On Equivalences, Metrics, and Polynomial Time*

Alberto Cappai† Ugo Dal Lago‡

Abstract

Interactive behaviors are ubiquitous in modern cryptography, but are also present in λ-calculi, in the form of higher-order constructions. Traditionally, however, typed λ-calculi simply do not fit well into cryptography, being both deterministic and too powerful as for the complexity of functions they can express. We study interaction in a λ-calculus for probabilistic polynomial time computable functions. In particular, we show how notions of context equivalence and context metric can both be characterized by way of traces when defined on linear contexts. We then give evidence on how this can be turned into a proof methodology for computational indistinguishability, a key notion in modern cryptography. We also hint at what happens if a more general notion of a context is used.

Modern cryptography [4] is centered around the idea that security of cryptographic constructions needs to be defined precisely and, in particular, that crucial aspects are *how* an adversary interacts with the construction, and *when* it wins this game. The former is usually specified by way of an *experiment*, while the latter is often formulated stipulating that the probability of a favorable result for the adversary needs to be small, where being "small" usually means being *negligible* in a security parameter. This framework would however be vacuous if the adversary had access to an unlimited amount of resources, or if it were deterministic. As a consequence the adversary is usually assumed to work within probabilistic polynomial time (PPT in the following), this way giving rise to a robust definition. Summing up, there are three key concepts here, namely *interaction*, *probability* and *complexity*. Security as formulated above can often be spelled out semantically as the so-called *computational indistinguishability* between two distributions, the first one being the one produced by the construction and the second one modeling an idealized construction or a genuinely random object.

Typed λ-calculi as traditionally conceived, do not fit well into this picture. Higher-order types clearly allow a certain degree of interaction, but probability and complexity are usually absent: reduction is deterministic (or at least confluent), while the expressive power of λ-calculi tends to be very high. This picture has somehow changed in the last ten years: there have been some successful attempts at giving probabilistic λ-calculi whose representable functions coincide with the ones which can be computed by PPT algorithms [5, 8, 2]. These calculi invariably took the form of restrictions on Gödel's T, endowed with a form of binary probabilistic choice. All this has been facilitated by implicit computational complexity, which offers the right idioms to start from [3], themselves based on linearity and ramification. The emphasis in all these works were either the characterization of probabilistic complexity classes [2], or more often security [8, 6, 7]: one could see λ-calculi as a way to specify cryptographic constructions and adversaries for them. The crucial idea here is that computational indistinguishability can be formulated as a form of context equivalence. The real challenge, however, is whether all this can be characterized by handier notions, which would alleviate the inherently difficult task of dealing with all contexts when proving two terms to be equivalent.

The literature offers many proposals going precisely in this direction: this includes logical relations, context lemmas, or coinductive techniques. In applicative bisimulation [1], as an example, terms are modeled as interactive objects. This way, one focuses on how the interpreted program

*This work is partially supported by the ANR project 12IS02001 PACE.

†Università di Bologna & INRIA Sophia Antipolis

‡Università di Bologna & INRIA Sophia Antipolis

interacts with its environment, rather than on its internal evolution. None of them have so far been applied to calculi capturing probabilistic polynomial time, and relatively few among them handle probabilistic behavior.

In this talk, we study notions of equivalence and distance in one of these λ-calculi, called RSLR [2]. More precisely:

- After having briefly introduced RSLR and studied its basic metatheoretical properties, we define *linear context equivalence*. We then show how the role of contexts can be made to play by *traces*. Finally, a coinductive notion of equivalence in the style of Abramsky's bisimulation is shown to be a congruence, thus included in context equivalence, but not to coincide with it. We also hint at how all this can be extended to metrics.
- We then introduce a notion of *parametrized context equivalence* for RSLR terms, showing that it coincides with computational indistinguishability when the compared programs are of base type. We then turn our attention to the problem of characterizing the obtained notion of equivalence by way of linear tests, giving a positive answer to that by way of a notion of parametrized trace metric. A brief discussion about the role of linear contexts in cryptography is also given.

References

[1] Samson Abramsky. The lazy lambda calculus. In D. Turner, editor, *Research Topics in Functional Programming*, pages 65–117. Addison Wesley, 1990.

[2] Ugo Dal Lago and Paolo Parisen Toldin. A higher-order characterization of probabilistic polynomial time. In *FOPARA*, volume 7177 of *LNCS*, pages 1–18. Springer, 2011.

[3] Martin Hofmann. A mixed modal/linear lambda calculus with applications to bellantoni-cook safe recursion. In *Computer Science Logic, 11th International Workshop, CSL '97, Annual Conference of the EACSL, Aarhus, Denmark, August 23-29, 1997, Selected Papers*, pages 275–294, 1997.

[4] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman and Hall/CRC Press, 2007.

[5] John C. Mitchell, Mark Mitchell, and Andre Scedrov. A linguistic characterization of bounded oracle computation and probabilistic polynomial time. In *39th Annual Symposium on Foundations of Computer Science, FOCS '98, November 8-11, 1998, Palo Alto, California, USA*, pages 725–733, 1998.

[6] David Nowak and Yu Zhang. A calculus for game-based security proofs. *IACR Cryptology ePrint Archive*, 2010:230, 2010.

[7] David Nowak and Yu Zhang. Formal security proof with minimal fuss: Implicit computational complexity at work. *Information and Computation [accepted, in publication]*, 2014.

[8] Yu Zhang. The computational SLR: a logic for reasoning about computational indistinguishability. *Mathematical Structures in Computer Science*, 20(5):951–975, 2010.