



STRESZCZENIE ROZPRAWY DOKTORSKIEJ

Synteza i optymalizacja kwantowych układów logicznych reprezentujących prymitywy kryptograficzne

mgr inż. Adam Jagielski

Praca porusza zagadnienia dotyczące badania kryptografii symetrycznej, logiki kwantowej i odwracalnej. W szczególności reprezentowania symetrycznych prymitywów kryptograficznych jako układy odwracalne. Badania skupione zostały na poszukiwaniu efektywnych metod modelowania szyfrów jako zoptymalizowane układy. Dalszy ciąg badań został poświęcony poszukiwaniom możliwości wnioskowania o bezpieczeństwie kwantowym szyfrów przy użyciu utworzonego układu.

Przeprowadzone i opisane wyniki następujących badań:

- Synteza optymalnych układów logiki odwracalnej reprezentujących skrzynki podstawieniowe SBOX wybranych szyfrów i kryptograficznych funkcji skrótu;
- Synteza kompletnej przestrzeni szablonów identyczności;
- Badanie korelacji pomiędzy klasycznymi właściwościami bezpieczeństwa skrzynek podstawieniowych SBOX, a optymalnym rozmiarem implementacji;
- Badanie bezpieczeństwa kwantowego szyfrów z rodziny SPARKLE;
- Badanie bezpieczeństwa kwantowego standardu szyfrowania lekkiego Ascon.

Badania wykorzystują nowoczesne techniki obliczeniowe, między innymi obliczenia HPC (*z j. ang. High Performance Computing*) i programowanie ograniczeń (*z j. ang. CP – Constraint Programming*) przy użyciu narzędzi typu SAT-solver.

Uzyskane w badaniach wyniki stanowią podstawę do dowodzenia bezpieczeństwa szyfru oraz SPARKLE standardu szyfrowania lekkiego Ascon. Wyniki badań przedstawiają po raz pierwszy optymalne implementacje skrzynek podstawieniowych w reżimie logiki odwracalnej wraz z dowodami optymalności. W ramach badań została udowodniona pozytywna korelacja pomiędzy klasycznymi parametrami bezpieczeństwa skrzynek podstawieniowych a rozmiarem implementacji jako kwantowy układ logiczny oraz wyznaczona została pełna przestrzeń układów realizujących funkcję identyczności o wymiarach nieprzekraczających 6×7 .

Słowa kluczowe: Logika kwantowa, Logika odwracalna, Kryptografia symetryczna, SAT-solver, Skrzynki podstawieniowe, SBOX, Sparkle, Ascon.