「ブロックチェーン技術概論 理論と実践」（第 1 刷）正誤表

最新情報は，サポートページ（https://github.com/blockchain-programming/book2021）をご覧ください．

2022 年 7 月 25 日時点

ページ	場所	誤	正
v.	一番下の行	（一番下の行に追加）	4.6 秘密計算……102
22	上から 1 行目	計算コストと考えます。	計算コスト [*6] と考えます。
31	上から 11–12 行目	メカニズム使用した	メカニズムを使用した
54	上から 11 行目	1996 年	1994 年
70	下から 2 行目	誤：https://cryptorating.eu/whitepapers/**イーサリアム**/**イーサリアム**_white_paper.pdf	
	（参考文献 [2]）	正：https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf	
75	上から 16, 19, 22 行目	生成限 g	生成元 g
93	上から 10 行目	公開鍵暗号と使って	公開鍵暗号を使って
99	上から 6–8 行目	誤：R については楕円曲線離散対数問題が困難であるという前提から rG の r を知ることは不可能とし，$s = (r + ed) \bmod n$ と $s = r$ が同じエントロピーをもつことを考えると検証者にはこの 2 つの確率変数はともに乱数と区別できません。したがってゼロ知識性 正：楕円曲線離散対数問題が困難であるという前提から，$R = rG$ から r を知ることや $eP = edG$ から ed を知ることは不可能です。$s = (r + ed) \bmod n$ と $s = r$ の s は確率変数として区別できないので ed はわかりません。したがって d に関するゼロ知識性	
100	下から 2 行目	誤：対偶をとれば「間違った命題は証明できない」ということになります。 正：対偶をとると「偽なる命題は証明によって否定される」ことになります。	
102	下から 9 行目	秘密計算	4.6 秘密計算
103	上から 9 行目	ブラックリーの (t, n) しきい値秘密分散法の例	ブラックリーの (t, n) しきい値秘密分散法の簡単な例
103	上から 10 行目	してみましょう。	してみましょう（図 4.14）。

ページ	場所	誤	正
103	下から 4 行目	誤：ブラークリーの (t, n) しきい値秘密分散法は，空間の次元を変えることで,	正：ブラークリーの (t, n) しきい値秘密分散法では，シェアを秘密情報の点 s とランダムな点 r を通る t 次元空間の中の $(t-1)$ 次元超平面とすることで,
121	上から 6 行目	ビットコインの	ビットコインを
130	上から 3 つ目のコード	誤：（実行結果が途中で切れています）	正：サポートページ（`https://github.com/blockchain-programming/book2021`）に完全版を掲載しています.
134	下から 3 行目	2140 年	2141 年ごろ
134	下から 2 行目	210000 btc	21000000 btc
134	下から 1 行目	$210000 = \sum_{i=0}^{\infty} 210000 \frac{50}{2^i}$	$21000000 = \sum_{i=0}^{\infty} 210000 \frac{50}{2^i}$
135	上から 11, 15 行目	係数	係数（のリトルエンディアン）
135	上から 16 行目	誤：0x 00000000 0004864c 00000000 00000000 00000000 00000000 00000000 00000000	
		正：0x 00000000 004c8604 00000000 00000000 00000000 00000000 00000000 00000000	
151	表 6.8 の説明	（行は前半 2 ビットで後半 3 ビット）	（行は前半 2 ビットで，列は後半 3 ビット）
151	上から 13 行目	ファーマット	フォーマット
167	上から 7 行目	ゲーム論	ゲーム理論
168	上から 7 行目	ゲーム論	ゲーム理論
221	下から 1 行目	ZK-Rolleup	ZK-Rollups
224	上から 20 行目	Locked	Lock
341	上から 4 行目	加法逆元演算 $-a$	加法逆元
347	下から 4 行目	$\theta^1 = 1$	$\theta^1 = \theta$
350	上から 9 行目	点を $R^{'}$	点 $R^{'}$
351	上から 6 行目	$\{(x, y) \mid x, y \in GF(p)\} \cup \{(\infty, \infty)\}$	$\{(x, y) \mid x, y \in GF(p)\} \cup \{(\infty, \infty)\}$. ここで (∞, ∞) は無限遠点 O.

ページ	場所	誤	正
352	上から 9 行目	$(x_3,\, y_3) = \big(\lambda^2 - x_1 - x_2,\, \lambda(x_3 - y_1) + y_1\big)$	$(x_3,\, y_3) = \big(\lambda^2 - x_1 - x_2,\, \lambda(x_3 - x_1) + y_1\big)$