Verifiable delay functions

Tomáš Krňák

Jarní škola algebry 2019

Structure

- motivation
- definition
- use cases
- constructions

Time capsules

Hash-chain

$$F(x,T) = \underbrace{H(H(\cdots H}_{T\text{-times}}(x)\cdots))$$

Encrypting to future

m ... message
T ... time
p, q ... primes
$N = p \cdot q$ ... RSA modulus
$y := x^{2^T} \bmod N$
$c := m \oplus y$

} $\rightsquigarrow$ time puzzles (c, T, x, N)

$y := x^{2^T} \bmod N$ — $O(T)$ / $O(\log T)$

Definition

$VDF = (Setup, Gen, Sol, Ver)$ where

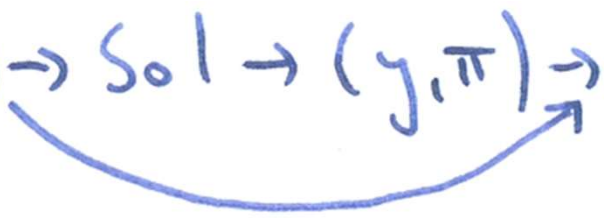
$Setup(1^\lambda) \to pp$

$Gen(pp, T) \to (x, T)$

$Sol(pp, (x, T)) \to (y, \pi)$

$Ver(pp, (x, T), (y, \pi)) \to \{accept, reject\}$

$T \to Gen \to (x, T) \to Sol \to (y, \pi) \to Ver \to \{0, 1\}$



Definition

- efficiency

$\mathrm{poly}(\log T, \lambda)$, $O(T)$

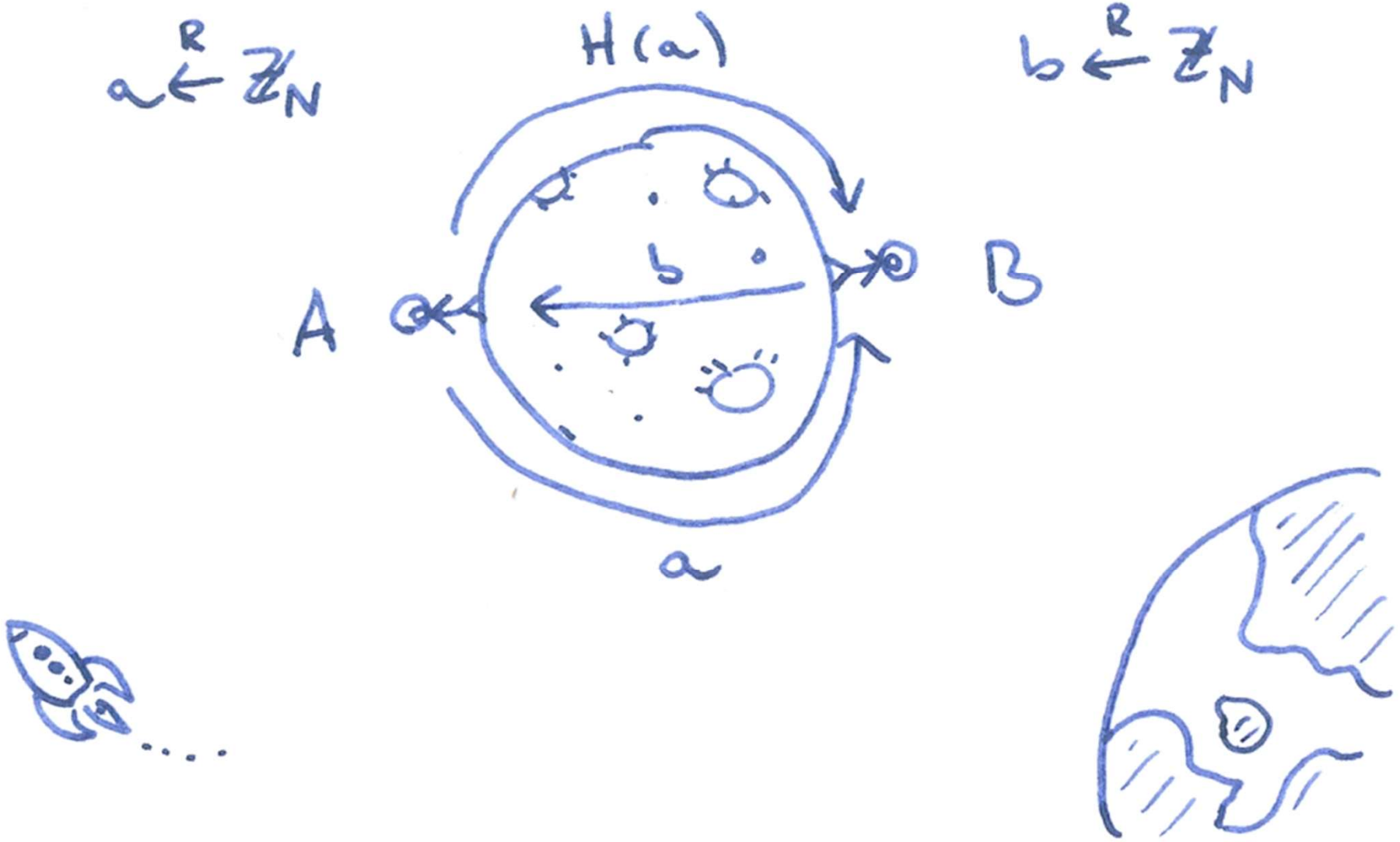
- completeness

- soundness

- sequentiality

Use cases

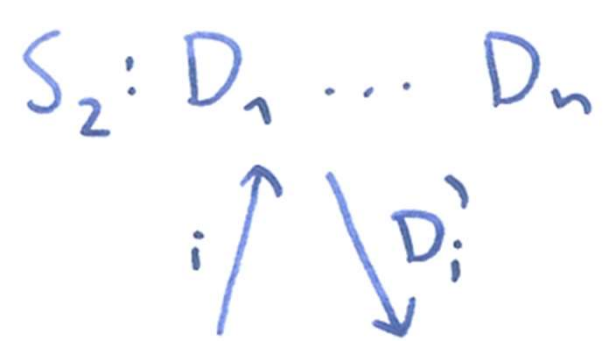
Non-Malleable Commitments

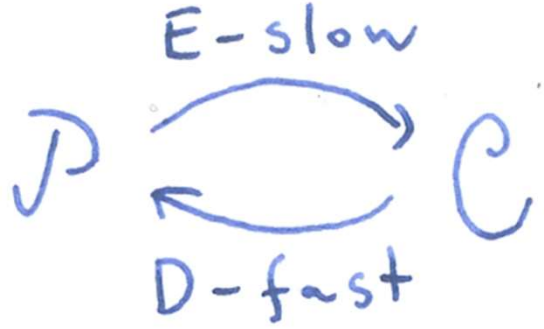


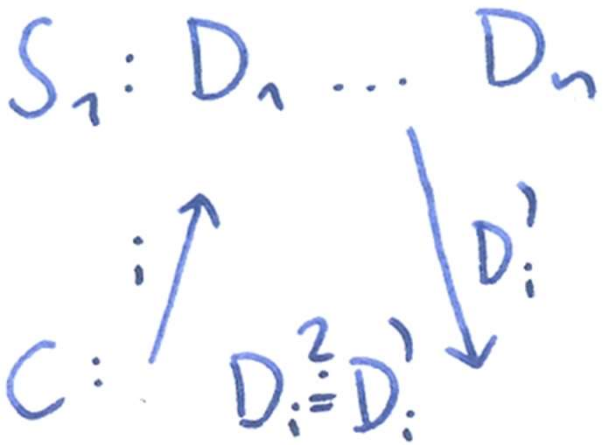
Non-Malleable Commitments

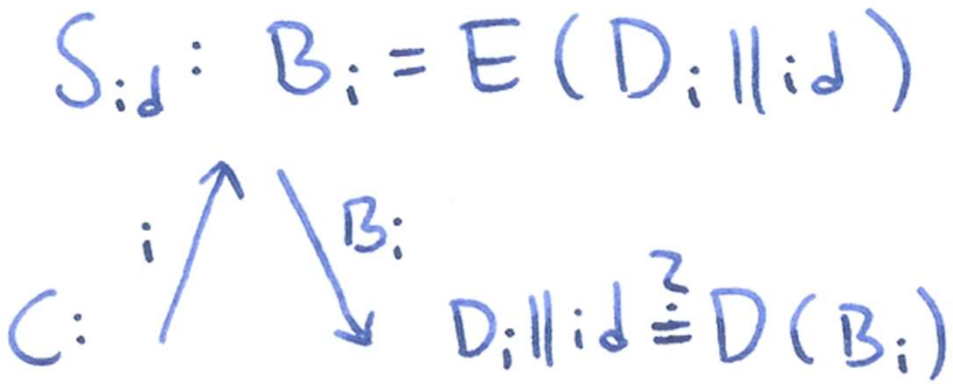
$$\left.\begin{array}{l} P_1 \to c_1 \\ \vdots \qquad \vdots \\ P_n \to c_n \end{array}\right\} \; x = H(c_1 \| \cdots \| c_n) \rightsquigarrow (y, \pi) = \mathrm{VDF}(x, T)$$

Proof-of-replication









Resource-efficient blockchains

Work Stake Space

$x_0 \xrightarrow{VDF} x_1 \xrightarrow{VDF} x_2 \xrightarrow{VDF} \dots$

$\downarrow$ $\downarrow$

$leader_1$ $leader_2$

- timestamps
- back-consistancy
- unpredictability

Constructions

Square roots

p ... prime $p \equiv 3 \bmod 4$

Gen: $r \xleftarrow{R} \mathbb{Z}_p^*$ $x := r^2$

Sol: $y := x^{\frac{p+1}{4}}$ $O(\log(p))$

Ver: $y^2 \overset{?}{\equiv} x$ $O(1)$

$$\left(x^{\frac{p+1}{4}}\right)^2 \equiv x^{\frac{p+1}{2}} \equiv x^{\frac{p-1}{2}} \cdot x \equiv \left(\frac{x}{p}\right) x \equiv x \pmod p$$

+ chaining

Injective rational maps

$F: \mathbb{F}_q^n \to \mathbb{F}_q^m \quad F = (f_1, \dots, f_m)$

$f_i: \mathbb{F}_q^n \to \mathbb{F}_q \quad$ from $\mathbb{F}_q(x_1, \dots, x_n)$

} rational function

for $S \subset \mathbb{F}_q[x_1, \dots, x_n]$

$V(S) := \{ P \in \mathbb{F}_q^n \mid \forall f \in S \; f(P) = 0 \}$

$X \subset \mathbb{F}_q^n$ algebraic set $\overset{\text{def}}{\leftrightarrow} \exists S : X = V(S)$

$F: X \hookrightarrow Y$ is injective rational map

↑ rational function ↖ ↑ algebraic sets

Examples: $n = m = 1$

$x^{p^i} : \mathbb{F}_{p^n} \twoheadrightarrow \mathbb{F}_{p^n} \quad 0 \leq i < n$

$x^e : \mathbb{F}_q \twoheadrightarrow \mathbb{F}_q$ for $\gcd(e, q-1) = 1$

Guralnick and Muller

$$\frac{(x^s - ax - a)(x^s - ax + a)^s + ((x^s - ax + a)^2 + 4a^2x)^{\frac{s+1}{2}}}{2x^s}$$

where $s = p^r$

a is not $(s-1)$st power in $\mathbb{F}_{p^m}$

Inverting inj. rat. map

def $\bar{x} := x_1, \ldots, x_n$

$F(\bar{x}) = g(\bar{x})/h(\bar{x})$

for β find α s.t. $F(\alpha) = \beta$

$\leftrightarrow g(\alpha)/h(\alpha) = \beta \leftrightarrow g(\alpha) - \beta \cdot h(\alpha) = 0$

$\leftrightarrow \left.\begin{array}{l} x-\alpha \mid g(x)-\beta h(x) \\ x-\alpha \mid x^q - x \end{array}\right\} x-\alpha \mid \gcd(x^q-x, g(x)-\beta \cdot h(x))$

$x-\alpha = \gcd(x^q-x, g(x)-\beta h(x))$

Inj. rat. maps setup

Setup: $f(x)$ $F(x)$ — hard to invert / easy to evaluate

Gen: $\beta \xleftarrow{R} \mathbb{F}_q$

Eval: compute gcd $(x^2+x-1)^d$

return α $O(d)$

Ver: $F(\alpha) \stackrel{?}{=} \beta$ $O(\log(d))$

Squaring in $\mathbb{Z}_N^*$

Gen: $x \leftarrow QR_N$

Setup: p, q ... safe primes, $N := p \cdot q$
($p = 2p' + 1$ for p' prime)

Eval: $y = x^{2^T} \bmod N$
generate π

Ver: verify π

Protocol scatch

$P \longleftarrow (N, x, T, y) \longrightarrow V$

$T = 2 \rightarrow x^{2^T} \stackrel{?}{\equiv} y$

μ

r

$x' := x^r \mu^2 \bmod N$

$y' := \mu^{2r} y \bmod N$

$y' = x'^{2^{T/2}} \bmod N$

$P \longleftarrow (N, x', T/2, y') \rightarrow V$

Conclusion

- Use cases
  - non-malleable commitments
  - blockchain
  - proof-of-replication
- Construction
  - hash-chaining
  - squarercoots + invertable + SNARK
  - rational maps + SNARK
  - squaring in $\mathbb{Z}_N$ + trapdoor

Questions