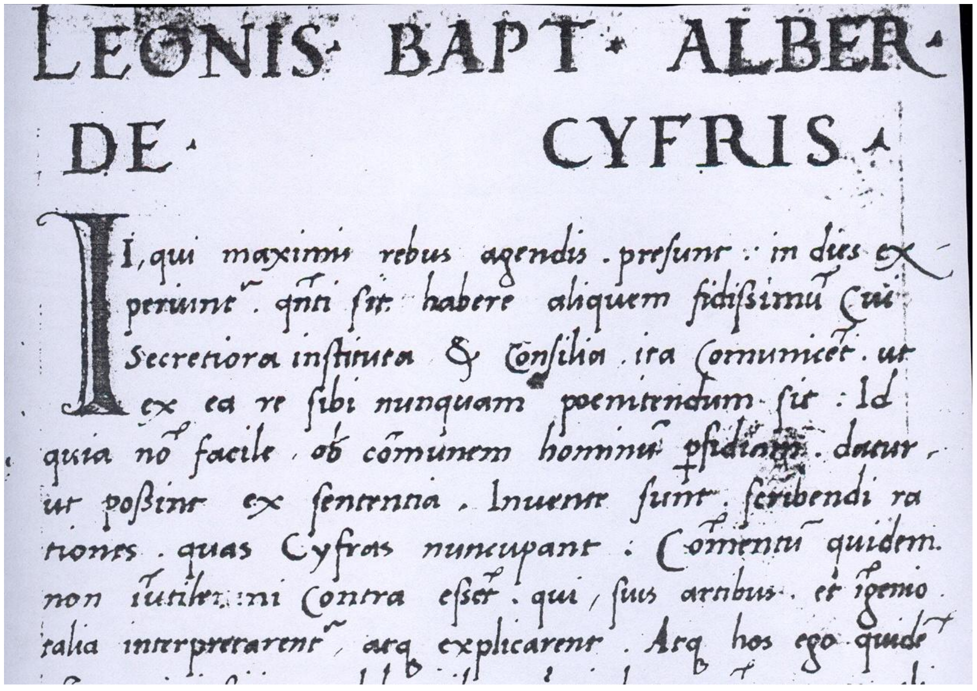

LEONIS BAPT ALBER
DE CYFRIS

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

De Cifris Athesis

UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Matematica

CENTER FOR CYBERSECURITY
FONDAZIONE BRUNO KESSLER

Tuesday 8th February 2022 – at 5:00 p.m.
Online Seminar via Zoom

Michele Orrù

University of California, Berkeley

Breaking 20 years of Schnorr-like blind signatures

Abstract: Blind signatures are cryptographic schemes that allow Alice to sign a document without knowing its content. Schnorr (blind) signatures, proposed more than 30 years ago, have been the foundation for dozens of cryptographic protocols of today, such as multisignatures, threshold signatures, zero-knowledge protocols, e-cash and electronic voting systems. Most of these protocols, when concurrent executions are allowed, hinge on a cryptographic assumption called ROS, whose hardness was already debated by Schnorr himself in 2001.

We present an algorithm solving the ROS (Random inhomogeneities in a Overdetermined Solvable system of linear equations) problem in polynomial time for $\ell > \log p$ dimensions. Our algorithm can be combined with Wagner's attack, and leads to a sub-exponential solution for any dimension ℓ with the best complexity known so far.

Our algorithm leads to practical attacks against blind signature schemes such as Schnorr and Okamoto–Schnorr blind signatures, threshold signatures such as GJKR and the original version of FROST, multisignatures such as CoSI and the two-round version of MuSig, partially blind signatures such as Abe–Okamoto, and conditional blind signatures such as ZGP17. Schemes for e-cash (such as Brands' signature) and anonymous credentials (such as Anonymous Credentials Light) are also affected.

This is joint work with Fabrice Benhamouda, Tancrède Lepoint, Julian Loss, and Mariana Raykova.

Iscrizione all'evento online *da effettuare entro il 7 febbraio* tramite il seguente link:

click here

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

Contact person: Massimiliano Sala

CONTATTI
Associazione De Componendis Cifris

segreteria@decifris.it
seminari@decifris.it