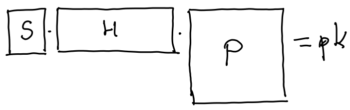
Криптосистема Мак Элиса.

Tuesday 17 November 2020 13:00

Предложена в 1978г.
Основана на кодах Гоппы
Модифицирована Нидеррайтером (код RS)

- KeyGen $(pp = (n, k, t))$
  1. C – лин. $[n, k, d = 2t+1]$ код над $\mathbb{F}_2$ (код Гоппы)
     с эффект. алг-мом декодирования
     $H \in \mathbb{F}_2^{n-k \times n}$ – проверочная матр. C
  2. Сгенерировать $S \in \mathbb{F}_2^{n-k \times n-k}$ – случ. невыр. матр.
  3. Сгенерировать $P \in \mathbb{F}_2^{n \times n}$ – случ. матр. перестановки
  4. $pk = H' = S \cdot H \cdot P \in \mathbb{F}_2^{n-k \times n}$
     $sk = (S, H, P)$



- Encrypt $(m \in \{0,1\}^k,\ wt(m) = t,\ pk = H')$
  1. $c = H' \cdot m \in \mathbb{F}_2^{n-k}$
- Decrypt $(c,\ sk = (S, H, P))$
  1. $y = S^{-1} \cdot c = \{ S^{-1} \cdot H' \cdot m = S^{-1} \cdot S \cdot H \cdot P \cdot m = H \cdot P_m \} \in \mathbb{F}_2^{n-k}$
  2. Используя алг-м Гаусса, найти $z \in \mathbb{F}_2^n$ т.ч. $H \cdot z = y = H \cdot P \cdot m$
  3. $m' = Decode(z)$, Decode – алг-м декодирования кода C
  4. $m = P^t \cdot m'$

Корректность

Пусть $c = H' \cdot m$ – корректно сформ. шифр-текст.
Тогда алг-м дешифр-ия Decrypt
1. $y = S^{-1} \cdot c = H \cdot P \cdot m$
2. $z: H \cdot z = y = H \cdot P \cdot m$

$$\Downarrow$$

$$H(z - P \cdot m) = 0$$

$$\Downarrow$$

$z - P \cdot m$ – кодовое слово из C

$wt(P_m) = wt(m) = t$ (т.к. P – матр-ца перестановки) $\Rightarrow \Delta(z, C) = t \Rightarrow Decode(z)$ вернёт $P \cdot m$

на шаге 4. $P^t \cdot P \cdot m = m$.
$(P^t \cdot P = P \cdot P^t = I)$

Безопасность

основана на трудности задачи декодирования случ. лин. $[n, k, d]$-кода
(по данным $(H,\ y \in \mathbb{F}_2^{n-k})$ найти $c \in C$ т.ч. $\Delta(c, y) - \min$.)
Предположение безопасности: код, полученный из H' – открытого ключа, ведёт себя как случ. линейный код.

Современные пар-ры: $n = 6960$
$k = 5413$ $\sim 2^{128}$ бит безопасности;
$t = 119$