Consiglio Nazionale delle Ricerche

Giovanni Schmid, ICAR

DeCifris@Cnr.it

Department of Engineering, ICT and Technologies

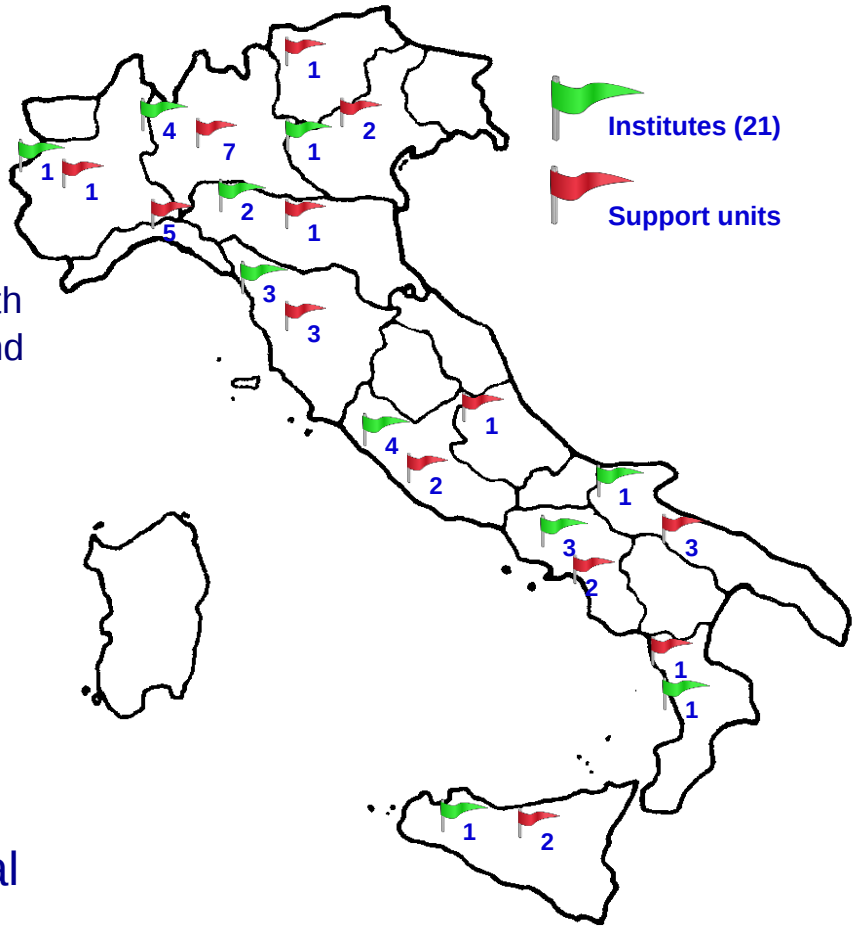
- 21 Institutes
- 1500+ FTE
- 900+ Researchers & Technologists
- About 19% of CNR
- National/international funded projects:

  50-60 Meuro per year; about 40% from contracts with third parties; 24 % from EU; 25% from Ministries and Regions, Local administrations; …

Main research areas:

Energy, Transportation, New materials;
Sensor technologies, Aerospace;
Manufacturing systems, Constructions;
ICT, Applied math, Applied physics

with applications to health & well being, cultural heritage, safety & security, agriculture & food,



Attività Progettuale *Cyber Security*

Privacy for big data – A. Monreale, ISTI

Cloud security – P. Mori, IIT

Information sharing and Analytics – G. Manco, ICAR

Secure software assurance – E. Marchetti, ISTI

Formal methods for cyber security – L. Durante, IEIIT

Applied cryptography - G. Schmid, ICAR

Digital forensics – M. Ianigro, ISSIA

Mobile device security – L. Caviglione, ISSIA

Application and system security – M. Ianigro, ISSIA

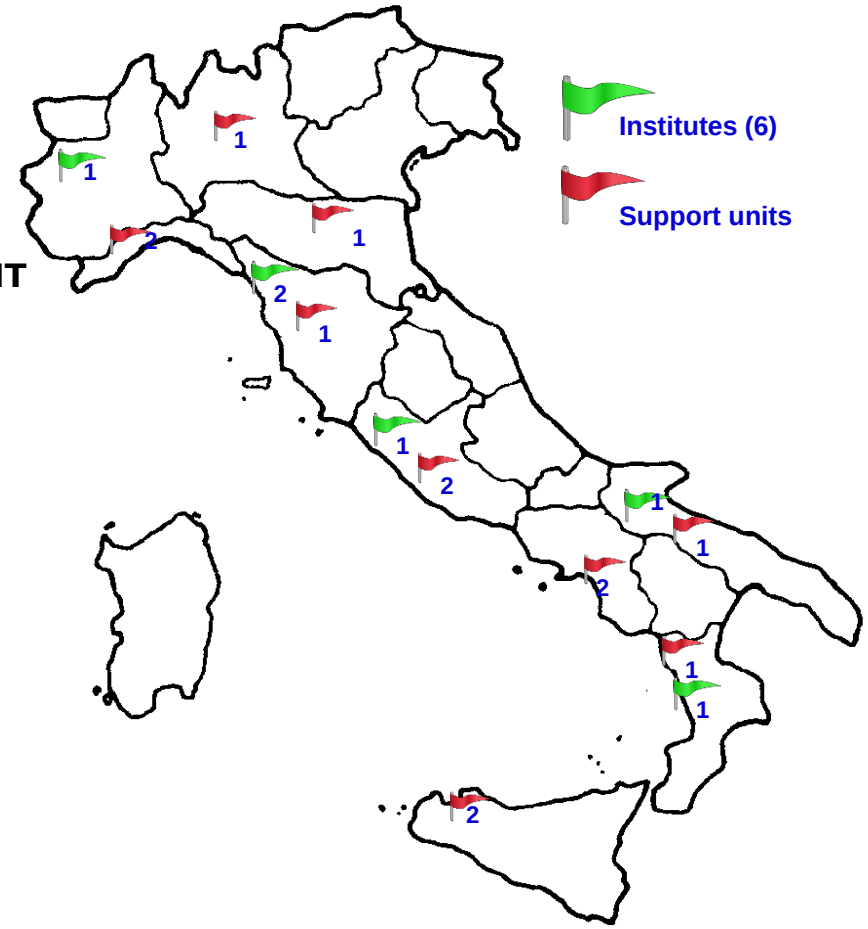
Trusted e-services – F. Martinelli, IIT

Access control – F. Martinelli, IIT

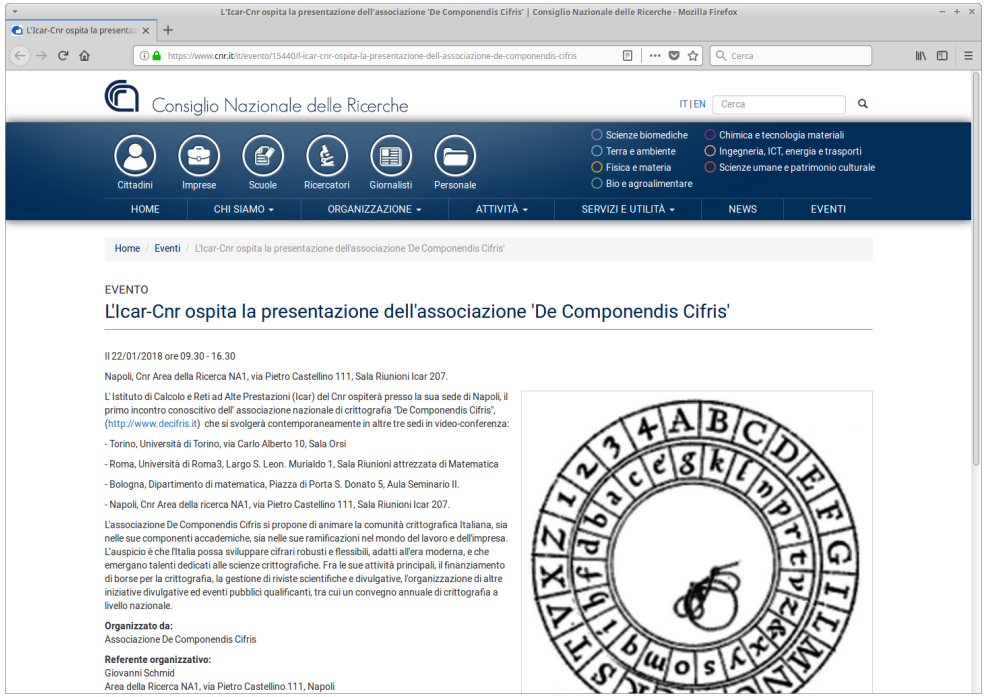
Network Security – M. Aiello, IEIIT

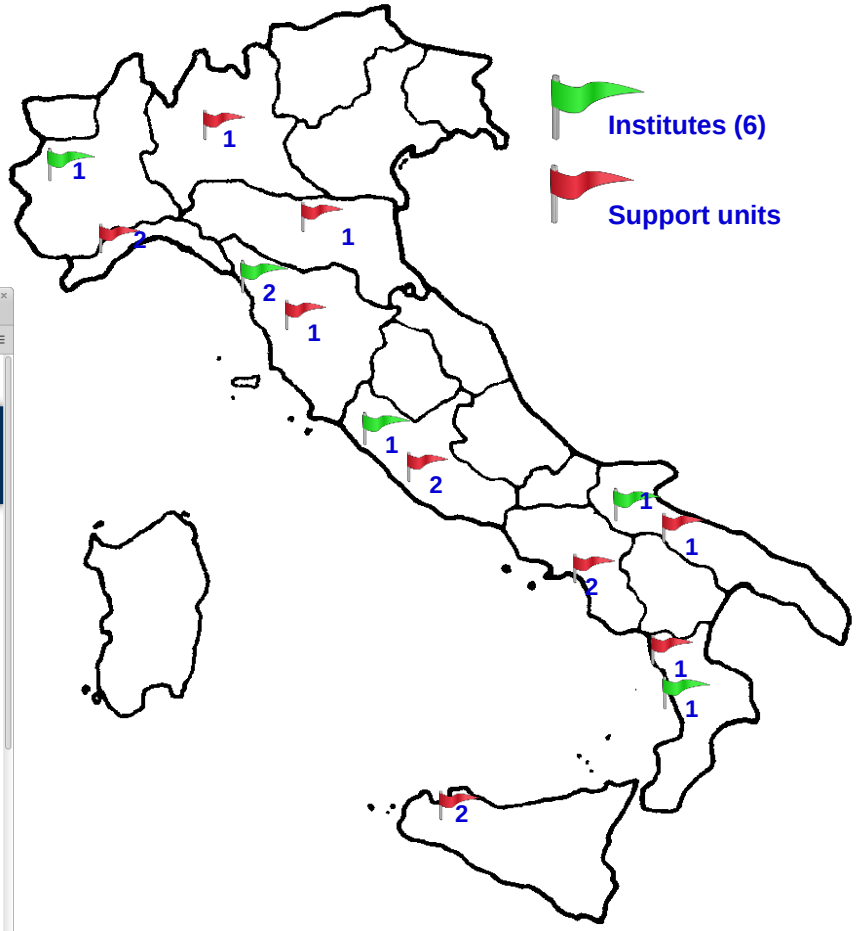
Cyberattacks – G. Papaleo, IEIIT

Risk management – A. Orlando, IAC

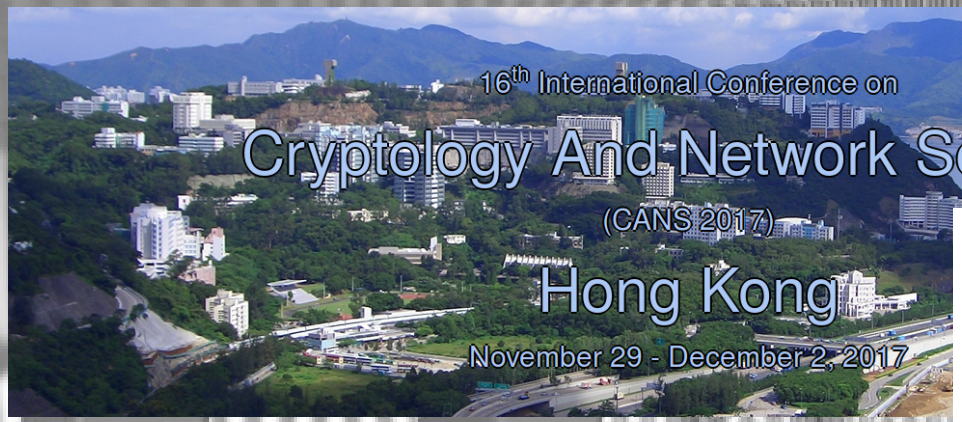


Attività Progettuale *Cyber Security con De Cifris*





Attività Progettuale *De Cifris*



CANS 2018

CANS 2018

The 17th International Conference on Cryptography and Network Security

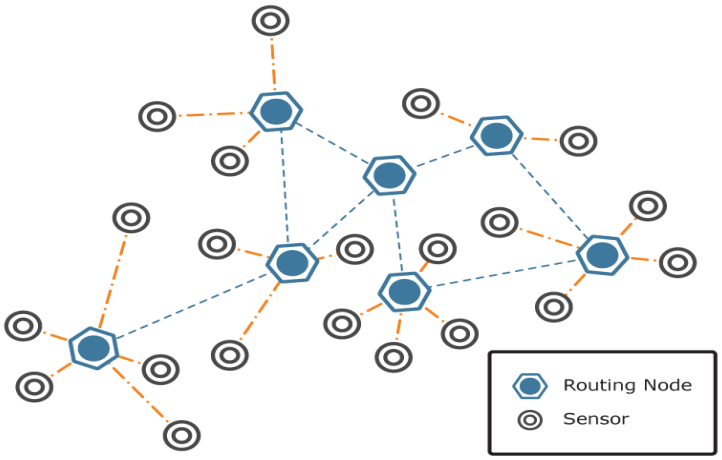

Contact address
giovanni.schmid@na.icar.cnr.it
giovanni.schmid@icar.cnr.it
giovanni.schmid@cnr.it

Giovanni Schmid, ICAR

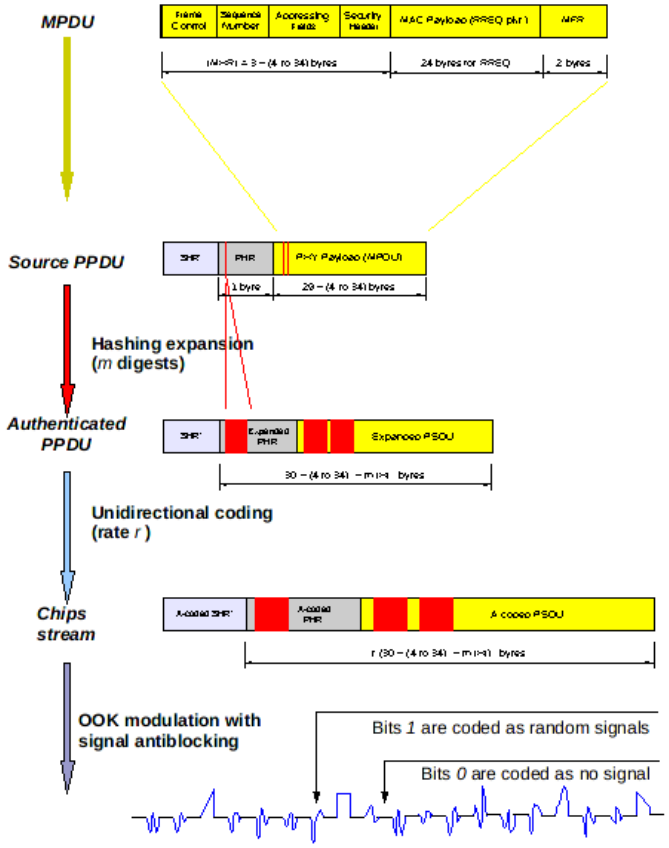
Consiglio Nazionale delle Ricerche

Cryptography@Cnr.it

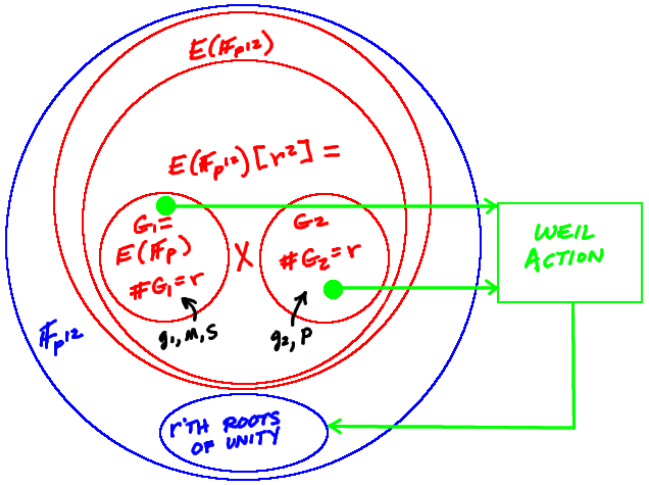
Secure Ad-hoc Routing

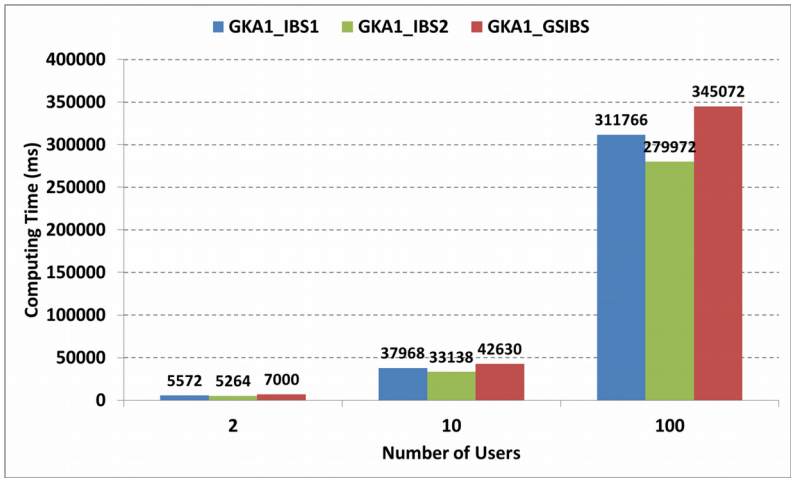


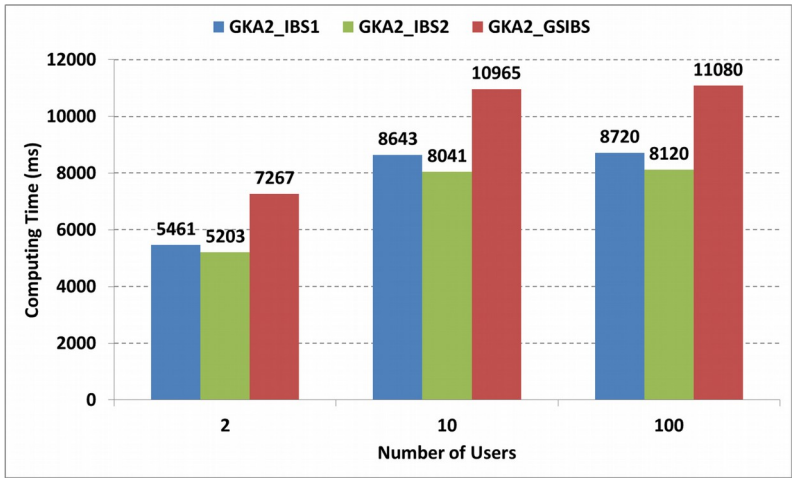
PHY type	Frequency Band (MHz)	IEEE Spreading factor	*Gain Factor* for the RREQ packet in AODV		
			m = 1	m = 2	m = 3
868/915 PBSK	868–868.6 / 902–928	15	3.66	2.24	1.62
2450 O-QPSK	2400-2483.5	8	1.95	1.20	0.86
915 ASK	902–928	6.4	1.49	0.91	0.65
868/915 O-QPSK	868–868.6 / 902–928	4	0.98	0.60	0.43
868 ASK	868–868.6	1.6	0.45	0.29	0.21



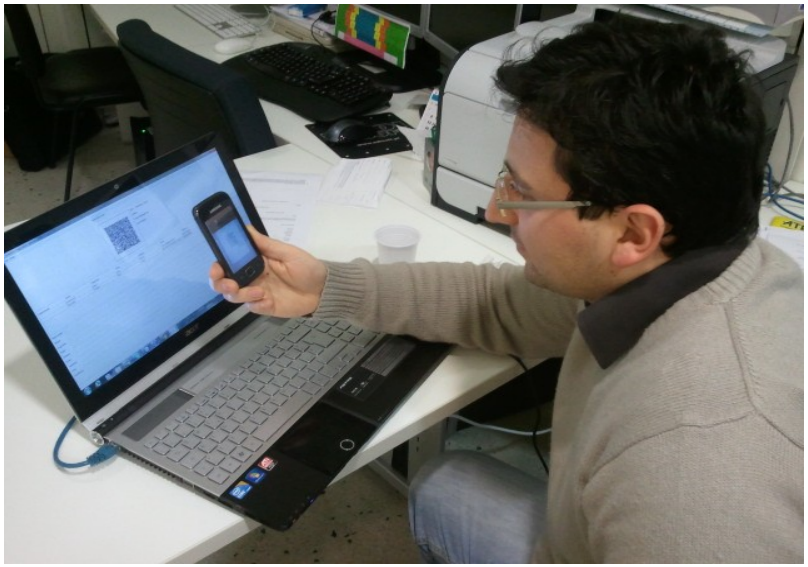
ID-based Group Key Agreement

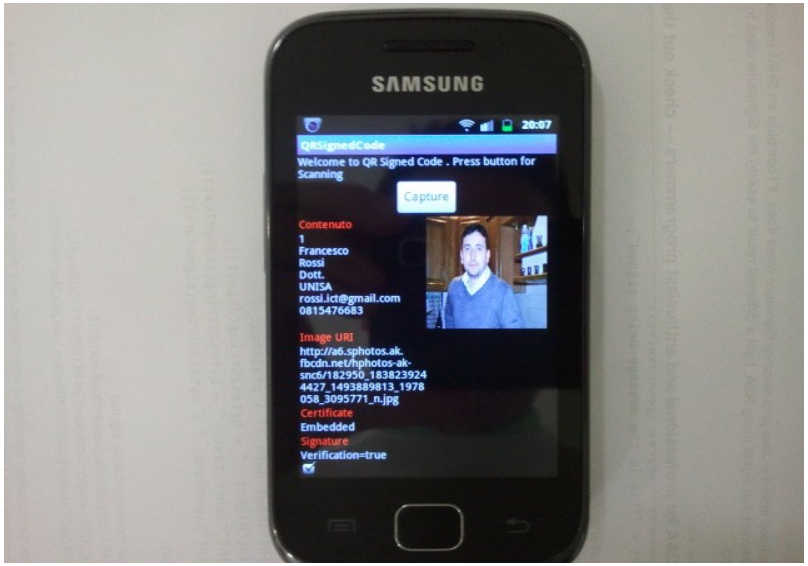




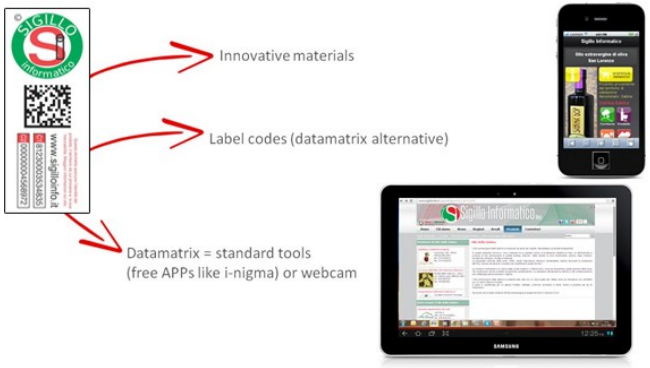


Authentication and Identification through mobile devices



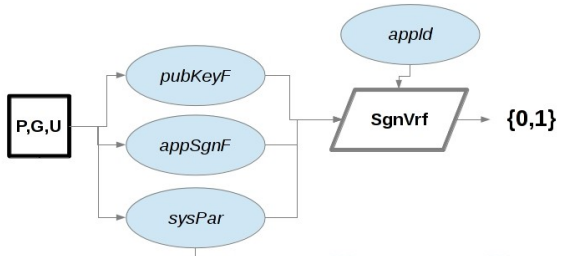


Physical Authentication Codes

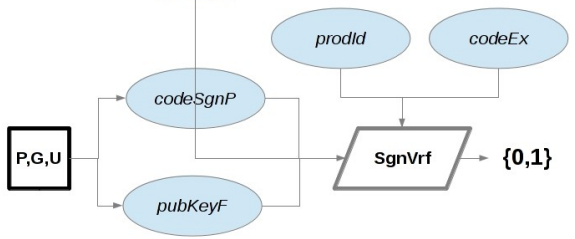


Denominazione o marchio (*proId*): specifiche atte ad individuare univocamente il prodotto	nome-prodotto
Item o Lotto (*prodNum*): valore alfanumerico indicante il numero seriale o di lotto che contraddistingue il prodotto	L309TA—13:16
Codifica UPC (*prodUpc*): valore Universal Product Code (UPC) indicante la tipologia di prodotto	80135876
Scadenza prodotto (*prodEx*): campo utilizzato per quei prodotti o mezzi di pagamento che riportano una data di scadenza.	05 nov 2014
Certificazione prodotto (*prodCer*): indica eventuali certificazioni relative al prodotto.	
Identificativo codice (*codeId*): indica in un formato opportuno un idenficativo univoco per il codice.	nome@17mar2014#00167
Scadenza codice (*codeEx*): indica in un formato opportuno la data di scadenza del codice	01 jan 2020 12:00:00 CET
Chiave pubblica servizio (*pubKeyF*): Chiave pubblica che rappresenta in modo univoco il servizio e la sua versione	2FA0189B3BC25FA833D66
Firma digitale (*codeSgnP*): valore ottenuto con l'algoritmo *SgnGen* e la chiave *secKeyP* a partire dai campi 2 – 6	A89FD15C7BE876A214A9 C675223AFFCBBD123411

VERIFICA APP:



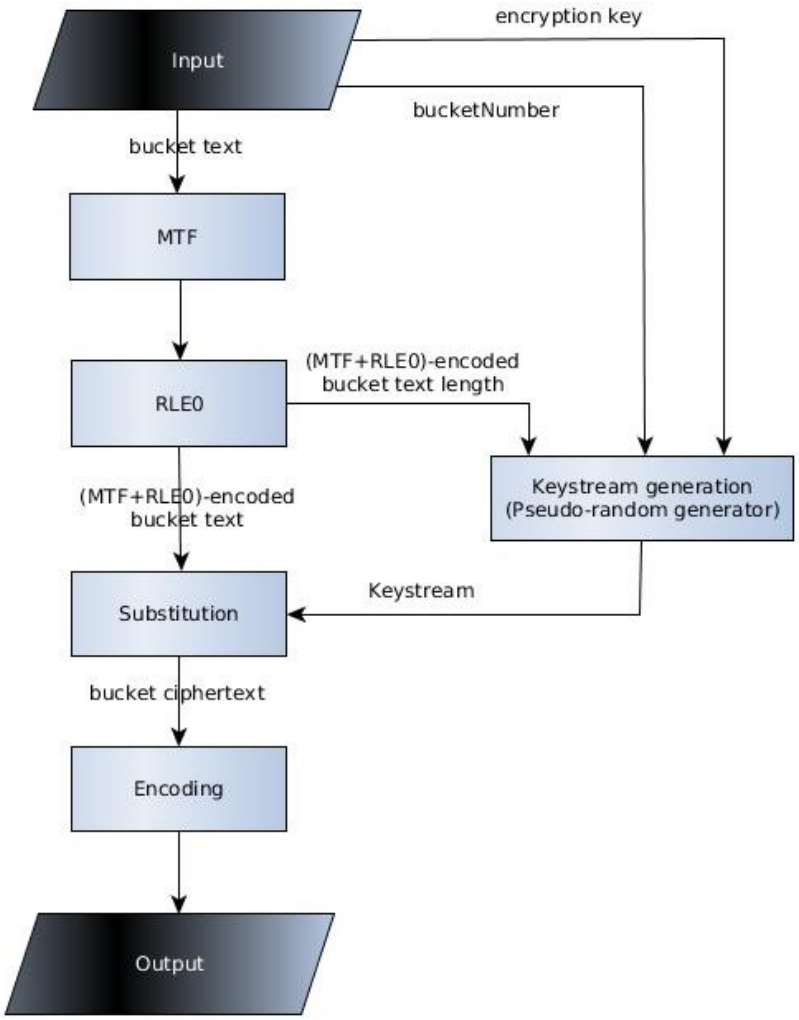
VERIFICA CODICE:

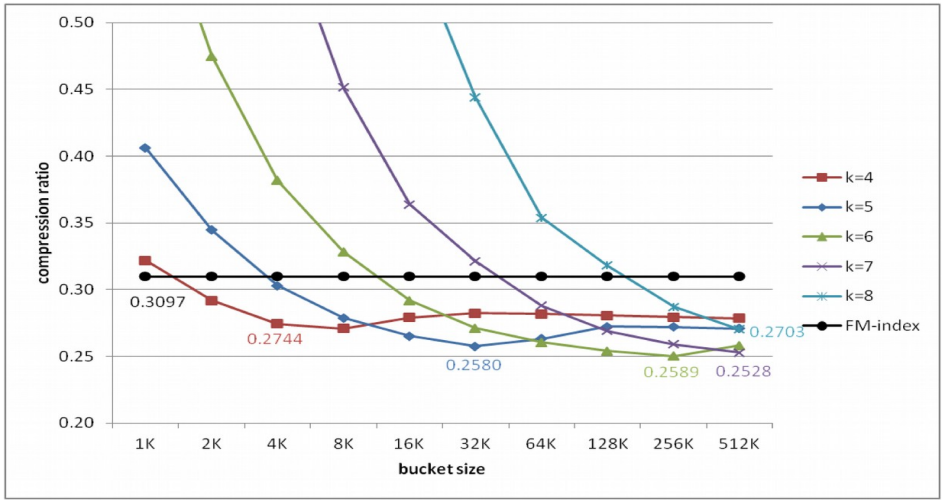


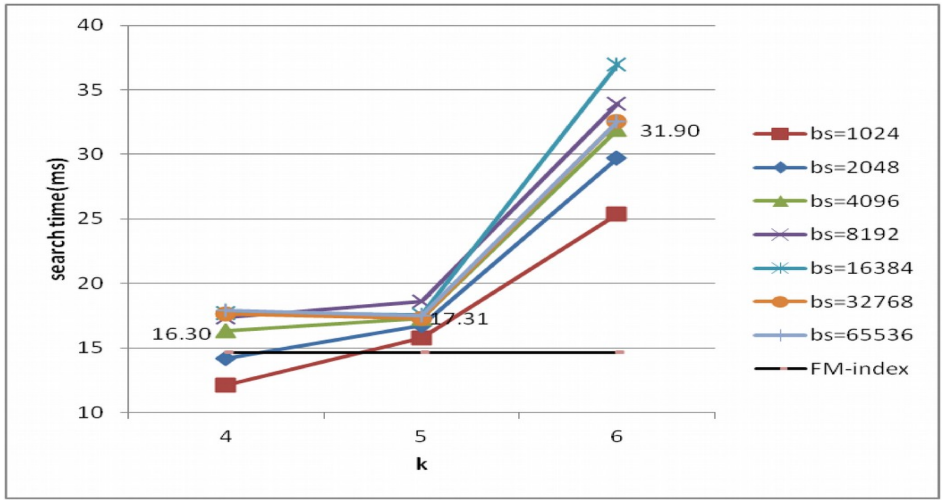
P=Produttore, G=Gestore, U=Utilizzatore,0=firma valida, 1=firma invalida

Dati pubblici

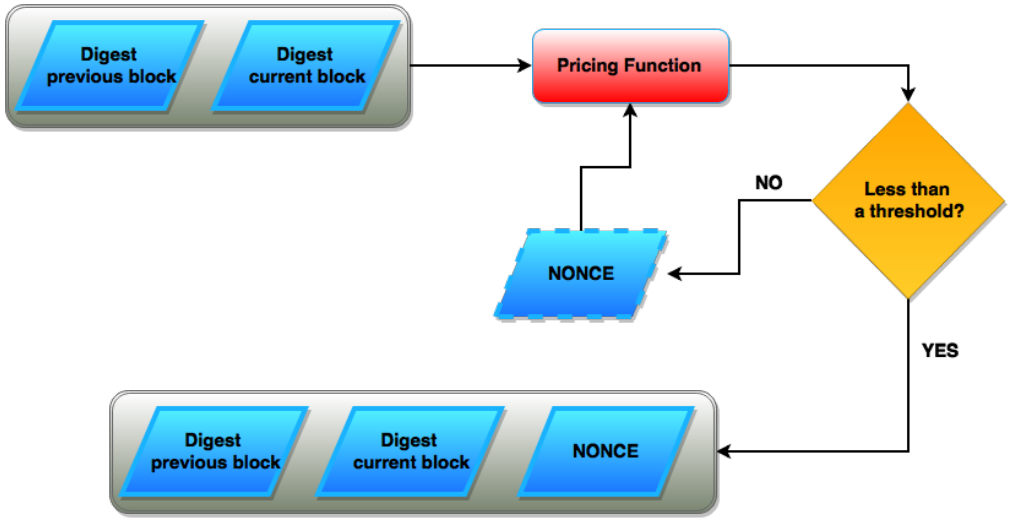
Crypto-compression of free form text data







Blockchain-based alternative systems (*)



(*) D. Romano and G. Schmid, *Beyond Bitcoin: A Critical Look at Blockchain-Based Systems*, Cryptography 2017, 1, 15; doi:10.3390/cryptography1020015

Blockchain-based alternative systems

MENU

la Repubblica.it

Economia&Finanza con Bloomberg

Seguici su

HOME MACROECONOMIA FINANZA LAVORO DIRITTI E CONSUMI AFFARI&FINANZA OSSERVA

Overview Borse Borsa Italia A-Z Valute Obbligazioni: Italia - Europa Fondi ETF Sedex Warrant Futures

Bitcoin & co: dietro i balzi stellari e i tracolli c'è il deserto delle regole

Attorno alle criptovalute regna ancora l'assoluta deregolamentazione da parte delle autorità di vigilanza. L'esperta: "Oggi le criptomonete sono associabili a strumenti di pagamento, non a valute. E in caso di contenziosi sarebbe molto difficile agire davanti a un giudice italiano"

1. CoinDash ICO Hack **$7M to $10M**
2. Parity Wallet Breach **$30M / 70,000 ethers**
3. Enigma Project Scam **1,500 ethers**
4. Parity Wallet Freeze **$275M**
5. Tether Token Hack **$30M**
6. Bitcoin Gold Scam **$3M**
7. NiceHash Market Breach **$78M / 4,700 BTC**

SOURCE:
https://www.coindesk.com/hacks-scams-attacks-blockchains-biggest-2017-disasters/

Blockchain-based alternative systems

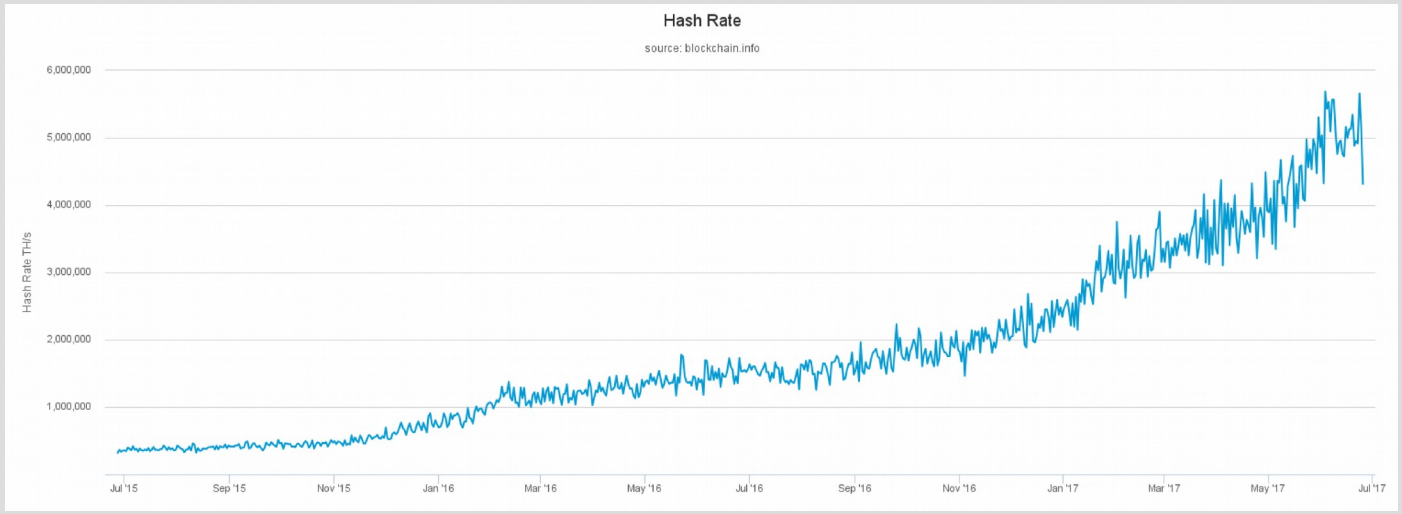
.....

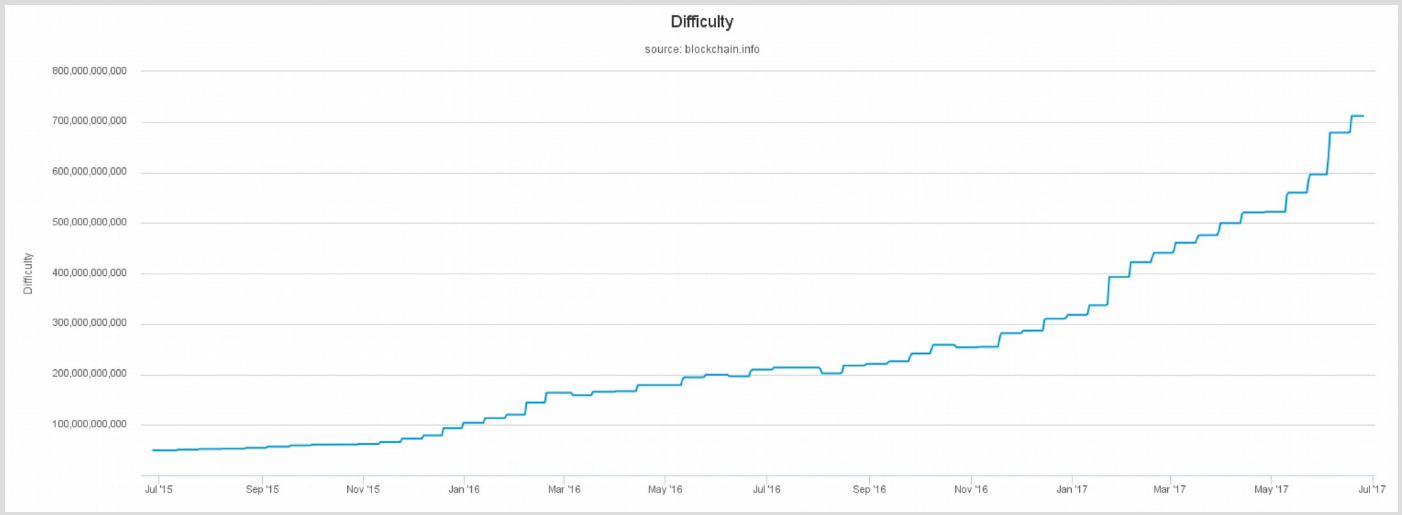
Where user based blockchains can get away with the need of identities by means of privacy preserving controls such as zero knowledge proofs and ring signatures that enhance anonymity of buyers and sellers, enterprise based blockchain applications need identity enabling controls to ensure that user identities of buyers and sellers can be attested by third party authorities and checked for sanctions by means of Know Your Customer (KYC) controls.

.....

Marco Mirko M.[orana], *The Long and Winding Road Ahead for Blockchain Security, 12/2017*

Blockchain-based alternative systems





Contact address: *Giovanni.Schmid@cnr.it*