「暗号と情報セキュリティ（リスク工学シリーズ8）」 正誤表

頁	行	誤	正
10	下から9	$a = 0$ のときは	$a \equiv 0 \bmod p$ のときは
10	下から8	$a \neq 0$ のとき	$a \not\equiv 0 \bmod p$ のとき
26	本文下から2	$y^x \equiv g^{xr} \bmod p$ を	$y^r \equiv g^{xr} \bmod p$ を
26	本文下から1	$y^x \bmod p$ を	$y^r \bmod p$ を
30	12	$Enc_R(M)$ を	$E_R(M)$ を
54	下から2	non-negligibile関数	negligible関数
72	本文下から5	$\langle P(x, g, p, q),$	$\langle P(s, g, p, q),$
73	7	$\langle P(x, g, p, q),$	$\langle P(s, g, p, q),$
73	10	$\langle P(x, g, p, q),$	$\langle P(s, g, p, q),$

①

最新の正誤表がコロナ社ホームページにある場合がございます。
下記URLにアクセスして[キーワード検索]に書名を入力して下さい。
http://www.coronasha.co.jp