Подписи на кодах

① Традиционные построения

1) Схемы шифрования открытым ключом ⊕ hash & sign → CFS (Courtois – Finiasz – Sendrier)

2) zkProof + эвристика Фиата – Шамира → CROSS

② Схема CFS

m – сообщ., $Enc_{pk}(m)$ – ф-я шифр. по откр. ключу pk

$Dec_{sk}(c)$ – ф-я расшифрования по секретному ключу

$hash$ – криптогр. хэш-функция → в пространстве шифр.-текстов.

Подпись:

$h = hash(m)$

$s = Dec_{sk}(h)$ – подпись

Проверка: (m, s)

$h = hash(m)$

$c = Enc_{pk}(s)$

$h \stackrel{?}{=} c$

CFS

перебираем i: $hash(m \| i)$ → будет декодироваться

подпись: $(s \| i)$

Мешок-Эллис: $c = m \cdot h + e$

Нидеррайтер: $c = H \cdot e(m)^T$

$\binom{n}{t}$ – синдром

$\frac{1}{t!}$ – вероятность подмены в пр-ве шифр.-текстов

③ Подпись на док-ве с нулевым разглашением

Zk Proof — доказывает знание секрета без разглашения.

Протокол Stern

Общие параметры: H, вес ошибки t

Генерация ключа: $sk = e$ — вектор веса t

$s = H \cdot e = pk$.

Доказывающий (P)

1) $y \xleftarrow{\$} \mathbb{F}_2^n$, δ — перест. $[1, \dots, n]$

$c_0 = hash(\delta \| H \cdot y)$

$c_1 = hash(\delta(y))$

$c_2 = hash(\delta(y \oplus e))$

(обязательства)

$\xrightarrow{c_0, c_1, c_2}$

Проверяющий (V)

$\xleftarrow{b}$ 2) $b \xleftarrow{\$} \{0, 1, 2\}$

P

3) a) $b = 0$ $\xrightarrow{\delta(y), \delta(e)}$

c_1, c_2

б) $b = 1$ $\xrightarrow{y \oplus e, \delta}$ ...

c_0, c_2

в) $b = 2$ $\xrightarrow{y, \delta}$ ...

c_0, c_1.

V

$c_1' = hash(\delta(y))$

$c_2' = hash(\delta(y) \oplus \delta(e))$

$c_1' \overset{?}{=} c_1$

$c_2' \overset{?}{=} c_2$

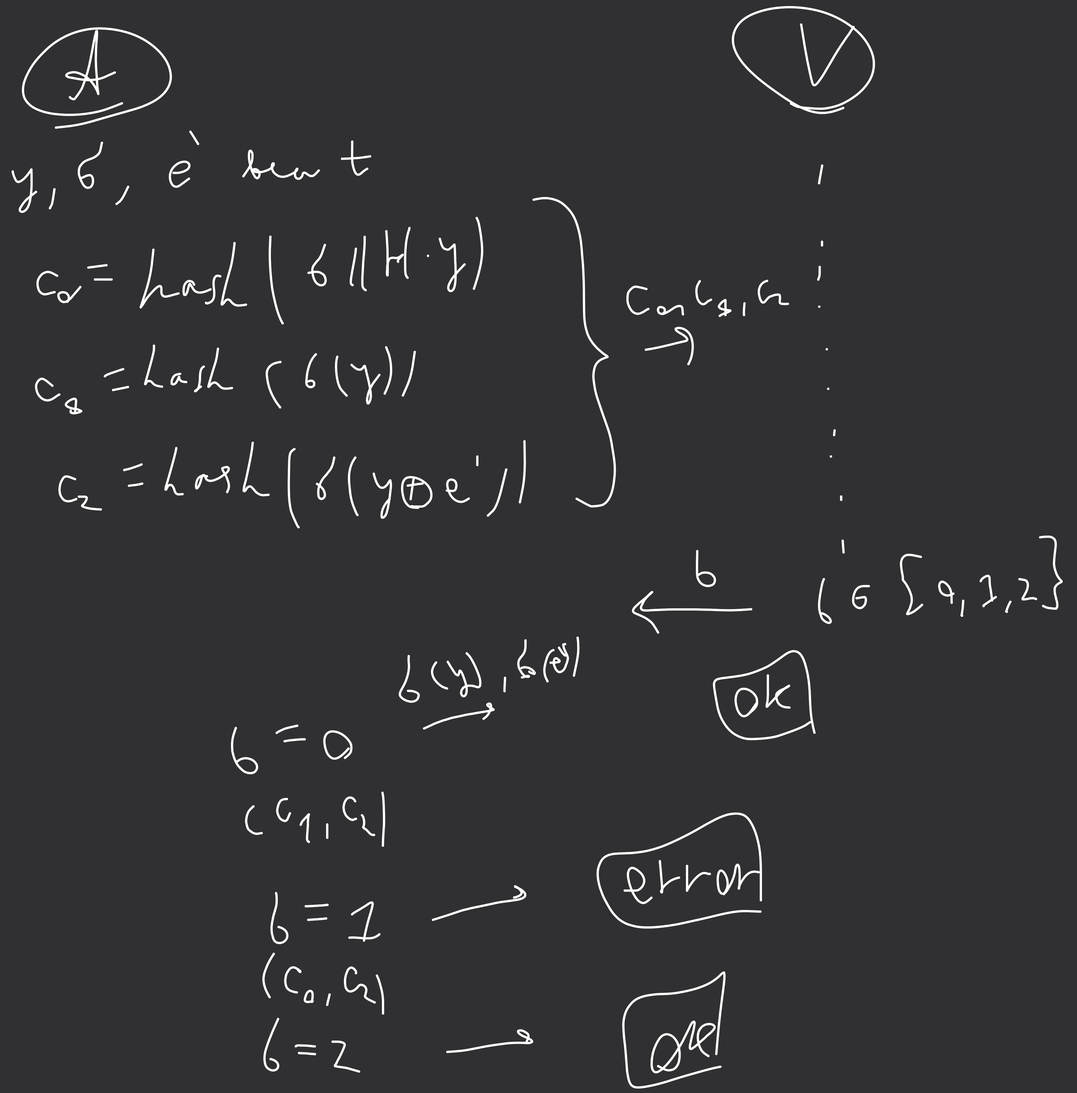
б) $c_0' = hash(\delta \| (H \times (y \oplus e) | \oplus s)$

$c_1' = hash(\delta(y \oplus e))$

$c_0' \overset{?}{=} c_0$

$c_2' \overset{?}{=} c_2$

④ Атака на Stern



Протокол повторяют k раз:

Вероятность успешной атаки $\left(\frac{2}{3}\right)^k$

$k \approx 137$ итераций протокола: $\frac{1}{2^{80}}$

(5) Подпись из ZKProof.

Идея: замена проверяющего на хеш-функцию.

Подпись:

1. Вычислим тройки (c_0, c_1, c_2) для t-раундов

$T = \{$ конкатенация (c_0, c_1, c_2) $(\text{для всех})\}$

2. $h = hash(m \| T)$

3. В качестве b для i-того раунда - i-бит из h.

4. Зашифровать свидетельства, которые соотв b:
   записать их все в бит. строку s.

5. Подпись: $T \| S$.

Безопасность:

$\left(\frac{2}{3}\right)^{-t}$ операций до взлома.

Подпись подписи: $sakt$ до 2^{80}

CROSS: CVE+ F: ab-Shamir