High-Level Programming for E-Cash

Pedro Adão[1⋆], Cédric Fournet[3,2], Nataliya Guts[2], and Francesco Zappa Nardelli[4,2]

[1] SQIG–Instituto de Telecomunicações and IST, TULisbon, Portugal
[2] MSR-INRIA Joint Centre
[3] Microsoft Research
[4] INRIA

Abstract. We consider symbolic characterizations of the Compact E-Cash protocol of Camenisch, Hohenberger, and Lysyanskaya [CHL05]. E-cash protocols [Cha82,CFN88] aim at providing robust abstractions for anonymous payment protocols. Properties of interest include, for instance, that users can spend coins anonymously, that users cannot forge coins, and that user should not spend the same coin twice without being eventually caught. These protocols involve sophisticated cryptographic constructions.

Relying on recent work on optimistic value commitment [FGN08], we design a calculus with E-cash primitives. Our calculus has a simple, symbolic semantics; it can be used for programming with E-cash and for reasoning on its properties, while shielding the programmer from its cryptographic implementation.

We consider two variants of the symbolic semantics. An abstract semantics rules out any double spending (by design). A more realistic, intermediate semantics accounts for the possibility of double spending, with reliable detection. We first relate these two semantics, then relate the intermediate semantics to the computational properties of the underlying E-cash protocol.

References

[AF06] Pedro Adão and Cédric Fournet. Cryptographically sound implementations for communicating processes. In *ICALP*, volume 4052 of *Lecture Notes in Computer Science*, pages 83–94. Springer, 2006.

[Cha82] David Chaum. Blind signatures for untraceable payments. In *CRYPTO*, pages 199–203, 1982.

[CFN88] David Chaum, Amos Fiat, and Moni Naor. Untraceable electronic cash. In *CRYPTO*, volume 403 of *Lecture Notes in Computer Science*, pages 319–327. Springer, 1988.

[CHL05] Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. Compact e-cash. In *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 302–321. Springer, 2005.

[FGN08] Cédric Fournet, Nataliya Guts, and Francesco Zappa Nardelli. A formal implementation of value commitment. *Programming Languages and Systems (ESOP'08)*, volume 4960 of *LNCS*, pages 383–397. Springer, 2008.

⋆ Partially supported by FEDER/FCT project KLog PTDC/MAT/68723/2006 and FEDER/FCT project QSec PTDC/EIA/67661/2006.