耐量子計算機暗号　正誤表

本書の内容に以下の誤りがございました。お詫びして訂正いたします。

お手持ちの本の「刷数」とこの表の「該当刷数」が一致する箇所をご参照ください。お手持ちの本の「刷数」の調べ方はこちら

（2023 年 12 月 28 日更新）

該当刷数	頁	行数など	誤	正
1	32	脚注 2	…（p，g は奇数でなければならない）	…（p，q は奇数でなければならない）
1	61	式（2.2）	$\cdots+\sum_{1\le j\le o+v}\beta^{\langle i\rangle}x_j+\gamma^{\langle i\rangle}$	$\cdots+\sum_{1\le j\le o+v}\beta_j^{\langle i\rangle}x_j+\gamma^{\langle i\rangle}$
1	67	10 行目	$\sigma\leftarrow S^{-1}\cdot{}^t\left(x_1,\ldots,x_o,a_{o+1},\ldots,a_{o+v}\right)\in K^{o+v}$	$\sigma\leftarrow S^{-1}\left({}^t\left(x_1,\ldots,x_o,a_{o+1},\ldots,a_{o+v}\right)\right)\in K^{o+v}$
1	89	10 行目	…の幅が ρ/n^2 未満であれば…	…の幅が ρ/n^2 未満（$\mathbf{w}_1,\ldots,\mathbf{w}_n$ が一次独立でない場合を含む）であれば…
1	106	下から 11 行目	…，したがって $\left\vert B_{k'}\right\vert$ …	…，したがって $B_{k'}$ …
1	108	下から 2 行目	テップ 4（a）で k の値が…	テップ 4（b）で k の値が…
1	120	下から 3 行目	…ノルムの最小値を B で表す.	…ノルムの 2 乗の最小値を B で表す.
1	136	15 行目	$\left(\partial_Y E\right)(P)=-2\beta-a_1C'Z-a_3=0$	$\left(\partial_Y E\right)(P)=-2\beta-a_1C'-a_3=0$