ICT-2007-216676

ECRYPT II

European Network of Excellence in Cryptology II

Network of Excellence

Information and Communication Technologies

D.MAYA.4
Wiki on Cryptographic Primitives and Hard Problems

Due date of deliverable: 18 January 2013
Actual submission date: 11 January 2013

Start date of project: 1 August 2008 Duration: 4 years

Lead contractor: Katholieke Universiteit Leuven (KUL)

Revision 1.0

Project co-funded by the European Commission within the 7th Framework Programme		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission services)	

Wiki on Cryptographic Primitives and Hard Problems

Editor
Fré Vercauteren (K.U.Leuven)

Contributors
Naomi Benger (University of Adelaide), David Bernhard (UNIVBRIS),
Dario Catalano (UNICT), Manuel Charlemagne (Shannon Institute),
David Conti (Shannon Institute), Biljana Cubaleska (RUB),
Hernando Fernando (Shannon Institute), Dario Fiore (UNICT),
Steven Galbraith (Auckland University), David Galindo (Uni.Lu),
Jens Hermans (K.U.Leuven), Vincenzo Iovino (UNISA),
Tibor Jager (RUB), Markulf Kohlweiss (MS Cambridge),
Benoit Libert (UCL), Richard Lindner (TUD),
Hans Loehr (RUB), Danny Lynch (Shannon Institute),
Richard Moloney (Shannon Institute), Khaled Ouafi (EPFL),
Benny Pinkas (University of Haifa), Frantisek Polach (Shannon Institute),
Mario Di Raimondo (UNICT), Markus Rückert (TUD),
Michael Schneider (TUD), Vijay Singh (Shannon Institute),
Nigel Smart (UNIVBRIS), Martijn Stam (UNIVBRIS),
Fré Vercauteren (K.U.Leuven), Jorge Villar Santos (UPC),
Steve Williams (UNIVBRIS)

11 January 2013
Revision 1.0

The work described in this report has in part been supported by the Commission of the European Communities through the ICT program under contract ICT-2007-216676. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Abstract

This report contains the official delivery D.MAYA.4 of the ECRYPT2 Network of Excellence (NoE), funded within the Information & Communication Technologies (ICT) Programme of the European Commission's Seventh Framework Programme (FP7).

The deliverable consists of an online repository, or so called "Wiki", that provides an extensive overview of the Cryptographic Primitives and Hard Problems that are currently being used in public key cryptography.

The Wiki has been set up at the following address: `http://www.ecrypt.eu.org/wiki/` and is a joint community effort to gather every known problem used in public key cryptography. It contains contributions from both ECRYPT2 and non-ECRYPT2 members. The main page has been visited over half a million times since its inception.