Ivan Visconti

Prof. Associato INF/01 (01/B1)
Dip. Ingegneria dell’Informazione e… (DIEM)
Università degli Studi di Salerno
visconti@unisa.it

Ivan Visconti

Temi di Ricerca Principali

- Protocolli Crittografici
  - Zero-Knowledge Proofs
  - Generic 2-Party and Multi-Party Computation (es. secure set intersection)
- Nozioni di Sicurezza nel Cyberspace
  - Universal Composability
  - Resettability (stateless computing)
- Hardware-Assisted Security
  - Tamper-Proof Tokens
  - Physically Uncloneable Functions
- Blockchain and Distributed Ledger Technology

Ivan Visconti
IACR

- IACR = International Association for Cryptologic Research
- Conferenze IACR
  - CRYPTO, EUROCRYPT, ASIACRYPT
  - TCC, CHES, FSE, PKC

- Miei Contributi
  - 14 comitati di programma IACR (2009-2018)
  - 32 pubblicazioni IACR (2004-2017)

https://www.iacr.org/cryptodb/data/stats.php

Ivan Visconti
Altre Attività

- Associate Editor
  - IEEE Transactions on Information Forensics and Security
- Publicazioni/Comitati di Programma
  - STOC (ACM), FOCS (IEEE), ICALP (EATCS)
- FP6/FP7/H2020
  - Networks of Excellence in Cryptology
    - ECRYPT 2004-2008 – ECRYPT2 2008-2013
  - Cost Action “Cryptography for Secure Digital Interaction” 2014-2018
  - Research and Innovation Action “PRIViLEDGE” 2018-2020

Ivan Visconti

Attuali Collaborazioni

- Nazionali
  - Dario Catalano (UniCA), Daniele Venturi (UniRoma1), Carlo Blundo e Giuseppe Persiano (UniSA)
- Internazionali
  - Sanjam Garg (UC Berkeley), Vincenzo Iovino (Uni Lux), Rafail Ostrovsky (UCLA), Alessandra Scafuro (NCSU)

Ivan Visconti
PRIViLEDGE 2018-2020

- Call: H2020-DS-2016-2017
  (Digital Security Focus Area)
  Cybersecurity Public-Private Partnership
  Cryptography
  Reseach and Innovation Action (RIA)

Ivan Visconti
PRIViLEDGE 2018-2020

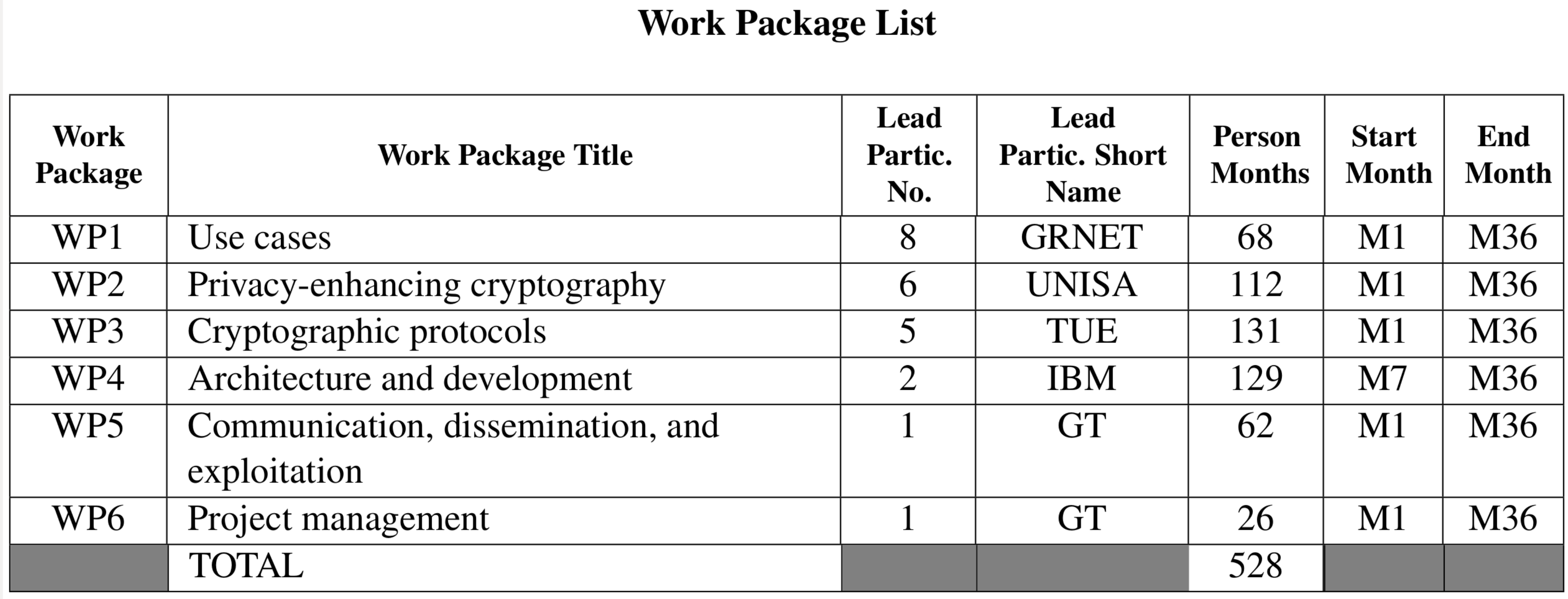
- PRIViLEDGE:
  Privacy-Enhancing Cryptography in Distributed Ledgers
- Budget Complessivo: circa 4.5 milioni di Euro
- Partners del Consorzio
  Privati: IBM Zurich, Guardtime, IOHK,
  Smartmatic-Cybernetica
  Pubblici: UniSA, Utartu, Uedinburgo, TUE,
  GUNET,GRNET

Ivan Visconti

PRIViLEDGE 2018-2020

UniSA (budget di circa 450 mila Euro)

- Ivan Visconti (Responsabile Scientifico)
- Carlo Blundo
- Giuseppe Persiano



Work Package List

Work Package	Work Package Title	Lead Partic. No.	Lead Partic. Short Name	Person Months	Start Month	End Month
WP1	Use cases	8	GRNET	68	M1	M36
WP2	Privacy-enhancing cryptography	6	UNISA	112	M1	M36
WP3	Cryptographic protocols	5	TUE	131	M1	M36
WP4	Architecture and development	2	IBM	129	M7	M36
WP5	Communication, dissemination, and exploitation	1	GT	62	M1	M36
WP6	Project management	1	GT	26	M1	M36
	TOTAL			528		

Ivan Visconti
PRIViLEDGE 2018-2020

- Verifiable online voting (Smartmatic-Cybernetica)
- Smart contracts for insurance markets (Guardtime)
- University diploma record ledger (GRNET)
- Update mechanism for stake-based ledgers (IOHK)
- Privacy in Hyperledger Fabric (IBM)

Ivan Visconti
PRIViLEDGE 2018-2020

- Hyperledger Fabric
  (opensource permissioned blockchain)

- KSI - Keyless Signature Infrastructure
  (permissioned blockchain)

- Cardano (supports both permissioned and
  permissionless blockchains)

Ivan Visconti

Opportunità

Assegni di ricerca su:

- cryptography for Ledger Technology
- cryptographic protocols da Ledger Technology
- environment-friendly Ledgers

Thanks!