

正誤表

| 報告書等 | 項目等 | 頁 | 改訂内容 |
|------------------------------------|------------------|-----|--|
| CRYPTREC Report 2002 (平成 15 年 3 月) | 「2.4.2.2 攻撃法」節の表 | 102 | (誤) $c \approx 1.4$ (正) $c = (32/9)^{1/3}$ |