Promotor: prof. Jerzy Jaworski

Łukasz Nitschke

Rozprawa doktorska z nauk matematycznych w zakresie informatyki

Bezpieczeństwo protokołów w środowisku o ograniczonym zaufaniu

Streszczenie

Niniejsza praca doktorska została poświęcona problemowi zapewniania bezpieczeństwa obliczeń w środowisku o ograniczonym zaufaniu. W pracy zaproponowane zostały modyfikacje znanych protokołów takich jak sieci mieszające, czy protokoły ustalania klucza (interakcyjne generowanie kluczy). Na bazie tych rozwiązań stworzone zostały autorskie protokoły zdalnych wyborów elektronicznych oraz zdalnych egzaminów. Szczególna uwaga została poświęcona sieciom mieszającym oraz możliwościom ich udoskonalenia pod kątem konkretnych zastosowań. Jeden z zaproponowanych protokołów wyborów elektronicznych wykorzystuje nowatorskie sieci mieszające wykonujące rozproszone obliczenia na zaszyfrowanych liczbach w arytmetyce modulo. W protokole tym oraz w protokołach egzaminów stosowana jest również modyfikacja procedury weryfikującej integralność sieci mieszających pozwalająca na dwukrotne wykorzystanie tej samej sieci. Znaczna część badań związanych z rozprawą poświęcona była analizie wpływu procedur częściowego sprawdzania sieci mieszających na uzyskany poziom anonimowości. Dla zaprezentowanego w pracy matematycznego modelu opisującego anonimowość sieci, opisany został proces zanikania wiedzy obserwatora, uzyskanej na podstawie częściowo ujawnionych przez serwery mieszające przekształceń, w zależności od liczby serwerów mieszających i wiadomości.

Łukasz Nitschke