正 誤 表

2014/03/27

このたびは森北出版発行の書籍をお買い求めいただき誠にありがとうございました．下記の書籍につきまして，誤りのある箇所がございましたので訂正させていただきます．

タイトル

情報セキュリティの理論と技術

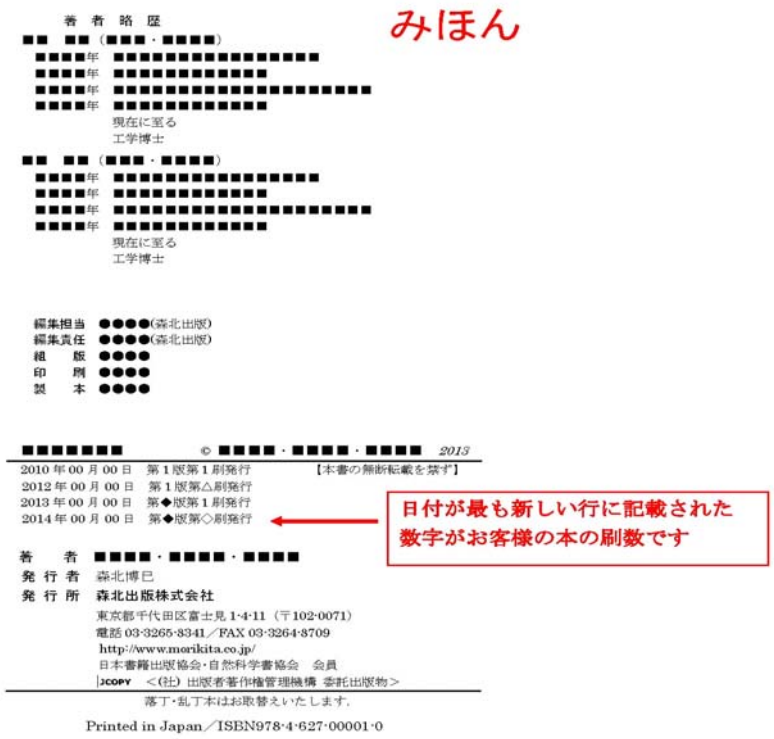
正誤対象

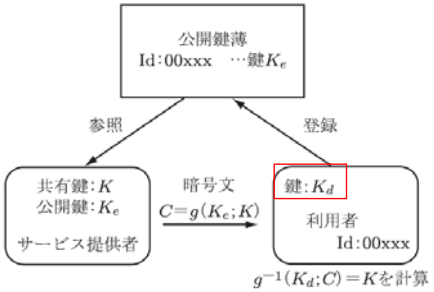
このページにある「刷数の調べ方」をご参照いただき，お持ちの本の刷数をお調べください．正誤表内に「対応刷数」という欄がございますので，該当する刷数の正誤情報をご確認ください．

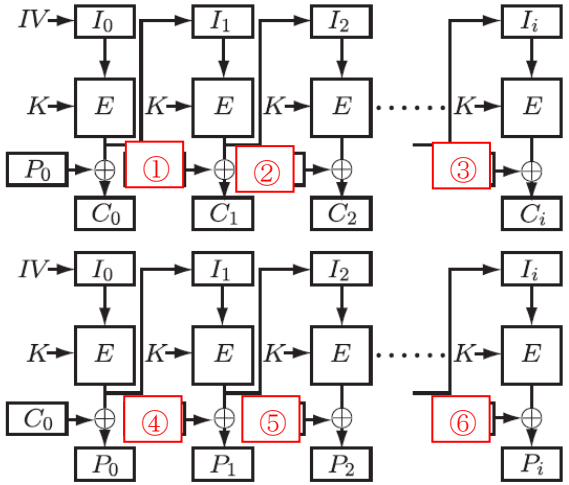
お持ちの本の刷数	
1　刷	対応刷数　1　をご参照ください．
それ以降	現在把握している訂正情報はございません．

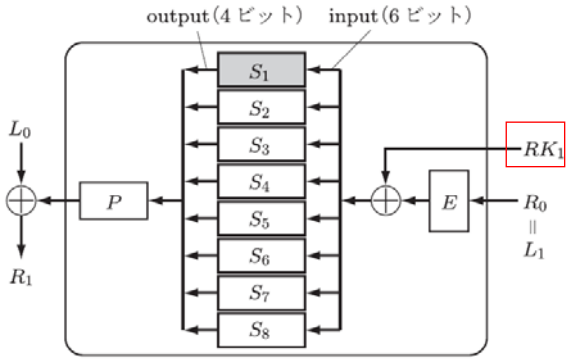
刷数の調べ方

広告や白ページを除く一番後ろに下図のようなページがございます．ご参照いただき，お客様の本の刷数をご確認ください．



対応刷数	頁	行数，図・表・式番号	誤	正
1	2	下から12行目	…公開鍵と暗号化鍵から…	…公開鍵である暗号化鍵から…
1	3	図 1.1		復号鍵: K_d
1	13	3行目	…条件に応じてデータの流れを変更する…	…条件に応じて命令の実行順序を変更する…
1	14	14行目	ADD R1 R2	ADD R1, R2
1	17	3行目	…最大公約数(greatest common divide)…	…最大公約数(greatest common divisor)…
1	20	下から11行目	ないときは STEP4 に進む．$a \le 0$ のとき，STEP4 に進む．	ないときは STEP4 に進む．
1	21	下から2行目	…すべての解は，m, n を任意の…	…すべての解は，n を任意の…
1	22	1行目	$\begin{cases} x = u + tm \\ y = v - sn \end{cases}$	$\begin{cases} x = u + tn \\ y = v - sn \end{cases}$
1	23	11行目	…もし，$q_{j+2} = 0$ となったら停止し，$r_{j+2}, x_{j+2}, y_{j+2}$ を出力し，…	…もし，$r_{j+2} = 0$ となったら停止し，$r_{j+1}(=d), x_{j+1}, y_{j+1}$ を出力し，…
1	27	下から2行目	…A から B への写像 f を考える．…	…A から B への単射を考える．…
1	29	13行目	における a の逆数という．	における a の逆数といい，$a^{-1} \pmod N$ のように表す．
1	45	下から4行目	$=(2+2)X^3+(1+1)X^2+(2+1)X+(1+1)$	削除

1	47	下から 4 行目	であり，余りは $2X$ であることがわかる．…	であり，余りは $-2X = X$ であることがわかる．…
1	47	図 3.10	X^2+X+1 $2X^2+2X+1 \overline{)\ 2X^4+X^3+2X^2+X+1}$ $-)\ 2X^4+2X^3+X^2$ $2X^3+X^2+X+1$ $-)\ 2X^3+2X^2+X$ $2X^2+1$ $-)\ 2X^2+2X+1$ $2X$	X
1	51	下から 10 行目	…もし，$q_{j+2}(X)=0$ となったら停止し，$r_{j+2}(X), f_{j+2}(X), g_{j+2}(X)$ を出力し，…	…もし，$r_{j+2}(X)=0$ となったら停止し，$r_{j+1}(X)(=d(X)), x_{j+1}(X), y_{j+1}(X)$ を出力し，…
1	71	下から 2 行目	…図 4.10 からすぐにわかるように，…	…すぐにわかるように，…
1	79	1 行目	…$\|p-1/2\|$ ができるだけ…	…$\lfloor p-1/2 \rfloor$ ができるだけ…
1	79	11 行目	…どのようにして $\|p-1/2\|$ が…	…どのようにして $\lfloor p-1/2 \rfloor$ が…
1	96	図 4.22 ｷｬﾌﾟｼｮﾝ	ShitRows()	ShiftRows()
1	96	下から 3 行目	…既約多項式 x^4+1 を法とする…	…既約多項式 $x^8+x^4+x^3+x+1$ を法とする…
1	97	3 行目	…は，$a(x)\cdot d(x)\equiv 1 (\mathrm{mod}\, x^4+1)$ となる…	…は，$a(x)\cdot d(x)\equiv 1 \ (\mathrm{mod}\, x^8+x^4+x^3+x+1)$ となる…
1	103	図 4.28		① $P_0 \rightarrow P_1$ ② $P_0 \rightarrow P_2$ ③ $P_0 \rightarrow P_i$ ④ $C_0 \rightarrow C_1$ ⑤ $C_0 \rightarrow C_2$ ⑥ $C_0 \rightarrow C_i$

1	146	式(5.26)	$D=-4a^3c+a^2b+19abc-4b^3-27c^2\neq 0$	$D=-4a^3c+a^2b+18abc-4b^3-27c^2\neq 0$
1	155	7 行目	入力 n , P , E , 出力 $Q=nP$	入力 n , P 出力 $Q=nP$
1	155	8 行目	$S=1$, $j=k-1$ とおく.	$Q=0$, $j=k-1$ とおく.
1	155	12 行目	… $d[\,j\,]=1$ であるとき，…	… $n[\,j\,]=1$ であるとき，…
1	189	図 6.8		RK_0
1	202	1 行目	次の行に右の文章を追加	ここで，$L_{16}[\,i\,]$などの$[\,i\,]$は，S_i ボックスへの入力に対応するビット群をあらわすことにする.
1	202	9 行目	となり，未知の R_{15} が消えた…	となり，未知の L_{15} が消えた…
1	202	下から 12 行目	. . . , 15)は，別々のレジスタに格納されるため， R_{15} の値だけを変化させることは非現実的ではない．しかし，わずか 32 ビットであるので，データ長が，1024 ビット以上にもなる RSA に対する DFA と比較すると難度は高い．…	. . . , 15)は，異なる時刻に処理されるため， R_{15} の値だけを変化させることは非現実的ではない．しかし，アタック対象のレジスタのサイズがわずか 32 ビットであるので，データ長が，1024 ビット以上にもなる RSA に対する DFA と比較すると難度は高い．…

2014.3 作成