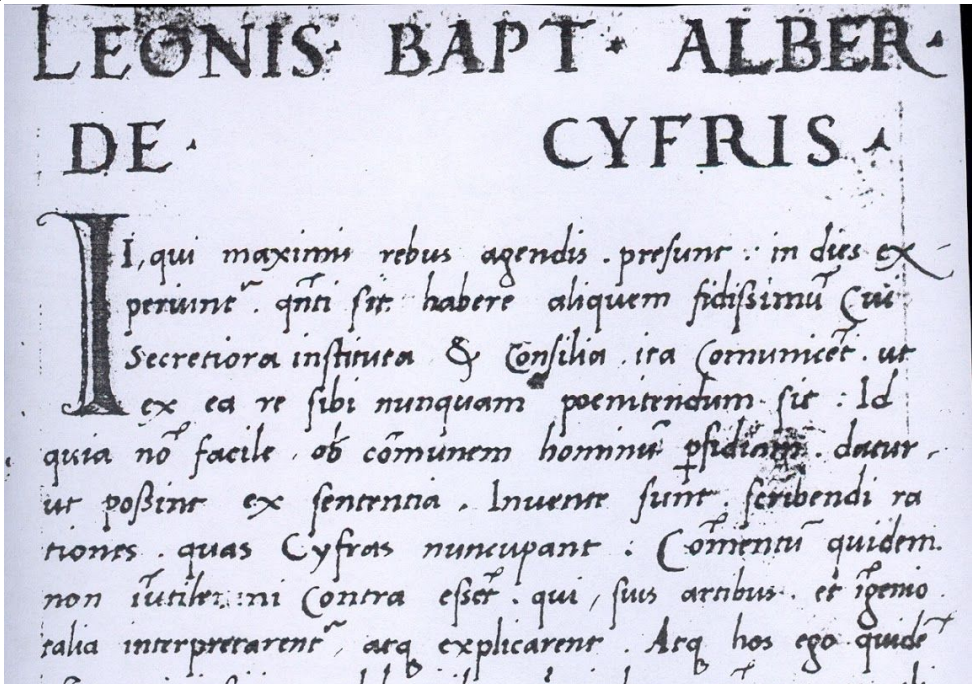
LEONIS BAPT. ALBER-
DE CYFRIS

II, qui maximis rebus agendis . presunt : in dies ex-
periunt . quã sit habere aliquem fidissimũ cui
Secretiora instituta & Consilia ita Communicet . ut
ex ea re sibi nunquam poeniteudum sit : Id
quia nõ facile . ob cõmunem hominũ pfidiam . datur
ut possint ex sententia . Inuenta sunt scribendi ra
tiones . quas Cyfras nuncupant : Comentu quidem
non iutilem Contra esset . qui , suis armis . et igemo
talia interpretarent , atq explicarent . Atq hos ego quide

De Cifris Athesis

UNIVERSITÀ DEGLI STUDI DI TRENTO
Dipartimento di Matematica

FONDAZIONE BRUNO KESSLER
ICT CENTER FOR INFORMATION AND COMMUNICATION TECHNOLOGY

Tuesday 10th September 2019 – at 11:00 a.m.
Department of Mathematics
Room A222, Povo 1, Via Sommarive, 9, Povo Trento

Ivan Visconti

Università degli Studi di Salerno

The Rush Dilemma: Attacking and Repairing Smart Contracts on Forking Blockchains

Abstract: We investigate the security of smart contracts within a blockchain that can fork (as Bitcoin and Ethereum). In particular, we focus on multi-party computation (MPC) protocols run on-chain with the aid of smart contracts, and observe that honest players face the following dilemma: Should I rush sending protocol's messages based on the current view of the blockchain, or rather wait that a message is confirmed on the chain before sending the next one?

To the best of our knowledge, the (implicit) default option used in previous work is the second one, and thus known on-chain MPC protocols take long time to be executed on those blockchains with a long confirmation time (e.g., 1 hour per transaction in Bitcoin). While the first option would clearly be preferable for efficiency, we show that this is not necessarily the case for security, as there are natural examples of on-chain MPC protocols that simply become insecure in presence of rushing players.

Our contributions are twofold:

• For the concrete case of fairly tossing multiple coins with penalties, we show that the lottery protocol of Andrychowicz et al. (S&P '14) becomes insecure in the presence of rushing players. In addition, we present a new protocol that instead retains security even if the players are rushing.

• We design a compiler that takes any on-chain MPC protocol and transforms it into another one (for the same task) that remains secure even in the presence of rushing players. The only (unavoidable) requirement is that honest players start to be rushing after the first round of the protocol (by all players) has been confirmed on the blockchain.

Our techniques are inspired by ideas on resettably secure computation (Goyal and Sahai, EUROCRYPT '09).

We also provide a prototype implementation of our coin tossing protocol using Ethereum smart contracts, and instantiate our generic compiler in a concrete setting, showing that both our constructions yield considerable improvements in terms of efficiency.

Joint work with: Vincenzo Botta (DIEM - University of Salerno), Daniele Friolo (La Sapienza University, Rome), Daniele Venturi (La Sapienza University, Rome)

Contact person: Massimiliano Sala

CONTATTI
Associazione De Componendis Cifris

direttore@decifris.it
segreteria@decifris.it