09. Analýza odpovědí SRAM PUF

SRAM PUF

Vaším úkolem je vyhodnotit vlastnosti SRAM PUF pro danou sadu měření. Musíte analyzovat obsah výpisů SRAM uvedených v následujícím souboru: SRAM_data.zip (../files/SRAM_data.zip) . Existuje 10 binárních souborů (chip[x].bin) obsahujících výpisy SRAM po opakovaném zapnutí - každý výpis je dlouhý 512 bajtů a v každém souboru je 1000 z nich. Považujte každý výpis SRAM za odpověď PUF. Vaším úkolem je:

- Vyhodnoťte Hammingovu vzdálenost odpovědí v rámci každého čipu (HDintra) a Hammingovu vzdálenost mezi čipy (HDinter) - viz níže uvedené vzorce.
- Některé buňky SRAM generují vysoce nestabilní bity (možná i náhodné). Musíte zvýšit stabilitu odpovědí PUF (nižší HDintra). Vaším cílem je vygenerovat PUF odpovědi, které jsou dlouhé 1024b pomocí HDintra < 1%. Proveďte předvýběr vhodných buněk SRAM, které se mají použít pro generování odpovědí PUF - vytvořte masku, která se použije k výběru bitů ze SRAM pro odpověď PUF. Každý čip bude mít vlastní masku.
- Vyhodnoťte HDintra a HDinter pro maskované odpovědi PUF. Existují nějaké rozdíly ve statistikách mezi maskovanými a nemaskovanými odpověďmi PUF a co je způsobilo?

Odevzdání a bodování

Řešením úkolu je program (C/C++/Python/Mathematica/Matlab apod.), který vypočítá a vypíše:

- hodnoty HDintra a HDinter pro nemaskované odpovědi – **2 body**
- bitové masky pro předvýběr 1024 bitů tak, aby byl splněn limit pro HDintra výše, vypsány do souboru ve formátu níže a
- hodnoty HDintra a HDinter pro 1024b maskované odpovědi – **2 body**

Odevzdání proveďte do repozitáře na Gitlabu, k tomu vytvořte nový adresář lab09_PUF. Předpokládejte, že data jsou již umístěna v podadresáři data, a tento podadresář nenahrávejte (pro úsporu místa).

Intra-Hamming distance

$$HD_{intra} = \frac{1}{N\,T} \sum_{i=1}^{N} \sum_{j=1}^{T} \frac{HD(R_{ref_i}, R_{i,j})}{L}\ 100\ [\%],$$

kde N je počet čipů, L je délka odpovědi PUF a T je počet měření. R_{ref_i} je referenční odpověď i-tého čipu, se kterou se ostatní odpovědi porovnávají. $R_{i,j}$ je j-tá odpověď i-tého čipu. Jako referenční odpověď R_{ref_i} použijeme "průměrnou" odpověď z i-tého čipu.

Inter-Hamming distance

$$HD_{inter} = \frac{2}{N\,(N-1)} \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} \frac{HD(R_{ref_i}, R_{ref_j})}{L}\ 100\ [\%].$$

Maska

Chcete-li předvolit vhodné buňky SRAM, které se mají použít pro PUF, musíte analyzovat stabilitu každé buňky SRAM. Všechna měření se provádějí pro stejných 512 B SRAM, proto 1. bit každé odpovědi odpovídá 1. buňce SRAM, 2. bit každé odezvy odpovídá 2. buňce SRAM atd. Vyhodnoťte stabilitu každé buňky SRAM a vyberte pouze ty buňky s vysokou stabilitou - pro dosažení požadovaného HDintra musíte určit vhodnou prahovou hodnotu z odpovědí PUF.

Uveďte nalezené masky pro každý čip v souboru. Maska bude binární řetězec v ASCII (4096 znaků, protože výpisy SRAM mají délku 4096b), kde 1 označuje stabilní bit používaný pro PUF a 0 znamená, že odpovídající bit nebude použit. Každý řádek v souboru obsahuje masku pro jeden čip, tj.

```
1111000100101...0110

0110100111001...1101

.

.

.

0001101110101...1001
```