『新版暗号技術入門』正誤表

結城浩

http://www.hyuki.com/cr/

2014 年 7 月 1 日更新

目次

1 2014-07-01: 第 9 刷：p.80, p.386：綴りの誤り

誤: Electric（エレクトリック）
正: Electronic（エレクトロニック）

2 2013-09-11: 第 8 刷: p.71, p.72：図の誤り

「Fig3-11 Rijndael 暗号化の 1 ラウンドの ShiftRows」と「Fig3-12 Rijndael 復号化の 1 ラウンドの InvShiftRows の矢印部分」が逆転している。

誤

Fig.3-11 ● Rijndael 暗号化の 1 ラウンド

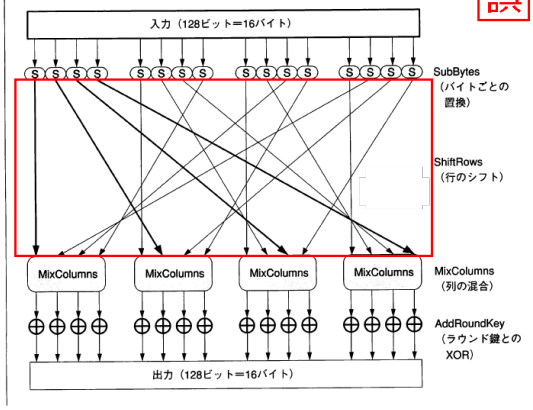
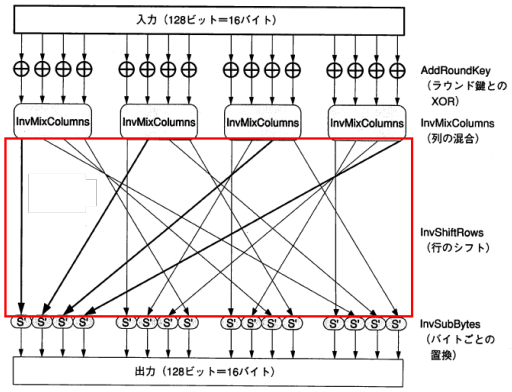


Fig.3-12 ● Rijndael 復号化の 1 ラウンド



正

Fig.3-11 ● Rijndael 暗号化の 1 ラウンド

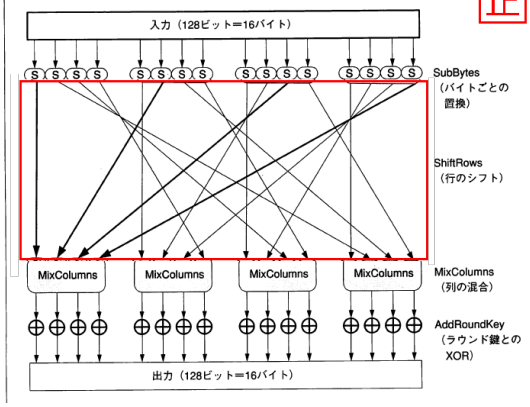
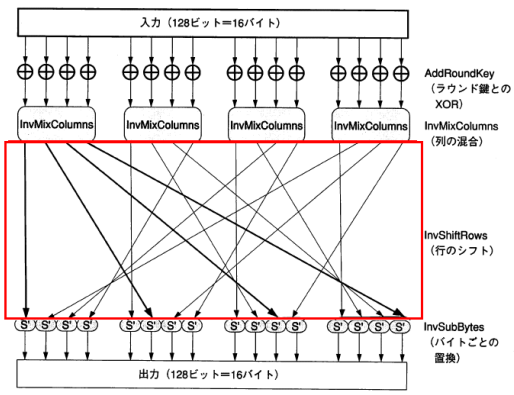


Fig.3-12 ● Rijndael 復号化の 1 ラウンド



3　2008-12-27: 第 1 刷： p.230： ElGamal 方式について

誤:　ElGamal 方式は、公開鍵暗号とデジタル署名に用いることができ、暗号ソフトウェア GnuPG でもアルゴリズムの 1 つとして使われています。

正:　ElGamal 方式は、公開鍵暗号とデジタル署名に用いることができます。暗号ソフトウェア GnuPG でも使われていましたが、バージョン 1.0.2 のデジタル署名の実装に脆弱性があったため、現在の GnuPG では公開鍵暗号のみに使われています。http://lists.gnupg.org/pipermail/gnupg-users/2003-November/020783.html

（荒川靖弘さん、ご指摘感謝）