New Directions in Efficient and Tamper-Resilient Public-Key Cryptography for Ubiquitous Computing

Results in Brief

Faster and better encryption

An EU project fostered collaboration in the field of cryptography. The resulting new applications of cryptographic algorithms mean faster and better encryption, and help to secure certain wireless devices.

DIGITAL ECONOMY

© Thinkstock

Certain kinds of computer networking systems, for example those connecting wireless sensors or tags, are vulnerable to hacking. While the systems are well protected against direct attacks, they can be accessed via indirect means that extract the cryptographic key and other secondary data.

Addressing the problem was the EU-funded 'New directions in efficient and tamper-resilient public-key cryptography for ubiquitous computing' (ND-ETCRYPTOUC) project. The main goal was to secure the relevant devices, by making effective public-key cryptography available for use in this context. The availability was to be achieved via three complex technical objectives based on cryptographic algorithms.

A further purpose was developing the career of one Turkish researcher, through a

series of collaborative exchanges, hence also fostering knowledge transfer with Europe. The project ran for four years, concluding in June 2014.

In the first reporting period, the first objective was fully achieved. The second two were partially accomplished, and will be completed during subsequent periods.

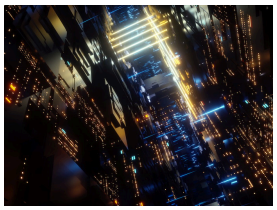
The researcher met and worked with numerous other researchers at universities and commercial organisations in Europe and Turkey. In a series of proposals, his applications of various algorithms helped improve cryptographic speed and performance. The results of the collaborations were published as conference and journal papers. He also presented various guest lectures and seminars, plus designed and taught several well-received comprehensive postgraduate courses. Additionally, he supervised a group of research students.

Thanks to the ND-ETCRYPTOUC project, vulnerable devices will be better protected. The exchanges have also led to positive collaboration with European researchers and institutions.

Keywords

Encryption | cryptography | wireless devices | hacking | secondary data | ubiquitous computing | knowledge transfer

Discover other articles in the same domain of application



New solutions to encryption: keeping data safe in the face of onslaught of quantum computation

7 June 2019

Blockchain technology makes secure, low-cost and simple payments a reality for all

26 June 2020

Centreing the citizen in demand response solutions

21 February 2024

New modular microservice-oriented platform redefines energy management for everyone

21 February 2024

Project Information

ND-ETCRYPTOUC

Grant agreement ID: 256544

Project closed

Start date
1 July 2010

End date
30 June 2014

Funded under
Specific programme "People" implementing the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007 to 2013)

Total cost
€ 100 000,00

EU contribution
€ 100 000,00

Coordinated by
BAHCESEHIR UNIVERSITESI
Türkiye

This project is featured in...

RESEARCH*EU MAGAZINE

Close-up on nanotechnology

Last update: 9 January 2015

Permalink: https://cordis.europa.eu/article/id/151367-faster-and-better-encryption