

# ISO/IEC 29192-3:2012-10 (E)

## Information technology - Security techniques - Lightweight cryptography - Part 3: Stream ciphers

---

| <b>Contents</b>  |   | <b>Page</b> |
|--|---|-------------|
| Foreword .....   |   | iv          |
| Introduction .....   |   | v           |
| 1  | Scope .....                             | 1           |
| 2  | Normative reference .....               | 1           |
| 3  | Terms and definitions .....             | 1           |
| 4  | Symbols and operational terms .....     | 3           |
| 5  | General models for stream ciphers ..... | 4           |
| 5.1  | General .....                           | 4           |
| 5.2  | Synchronous Keystream generators .....  | 4           |
| 5.3  | Output functions .....                  | 4           |
| 6  | Dedicated keystream generators .....    | 5           |
| 6.1  | Enocoro-128v2 keystream generator ..... | 5           |
| 6.2  | Enocoro-80 keystream generator .....    | 10          |
| 6.3  | Trivium keystream generator .....       | 13          |
| Annex A (normative) Object Identifiers .....                   |   | 16          |
| Annex B (informative) Test vectors .....                       |   | 17          |
| Annex C (informative) Guidance on implementation and use ..... |   | 24          |
| Annex D (informative) Feature Table .....                      |   | 26          |
| Annex E (informative) Computation over a finite field .....    |   | 27          |
| Bibliography .....   |   | 28          |