【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第２区分
【発行日】平成18年11月24日(2006.11.24)

【公表番号】特表2002-528771(P2002-528771A)
【公表日】平成14年9月3日(2002.9.3)
【出願番号】特願2000-578723(P2000-578723)
【国際特許分類】
Ｇ０９Ｃ　1/00　(2006.01)
【ＦＩ】
Ｇ０９Ｃ　1/00　６２０Ｚ

【手続補正書】
【提出日】平成18年10月2日(2006.10.2)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
体上に定義された楕円曲線上の点Ｐの倍数ｋを算出する方法であって、
ａ）ナンバーｋをビット列k_iからなる二進ベクトルとして表し；
ｂ）点P_1およびP_2の順序対を形成し、点P_1およびP_2は最大でＰだけ異なり；そして、
ｃ）上記ビット列k_iの各々を順次選択し、上記ビット列k_iのそれぞれに対して；
ｉ）k_iが０のとき、一番目の点P_1を二倍算して点P_1'を得、これにより一番目のパワーシグニチャーを生じさせ；そして続けて、P_1およびP_2を加算して点P_2'を得、これにより２番目のパワーシグニチャーを生じさせ、点P_1'、P_2'の新しいセットを算出し；
あるいは、
ｉｉ）k_iが１のとき、二番目の点P_2を二倍算して点P_2'を得、これにより一番目のパワーシグニチャーを生じさせ；そして続けて、点P_1およびP_2を加算して点P_1'を得、これにより２番目のパワーシグニチャーを生じさせ、点P_1'、P_2'の新しいセットを算出するステップを含み、
それによって、上記二倍算あるいは加算が、常に上記ビット列k_iの各々に対して同じ順序で実行され、これにより、一貫したパワーシグニチャー波形を生成し、本方法におけるタイミングアタックを極小化する方法。
【請求項２】
上記体が、F_{2^m}上で定義されている請求項１に記載の方法。
【請求項３】
上記体が、F_p上で定義されている請求項１に記載の方法。