

# How to Use the IACR Communications in Cryptology Class

## A Template

Joppe W. Bos<sup>a,1</sup>   and Kevin S. McCurley<sup>2</sup> 

<sup>1</sup> NXP Semiconductors, Leuven, Belgium

<sup>2</sup> Self

**Abstract.** The abstract goes here. You may use mathematics and macros in your abstract, but do not use `\cite` or footnotes. The abstract should be self-contained.

**Keywords:** Dirac  $\delta$  function · unit impulse

## 1 Introduction

This is the template showing how to use the IACR Communications in Cryptology L<sup>A</sup>T<sub>E</sub>X class. See the “How to Use the IACR Communications in Cryptology Class” for more details.

## 2 Bibliography

Citing papers is done in the usual way using BibTeX or `biblatex` commands. For example: the RSA paper [RSA78].

It is highly encouraged to use CyptoBib from <https://cryptobib.di.ens.fr>

## References

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978. doi:10.1145/359340.359342.

---

E-mail: [joppe.bos@nxp.com](mailto:joppe.bos@nxp.com) (Joppe W. Bos), [mccurley@digicrime.com](mailto:mccurley@digicrime.com) (Kevin S. McCurley)

<sup>a</sup>This is an example footnote.

