

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ(12) **ЗАЯВКА НА ИЗОБРЕТЕНИЕ**

(21)(22) Заявка: 2012102991/08, 28.06.2010

Приоритет(ы):

(30) Конвенционный приоритет:
30.06.2009 FR 0954473

(43) Дата публикации заявки: 27.08.2013 Бюл. № 24

(85) Дата начала рассмотрения заявки РСТ на
национальной фазе: 30.01.2012(86) Заявка РСТ:
FR 2010/051339 (28.06.2010)(87) Публикация заявки РСТ:
WO 2011/001093 (06.01.2011)Адрес для переписки:
109012, Москва, ул. Ильинка, 5/2, ООО
"Союзпатент"(71) Заявитель(и):
МОРФО (FR)(72) Автор(ы):
**ИКАР Тома (FR),
ШАБАНН Эрве (FR)**(54) **КРИПТОГРАФИЯ С ПАРАМЕТРИЗАЦИЕЙ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ**

(57) Формула изобретения

1. Способ проверки устройства (10) с помощью контроллера (11) на основе пароля (π), содержащий следующие этапы, выполненные в устройстве или контроллере:

/1/ на основе случайного числа r_1 определяют точку $P(X, Y)$ на эллиптической кривой в конечном поле F_g , где q - целое число, а кривая задается уравнением:

$$E_{a,b}(x, y): x^3 + ax + b = y^2; \quad (1)$$

/2/ получают первый и второй параметры k и k' , такие, что

$$P = F(k, k'),$$

где F - сюръективная функция $F_q \times F_{q'}$ в F_q ;

/3/ получают первый и второй параметры в зашифрованном виде посредством шифрования в виде функции, зависящей от пароля; и

/4/ передают упомянутые первый и второй параметры контроллеру;

при этом функция F такова, что независимо от входных элементов z и z' из F_q , $F(z, z')$ является точкой на эллиптической кривой и входные элементы не удовлетворяют уравнению (1).

2. Способ проверки по п.1, в котором функция F имеет вид:

$$F(k, k') = f(k') + f_{a,b}(k),$$

где $f_{a,b}$ - обратимая функция, основанная на коэффициентах a и b эллиптической кривой, на вход которой подают входной параметр и на выходе получают точку на

эллиптической кривой;

f' - функция генерации точки на эллиптической кривой, зависящая от параметра;
причем на этапе /2/ параметры k и k' получают в ходе следующих этапов:
случайно генерируют значение параметра k' ;
вычисляют значение $f'(k')$;
определяют значение параметра k из следующего выражения:

$$k = f_{a,b}^{-1}(P(X, Y) - f'(k')) .$$

3. Способ проверки по п.2, в котором функция f' имеет вид:

$$f'(k') = k' \cdot G,$$

где G - генератор множества точек на эллиптической кривой; а
значение параметра k определяют из следующего выражения:

$$k = f_{a,b}^{-1}(P(X, Y) - k' \cdot G) .$$

4. Способ проверки по п.2, в котором функция f' имеет вид:

$$f'(k') = f_{a,b}(k'),$$

а значение параметра k определяют из следующего выражения:

$$k = f_{a,b}^{-1}(P(X, Y) - f_{a,b}(k'))$$

5. Способ проверки по любому из пп.1-4, в котором функция F содержит по меньшей мере одну обратимую функцию $f_{a,b}$, полученную с помощью многочленов $X_1(k)$, $X_2(k)$, $X_3(k)$ и $U(k)$, которые удовлетворяют равенству Скальба:

$$f(X_1(k)) \cdot f(X_2(k)) \cdot f(X_3(k)) = U(k)^2,$$

где f - многочлен, который определяет эллиптическую кривую $E_{a,b}$.

6. Способ проверки по п.5, в котором функция $f_{a,b}$ сопоставляет паре параметров $(x,$

$y)$ в F_q^2 параметр u в F_q , где q равен $2 \bmod 3$, так что:

$$x = (v^2 - b - u^6/27)^{1/3} + u^2/3$$

и

$$y = u \cdot x + v,$$

$$\text{где } v = \frac{3a - u^4}{6u},$$

$$\text{и } f_{a,b}(0) = 0.$$

7. Способ проверки по п.1, дополнительно включающий следующие этапы:

получают сообщение, содержащее первый и второй параметры, зашифрованные с помощью пароля;

расшифровывают первый и второй параметры и получают параметры p и p' ; и

вычисляют общее секретное значение K с помощью контроллера и в соответствии со следующим выражением:

$$K = g_1 \cdot F(p, p'),$$

где g_1 - указанное случайное число, использованное на этапе /1/.

8. Электронное устройство в системе проверки с помощью пароля, содержащее:

блок (41) определения, выполненный с возможностью определения точки $P(X, Y)$ на эллиптической кривой в конечном поле F_q , где q - целое число, на основе случайного числа g_1 , причем эллиптическая кривая удовлетворяет уравнению:

$$E_{a,b}(x, y): x^3 + ax + b = y^2; \quad (1)$$

блок (42) получения, выполненный с возможностью получения первого и второго

параметров k и k' , таких, что

$$P=F(k,k'),$$

где F - сюръективная функция $F_q \times F_q \rightarrow F_q$;

блок (43) шифрования, выполненный с возможностью получения первого и второго параметров в зашифрованном виде посредством шифрования в виде функции от пароля;

и

блок (44) сопряжения, выполненный с возможностью передачи упомянутых первого и второго зашифрованных параметров контроллеру,

при этом функция F такова, что независимо от входных элементов z и z' из F_q , $F(z,z')$ является точкой на эллиптической кривой, а входные элементы не удовлетворяют уравнению (1).

9. Электронное устройство по п.8, содержащее средство для осуществления способа проверки по п.1.

10. Система проверки с помощью пароля, содержащая по меньшей мере одно первое электронное устройство по п.8 или 9 в качестве контроллера, и второе электронное устройство по п.8 или 9 в качестве проверяемого устройства.