Streszczenie:

W ostatnich czasach Internet of Things (IoT) zyskuje coraz większą popularność i coraz więcej urządzeń można do niego podłączyć. Reklamowane są samochody, w których można sprawdzić poziom oleju w silniku korzystając z aplikacji w telefonie. Reklamowane są piekarniki, którymi można sterować przez Internet. Wizja domu, w którym żaluzje i oświetlenie są sterowane komputerem, a obraz z kamery ustawionej w domu można oglądać w dowolnym miejscu na świecie stała się rzeczywistością. Te i inne urządzenia podłączone do IoT są sterowane za pomocą układów elektronicznych, które zużywają niewiele energii, posiadają stosunkowo niewielką moc obliczeniową oraz potrafią dobierać, przetwarzać, zapisywać i wysyłać dane odbierane z sensorów do nich podłączonych. Rozwój technologii oraz jej powszechność stawia wyzwanie: jak powinniśmy prawidłowo obsłużyć dane (ich przesyłanie, przetwarzanie, zapisywanie oraz zabezpieczanie), korzystając z komputerów o niewielkiej mocy obliczeniowej. Wyzwanie jest aktualne, ponieważ przewiduje się, że przesyłanie zdjęć i plików wideo (wykonywane przez urządzenia IoT) już w roku 2019 będzie stanowiło 80% całkowitego ruchu w Internecie. Najważniejsi gracze rynku IT, chcąc nadążyć za oczekiwaniami użytkowników, rozwijają swoje produkty i zwiększają limity danych, które można za ich pomocą przesyłać, przetwarzać i przechowywać. Są oni jednak ograniczeni przez używaną technologię. A zastąpienie jej przez coś nowszego może okazać się zbyt kosztowne.

W ramach projektu badany będzie problem połączenia kompresji z szyfrowaniem. Takie rozwiązanie pozwoli osiągnąć efektywną kompresję (bliską optymalnej) i szyfrowanie. Oczywiście, istnieje trywialne rozwiązanie, w którym najpierw dane są kompresowane a dopiero potem są szyfrowane. Celem projektu jest użycie szyfrowania w czasie wykonywania kompresji. Można tego dokonać przez manipulowanie tzw. „wolnymi parametrami“ algorytmu kompresji. W wyniku prac nad projektem powstanie algorytm nazywany ComCrypt (od anglojęzycznych słów Compression i Encryption). Projekt będzie bazował na polskim kodowaniu ANS zaprojektowanym przez Jarka Dudę, który jest członkiem zespołu badawczego. Kodowanie ANS wypiera standardowe metody dzięki poprawionym własnościom i jest używane m.in. w produktach firm Apple, Facebook, Google.