ACRONYMS

AES    Advanced Encryption Standard
ANSI   American National Standards Institute
ASIC   Application-Specific Integrated Circuit
BEA    Binary Extended Algorithm
DES    Data Encryption Standard
DH     Diffie-Hellman
DHP    Diffie-Hellman Problem
DL     Discrete Logarithm
DLP    Discrete Logarithm Problem
DPA    Differential Power Analysis
DSA    Digital Signature Algorithm
DSS    Digital Signature Standard
ECC    Elliptic Curve Cryptography
ECDDHP Elliptic Curve Decision Diffie-Hellman Problem
ECDH   Elliptic Curve Diffie-Hellman
ECDHP  Elliptic Curve Diffie-Hellman Problem
ECDLP  Elliptic Curve Discrete Logarithm Problem
ECDSA  Elliptic Curve Digital Signature Algorithm
ECIES  Elliptic Curve Integrated Encryption Scheme
EC-KCDSA Elliptic Curve Korean Certificate-based Digital Signature Algorithm
ECMQV  Elliptic Curve Menezes-Qu-Vanstone
EEA    Extended Euclidean Algorithm
FIPS   Federal Information Processing Standards
FPGA   Field-Programmable Gate Array
GCD    Greatest Common Divisor
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GHS</td>
<td>Gaudry-Hess-Smart</td>
</tr>
<tr>
<td>HCDLP</td>
<td>Hyperelliptic Curve Discrete Logarithm Problem</td>
</tr>
</tbody>
</table>