DE CYFRIS A I, qui maximi rebus agendis presunt in dies ex periunt anni sit habere aliquem sidissimu cui secretiora instituea & Constitio ita comunicet ur ex ea re sibi nunquam poemtendum sie ild quia no facile ob comunem hommus psidinisi datur ur possine ex sentenna inuente sum seribendi ra trones auas Cyfros nuncupant: Comensu quidem.

De Cifris Augustae Taurinorum









Monday, 15 July 2019 – at 14.30 Aula Buzano, Politecnico di Torino

Giuseppe D'Alconzo Telsy S.p.A.

An introduction to secure multi-party computation

Abstract: Secure Multi Party Computation (MPC) is a branch of cryptography that allows a set of players to evaluate a public function on private inputs, revealing no information about them apart from the computed output. It is an alternative to the strong assumption of the existence of a trusted party. It was born in the 1980s as a theoretical and not so treatable field for its computational complexity, but the developments of the last years made MPC a powerful tool to solve real-world problems: numerous applications have been developed and its popularity is in strong

growth. In this talk the ideas underlying this practice and the various application scenarios will be exposed, together with a current state of the art.

For Information: fabio.fiori@food-chain.it, guglielmo.morgari@telsy.it,

nadir.murru@polito.it, lea.terracini@unito.it.

CONTATTI

Associazione De Componendis Cifris direttore@decifris.it, segreteria@decifris.it