SCIS 2022 2022 Symposium on Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 — 21, 2022
The Institute of Electronics, Information and Communication Engineers

上質の電子署名アルゴリズム
Premium Digital Signature Algorithm

安田　英幸 *
Hideyuki YASUDA

キーワード　公開鍵暗号、電子署名 、
DSA、ECDSA、PDSA、ECPDSA、cryptography、digital signatures、public key cryptography、離散対数問題、 怪人暗号、怪人署名、 Phantom Crypt、 Phantom Signature

あらまし

筆者は、１７年前にDSA等からアイデアを得て不定方程式による暗号を研究し、実現しました。令和３年９月以降の、この暗号の研究過程において、存在を消す性質を持つ項を発見し、この性質を指して、怪人項と名付けました。そして、怪人項に由来させて、この暗号を怪人暗号と名付けました。

時は遡り令和３年３月、怪人暗号は電子署名も実現出来るという一念から、怪人暗号の公開鍵による電子署名方法を研究しました。

そして、本研究の核心部分においてDSAに助けを求めた上で達成した電子署名方法は、DSAよりも優れています。

なぜなら、DSAの検証鍵を使用してDHM-key exchangeを使用しても、任意の情報を暗号化して送信出来ません。しかし、本研究の成果である電子署名方法では、検証鍵は怪人暗号の公開鍵と同一であり、検証鍵が暗号化機能を実現しているからです。

この優れている事実を形容する日本語として、「上質の」を選びました。そして、訳語として「premium」を当てました。

そして、本研究の成果を「PDSA」と名付けました。

筆者としては、「青は藍より出て藍より青し。」を体現出来たこと、感無量です。

以上

* 個人、住所は不詳、umedoblock@gmail.com