні програмні засоби можуть як завгодно вводитися, конфігуруватися і погоджуватися без погіршення безпеки різних криптофункцій, що здійснюються алгоритмічними модулями

Завдяки удосконаленню мікросхеми безпеки відповідно до пункту 5 формули винаходу стає можливим розпізнавати зазіхання на підключення до мікросхеми безпеки і, при потребі, реагувати на них стиранням усіх даних

Способи удосконалення відповідно до даного винаходу випливають з відповідних пунктів формули винаходу

Переважний приклад виконання винаходу подано на фігурах і описано далі більш докладно

При цьому

Фігура 1 - ескіз можливого компонування мікросхеми безпеки,

Фігура 2 - блок-схема можливих алгоритмічних модулів,

Фігура 3 - компонування безпечного таймера

За допомогою Фігур 1-3 винахід пояснюється більш докладно

На Фігурі 1 показано компонування мікросхеми безпеки SC

Мікросхема безпеки SC містить в собі, щонайменше, такі компоненти

процесор P,

набір VZ незалежних алгоритмічних модулів

Амі, що забезпечує здійснення алгоритмів шифрування,

запам'ятовуючий пристрій SP,

інтерфейс даних DS, незалежний від продуктивності процесора P,

безпечний інтерфейс команд BS, що здійснює з'єднання або з власною внутрішньою шиною даних DB мікросхеми, або безпосередньо з процесором P,

власну внутрішню шину даних DB мікросхеми, через яку набір VZ незалежних алгоритмічних модулів Амі зв'язаний з інтерфейсом даних DS,

власну внутрішню шину IB мікросхеми, з якою зв'язані всі компоненти крім інтерфейсу даних DS

Завдяки розв'язці інтерфейсу даних DS від внутрішньої шини мікросхеми IB потужність шифрування більше не залежить від процесора P. Крім того внутрішні дані мікросхеми з внутрішньої шини мікросхеми IB не можуть змінюватися або, відповідно, прослуховуватися сторонніми особами, зокрема, на інтерфейсі даних DS

Мікросхема безпеки SC може містити й такі компоненти

таймер ZM,

сенсорний модуль SM,

актуаторний модуль AKM,

Ці компоненти також зв'язані з внутрішньою для мікросхеми шиною IB

Для здійснення зв'язку між окремими компонентами, тобто керування послідовністю операцій, можуть використовуватися різні протоколи зв'язку, незалежно від протоколів зв'язку з під'єднуваними апаратними засобами AHW

Інтерфейс даних DS і інтерфейс команд BS є єдиними точками доступу під'єднаних апаратних засобів AHW до мікросхеми безпеки SC

Приєднані апаратні засоби AHW не мають іншої можливості доступу до мікросхеми безпеки SC і, таким чином, до суттєвих для безпеки даних, що застосовуються і/або запам'ятовуються в мікросхемі безпеки SC

Завдяки цій розв'язці мікросхеми безпеки SC від її "зовнішнього світу", для сторонніх осіб, тобто для злоумисників, надалі стає неможливим одержати з мікросхеми безпеки SC будь-які суттєві для безпеки дані

Процесор P може бути будь-яким процесором, що має достатню щодо вимог запланованого застосування швидкість

Алгоритмічні модулі Амі є незалежними модулями, кожний з яких "відповідає" за конкретний криптографічний протокол або за відповідний спосіб шифрування. Під цим розуміють, наприклад, способи або протоколи шифрування і дешифрування корисних даних, захисту цілісності або цифрового підпису, або утворення хеш-значень. Індекс "i" однозначно ідентифікує кожний алгоритмічний модуль Амі. Він є довільним натуральним числом в області від 1 до n. При цьому n є кількістю алгоритмічних модулів Амі, реалізованих на мікросхемі безпеки SC

Можливі приклади виконання алгоритмічних модулів Амі наведено далі

Алгоритмічний модуль Амі може, наприклад, спеціально призначатися для здійснення криптографічного симетричного способу шифрування SV,

наприклад, стандартного способу шифрування даних (= Data Encryption Standard = DES) Модуль може бути виконаний так, щоб він міг здійснювати DES-шифрування при різних довжинах ключа, наприклад, потрійне DES-шифрування. Інші симетричні криптографічні способи можуть бути реалізовані в інших алгоритмічних модулях АМі.

У іншому прикладі застосування передбачено виконувати в алгоритмічних модулях АМі також асиметричні криптографічні алгоритми АВ. Приклади асиметричних криптографічних алгоритмів АВ достатньо відомі фахівцям, наприклад, RSA-шифрування.

Згадані вище симетричні алгоритми шифрування SV і асиметричні криптографічні алгоритми АВ можуть бути передбачені як окремо, так і разом у різних алгоритмічних модулях АМі на мікросхемі безпеки SC.

На мікросхемі безпеки SC може бути передбачений також набір алгоритмічних модулів АМі однакового типу для здійснення того самого способу шифрування, наприклад, для підвищення продуктивності мікросхеми безпеки SC. Це може, наприклад, передбачати щоб один алгоритмічний модуль АМі був призначений для обробки вхідного потоку даних, а інший алгоритмічний модуль АМі того ж типу - для обробки вихідного потоку даних.

Алгоритмічні модулі АМі служать також для шифрування корисних даних, що через інтерфейс даних DS відкритим текстом подаються під'єднуваними апаратними засобами АНВ на власну внутрішню шину мікросхеми даних DB і можуть шифруватися будь-яким установленим користувачем апаратним засобом АНВ через інтерфейс команд BS, способом шифрування, при якому вибирається також застосований алгоритмічний модуль АМі з набору VZ незалежних алгоритмічних модулів АМі.

Зашифровані в будь-якому алгоритмічному модулі АМі корисні дані знову передаються через власну внутрішню шину мікросхеми даних DB і інтерфейс даних DS, тепер у зашифрованій формі, на під'єднувані апаратні засоби АНВ.

Через інтерфейс даних DS під'єднувані апаратні засоби АНВ повідомляють мікросхемі безпеки SC параметри відповідного запиту на кодування корисних даних. Це може бути, наприклад, заданий алгоритм шифрування, довжина ключа або подібні параметри, необхідні для шифрування корисних даних. Далі з допомогою під'єднуваних апаратних засобів АНВ через інтерфейс даних DS запускається, наприклад, операція шифрування корисних даних.

Процесор Р керує адміністративним протіканням процесів шифрування даних у мікросхемі безпеки SC, а також роботою описаних далі криптографічних протоколів.

Проте, процесор Р не обов'язково транспортує зашифровані, розшифровані або відповідно оброблені криптографічним способом корисні дані. Звичайно, якщо вони не транспортуються процесором Р, вони транспортуються через власну внутрішню шину мікросхеми даних DB, що є ще однією перевагою мікросхеми безпеки SC - продуктивність шифрування SC не залежить від процесора Р.

Крім того, завдяки розв'язці внутрішньої шини даних мікросхеми DB від внутрішньої шини мікросхеми IB унеможливорюється прослуховування або зміна на інтерфейсі DS внутрішніх даних, що транспортуються через власну внутрішню шину мікросхеми IB.

Це значно поліпшує характеристики безпеки мікросхеми безпеки SC у порівнянні з відомими модулями безпеки, оскільки суттєві для безпеки дані, наприклад, застосований для шифрування криптографічний ключ, не можуть бути розпізнаваними сторонньою особою.

У запам'ятовуючому пристрої SP запам'ятовують як незашифровані дані, так і дані, що повинні тимчасово запам'ятовуватися для здійснення криптоалгоритмів, наприклад, проміжні ключі в способах шифрування, що працюють за принципом експоненціальної зміни ключа, або проміжні ключі, що застосовують у DES-шифруванні.

Алгоритмічні модулі АМі можуть також призначатися для здійснення різних засобів безпеки, наприклад відомих протоколів автентифікування або також для здійснення способів зміни ключа, або генерування криптографічних ключів.

За допомогою сенсорного модуля SM виявляють фізичні зазіхання на підключення до мікросхеми безпеки SC, можна також оцінювати й повідомляти про це процесор Р, через власну внутрішню шину мікросхеми IB.

У виконавчому модулі АКМ за командою з процесора Р вживаються заходи для знешкодження виявлених сенсорним модулем SM зазіхань. Таким засобом безпеки може бути, наприклад, стирання всіх запам'ятованих на даний момент в запам'ятовуючому пристрої даних.

Таймер ZM містить в собі, щонайменше, такі компоненти:

- інтерфейс таймера ZIO,
- контролер таймера ZC,
- лічильну схему ZS, причому лічильна схема ZS містить в собі, щонайменше
- буфер даних DB,
- лічильник реального часу RZ,
- узгоджувач такту TA, і
- комутатор лічильника ZU.

Таймер ZM виконує автономні завдання, наприклад, видачу миток часу Мпкі часу через інтерфейс таймера ZIO подаються на інші під'єднувані до мікросхеми безпеки SC апаратні засоби.

Контролер таймера ZC забезпечує керування послідовністю операцій таймера ZM.

Інтерфейс таймера ZIO є інтерфейсом шини таймера ZM до внутрішньої шини IB мікросхеми. Інтерфейс таймера ZIO використовується в першу чергу для здійснення зв'язку з зовнішніми контролерами - у варіанті з застосуванням мікросхеми безпеки SC з процесором Р.

Також передбачені виводи для керування послідовністю операцій криптографічного протоколу зв'язку, тобто для керування зв'язком з іншими контролерами, зокрема, з процесором Р. Також передбачений вивід, через котрий таймер ZM сигналізує про спроби змін, виявлені сенсорним модулем SM, наприклад, змін в такті. Інші виводи призначені для обміну даними таймера ZM, тобто сигналами абсолютного або відносного масу, що

задаються модулем таймера ZM

У самому модулі таймера ZM криптоалгоритми не виконуються. За виконання протоколів автентифікування й інших заходів безпеки відповідають інші передбачені модулі мікросхеми безпеки SC. Процесор P повинен вирішувати і керувати правами доступу, через інтерфейс таймера ZIO, до таймера ZM.

Контролер таймера ZC керує інтерфейсом таймера ZIO та лічильною схемою ZS. Крім того, контролер таймера ZC приймає, через інтерфейс таймера ZIO, логічні команди від процесора P.

Логічні команди процесора P інтерпретуються контролером таймера ZC і перетворюються в сигнали внутрішнього керування модулем таймера ZM. Так контролер таймера ZC контролює функціональний хід операцій усього модуля. Таким чином, він є блоком керування усім модулем таймера ZM. Команди, якими контролер таймера ZC впливає на хід операцій таймера ZM, можуть, наприклад, забезпечувати такі операції:

- установлення астрономічного часу на годиннику таймера ZM (дата, час, механізм синхронізації),

- приймання завантажених параметрів в актуальну часову функцію,

- зчитування часу з годинника таймера ZM,

- установлення календарних функцій (місячний ритм, урахування високосних років, урахування літнього часу і тому подібного),

- установлення функції оберненого установлення годин, тобто - чи повинна обернене установлення провадитися в зазначений або в будь-який час,

- запуск і призупинення таймера ZM,

- параметрування узгоджувача такту TA, тобто встановлення параметрів, потрібних для узгоджувача такту TA,

- параметрування роздільної здатності модуля таймера ZM, тобто установлення таймера ZM на вимірювати часу у секундах, у мілісекундах або в мікросекундах,

- параметрування формату передачі часу таймером ZM,

- зчитування через таймер ZM інформації про статус,

- параметрування способу лічби - повинен він

провадитися двійкове чи за модулем,

вмикання і вимикання режиму тестування таймера ZM.

Крім того, за допомогою контролера таймера ZC здійснюють контроль доступу до даних і контроль функціонального доступу. Під цим у даному разі мають на увазі, наприклад, такі режими:

- доступ до таймера ZM дозволяється тільки після успішної перевірки секретного номера,

- доступ дозволений тільки після успішного автентифікування,

- доступ дозволений тільки для зчитування,

- доступ дозволений тільки для запису.

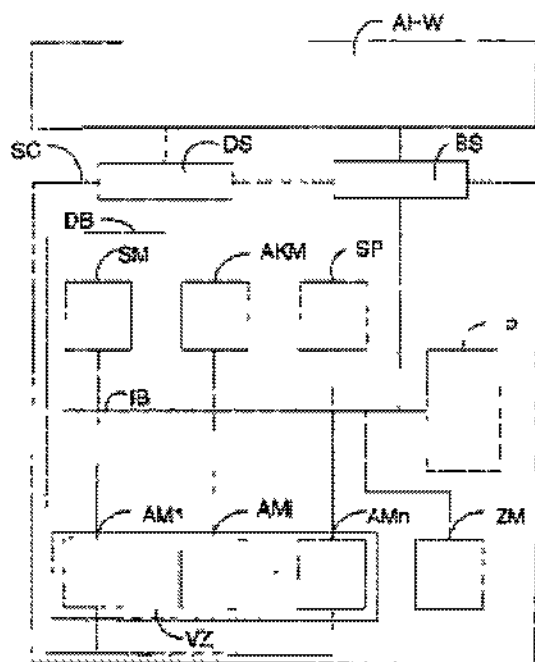
Лічильна схема ZS таймера ZM містить в собі, як описано вище, й лічильник реального часу RZ.

Лічильник реального часу RZ є схемою лічби за модулем, що виконана з каскадованих лічильників. Каскадування і синхронізація лічильника реального часу RZ може відбуватися з урахуванням особливостей часових стрибків, викликаних, наприклад, переходом на літній час або високосним роком і тому подібним. Для деяких криптографічних застосувань також передбачена лічба "відносного" часу, тобто достатньої розрядності, відповідно до потрібного часу, монотонний двійковий лічильник.

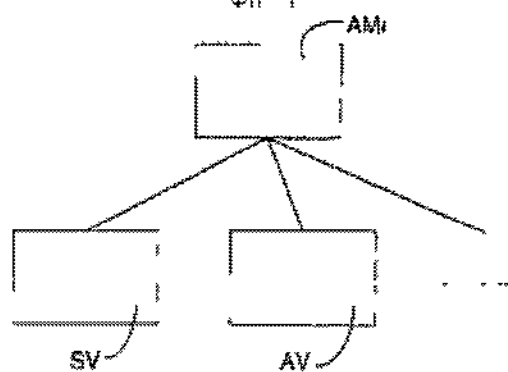
Узгоджувач такту TA служить для формування потрібної часової бази виміру часу в модулі таймера ZM при зовнішньому тактуванні, як це має місце, наприклад, у випадку застосування звичайних у наш час чіп-карт.

Буфер даних DB служить для запам'ятовування необхідних для роботи таймера ZM даних.

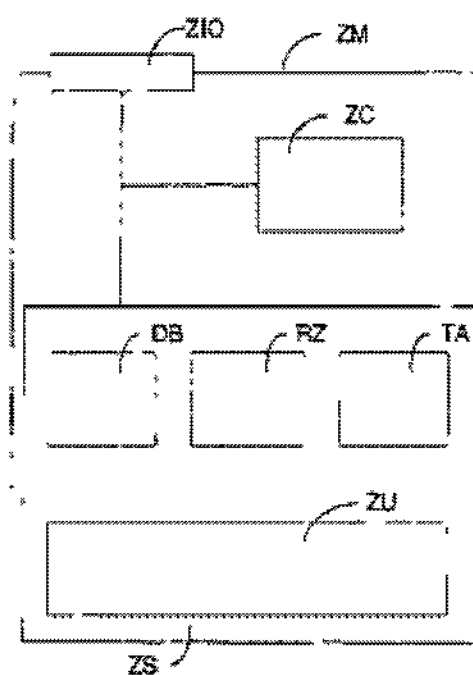
Керування ключем в алгоритмічних модулях АМІ доцільно здійснювати безпосередньо в апаратному забезпеченні. Цим значно підвищується продуктивність роботи насамперед при швидкій зміні ключа між по-різному зашифрованими потоками даних. Це особливо важливо для пакетно-орієнтованого зв'язку або при з'єднанні даних, при роботі в системах колективного застосування або у засобах масової інформації, наприклад, у локальній обчислювальній мережі (ЛОМ), у котрій різним партнерам по зв'язку потрібно передавати і по-різному криптографічне опрацьовувати багато пакетів.



Фиг 1



Фиг 2



Фиг 3

ДП «Український інститут промислової власності» (Укрпатент)

вул. Сим'ї Хохлових, 15, м. Київ, 04119, Україна

(044) 456 – 20 – 90

ТОВ «Міжнародний науковий комітет»

вул. Артема, 77, м. Київ, 04050, Україна

(044) 216 – 32 – 71