『暗号技術入門 第3版 秘密の国のアリス』正誤表

結城浩

https://www.hyuki.com/cr/pdf/errata_cr3.pdf

2023年10月21日更新

目次

1　第 1 刷

1.1　2015-08-29: 第 1 刷: p.v: 下から 11 行目: 不要な句点

誤:　注目されている認証付き暗号も紹介します。。
正:　注目されている認証付き暗号も紹介します。

1.2　2015-09-03: 第 1 刷: p.83: 9–10 行目

誤:　AES のブロック長は 128 ビット、192 ビット、256 ビットのいずれかから選べます。128 ビットのブロック長を選んだ場合、AES は 128 ビットの平文をまとめて暗号化して、128 ビットの暗号文を作ります。
正:　AES のブロック長は 128 ビットです。したがって、AES は 128 ビットの平文をまとめて暗号化して、128 ビットの暗号文を作ります。

1.3　2015-09-03: 第 1 刷: p.391: 12–13 行目

誤:　デジタル署名のアルゴリズムとして、鍵や初期化ベクトルやノンスなどを作るために用いられています。
正:　デジタル署名のアルゴリズムとして、RSA や ElGamal, DSA, 楕円曲線 DSA（ECDSA）, エドワーズ曲線 DSA（EDDSA）などが用いられています。

1.4　2015-09-06: 第 1 刷: p.202: 4 行目: 文字のヨゴレ

誤:　ハッシュ値を
正:　ハッシュ値を

2　第 2 刷

2.1　2015-10-14: 第 2 刷: p.445: 索引項目の漏れ

誤:　（なし）
正:　復号オラクル　……　145

2.2　2015-10-14: 第 2 刷: p.198: 19 行目: 不正確な記述

誤:　SHA3-512 の場合、ハッシュ値は 512 ビットですから、2^{512} 回の試行回数を行えば目的のメッセージが確実に見つかります。これは現実的には不可能な回数です。
正:　SHA3-512 の場合、ハッシュ値は 512 ビットです。n 個のメッセージを用意すれば、目的のハッシュ値を持つメッセージは平均して $\frac{n}{2^{512}}$ 個含まれています（期待値）。期待値を 1 にするためには 2^{512} 個のメッセージが必要になりますが、これは現実的には不可能な個数です。

3　第 3 刷

3.1　2015-11-24: 第 3 刷: p.95: 下から 11 行目: 誤植

誤:　暗号化ブロックをパディングの代わりに利用
正:　暗号文ブロックをパディングの代わりに利用

3.2　2015-11-24: 第 3 刷: p.106: 下から 3 行目: 参考文献の参照漏れ

誤:　*Practical Cryptography* では
正:　*Practical Cryptography*[Schneier, 2003] では

3.3　2015-11-24: 第 3 刷: p.259: Table 10-1 の 7 行目: 補足

誤:　有効期限
正:　有効期限（開始日時）

3.4　2015-11-24: 第 3 刷: p.259: Table 10-1 の 8 行目: 補足

誤:　有効期限
正:　有効期限（終了日時）

3.5　2015-11-24: 第 3 刷: p.397: 18 行目: 誤植

誤:　2 つを通してハッシュ値を
正:　2 つに通してハッシュ値を

3.6　2015-11-24: 第 3 刷: p.397: 20 行目: 誤植

誤:　Base56Check 符号化
正:　Base58Check 符号化

3.7　2015-12-09: 第 3 刷: p.402: 3 行目: 誤解を招く表現

誤:　分岐が発生した場合、P2P ネットワークの各ノードは計算がたいへんなほうを選択し、ブロックチェーンの分岐を抑止するのです。

正:　ノードは、最初に受信したブロックをブロックチェーンに暫定的に追加しますが、同時に受信した他のブロックも念のために保存します。そして、これ以降のブロック受信によって、どちらか長く伸びた方を「正しい」と判断するのです。

3.8　2015-12-09: 第 3 刷: p.7: 下から 2 行目: スペルミス

誤:　cryptgraphy

正:　cryptography

3.9　2016-02-23: 第 3 刷: p.142: 11 行目以降: RSA と素因数分解の等価性

誤:　N を素因数分解して p と q を求めることができれば、D を求めることができます。

しかし「D を求めること」が「N を素因数分解すること」と等価であるかどうかは、数学的に証明されているわけではありません。もしかしたら、N を素因数分解せずとも（p と q を知らなくても）、E と N から D を求める方法が発見されるかもしれません。

このような方法はまだ見つけられていませんし、そもそも存在するのかどうかもわかっていません。

正:　N を素因数分解して p と q を求めることができれば、D を求めることができます。

しかし「D を求めること」と「N を素因数分解すること」とが等価であるかどうかは、数学的に証明しなければならないことです。「D を求めること」と「N を素因数分解すること」が決定的多項式時間で等価であることは、2004 年に Alexander May が証明しています。

（脚注追加）

Alexander May, Computing the RSA Secret Key is Deterministic Polynomial Time Equivalent to Factoring, *Advances in Cryptography, CRYPTO '04*, Springer-Verlag, 2004.

`https://www.iacr.org/archive/crypto2004/31520213/det.pdf`

3.10　2016-02-23: 第 3 刷: p.149: 15 行目以降: RSA と素因数分解の等価性

誤:

等価かどうか、まだわかっていません。

確かに、素因数分解が高速にできれば、RSA は解読されます。しかし、RSA を解読するのに素因数分解を行わなければならない、ということが証明されているわけではありません。もしかしたら、素因数分解を行わなくても解読できる方法が見つかるかもしれません。

正:

RSA のプライベート鍵を求めることが N の素因数分解と等価であることは、2004 年に Alexander May が証明しました。

3.11　2016-02-23: 第 3 刷: p.153: 下から 3 行目以降: RSA と素因数分解の等価性

誤:

ただし、素因数分解を解くことと、RSA 暗号を解くことが等価であることは証明されていません。すなわち、素因数分解ができなくても、RSA 暗号を高速に解くアルゴリズムが発見される可能性はゼロではありません。

正:

その通りです。

4　第 4 刷

4.1　2016-04-20: 第 4 刷: p.71: 7〜9 行目: Rijndael のブロック長

誤:　Rijndael のブロック長は 128 ビットで、鍵のビット長は 128 ビットから 256 ビットまで 32 ビット単位で選択することができます（ただし、AES の規格上では、鍵長は 128, 192, 256 ビットの 3 種類だけです）。

正:　Rijndael のブロック長と鍵のビット長はそれぞれ独立に、128 ビットから 256 ビットまでの 32 ビット単位で選択することができます。ただし、AES の規格では、ブロック長は 128 ビット固定で、鍵のビット長は 128, 192, 256 ビットの 3 種類だけです。

4.2　2016-04-20: 第 4 刷: p.187: 1 行目: 誤植

誤:　Keccak では、

正:　Keccak では、

5　第 5 刷

6　第 6 刷

7　第 7 刷

8　第 8 刷

8.1　2019-05-29: 第 8 刷: p.337: 12 行目: 誤植

誤:　OSCP

正:　OCSP

8.2　2019-05-29: 第 8 刷: p.372: 下から 8 行目: マスターシークレットの扱い

誤:　CBC モードの初期化ベクトル（IV）は、マスターシークレット（p.380）から生成し、

正:　（削除）

8.3　2019-05-29: 第 8 刷: p.378: 9 行目: マスターシークレットの扱い

誤:　対称暗号の CBC モードで用いる初期化ベクトル（IV）

正:　GCM モードや CCM モードで用いる初期化ベクトル（IV）の一部

8.4　2019-05-29: 第 8 刷: p.381: 下から 2 行目: マスターシークレットの扱い

誤:

対称暗号の CBC モードで用いる初期化ベクトル（クライアント→サーバ）

対称暗号の CBC モードで用いる初期化ベクトル（クライアント←サーバ）

正:

GCM モードや CCM モードで用いる初期化ベクトル（IV）の一部（クライアント→サーバ）
GCM モードや CCM モードで用いる初期化ベクトル（IV）の一部（クライアント←サーバ）

8.5 2019-05-29: 第 8 刷: p.382: Fig.14-8: マスターシークレットの扱い

誤:

CBC モードの
初期化ベクトル

正:

GCM モードや CCM モードの
初期化ベクトルの一部

9 第 9 刷

10 第 10 刷

11 第 11 刷

11.1 2021-03-21: 第 11 刷: p.28: 下から 7 行目: 誤植

誤: 約 1000 兆倍
正: 約 100 兆倍

12 第 12 刷

13 第 13 刷

13.1 2022-12-16: 第 13 刷: p.391: 13 行目: 誤植

誤: EDDSA
正: EdDSA

14 第 14 刷

14.1 2023-10-21: 第 14 刷: p.34: 6 行目: エニグマ

誤: ドイツ語で「謎」を意味します。

正: 古代ギリシア語に由来する言葉で「謎」を意味します。

14.2 2023-10-21: 第 14 刷: p.107: CFB モードの欠点

誤: 1 ブロック全体と次のブロックの対応するビットがエラーになる
正: 1 ブロックの対応するビットと、次のブロック全体がエラーになる

14.3 2023-10-21: 第 14 刷: p.400: 下から 2 行目: ビットコインの方程式

誤: $x^2 = y^3 + 7$
正: $y^2 = x^3 + 7$