# Kryptografia implementowana na urządzeniach nie w pełni bezpiecznych

Tomasz Kazana
Uniwersytet Warszawski

**Streszczenie**

Wiele protokołów kryptograficznych jest bezpiecznych, ale wymusza trudne obliczenia. Stosujemy ją w praktyce, choć przecież nikt (jak każe protokół!) samodzielnie nie dodaje punktów na krzywej eliptycznej, czy nie podnosi dużych liczb do dużej potęgi. Robią to za nas oczywiście komputery czy karty chipowe. To jednak sprawia, że złośliwy przeciwnik ma potencjalnie więcej możliwości - może atakować nasz sprzęt (kluczyk od samochodu, kartę kredytową), który zawiera tajny klucz i wykonuje obliczenia. Problemem są tu wirusa oraz tzw. side-channel attacks, czyli ataki polegające na mierzeniu fizycznych własności urządzeń, np poboru prądu czy czasu wykonywania obliczeń. W referacie przedstawię swoje wyniku z tej dziedziny: a więc zaproponuję model obliczeń przydatny w tej klasie problemów oraz opowiem, jakie protokoły udało się wymyślić w tym modelu.