Krzysztof Kanciak
Wojskowa Akademia Techniczna, Wydział Cybernetyki

Dowodzenie poprawności implementacji algorytmów kryptograficznych z wykorzystaniem metod formalnych

W rozwoju rozwiązań kryptograficznych kluczowym wymaganiem jest przedstawienie dowodu bezpieczeństwa rozumianego jako wykazanie, że złożoności obliczeniowa i pamięciowa znanych metod kryptoanalizy są większe od złożoności ataku przeszukiwania brutalnego. Jednak dla bezpieczeństwa rozwiązania kryptograficznego kluczowa pozostaje jego implementacja w docelowym środowisku. Problem weryfikacji poprawności implementacji algorytmów kryptograficznych pozostawał bez możliwości przeprowadzenia odpowiedniego dowodu, a sprawdzane było dotąd jedynie zachodzenie pojedynczych przypadków (wektorów testowych).

Praca opisuje model wytwarzania algorytmów kryptograficznych, który niejako skraca odległość między teoretyczną specyfikacją sformułowaną językiem matematyki (podlegającą dowodowi), a zoptymalizowaną implementacją sprzętową wyrażoną za pomocą macierzy bramek logicznych. W szczególności rozwój narzędzi rozwiązujących problem spełnialności rachunku zdań oraz metod przetwarzania grafów typu and-inverter (składających się jedynie z węzłów realizujących operację koniunkcji oraz negacji) otworzył możliwość dowodzenia zgodności między modelem matematycznym przekształceń na skończonym zbiorze możliwych argumentów (wyrażonym w języku wysokiego poziomu jak np. Julia), a opisem ich sprzętowej realizacji.

Wykorzystanie metod formalnych do dowodzenia zgodności implementacji ma zastosowanie w kryptografii symetrycznej, która w odróżnieniu od asymetrycznej nie uzależnia przebiegu wykonania np. szyfrowania bloku od zadanych danych tj. ma stałą złożoność obliczeniową.

Słowa kluczowe: high assurance cryptography, AIG, SMT, Julia.