iniziativa nazionale

CifrisCloud

Il prossimo incontro telematico si terrà
mercoledì **28/4/2021 alle ore 17.00** con il contributo di

Marcello Paris
Attribute-based encryption and signatures

Chiunque fosse interessato a restare in contatto con i nostri annunci
può chiedere di essere inserito nella mailing list all’indirizzo
cloud@decifris.it

News

Link della prossima riunione

Topic: CifrisCloud - Attribute Based Encryption and Signatures
Time: Apr 28, 2021 05:00 PM Rome
https://us02web.zoom.us/j/85987848606?pwd=cnB2eGVmajZrWFdKME5vNVVIb1R2Zz09
Meeting ID: 859 8784 8606
Passcode: 8@-#28Fpf8

Titolo: Attribute-based encryption and signatures.

Abstract:
Users (people or entities) could have their bag of attributes (say, labels), given by an authority. These attributes can be combined in policies (i.e. expressions on attributes), each of them will be (possibly) satisfied by some subset of users (according to their bag of attributes).

Attribute-based encryption is about encrypting a message according to a given policy so that the message is meant for all those having a set of attributes that could satisfy the policy. Attribute-based signatures are about signing a message according to a given policy so that these signatures could be verified, proving that the signer had a set of attributes satisfying the policy.

The availability of both encrypt/decrypt and sign/verify primitives allows designing interesting attribute-based analogues of standard constructions for messaging, authentication, access control and ownership.

In this talk, we give an overview of attribute-based encryption and signatures and discuss the above-mentioned applications.

Relatore: Marcello Paris

Gruppo di Studio

Il gruppo di studio CifrisCloud - Data Analysis coordinato da Michela Iezzi (Banca d'Italia) ha individuato un interessante repository di risorse in via di sviluppo per homomorphic encryption:

https://github.com/jonaschn/awesome-he

Il gruppo si incontra con cadenza settimanale il venerdì mattina.

Newsletter

Per iscriversi alla newsletter inviare una mail all'indirizzo del gruppo di lavoro:
cloud@decifris.it

Contacts:

cloud@decifris.it

segreteria@decifris.it

marco.pedicini@uniroma3.it
(Coordinatore)