Template for Noise Extensions

First Author (first@email) Second Author (second@email)

Revision 1, 2017-11-12, unofficial/unstable

Contents

1. Introduction **1**

2. Overview **1**

3. More sections **2**
3.1. Subsections 3

4. Even more sections **3**

5. Security considerations **3**

6. Rationales **4**

7. IPR **4**

8. Acknowledgements **4**

9. References **4**

1. Introduction

This is a template document for writing Noise extension specifications.

This section should contain a few sentences describing the purpose of this extension.

2. Overview

This section should give a brief overview of how your extension works.

Introduce new terms in **bold**. Use internal references such as Section 1. Use bibliographic references such as [1], [2], [3] that refer to bibtex entries in either the `spectools/*.bib` files or the local `my.bib` file.

3. More sections

Some guidelines:

0. Use bullets, `inline code` for `variable names` and similar, and pre-formatted text blocks when needed.
1. Follow the same style as the Noise Specification.
2. To insert pagebreaks in the PDF document, use the LaTeX `\newpage` command like so:

3. Use Pandoc-specific features sparingly, but Pandoc has a few nice features:
    - Subscripts$_1$ and superscripts^2
    - Tables (see later)
    - Ability to control numbering of lists (e.g. this list starts at 0).

3.1. Subsections

Add as needed.

4. Even more sections

Pandoc tables are helpful for displaying patterns:

```
NN():                    KN(s):
  -> e                     -> s
  <- e, ee                 ...
                           -> e
                           <- e, ee, se

NK(rs):                  KK(s, rs):
  <- s                     -> s
  ...                      <- s
  -> e, es                 ...
  <- e, ee                 -> e, es, ss
                           <- e, ee, se
```

5. Security considerations

You must list security considerations for using your extension, for example a bulleted list like so:

- **Confidentiality**: Some stuff.
- **Integrity**: Other stuff.

6. Rationales

Not required, but might be a good idea to explain nonobvious design decisions.

7. IPR

8. Acknowledgements

Make sure to acknowledge prior and related work, and others who contributed.

9. References

[1] H. Krawczyk, "'Cryptographic extraction and key derivation: The hkdf scheme'." Cryptology ePrint Archive, Report 2010/264, 2010. http://eprint.iacr.org/2010/264

[2] C. Kudla and K. G. Paterson, "Modular Security Proofs for Key Agreement Protocols," in Advances in Cryptology - ASIACRYPT 2005: 11th International Conference on the Theory and Application of Cryptology and Information Security, 2005. http://www.isg.rhul.ac.uk/~kp/ModularProofs.pdf

[3] H. Krawczyk and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)." Internet Engineering Task Force; RFC 5869 (Informational); IETF, May-2010. http://www.ietf.org/rfc/rfc5869.txt