The llncscrypto Package: Enhanced LaTeX Style for LNCS + Cryptography

Matteo Campanelli and Agni Datta

Some Randomly Sampled University

Abstract. The llncscrypto package extends the LNCS (Lecture Notes in Computer Science) document class with advanced features for cryptography and theoretical computer science papers. This package provides enhanced theorem environments, TikZ graphics support, improved captions, and specialized tools for cryptographic notation and diagrams. It is designed to work seamlessly with the LNCS document class while adding powerful features for modern academic writing in cryptography and related fields.

1 Introduction

The llncscrypto package is designed to enhance the standard LNCS document class with features commonly needed in cryptography and theoretical computer science research. It provides a comprehensive set of tools while maintaining compatibility with LNCS formatting requirements.

2 Package Features

2.1 Enhanced Theorem Environments

When the `theorems` option is enabled, the package provides enhanced theorem environments:

Theorem 1 (Security Property). For any probabilistic polynomial-time adversary $\mathcal{A}$, the probability of breaking the security property is negligible.

Proof. The proof follows from the hardness assumption and the security reduction. □

Definition 1 (Cryptographic Primitive). A cryptographic primitive is a basic cryptographic algorithm that provides a specific security service.

Lemma 1 (Key Lemma). This is a key lemma that supports the main theorem.

2.2 TikZ Graphics Support

The `tikz` option enables comprehensive TikZ graphics support:

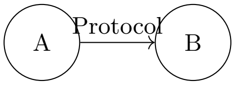

Fig. 1. Simple protocol diagram

Algorithm	Security Level	Key Size
AES-128	128 bits	128 bits
AES-256	256 bits	256 bits
RSA-2048	112 bits	2048 bits

Table 1. Cryptographic algorithms comparison

2.3 Enhanced Captions

The `captions` option provides improved caption formatting:

2.4 Cryptography Macros

The `crypto` option provides specialized macros for cryptographic notation:

- $\mathcal{K}$ - Key space
- $\mathcal{M}$ - Message space
- $\mathcal{C}$ - Ciphertext space
- Gen - Key generation algorithm
- Enc - Encryption algorithm
- Dec - Decryption algorithm

3 Usage Examples

3.1 Basic Usage

For basic usage with minimal features:

```
\documentclass{llncs}
\usepackage{llncscrypto}
```

3.2 Full Feature Set

For all features:

```
\documentclass{llncs}
\usepackage[captions,tikz,appendix,crypto,theorems]{llncscrypto}
```

3.3 Selective Features

For specific features only:

```
\documentclass{llncs}
\usepackage[tikz,theorems]{llncscrypto}
```

4 Advanced Features

4.1 Cross-Referencing

The package provides enhanced cross-referencing capabilities. For example, we can reference Theorem 1, Definition 1, and Figure 1.

4.2 Appendix Support

The `appendix` option enables enhanced appendix management:

```
\appendix
\section{Additional Proofs}
```

5 Compatibility

The llncscrypto package is designed to be fully compatible with:

- LNCS document class
- Standard LaTeX packages
- pdfLaTeX, XeLaTeX, and LuaLaTeX engines
- Major TeX distributions

6 Conclusion

The llncscrypto package provides a comprehensive solution for enhancing LNCS documents with advanced features for cryptography and theoretical computer science research. It maintains compatibility with LNCS requirements while adding powerful tools for modern academic writing.

References

[1] Author, A.: Title of the paper. In: Proceedings of the Conference, pp. 1–10 (2023)

[2] Author, B., Author, C.: Another important paper. Journal of Cryptography 15(2), 123–145 (2024)