Trezor Shamir, BTC FW

Single Shamir, group/hierarchical
Shamir, BTC-only firmware

abyssal • **9.5.2019**

Jak rozdělit klíč

- Shamir secret sharing scheme
- je založeno na jednoduchém principu, že na jednoznačné skonstruování polynomu stupně N potřebujete N+1 bodů
  - na přímku 2 body (stupeň 1)
  - na parabolu 3 body (stupeň 2)
  - kubická funkce 4 body (stupeň 3)
  - …. N+1 bodů pro řád N

Proč to funguje

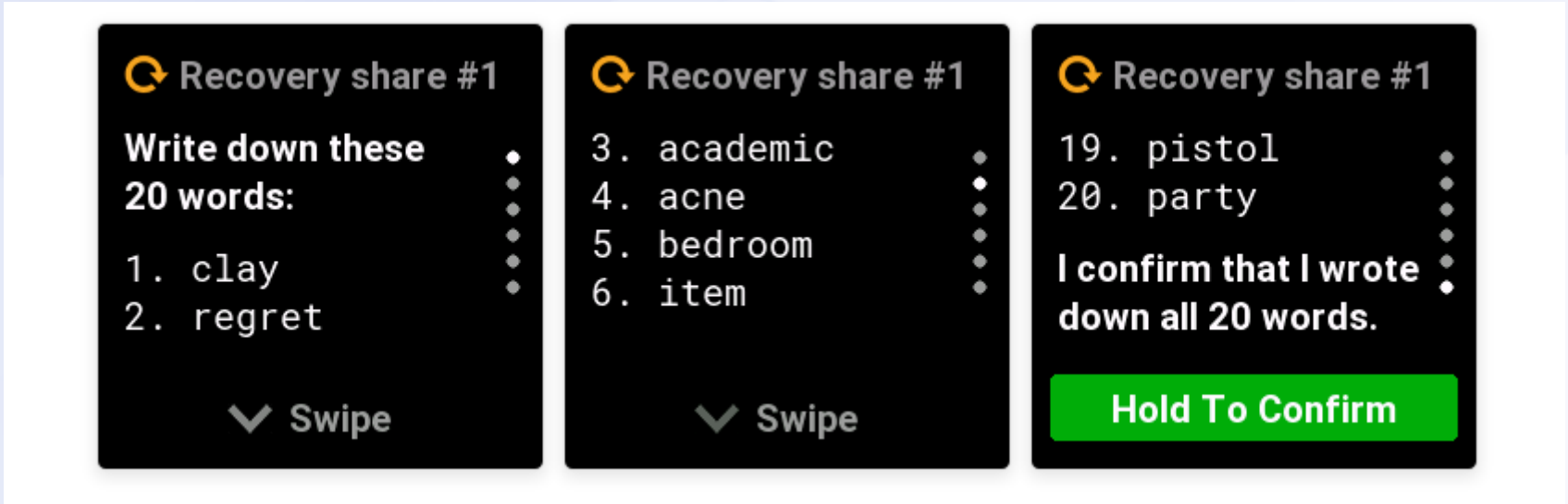
- pokud chybí jenom jeden bod, je množství polynomů nekonečné (v nekonečně velkém tělese) nebo velmi velké (v konečných tělesech)
- pokud chceme dát části klíče M, a na rekonstrukci má stačit N, N<M, tak stupeň polynomu bude N-1, vygenerujeme M bodů a ty rozdáme jako části klíče
- pro klíče se pracuje v konečných tělesech

Konečná tělesa

- příklad: integery modulo *p*, *p* prvočíslo
  - Z_5 – 0, 1, 2, 3, 4
  - 0 – aditivní identita, 1 – multiplikativní identita
  - 2+2=4, 3+3 = 1 (6 modulo 5 == 1)
- mnohem složitější konečná tělesa:
  - Galois fields s neprvočíselnými řády
  - eliptické křivky (mnoho druhů)

SLIP 39: Shamir => mnemonic

- „normální“ Shamir jsou jen body na křivce
- pro UX se to mapuje na mnemonic podobně jako seed



Shamir demo

- trezorctl reset-device -e -t 256 -b shamir

Group/hierarchic Shamir

- usecase: chcete rozdělit seed nejenom mezi pár lidí, ale organizací (pro exchange)
- v rámci každé organizace opět platí schéma n-of-m
- tudíž v rámci každé organizace se musí sejít např. 3 z 5 lidí
- např. v každé organizaci se musí sejít 3 z 5 částí, a pak ještě nad tím 3 z 5 organizací

BTC-only firmware

- proč?
- protože míň kódu má méně chyb
- uživatel si může zvolit jestli chce plný firmware s altcoinama, U2F, OpenPGP, atd.
- BTC-only firmware má menší attack surface

Thanks

abyssal