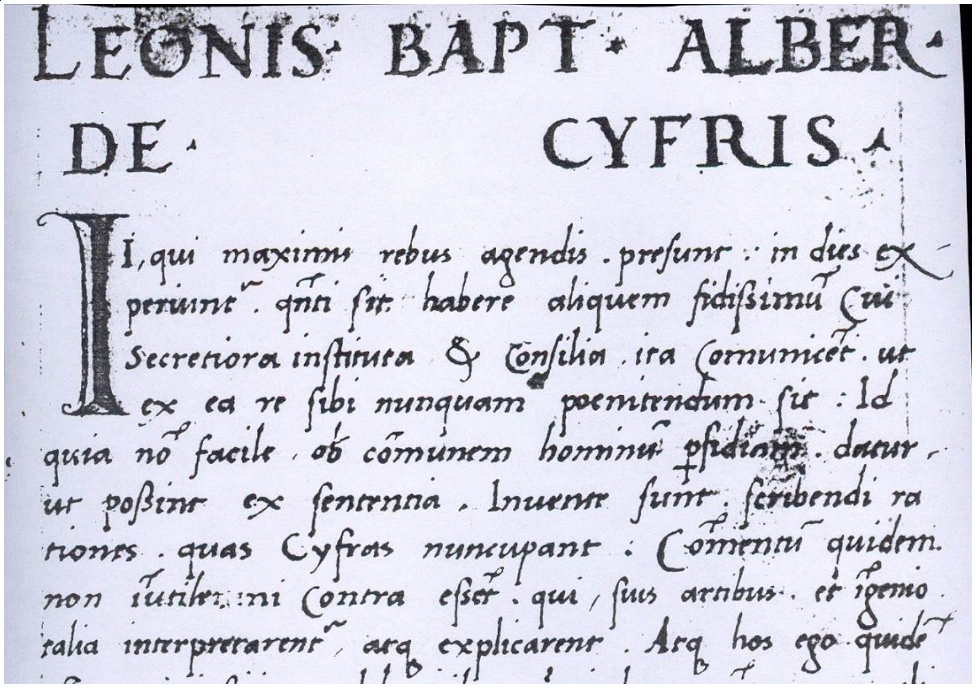

LEONIS BAPT ALBER
DE CYFRIS

II, qui maximis rebus agendis . preſunt : in dies experiunt. quāti ſit habere aliquem fidiſſimū cui Secretiora inſtituta & Conſilia . ita comunicet . ut ex ea re ſibi nunquam poenitendum ſit : Id quia nō facile . ob cōmunem hominū pfidiam . datur . ut poſſint ex ſententia . Inuente ſunt . ſcribendi rationes . quas Cyfras nuncupant : Cōmentū quidem . non inutile . ni contra eſſet . qui ſuis artibus . et ingenio . talia interpretarent . atq explicarent . Atq hos ego quidē

De Cifris Mediolanensibus

UNIVERSITÀ DEGLI STUDI DI MILANO

POLITECNICO MILANO 1863

UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

Thursday 9rh December 2020 – at 14:30
Online Seminar via Zoom

Lorenzo Grassi

University of Technology of Graz

Symmetric-Key Encryption Schemes for MPC Applications

Abstract: Modern cryptography developed many techniques that go well beyond solving traditional confidentiality and authenticity problems in two-party communication. In this presentation, we focus on the design (strategy) of new block ciphers/permutations/hash functions which are targeted for new applications in e.g. Multi-Party computation (MPC) application. This is motivated by recent progress in this (and other) new applications, where primitives from symmetric cryptography are needed and where the cost metric is different from the tradition one in which linear and non-linear computations have (almost) the same cost. Our first contribution here is the development of a new cipher -- called MiMC (Asiacrypt 2016) -- with low multiplicative complexity, which resembles a cipher proposed by Knudsen and Nyberg in 1995. As a generalization of such design and of Partial-SPN ciphers in general, we propose a high-level design approach for cryptographic (keyed/unkeyed) permutations -- called Hades (Eurocrypt 2020) -- addressing both needs of new applications that emphasize the role of non-linear operations and at the same time with a focus on simple arguments for its security. The design is mainly built up on the Wide-Trail design strategy for SP-Networks. At the same time, the crucial feature of such design is of moving from an even to a highly uneven distribution of non-linearity. Finally, we present an algebraic attack on full MiMC over GF(2^n), recently presented at Asiacrypt 2020. Such attack is based both the interpolation and the higher-order differential techniques.

Iscrizione all'evento online *da effettuare entro l'8* dicembre tramite il seguente link:

click here

Gli iscritti riceveranno l'ID Zoom un'ora prima dell'inizio dell'evento.

Contact person: Andrea Visconti

CONTATTI
Associazione De Componendis Cifris

seminari@decifris.it
segreteria@decifris.it