

# ISO/IEC 29192-4:2013-06 (E)

## Information technology - Security techniques - Lightweight cryptography - Part 4: Mechanisms using asymmetric techniques

---

Contents	Page
<b>Foreword .....</b>	<b>iv</b>
<b>Introduction .....</b>	<b>v</b>
<b>1 Scope .....</b>	<b>1</b>
<b>2 Normative references .....</b>	<b>1</b>
<b>3 Terms and definitions .....</b>	<b>1</b>
<b>4 Symbols and abbreviated terms .....</b>	<b>4</b>
<b>5 Unilateral authentication mechanism based on discrete logarithms on elliptic curves .....</b>	<b>6</b>
<b>5.1 General .....</b>	<b>6</b>
<b>5.2 Security requirements for the environment .....</b>	<b>6</b>
<b>5.3 Key production .....</b>	<b>7</b>
<b>5.4 Unilateral authentication mechanism .....</b>	<b>8</b>
<b>6 Unilateral authenticated key exchange mechanism based on encryption .....</b>	<b>9</b>
<b>6.1 General .....</b>	<b>9</b>
<b>6.2 Security requirements for the environment .....</b>	<b>10</b>
<b>6.3 Key production .....</b>	<b>10</b>
<b>6.4 Unilateral authentication exchange .....</b>	<b>11</b>
<b>6.5 Session-key derivation .....</b>	<b>12</b>
<b>7 Identity-based signature mechanism .....</b>	<b>12</b>
<b>7.1 General .....</b>	<b>12</b>
<b>7.2 Security requirements for the environment .....</b>	<b>12</b>
<b>7.3 Key production .....</b>	<b>13</b>
<b>7.4 Sign .....</b>	<b>13</b>
<b>7.5 Verify .....</b>	<b>13</b>
<b>Annex A (normative) Object identifiers .....</b>	<b>14</b>
<b>Annex B (normative) Memory-Computation Trade-Off Technique .....</b>	<b>15</b>
<b>Annex C (informative) Numerical examples .....</b>	<b>16</b>
<b>C.1 cryptoGPS mechanism .....</b>	<b>16</b>
<b>C.1.1 Key production .....</b>	<b>16</b>
<b>C.1.2 Authentication exchange .....</b>	<b>16</b>
<b>C.2 ALIKE mechanism .....</b>	<b>18</b>
<b>C.2.1 Key production .....</b>	<b>18</b>
<b>C.2.2 Authentication exchange .....</b>	<b>18</b>
<b>C.2.3 Session-key derivation .....</b>	<b>19</b>
<b>C.3 Identity-based signature mechanism .....</b>	<b>19</b>
<b>C.3.1 Key production .....</b>	<b>19</b>
<b>C.3.2 Sign .....</b>	<b>20</b>
<b>C.3.3 Verify .....</b>	<b>21</b>
<b>Annex D (informative) Features .....</b>	<b>22</b>
<b>Bibliography .....</b>	<b>25</b>