# MI-PB-3

**Návrh fyzicky neklonovatených funkcí (PUF) a generátorů skutečně náhodných čísel (TRNG) odolných vůči útokům.**

## Fyzicky neklonovatelné funkce

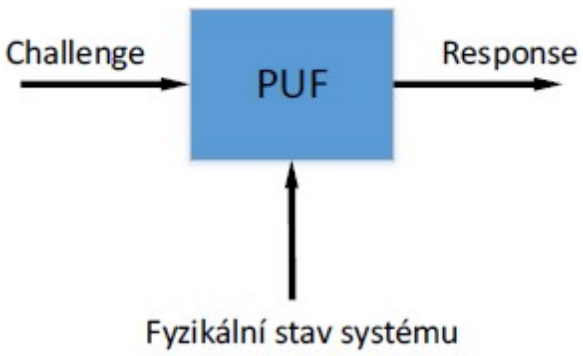
Využívají **jedinečných fyzikálních vlastností** každého zařízení

Vznikají působením **náhodných a nekontrolovatelných vlivů** během výrobního procesu

**Jednosměrná funkce:** Na základě vstupu vygeneruje "příslušný" výstup
Vstupy:

- Fyzikální stav systému
- Výzva (challenge) -- někde není potřeba

Výstup: odpověď (response)




**Využití:**

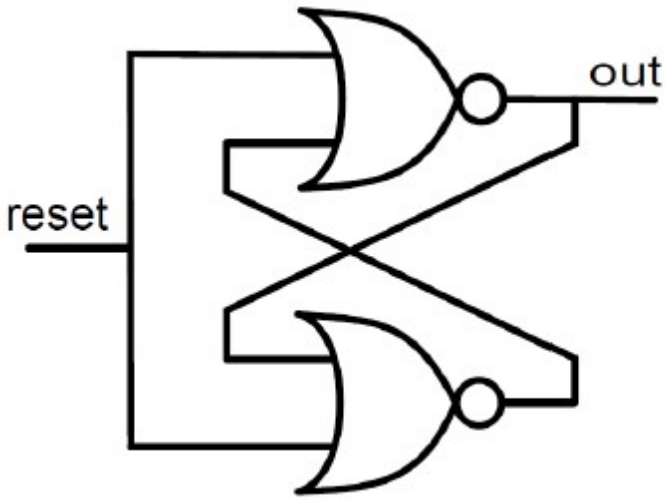
- Identifikace zařízení
- Autentizace
- Generování kryptografických klíčů
- Bezpečné úložiště kryptografických klíčů
- Ochrana proti padělání
- Ochrana duševního vlastnictví

**Požadované vlastnosti:**

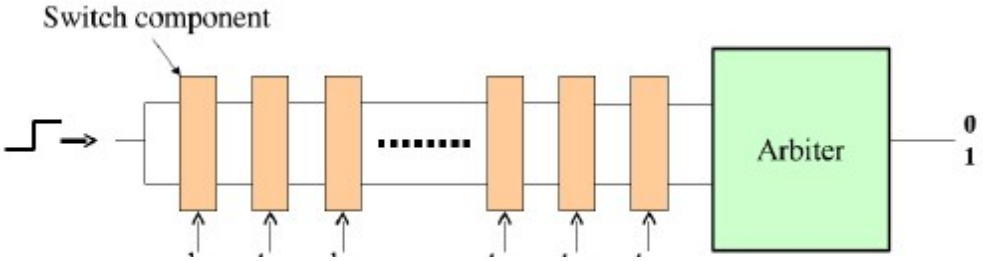
- **Snadná vyhodnotitlenost:** čas, plocha, napájení, spotřeba, cena
- **Reprodukovatelnost:** pro daný PUF a výzvu vždy stejná odpověď
  - Vliv fyzikálních podmínek -- ve výstupu jsou chyby (dostatečně malé ale nevadí)
- **Jedinečnost:** odpovědi na různých zařízeních pro stejnou výzvu by se měly co nejvíc lišit (ideálně 50 %)
- **Fyzická neklonovatelnost:** techinicky velmi obtížné vyrobit dvě identická zařízení (z hlediska fyzikálních vlastností)
- **Matematická neklonovatelnost:** náhodné odpovědi PUFu pro různé výzvy nebo na různých zařízeních -- nemožné predikovat

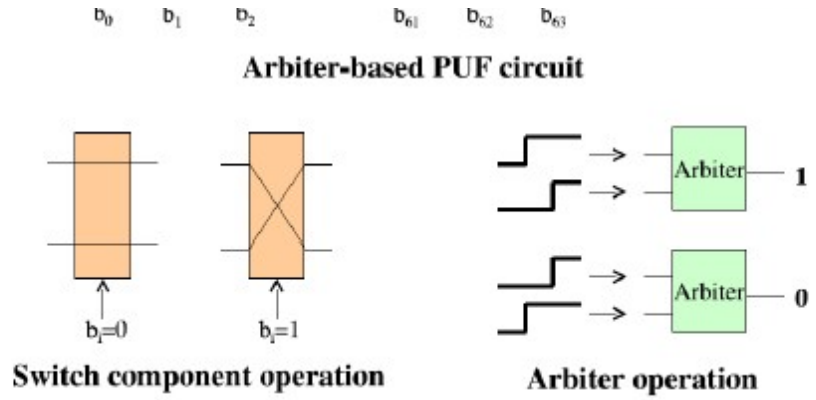
**Typy:**
Podle zdrojů náhodnosti:

- **Paměťové:**
  - SRAM: obsah paměti po zapnutí napájení (každá buňka má preferenci 0 nebo 1, případně ani jednu a chová se náhodně)
  - Butterfly: obvod napodobující SRAM
  - Latch: podobné butterfly (při 1 nestabilní stav, zpět do 0 - ustálení)

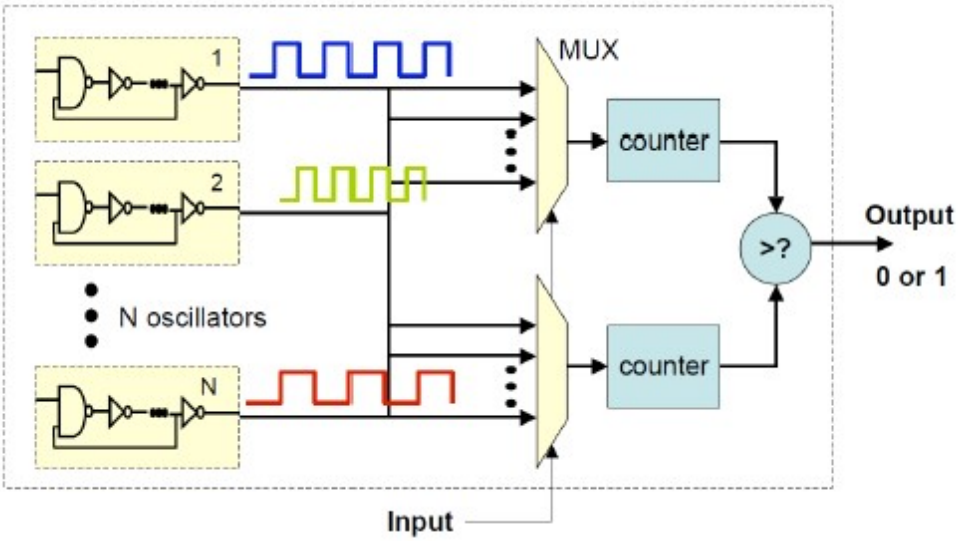



  - Flip-flop
- **Zpoždění obvodu:**
  - Arbiter: 2 symetrické cesty, arbiter detekuje, po které signál přišel rychleji

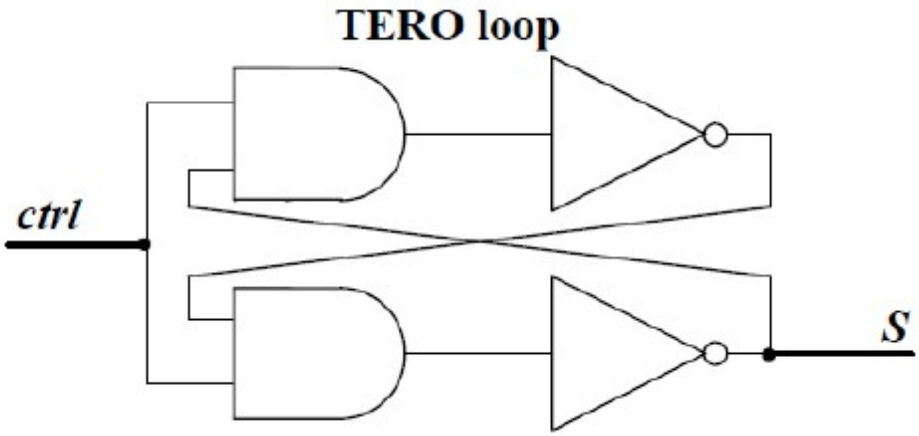





- Ring Oscillator: zdroj entropie -- náhodné odchylky ve zpoždění hradel. Oscilátory vzájemně symetrické, porovnávání frekvencí páru oscilátorů, z každého páru 1 bit výstupu




- Glitch: časový rozdíl mezi změnami výstupu od změny vstupu logického obvodu
- Transient Effect Ring Oscillator: počet oscilací od nastavení do 1 po ustálení




**Identifikace zařízení:**

Každé zařízení lze jednoznačně identifikovat pomoci jeho jedinečných fyzikálních vlastností.

Odpovědi z 1 PUF na 1 zařízení musí být velmi podobné, na různých zařízeních dostatečně odlišné

**Autentizace:**

Pro každé zařízení uloženy výzvy a příslušné odpovědi

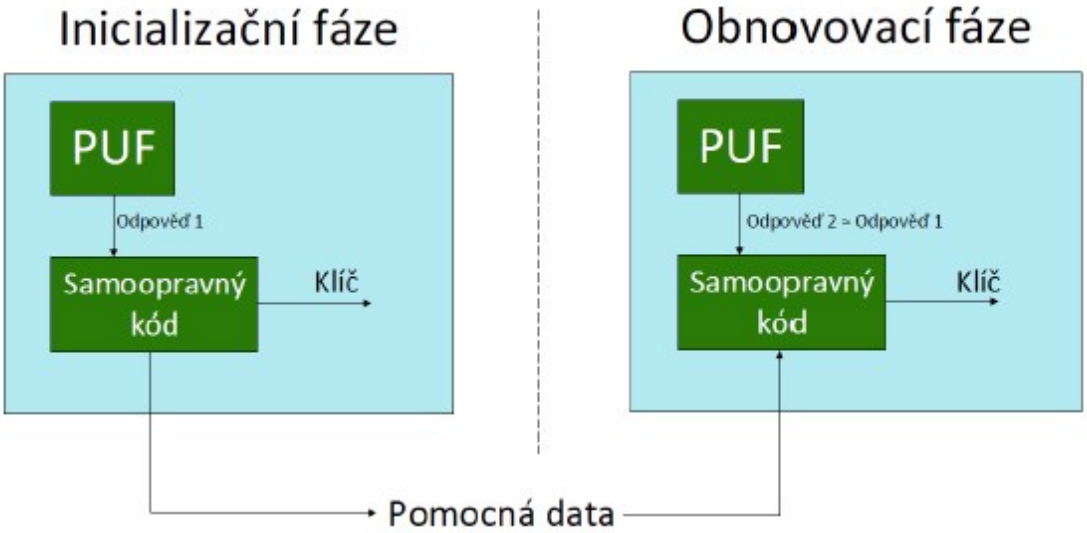
Průběh:

- Zařízení se identifikuje svým ID
- Odešle se challenge zařízení
- Zařízení odešle response
- Pokud response dostatečně podobná té v databázi, ověřeno
- Použitý pár challenge-response vymazat z DB

**Generování klíčů:**

Inicializační fáze: generování klíče a pomocných dat

Pomocná data: informace pro samoopravný kód, konfigurace PUF




## Generátory náhodných čísel

**Generátor náhodných čísel:** proces, jehož výsledkem je posloupnost statisticky nezávislých hodnot, které nelze předem předpovědět

**Využití náhodných čísel v kryptografii:**

- padding
- nonce
- obrana proti útokům postranními kanály
- generování klíčů

**Požadavky:**

- **Dobré statistické vlastnosti:** rovnoměrné rozdělení ($P(0) \approx P(1) \approx 1/2$), maximální entropie, maximální délka
- **Nepředvídatelný výstup**
- **Rychlost** (bit/s, ..., Mbit/s)
- **Složitost** realizace
- **Bezpečnost**
  - Odolnost před útoky, testovatelnost zdroje entropie

## Generátory pseudonáhodných čísel (PRNG)

Pracuje **deterministicky** -- pokud použita znovu stejná počáteční hodnota (seed), vygeneruje stejnou posloupnost

Snadná realizace (algoritmus, automat), rychlý

Výstupní posloupnost zpravidla dobré statistické vlastnosti, ale není skutečně náhodná (pro některá použití nevadí)

**Kryptograficky bezpečný PRNG:**

- Projde **statistickými testy náhodnosti**
- **Next-bit test:** Znám prvních $k$ bitů vygenerované posloupnosti. Neexistuje žádný algoritmus s polynomiální složitostí, který by předpověděl $(k+1)$. bit s pravděpodobností vyšší než $1/2$
- **State compromise:** Zjištěn stav generátoru $\Rightarrow$ nelze zpětně zrekonstruovat dosavadní vygenerovanou náhodnou posloupnost

**Lineární kongruenční generátor:**
$x_{n+1} = (ax_n + c) \pmod m$
Pseudonáhodná posloupnost opakována nejvýše po $m$ iteracích
**Problematický** pro kryptografii: závislost mezi po sobě jdoucími prvky
Při známém $m$ a 3 výstupech lze $a$ a $c$ dopočítat soustavou lineárních rovnic

**Blum-Blum-Shub:**
$x_{n+1} = x_n^2 \pmod m$, kde $m = pq, pq$ prvočísla
**Kryptograficky bezpečný**
Lze přímo spočítat $i$-tý prvek: $x_i = x_0^{2^i \bmod (p-1)(q-1)} \bmod m$

**Hešovací funkce na čítač:**
Hešování hodnot $seed$, $seed + 1$, ...
**Problém:** Odhalení vnitřního stavu $\Rightarrow$ zpětná rekonstrukce posloupnosti

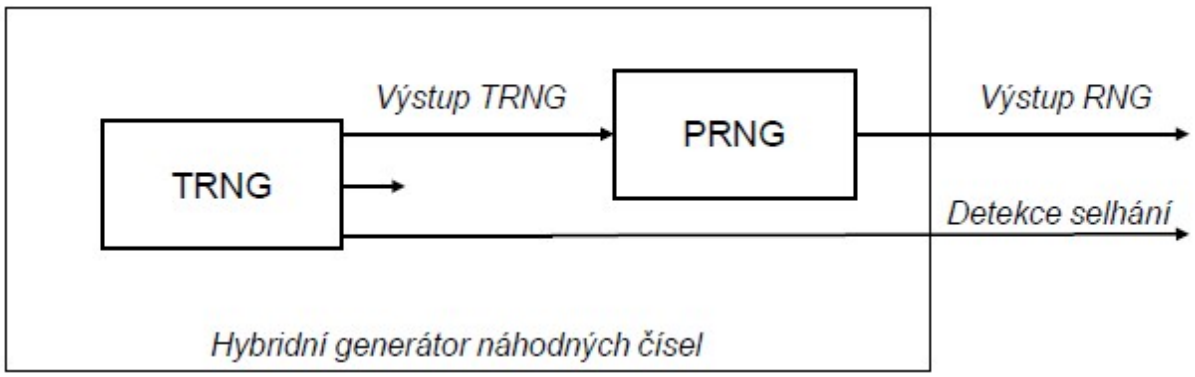
**Bloková šifra v režimu čítače:**
Náhodný klíč $k$, počáteční $seed$
Klíčem $k$ šifrovány hodnoty $seed$, $seed + 1$, ...
Opět nesmí dojít k prozrazení $k, seed$

**Útoky:**

- Bezpečnost systému ohrožena slabým PRNG (LSFR, kongruenční, ...), slabým (málo náhodným, krátkým) seedem, prozrazením vnitřního stavu PRNG

## Hybridní generátor náhodných čísel

Dobrý PRNG inicializovaný skuteně náhodnou hodnotou

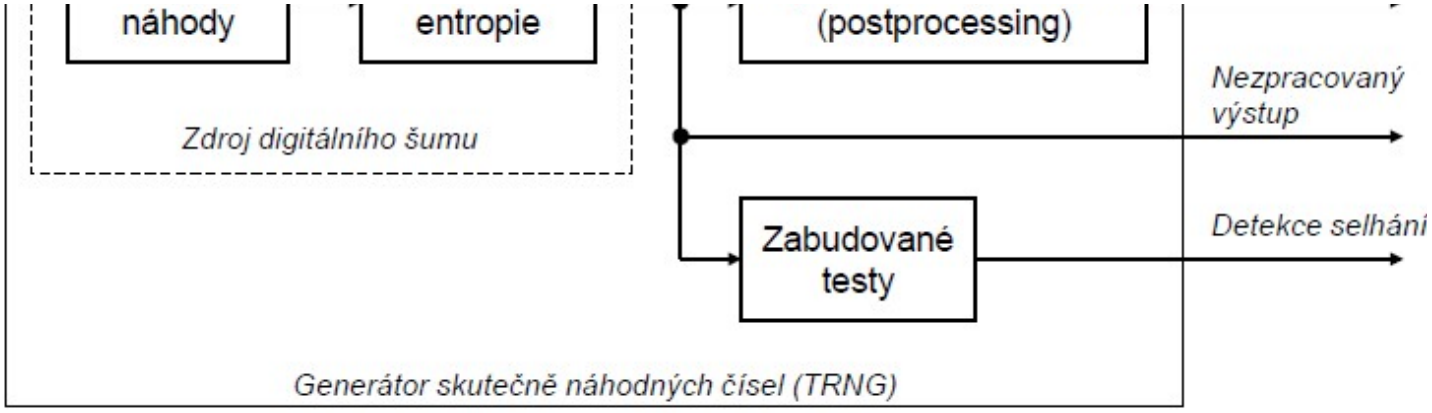



## Generátor skutečně náhodných čísel (TRNG)

**Nedeterministický,** nepředvídatelný výstup, neopakovatelný

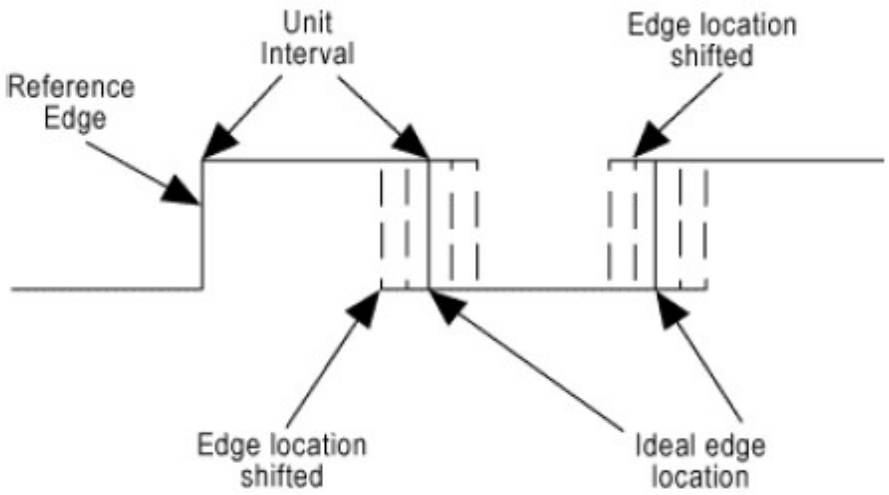
Složitá analýza, obtížnější realizace, pomalejší

**Horší statistické vlastnosti** $\Rightarrow$ postprocessing




**Zdroj entropie:**
Fyzikální děj náhodný ze své podstaty, proces silně citlivý na nepatrné změny parametrů

- radioaktivní rozpad
- tepelný šum
- kvantové jevy
- **nestabilita oscilátorů (jitter):** hrana nenastane přesně v ideálním okamžiku




- **metastabilní stav klopného obvodu:** Obvod má dvě podmínky: $t_{setup}$ (čas, po který se nesmí stav měnit před náběžnou hranou CLK) a $t_{hold}$ (čas, po který se nesmí stav měnit po náběžné hraně CLK). Porušení podmínek -- metastabilní stav (výstup po určitou dobu někde mezi 0 a 1)
- kruhový oscilátor
- chování uživatele

**Zpracování výstupu TRNG:**
Vylepšení statistických vlastností: bias (poměr 0 a 1), entropie, runs (dlouhé posloupnosti 0 nebo 1)

- **XOR korektor:** Ze 2 nebo více bitů vstupu vytvoří jden na výstupu
  Lepší bias, entropie, zachovává nezávislost výstupu, jednoduchý
- **Von Neumannův korektor:** Dvojice $00$ a $11$ se zahodí, jinak $01 \rightarrow 1, 10 \rightarrow 0$

- Iterativní von Neumannův korektor: aplikace korektoru na zahozené bity

**Testování TRNG:**
**Při návrhu:** ověření požadovaných vlastností, možnost složitých testů
**Za běhu:** generátor se může porouchat, může být podroben útoku. Lze použít jen jednodušší testy

Statistický aparát pro testování hypotéz: $H_0$ **:** posloupnost je náhodná

Většina testů vyvinuta pro PRNG $\Rightarrow$ nezjistí některé problémy TRNG

**Typy testů:**

- **Frekvenční:** poměr počtu 1 a 0 se musí blížit 1
- **Runs test:** délka a četnost úseků 000...0 a 111...1
- **Test $n$-tic:** posloupnost se rozdělí na $k$-bitové úseky, vyhodnocení četnosti $k$-bitových sekvencí
- **Spektrální test:** Fourierova transformace (posloupnost jako digitální signál, hledání periodických složek)
- **Testy autokorelací:** opakování stejných nebo podobných úseků v posloupnosti
- **Komprese:** skutečně náhodnou sekvenci nelze bezztrátově zkomprimovat

Existují testovací baterie (FIPS 140-1, NIST Statistical Test Suite, Diehard)

**Útoky:**

- Pasivní: postranní kanály
- Aktivní: ovlivnění činnosti TRNG (elektromagnetické pole, špičky napájení, napětí, teplota)