A Proof Theory for Distributed Evidential Transactions

Vivek Nigam
fortiss GmbH, Germany
nigam@fortiss.org

Giselle Reis
CMU Qatar
giselle@cmu.edu

Dian Balta
fortiss GmbH, Germany
balta@fortiss.org

Tewodros Beyene
fortiss GmbH, Germany
beyene@fortiss.org

Harald Ruess
fortiss GmbH, Germany
ruess@fortiss.org

Natarajan Shankar
SRI International, USA
shankar@csl.sri.com

Evidential transactions (ETs) provide auditable and composable evidence that serves as a witness or a proof that a transaction has been correctly executed by the named parties. For example, for issuing a Visa, an applicant demonstrates, among other evidence, that he has sufficient financial means to visit a foreign country. The form of evidence in ETs has traditionally been unstructured and informal, in the form of paper-based evidence. This talk proposes a formal treatment of evidence based on proof theory. In particular, we investigate the proof theory of Cyberlogic, an assertion logic for ETs, that enables the combination of evidence represented as logical derivations and as digital certificates, i.e., electronic evidence signed by a principals secret key. We propose a proof system for Cyberlogic, refining it with further constructions that support a wider range of ETs. We prove that the proof system admits cut-elimination. Moreover, we propose a sound and complete focused proof system for the refinement of Cyberlogic thus enabling efficient proof-search. Furthermore, we identify a fragment of Cyberlogic, called Cyberlogic Programs, that can be used to efficiently program ETs using a variety of FOL engines. Finally, we propose Proof Certificate format for Cyberlogic Programs inspired by Foundational Proof Certificates as a means to communicate evidence and check its validity.

1 Introduction

Trust in distributed exchanges in electronic commerce, business and administrative processes, and digital government may be based on reputation measures or on audits of explicitly generated evidence of the effects of such a transaction. The verification approach towards trustworthy exchanges as developed here is based on the central notion of *evidential distributed transaction*, which involve the exchange of various forms of *verifiable evidence*. For example, an evidential transaction (ET) might issue a visa, given that, say, additional proof of sufficient financial means has been provided in the form of a digital certificate whose validity can then be verified by customs authorities upon entry.

In earlier work we proposed Cyberlogic as a foundational logic for evidential transactions, where some of the evidence can be in the form of digital certificates [3, 18]. Encryption in the form of digital signatures provides the underlying mechanism for transferring evidence in Cyberlogic, whereas the verification of evidence is based on decryption.

In Cyberlogic, cryptographic keys K are identified with specific authorities, and attestations $K \mathit{says} A$ express the fact that principal K attests to statement A. In the example above, K may be the visa-granting authority and A the statement that the visa requester is authorized to enter the specified country no later than, say, by the end of the year and at most once. These kinds of statements are signed by the private key of an authorized principal K to obtain a digital certificate c, so that c is evidence for the claim that K attests to the statement A. This can be verified by decrypting c with the corresponding public key of K to see it it gives A.

Submitted to:
TEASE 2020

These basic ingredients of Cyberlogic are expressive enough for encoding some enabling mechanisms of trust management [2, 5, 4, 14] including the delegation and revocation of authorities, and also temporal attestations [3]. Underlying principles of Cyberlogic have been applied, among others, to the forensics of software systems [12], accountable clouds [11], correct-by-design smart contracts [10], and accountable blockchain transactions [9]. The relationship of the Curry-Howard isomorphism for software certificates has been studied previously [13], but a complete formal treatment of the proof theory of Cyberlogic has been missing.

Our first contribution is a Gentzen style proof system for Cyberlogic that admits cut elimination. A feature of the proof system is that it enables the combination of evidence represented as logical derivations as well as digital evidence, *e.g.*, signed hashes of tickets, certificates, financial statements, medical records. We also identify a knowledge operator for collections of principals, which may simplify Cyberlogic encodings and corresponding derivations considerably. An evidence associated to an ET is formalized as a Cyberlogic proof, that is, a proof of an assertion of the form K$saysA$ from a given set of Cyberlogic theories and digital certificates.

Two main challenges emerge from the fact that such evidence, *i.e.*, Cyberlogic proof, is often constructed involving different principals that do not necessarily share the same (physical nor logical) location. The first challenge is how to build efficient, sound and complete distributed proof search mechanisms for Cyberlogic. The second challenge is how to efficiently communicate such evidence. Proof theory lays the foundations for addressing these two challenges. In particular, focused proof systems [1] have been used to explain proof search heuristics used in logic programming [15, 6], and also as the basis for proposing proof certificate formats [16, 7]. Our second contribution, a sound and complete focused proof system for Cyberlogic.

Our third contribution addresses the challenge related to distributed proof search. We identify a fragment of Cyberlogic, called Cyberlogic Programs, that resembles the class of Horn formulas used in logic programming. By studying Cyberlogic programs's proof search behavior from the lenses of focusing, we establish a sound and complete distributed proof search heuristic. We argue by example that the proposed heuristic is adequate for implementation, as it can build on existing FOL proof search tool, *e.g.*, Prolog and Datalog. Indeed, our proposed heuristic can be viewed as an extension of distributed logic programs [17, 8].

Furthermore, our fourth contribution addresses the challenge of how to efficiently communicate evidence. We propose a Proof Certificate format for Cyberlogic Programs inspired by Foundational Proof Certificates (FPCs) [7]. FPCs enable the construction of parts of a proof by using logic programs and engines. This means that FPCs and our Proof Certificates do not need to contain data that can be easily reconstructed or for which one is willing to reconstruct.

We illustrate these proof-theoretic developments using the Visa example. We conclude with a discussion on related and future work. Proof sketches of the most interesting results are available in the Appendix.

References

[1] Jean-Marc Andreoli (1992): *Logic Programming with Focusing Proofs in Linear Logic*. Joural of Logic and Computation 2(3), pp. 297–347. Available at `http://dx.doi.org/10.1093/logcom/2.3.297`.

[2] Andrew W. Appel & Edward W. Felten (1999): *Proof-carrying authentication*. In: *ACM Conference on Computer and Communications Security*, pp. 52–62.

[3] Vincent Bernat, Harald Ruess, & Natarajan Shankar (2004): *First-order Cyberlogic*. Technical Report CSL-SRI-04-03, SRI International Computer Science Laboratory.

[4] M. Blaze, J. Feigenbaum & J. Lacy (1996): *Decentralized trust management*. In: *Proceedings 1996 IEEE Symposium on Security and Privacy*, pp. 164–173.

[5] Keromytis A.D. Blaze M., Feigenbaum J. (1998): *KeyNote: Trust Management for Public-Key Infrastructures*. In Christianson B., Crispo B., Harbison W.S. & Roe M., editors: *Security Protocols*, Lecture Notes in Computer Science, Springer.

[6] Kaustuv Chaudhuri, Frank Pfenning & Greg Price (2006): *A Logical Characterization of Forward and Backward Chaining in the Inverse Method*. In: *Automated Reasoning, Third International Joint Conference, IJCAR, Proceedings*, pp. 97–111, doi:10.1007/11814771_9.

[7] Zakaria Chihani, Dale Miller & Fabien Renaud (2017): *A Semantic Framework for Proof Evidence*. *J. Autom. Reasoning* 59(3), pp. 287–330, doi:10.1007/s10817-016-9380-6.

[8] Simon Cruanes, Grégoire Hamon, Sam Owre & Natarajan Shankar (2013): *Tool Integration with the Evidential Tool Bus*. In: *Verification, Model Checking, and Abstract Interpretation, 14th International Conference, VMCAI. Proceedings*.

[9] Zaynah Dargaye, Antonella Del Pozzo & Sara Tucci Piergiovanni (2018): *Pluralize: a Trustworthy Framework for High-Level Smart Contract-Draft*. *CoRR* abs/1812.05444. Available at `http://arxiv.org/abs/1812.05444`.

[10] Zaynah Lea Dargaye, Florent Kirchner, Sara Tucci-Piergiovanni & Önder Gürcan (2018): *Towards Secure and Trusted-by-Design Smart Contracts*. In: *Les vingt-neuvièmes Journées Francophones des Langages Applicatifs (The 29th Francophone Days of Application Languages - JFLA 2018)*, Banyuls-sur-Mer, France. Available at `https://hal-cea.archives-ouvertes.fr/cea-01807036`.

[11] A. Gehani, G. F. Ciocarlie & N. Shankar (2013): *Accountable clouds*. In: *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, pp. 403–407, doi:10.1109/THS.2013.6699038.

[12] Ashish Gehani, Florent Kirchner & Natarajan Shankar (2009): *System Support for Forensic Inference*. In Gilbert Peterson & Sujeet Shenoi, editors: *Advances in Digital Forensics V*, Springer Berlin Heidelberg, pp. 301–316.

[13] Amrit Kumar, Pierre-Alain Fouque, Thomas Genet & Mehdi Tibouchi (2012): *Proofs as Cryptography: a new interpretation of the Curry-Howard isomorphism for software certificates*. Available at `https://hal.archives-ouvertes.fr/hal-00715726`. 19 pages.

[14] Ninghui Li, Benjamin N. Grosof & Joan Feigenbaum (2003): *Delegation Logic: A Logic-Based Approach to Distributed Authorization*. *ACM Trans. Inf. Syst. Secur.* 6(1), p. 128171, doi:10.1145/605434.605438. Available at `https://doi.org/10.1145/605434.605438`.

[15] Chuck Liang & Dale Miller (2009): *Focusing and polarization in linear, intuitionistic, and classical logics*. *Theor. Comput. Sci.* 410(46), pp. 4747–4768, doi:10.1016/j.tcs.2009.07.041.

[16] Dale Miller & Vivek Nigam (2007): *Incorporating tables into proofs*. In J. Duparc & T. A. Henzinger, editors: *CSL*, *LNCS* 4646, pp. 466–480.

[17] Vivek Nigam, Limin Jia, Boon Thau Loo & Andre Scedrov (2012): *Maintaining distributed logic programs incrementally*. *Computer Languages, Systems & Structures* 38(2), pp. 158–180, doi:10.1016/j.cl.2012.02.001.

[18] Harald Rueß
surnameend & Natarajan Shankar (2003): *Introducing Cyberlogic*. In: *Proceedings of the 3rd Annual High Confidence Software and Systems Conference*.