РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2005 121 915** (13) **A**

(51) МПК
G06F 1/00 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21), (22) Заявка: **2005121915/09, 04.05.2004**

(30) Конвенционный приоритет:
12.05.2003 US 10/435,916

(43) Дата публикации заявки: **20.06.2007 Бюл. № 17**

(85) Дата перевода заявки PCT на национальную фазу:
12.12.2005

(86) Заявка PCT:
GB 2004/001928 (04.05.2004)

(87) Публикация PCT:
WO 2004/099950 (18.11.2004)

Адрес для переписки:
101000, Москва, М.Златоустинский пер., 10, кв.15, "ЕВРОМАРКПАТ", пат.пов. И.А.Веселицкой, рег. № 11

(71) Заявитель(и):
ИНТЕРНЭШНЛ БИЗНЕС МАШИНЗ КОРПОРЕЙШН (US)

(72) Автор(ы):
ЛУНДВАЛЛ Шон (US),
СМИТ Роналд (US),
Е Фил Чичун (US)

(54) КОМАНДЫ ДЛЯ ПОДДЕРЖКИ ОБРАБОТКИ ШИФРОВАННОГО СООБЩЕНИЯ

(57) Формула изобретения

1. Способ шифрования и расшифрования памяти вычислительной среды, заключающийся в том, что посредством команды микропроцессора задают единицу памяти, подлежащую шифрованию или расшифрованию, и зашифровывают или расшифровывают эту единицу памяти, причем указанная команда соотнесена с полем, определяющим значение кода функции, и еще одним полем, определяющим значение бита-модификатора, а выполняющий команду процессор определяет, подлежит ли выполнению операция шифрования или операция расшифрования, на основании значения кода функции и значения бита-модификатора, и одно дополнительное значение кода функции соответствует операции запроса, вызывающей сохранение в блоке параметров слова состояния, имеющего множество разрядов, причем если определенный разряд слова состояния имеет первое двоичное значение, то этот разряд соответствует значению кода функции, соответствующему установленной функции, а если определенный разряд слова состояния имеет второе двоичное значение, то этот разряд соответствует значению кода функции, соответствующему не установленной функции.

2. Способ по п.1, в котором указанная команда при ее выполнении процессором сохраняет результат шифрования или расшифрования в первом операнде.

3. Способ по п.2, в котором команда включает в себя поле кода операции, поле R2, указывающее один из нескольких регистров общего назначения процессора, содержащий адрес второго операнда, представляющий собой единицу памяти, заданную посредством этой команды, поле R1, указывающее второй регистр общего назначения процессора, содержащий адрес первого операнда и задающий длину второго операнда, причем

RU 2005121915 A

RU 2005121915 A

значение кода функции получают из заданного регистра из числа регистров общего назначения процессора, в заданном регистре из числа регистров общего назначения содержится адрес хранящегося в памяти блока параметров, содержащего пользовательский криптографический ключ, используемый для шифрования и расшифрования по алгоритму шифрования данных (DEA), часть первого операнда включает в себя по меньшей мере часть второго операнда.

4. Способ по п.3, в котором заданный регистр общего назначения, содержащий значение кода функции, является регистром 0 общего назначения, а заданный регистр общего назначения, содержащий адрес хранящегося в памяти блока параметров, является регистром 1 общего назначения.

5. Способ по п.1, в котором если значение кода функции соответствует операции запроса, то указанная команда содержит поле кода операции и никаких иных полей.

6. Способ по п.1, в котором значение кода функции соответствует любой из следующих операций: операция запроса шифрования сообщения (KM), криптографическая операция с 64-разрядным ключом по алгоритму DEA (KM-DEA), криптографическая операция с двумя 64-разрядными ключами по алгоритму Triple DEA (KM-TDEA) и криптографическая операция с тремя 64-разрядными ключами по алгоритму Triple TDEA (KM-TDEA).

7. Способ по п.1, в котором указанная команда имеет формат, соответствующий собственной архитектуре команды процессора.

8. Компьютерный программный продукт, хранящийся на машиночитаемом носителе данных и обеспечивающий при его выполнении в вычислительной системе осуществление способа по любому из пп.1-7.

9. Устройство для шифрования и расшифрования памяти вычислительной среды, содержащее средства задания единицы памяти, подлежащей шифрованию или расшифрованию, посредством команды микропроцессора и средства шифрования или расшифрования этой единицы памяти, причем указанная команда соотнесена с полем, определяющим значение кода функции, и еще одним полем, определяющим значение бита-модификатора, а выполняющий команду процессор определяет, подлежит ли выполнению операция шифрования или операция расшифрования, на основании значения кода функции и значения бита-модификатора, и одно дополнительное значение кода функции соответствует операции запроса, вызывающей сохранение в блоке параметров слова состояния, имеющего множество разрядов, причем если определенный разряд слова состояния имеет первое двоичное значение, то этот разряд соответствует значению кода функции, соответствующему установленной функции, а если определенный разряд слова состояния имеет второе двоичное значение, то этот разряд соответствует значению кода функции, соответствующему не установленной функции.

10. Устройство по п.9, в котором указанная команда при ее выполнении процессором сохраняет результат шифрования или расшифрования в первом операнде.

11. Устройство по п.10, в котором команда включает в себя поле кода операции, поле R2, указывающее один из нескольких регистров общего назначения процессора, содержащий адрес второго операнда, представляющий собой единицу памяти, заданную посредством этой команды, поле R1, указывающее второй регистр общего назначения процессора, содержащий адрес первого операнда и задающий длину второго операнда, причем значение кода функции получают из заданного регистра из числа регистров общего назначения процессора, в заданном регистре из числа регистров общего назначения содержится адрес хранящегося в памяти блока параметров, содержащего пользовательский криптографический ключ, используемый для шифрования и расшифрования по алгоритму шифрования данных (DEA), часть первого операнда включает в себя по меньшей мере часть второго операнда.

12. Устройство по п.11, в котором заданный регистр общего назначения, содержащий значение кода функции, является регистром 0 общего назначения, а заданный регистр общего назначения, содержащий адрес хранящегося в памяти блока параметров, является регистром 1 общего назначения.

13. Устройство по п.9, в котором если значение кода функции соответствует операции запроса, то указанная команда содержит поле кода операции и никаких иных полей.

RU 2005121915 A

RU 2005121915 A

14. Устройство по п.9, в котором значение кода функции соответствует любой из следующих операций: операция запроса шифрования сообщения (КМ), криптографическая операция с 64-разрядным ключом по алгоритму DEA (КМ-DEA), криптографическая операция с двумя 64-разрядными ключами по алгоритму Triple DEA (КМ-TDEA) и криптографическая операция с тремя 64-разрядными ключами по алгоритму Triple TDEA (КМ-TDEA).

15. Устройство по п.9, в котором указанная команда имеет формат, соответствующий собственной архитектуре команды процессора.

RU 2005121915 A