(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112769552 B
(45)授权公告日 2022.08.23

(21)申请号 202011609314.3

(22)申请日 2020.12.30

(65)同一申请的已公布的文献号
申请公布号 CN 112769552 A

(43)申请公布日 2021.05.07

(73)专利权人 北京宏思电子技术有限责任公司
地址 100085 北京市海淀区学清路9号汇智大厦B座15层1505

(72)发明人 王亚伟 司明 王磊 雷艳

(51)Int.Cl.
H04L 9/08(2006.01)
G06F 9/30(2006.01)

(56)对比文件
CN 111106936 A,2020.05.05
CN 107896142 A,2018.04.10
CN 111490871 A,2020.08.04
US 2008285743 A1,2008.11.20
郝中源.基于FPGA的双线性对密码算法并行架构设计.《南开大学学报(自然科学版)》.2018,第51卷(第3期),全文.
Yihong Long et al..Collaborative Generations of SM9 Private Key and Digital Signature using Homomorphic Encryption.《2020 5th International Conference on Computer and Communication Systems(ICCCS)》.2020,全文.

审查员 潘小丹

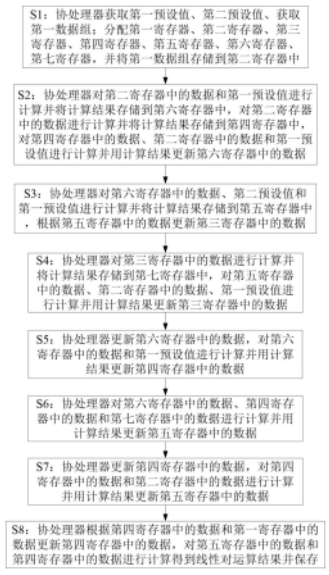
权利要求书6页 说明书16页 附图4页

(54)发明名称

一种在嵌入式系统中加快线性对运算的实现方法及装置

(57)摘要

本发明公开一种在嵌入式系统中加快线性对运算的实现方法及装置,涉及信息安全领域。该方法包括:协处理器获取第一预设值、第二预设值、获取第一数据组;将第一数据组存储到第二寄存器中;对第一预设值、第二预设值、第一寄存器中的数据、第二寄存器中的数据、第三寄存器中的数据、第四寄存器中的数据、第五寄存器中的数据、第六寄存器中的数据、第七寄存器中的数据进行计算得到线性对运算结果并保存。本发明技术方案应用于解密、签名等过程,通过对线性对运算进行拆分,大大减少了运算时间,进一步地提高使用本发明技术方案的各种安全应用的效率。



CN 112769552 B

1.一种在嵌入式系统中加快线性对运算的实现方法,其特征在于,包括:

步骤S1:协处理器获取第一预设值、第二预设值、获取第一数据组;分配第一寄存器、第二寄存器、第三寄存器、第四寄存器、第五寄存器、第六寄存器、第七寄存器,并将所述第一数据组存储到所述第二寄存器中;所述第一数据组为12维数据;

步骤S2:所述协处理器对所述第二寄存器中的数据和所述第一预设值进行计算并将计算结果存储到所述第六寄存器中,对所述第二寄存器中的数据进行计算并将计算结果存储到第四寄存器中,对所述第四寄存器中的数据、所述第二寄存器中的数据和所述第一预设值进行计算并用计算结果更新所述第六寄存器中的数据;

步骤S3:所述协处理器对所述第六寄存器中的数据、所述第二预设值和所述第一预设值进行计算并将计算结果存储到第五寄存器中,根据所述第五寄存器中的数据更新所述第三寄存器中的数据;

步骤S4:所述协处理器对所述第三寄存器中的数据进行计算并将计算结果存储到所述第七寄存器中,对所述第五寄存器中的数据、所述第二寄存器中的数据、所述第一预设值进行计算并用计算结果更新所述第三寄存器中的数据;

步骤S5:所述协处理器更新所述第六寄存器中的数据,对所述第四寄存器中的数据和所述第一预设值进行计算并用计算结果更新所述第四寄存器中的数据;

步骤S6:所述协处理器对所述第六寄存器中的数据、所述第四寄存器中的数据和所述第七寄存器中的数据进行计算并用计算结果更新所述第五寄存器中的数据;

步骤S7:所述协处理器更新所述第四寄存器中的数据,对所述第四寄存器中的数据和第二寄存器中的数据进行计算并用计算结果更新所述第五寄存器中的数据;

步骤S8:所述协处理器根据所述第四寄存器中的数据和所述第一寄存器中的数据更新所述第四寄存器中的数据,对所述第五寄存器中的数据和所述第四寄存器中的数据进行计算得到线性对运算结果并保存。

2.如权利要求1所述的方法,其特征在于,所述步骤S2包括:

步骤S2-1:所述协处理器用所述第一预设值作为底数进行6次幂运算得到第一中间值,将所述第二寄存器中的数据作为底数、所述第一中间值作为指数进行幂运算并将运算结果存储到所述第六寄存器中;对所述第二寄存器中的数据进行逆元计算并将计算结果存储到所述第四寄存器中;

步骤S2-2:所述协处理器对所述第六寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新第六寄存器中的数据;

步骤S2-3:所述协处理器用所述第一预设值作为底数进行2次幂运算得到第二中间值,用所述第六寄存器中的数据作为底数、所述第二中间值作为指数进行幂运算并用运算结果更新所述第四寄存器中的数据;

步骤S2-4:所述协处理器对所述第六寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新所述第二寄存器中的数据;

步骤S2-5:所述协处理器用所述第二寄存器中的数据作为底数、所述第二预设值作为指数进行幂运算并用运算结果更新所述第四寄存器中的数据;

步骤S2-6:所述协处理器用所述第四寄存器中的数据作为底数、所述第二预设值作为指数进行幂运算并用运算结果更新所述第六寄存器中的数据。

3.如权利要求2所述的方法,其特征在于,所述步骤S3包括:

步骤S3-1:所述协处理器用所述第六寄存器中的数据作为底数、所述第二预设值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据;

步骤S3-2:所述协处理器用所述第三寄存器中的数据作为底数、所述第一预设值作为指数进行幂运算并用运算结果更新所述第五寄存器中的数据;

步骤S3-3:所述协处理器对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第三寄存器中的数据。

4.如权利要求3所述的方法,其特征在于,所述步骤S4包括:

步骤S4-1:所述协处理器对所述第三寄存器中的数据进行逆元计算并用计算结果更新所述第七寄存器中的数据;

步骤S4-2:所述协处理器用所述第二寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据;

步骤S4-3:所述协处理器用所述第一预设值作为底数进行2次幂运算得到第三中间值,用所述第二寄存器中的数据作为底数、所述第三中间值作为指数进行幂运算并用运算结果更新所述第五寄存器中的数据;

步骤S4-4:所述协处理器对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第三寄存器中的数据;

步骤S4-5:所述协处理器用所述第一预设值作为底数进行3次幂运算得到第四中间值,用所述第二寄存器中的数据作为底数、所述第四中间值作为指数进行幂运算并用运算结果更新所述第五寄存器中的数据;

步骤S4-6:所述协处理器对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并将运算结果存储到所述第一寄存器中;

步骤S4-7:所述协处理器用所述第六寄存器中的数据作为底数、所述第一预设值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据;

步骤S4-8:所述协处理器对所述第四寄存器中的数据与所述第三寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据;

步骤S4-9:所述协处理器对所述第五寄存器中的数据进行逆元计算并用计算结果更新所述第五寄存器中的数据;

步骤S4-10:所述协处理器用所述第一预设值作为底数进行2次幂运算得到第五中间值,用所述第六寄存器中的数据作为底数、所述第五中间值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据。

5.如权利要求4所述的方法,其特征在于,所述步骤S5包括:

步骤S5-1:所述协处理器对所述第六寄存器中的数据进行逆元计算并用计算结果更新所述第六寄存器中的数据;

步骤S5-2:所述协处理器用所述第四寄存器中的数据作为底数、所述第一预设值作为指数进行幂运算并用运算结果更新所述第四寄存器中的数据;

步骤S5-3:所述协处理器对所述第四寄存器中的数据进行逆元计算并用计算结果更新所述第四寄存器中的数据。

6.如权利要求5所述的方法,其特征在于,所述步骤S6包括:

步骤S6-1:所述协处理器对所述第二寄存器中的数据进行逆元计算并用计算结果更新所述第二寄存器中的数据;

步骤S6-2:所述协处理器对所述第六寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据;

步骤S6-3:所述协处理器对所述第六寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据;

步骤S6-4:所述协处理器对所述第七寄存器中的数据与所述第七寄存器中的数据进行12次域乘法运算并用运算结果更新所述第七寄存器中的数据;

步骤S6-5:所述协处理器对所述第七寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据;

步骤S6-6:所述协处理器对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据;

步骤S6-7:所述协处理器对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据;

步骤S6-8:所述协处理器对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据。

7.如权利要求6所述的方法,其特征在于,所述步骤S7包括:

步骤S7-1:所述协处理器对所述第四寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据;

步骤S7-2:所述协处理器对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据;

步骤S7-3:所述协处理器对所述第四寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据;

步骤S7-4:所述协处理器对所述第四寄存器中的数据与所述第二寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据。

8.如权利要求7所述的方法,其特征在于,所述步骤S8包括:

步骤S8-1:所述协处理器对所述第四寄存器中的数据与所述第一寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据;

步骤S8-2:所述协处理器对所述第五寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据;

步骤S8-3:所述协处理器对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第二寄存器中的数据,将所述第二寄存器中的数据作为线性对运算结果进行保存。

9.一种在嵌入式系统中加快线性对运算的实现装置,其特征在于,所述装置设置在协处理器中,所述装置包括:

获取分配存储模块,用于获取第一预设值、第二预设值、获取第一数据组;分配第一寄存器、第二寄存器、第三寄存器、第四寄存器、第五寄存器、第六寄存器、第七寄存器,并将所述第一数据组存储到所述第二寄存器中;所述第一数据组为12维数据;

计算存储更新模块,用于对所述第二寄存器中的数据和所述第一预设值进行计算并将

计算结果存储到所述第六寄存器中，对所述第二寄存器中的数据进行计算并将计算结果存储到第四寄存器中，对所述第四寄存器中的数据、所述第二寄存器中的数据和所述第一预设值进行计算并用计算结果更新所述第六寄存器中的数据；

第一计算更新模块，用于对所述第六寄存器中的数据、所述第二预设值和所述第一预设值进行计算并将计算结果存储到第五寄存器中，根据所述第五寄存器中的数据更新所述第三寄存器中的数据；

第二计算更新模块，用于对所述第三寄存器中的数据进行计算并将计算结果存储到所述第七寄存器中，对所述第五寄存器中的数据、所述第二寄存器中的数据、所述第一预设值进行计算并用计算结果更新所述第三寄存器中的数据；

第三计算更新模块，用于更新所述第六寄存器中的数据，对所述第四寄存器中的数据和所述第一预设值进行计算并用计算结果更新所述第四寄存器中的数据；

第四计算更新模块，用于对所述第六寄存器中的数据、所述第四寄存器中的数据和所述第七寄存器中的数据进行计算并用计算结果更新所述第五寄存器中的数据；

第五计算更新模块，用于更新所述第四寄存器中的数据，对所述第四寄存器中的数据和第二寄存器中的数据进行计算并用计算结果更新所述第五寄存器中的数据；

第六计算更新模块，用于根据所述第四寄存器中的数据和所述第一寄存器中的数据更新所述第四寄存器中的数据，对所述第五寄存器中的数据和所述第四寄存器中的数据进行计算得到线性对运算结果并保存。

10.如权利要求9所述的装置，其特征在于，所述计算存储更新模块包括：

第一计算存储单元，用于用所述第一预设值作为底数进行6次幂运算得到第一中间值，将所述第二寄存器中的数据作为底数、所述第一中间值作为指数进行幂运算并将运算结果存储到所述第六寄存器中；对所述第二寄存器中的数据进行逆元计算并将计算结果存储到所述第四寄存器中；

第一运算更新单元，用于对所述第六寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新第六寄存器中的数据；

第二运算更新单元，用于用所述第一预设值作为底数进行2次幂运算得到第二中间值，用所述第六寄存器中的数据作为底数、所述第二中间值作为指数进行幂运算并用运算结果更新所述第四寄存器中的数据；

第三运算更新单元，用于对所述第六寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新所述第二寄存器中的数据；

第四运算更新单元，用于用所述第二寄存器中的数据作为底数、所述第二预设值作为指数进行幂运算并用运算结果更新所述第四寄存器中的数据；

第五运算更新单元，用于用所述第四寄存器中的数据作为底数、所述第二预设值作为指数进行幂运算并用运算结果更新所述第六寄存器中的数据。

11.如权利要求10所述的装置，其特征在于，所述第一计算更新模块包括：

第六运算更新单元，用于用所述第六寄存器中的数据作为底数、所述第二预设值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据；

第七运算更新单元，用于用所述第三寄存器中的数据作为底数、所述第一预设值作为指数进行幂运算并用运算结果更新所述第五寄存器中的数据；

第八运算更新单元，用于对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第三寄存器中的数据。

12.如权利要求11所述的装置，其特征在于，所述第二计算更新模块包括：

第九运算更新单元，用于对所述第三寄存器中的数据进行逆元计算并用计算结果更新所述第七寄存器中的数据；

第十运算更新单元，用于用所述第二寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据；

第十一运算更新单元，用于用所述第一预设值作为底数进行2次幂运算得到第三中间值，用所述第二寄存器中的数据作为底数、所述第三中间值作为指数进行幂运算并用运算结果更新所述第五寄存器中的数据；

第十二运算更新单元，用于对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第三寄存器中的数据；

第十三运算更新单元，用于用所述第一预设值作为底数进行3次幂运算得到第四中间值，用所述第二寄存器中的数据作为底数、所述第四中间值作为指数进行幂运算并用运算结果更新所述第五寄存器中的数据；

第十四运算更新单元，用于对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并将运算结果存储到所述第一寄存器中；

第十五运算更新单元，用于用所述第六寄存器中的数据作为底数、所述第一预设值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据；

第十六运算更新单元，用于对所述第四寄存器中的数据与所述第三寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据；

第十七运算更新单元，用于对所述第五寄存器中的数据进行逆元计算并用计算结果更新所述第五寄存器中的数据；

第十八运算更新单元，用于用所述第一预设值作为底数进行2次幂运算得到第五中间值，用所述第六寄存器中的数据作为底数、所述第五中间值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据。

13.如权利要求12所述的装置，其特征在于，所述第三计算更新模块包括：

第十九运算更新单元，用于对所述第六寄存器中的数据进行逆元计算并用计算结果更新所述第六寄存器中的数据；

第二十运算更新单元，用于用所述第四寄存器中的数据作为底数、所述第一预设值作为指数进行幂运算并用运算结果更新所述第四寄存器中的数据；

第二十一运算更新单元，用于对所述第四寄存器中的数据进行逆元计算并用计算结果更新所述第四寄存器中的数据。

14.如权利要求13所述的装置，其特征在于，所述第四计算更新模块包括：

第二十二运算更新单元，用于对所述第二寄存器中的数据进行逆元计算并用计算结果更新所述第二寄存器中的数据；

第二十三运算更新单元，用于对所述第六寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据；

第二十四运算更新单元，用于对所述第六寄存器中的数据与所述第四寄存器中的数据

进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

第二十五运算更新单元，用于对所述第七寄存器中的数据与所述第七寄存器中的数据进行12次域乘法运算并用运算结果更新所述第七寄存器中的数据；

第二十六运算更新单元，用于对所述第七寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据；

第二十七运算更新单元，用于对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

第二十八运算更新单元，用于对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

第二十九运算更新单元，用于对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据。

15.如权利要求14所述的装置，其特征在于，所述第五计算更新模块包括：

第三十运算更新单元，用于对所述第四寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

第三十一运算更新单元，用于对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

第三十二运算更新单元，用于对所述第四寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

第三十三运算更新单元，用于对所述第四寄存器中的数据与所述第二寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据。

16.如权利要求15所述的装置，其特征在于，所述第六计算更新模块包括：

第三十四运算更新单元，用于对所述第四寄存器中的数据与所述第一寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

第三十五运算更新单元，用于对所述第五寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据；

第三十六运算更新单元，用于对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第二寄存器中的数据，将所述第二寄存器中的数据作为线性对运算结果进行保存。

一种在嵌入式系统中加快线性对运算的实现方法及装置

技术领域

[0001] 本发明涉及信息安全领域，尤其涉及一种在嵌入式系统中加快线性对运算的实现方法及装置。

背景技术

[0002] 当前，IBC(标识密码系统)快速发展，该系统理论上可去除CA(证书颁发机构)，从而在使用上存在很大的便利性；而SM9是国际标准中唯一的一套标识密码系统。SM9算法不需要申请数字证书，适用于互联网行业的各种新兴应用。如基于云技术的密码服务、电子邮件安全、智能终端保护、物联网安全、云存储安全等各种安全应用中。这些安全应用可采用手机号码或邮件地址作为公钥，实现数据加密、身份认证、通话加密、通道加密等安全应用，并具有使用方便，易于部署的特点。SM9密码系统运算的核心部分为线性对运算，而线性对运算中最耗时部分为Final Exponentiation运算，该运算的表示形式为 $f^{(q^{12}-1)/r}$，如果直接强制运算，运算时间特别长，将导致使用SM9的各种安全应用的效率降低。

发明内容

[0003] 本发明的目的是为了克服现有技术的不足，提供一种在嵌入式系统中加快线性对运算的实现方法及装置。

[0004] 本发明提供了一种在嵌入式系统中加快线性对运算的实现方法，包括：

[0005] 步骤S1：协处理器获取第一预设值、第二预设值、获取第一数据组；分配第一寄存器、第二寄存器、第三寄存器、第四寄存器、第五寄存器、第六寄存器、第七寄存器，并将所述第一数据组存储到所述第二寄存器中；所述第一数据组为12维数据；

[0006] 步骤S2：所述协处理器对所述第二寄存器中的数据和所述第一预设值进行计算并将计算结果存储到所述第六寄存器中，对所述第二寄存器中的数据进行计算并将计算结果存储到第四寄存器中，对所述第四寄存器中的数据、所述第二寄存器中的数据和所述第一预设值进行计算并用计算结果更新所述第六寄存器中的数据；

[0007] 步骤S3：所述协处理器对所述第六寄存器中的数据、所述第二预设值和所述第一预设值进行计算并将计算结果存储到第五寄存器中，根据所述第五寄存器中的数据更新所述第三寄存器中的数据；

[0008] 步骤S4：所述协处理器对所述第三寄存器中的数据进行计算并将计算结果存储到所述第七寄存器中，对所述第五寄存器中的数据、所述第二寄存器中的数据、所述第一预设值进行计算并用计算结果更新所述第三寄存器中的数据；

[0009] 步骤S5：所述协处理器更新所述第六寄存器中的数据，对所述第六寄存器中的数据和所述第一预设值进行计算并用计算结果更新所述第四寄存器中的数据；

[0010] 步骤S6：所述协处理器对所述第六寄存器中的数据、所述第四寄存器中的数据和所述第七寄存器中的数据进行计算并用计算结果更新所述第五寄存器中的数据；

[0011] 步骤S7：所述协处理器更新所述第四寄存器中的数据，对所述第四寄存器中的数

据和第二寄存器中的数据进行计算并用计算结果更新所述第五寄存器中的数据；

[0012] 步骤S8:所述协处理器根据所述第四寄存器中的数据和所述第一寄存器中的数据更新所述第四寄存器中的数据,对所述第五寄存器中的数据和所述第四寄存器中的数据进行计算得到线性对运算结果并保存。

[0013] 进一步地,所述步骤S2包括:

[0014] 步骤S2-1:所述协处理器用所述第一预设值作为底数进行6次幂运算得到第一中间值,将所述第二寄存器中的数据作为底数、所述第一中间值作为指数进行幂运算并将运算结果存储到所述第六寄存器中;对所述第二寄存器中的数据进行逆元计算并将计算结果存储到所述第四寄存器中;

[0015] 步骤S2-2:所述协处理器对所述第六寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新第六寄存器中的数据;

[0016] 步骤S2-3:所述协处理器用所述第一预设值作为底数进行2次幂运算得到第二中间值,用所述第六寄存器中的数据作为底数、所述第二中间值作为指数进行幂运算并用运算结果更新所述第四寄存器中的数据;

[0017] 步骤S2-4:所述协处理器对所述第六寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新所述第二寄存器中的数据;

[0018] 步骤S2-5:所述协处理器用所述第二寄存器中的数据作为底数、所述第二预设值作为指数进行幂运算并用运算结果更新所述第四寄存器中的数据;

[0019] 步骤S2-6:所述协处理器用所述第四寄存器中的数据作为底数、所述第二预设值作为指数进行幂运算并用运算结果更新所述第六寄存器中的数据。

[0020] 进一步地,所述步骤S3包括:

[0021] 步骤S3-1:所述协处理器用所述第六寄存器中的数据作为底数、所述第二预设值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据;

[0022] 步骤S3-2:所述协处理器用所述第三寄存器中的数据作为底数、所述第一预设值作为指数进行幂运算并用运算结果更新所述第五寄存器中的数据;

[0023] 步骤S3-3:所述协处理器对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第三寄存器中的数据。

[0024] 进一步地,所述步骤S4包括:

[0025] 步骤S4-1:所述协处理器对所述第三寄存器中的数据进行逆元计算并用计算结果更新所述第七寄存器中的数据;

[0026] 步骤S4-2:所述协处理器用所述第二寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据;

[0027] 步骤S4-3:所述协处理器用所述第一预设值作为底数进行2次幂运算得到第三中间值,用所述第二寄存器中的数据作为底数、所述第三中间值作为指数进行幂运算并用运算结果更新所述第五寄存器中的数据;

[0028] 步骤S4-4:所述协处理器对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第三寄存器中的数据;

[0029] 步骤S4-5:所述协处理器用所述第一预设值作为底数进行3次幂运算得到第四中间值,用所述第二寄存器中的数据作为底数、所述第四中间值作为指数进行幂运算并用运

算结果更新所述第五寄存器中的数据；

[0030] 步骤S4-6:所述协处理器对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并将运算结果存储到所述第一寄存器中；

[0031] 步骤S4-7:所述协处理器用所述第六寄存器中的数据作为底数、所述第一预设值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据；

[0032] 步骤S4-8:所述协处理器对所述第四寄存器中的数据与所述第三寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据；

[0033] 步骤S4-9:所述协处理器对所述第五寄存器中的数据进行逆元计算并用计算结果更新所述第五寄存器中的数据；

[0034] 步骤S4-10:所述协处理器用所述第一预设值作为底数进行2次幂运算得到第五中间值,用所述第六寄存器中的数据作为底数、所述第五中间值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据。

[0035] 进一步地,所述步骤S5包括：

[0036] 步骤S5-1:所述协处理器对所述第六寄存器中的数据进行逆元计算并用计算结果更新所述第六寄存器中的数据；

[0037] 步骤S5-2:所述协处理器用所述第四寄存器中的数据作为底数、所述第一预设值作为指数进行幂运算并用运算结果更新所述第四寄存器中的数据；

[0038] 步骤S5-3:所述协处理器对所述第四寄存器中的数据进行逆元计算并用计算结果更新所述第四寄存器中的数据。

[0039] 进一步地,所述步骤S6包括：

[0040] 步骤S6-1:所述协处理器对所述第二寄存器中的数据进行逆元计算并用计算结果更新所述第二寄存器中的数据；

[0041] 步骤S6-2:所述协处理器对所述第六寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据；

[0042] 步骤S6-3:所述协处理器对所述第六寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

[0043] 步骤S6-4:所述协处理器对所述第七寄存器中的数据与所述第七寄存器中的数据进行12次域乘法运算并用运算结果更新所述第七寄存器中的数据；

[0044] 步骤S6-5:所述协处理器对所述第七寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据；

[0045] 步骤S6-6:所述协处理器对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

[0046] 步骤S6-7:所述协处理器对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

[0047] 步骤S6-8:所述协处理器对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据。

[0048] 进一步地,所述步骤S7包括：

[0049] 步骤S7-1:所述协处理器对所述第四寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

[0050] 步骤S7-2:所述协处理器对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据;

[0051] 步骤S7-3:所述协处理器对所述第四寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据;

[0052] 步骤S7-4:所述协处理器对所述第四寄存器中的数据与所述第二寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据。

[0053] 进一步地,所述步骤S8包括:

[0054] 步骤S8-1:所述协处理器对所述第四寄存器中的数据与所述第一寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据;

[0055] 步骤S8-2:所述协处理器对所述第五寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据;

[0056] 步骤S8-3:所述协处理器对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第二寄存器中的数据,将所述第二寄存器中的数据作为线性对运算结果进行保存。

[0057] 本发明又提供了一种在嵌入式系统中加快线性对运算的实现装置,所述装置设置在协处理器中,所述装置包括:

[0058] 获取分配存储模块,用于获取第一预设值、第二预设值、获取第一数据组;分配第一寄存器、第二寄存器、第三寄存器、第四寄存器、第五寄存器、第六寄存器、第七寄存器,并将所述第一数据组存储到所述第二寄存器中;所述第一数据组为12维数据;

[0059] 计算存储更新模块,用于对所述第二寄存器中的数据和所述第一预设值进行计算并将计算结果存储到所述第六寄存器中,对所述第二寄存器中的数据进行计算并将计算结果存储到第四寄存器中,对所述第四寄存器中的数据、所述第二寄存器中的数据和所述第一预设值进行计算并用计算结果更新所述第六寄存器中的数据;

[0060] 第一计算更新模块,用于对所述第六寄存器中的数据、所述第二预设值和所述第一预设值进行计算并将计算结果存储到第五寄存器中,根据所述第五寄存器中的数据更新所述第三寄存器中的数据;

[0061] 第二计算更新模块,用于对所述第三寄存器中的数据进行计算并将计算结果存储到所述第七寄存器中,对所述第五寄存器中的数据、所述第二寄存器中的数据、所述第一预设值进行计算并用计算结果更新所述第三寄存器中的数据;

[0062] 第三计算更新模块,用于更新所述第六寄存器中的数据,对所述第六寄存器中的数据和所述第一预设值进行计算并用计算结果更新所述第四寄存器中的数据;

[0063] 第四计算更新模块,用于对所述第六寄存器中的数据、所述第四寄存器中的数据和所述第七寄存器中的数据进行计算并用计算结果更新所述第五寄存器中的数据;

[0064] 第五计算更新模块,用于更新所述第四寄存器中的数据,对所述第四寄存器中的数据和第二寄存器中的数据进行计算并用计算结果更新所述第五寄存器中的数据;

[0065] 第六计算更新模块,用于根据所述第四寄存器中的数据和所述第一寄存器中的数据更新所述第四寄存器中的数据,对所述第五寄存器中的数据和所述第四寄存器中的数据进行计算得到线性对运算结果并保存。

[0066] 进一步地,所述计算存储更新模块包括:

[0067] 第一计算存储单元，用于用所述第一预设值作为底数进行6次幂运算得到第一中间值，将所述第二寄存器中的数据作为底数、所述第一中间值作为指数进行幂运算并将运算结果存储到所述第六寄存器中；对所述第二寄存器中的数据进行逆元计算并将计算结果存储到所述第四寄存器中；

[0068] 第一运算更新单元，用于对所述第六寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新第六寄存器中的数据；

[0069] 第二运算更新单元，用于用所述第一预设值作为底数进行2次幂运算得到第二中间值，用所述第六寄存器中的数据作为底数、所述第二中间值作为指数进行幂运算并用运算结果更新所述第四寄存器中的数据；

[0070] 第三运算更新单元，用于对所述第六寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新所述第二寄存器中的数据；

[0071] 第四运算更新单元，用于用所述第二寄存器中的数据作为底数、所述第二预设值作为指数进行幂运算并用运算结果更新所述第四寄存器中的数据；

[0072] 第五运算更新单元，用于用所述第四寄存器中的数据作为底数、所述第二预设值作为指数进行幂运算并用运算结果更新所述第六寄存器中的数据。

[0073] 进一步地，所述第一计算更新模块包括：

[0074] 第六运算更新单元，用于用所述第六寄存器中的数据作为底数、所述第二预设值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据；

[0075] 第七运算更新单元，用于用所述第三寄存器中的数据作为底数、所述第一预设值作为指数进行幂运算并用运算结果更新所述第五寄存器中的数据；

[0076] 第八运算更新单元，用于对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第三寄存器中的数据。

[0077] 进一步地，所述第二计算更新模块包括：

[0078] 第九运算更新单元，用于对所述第三寄存器中的数据进行逆元计算并用计算结果更新所述第七寄存器中的数据；

[0079] 第十运算更新单元，用于用所述第二寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据；

[0080] 第十一运算更新单元，用于用所述第一预设值作为底数进行2次幂运算得到第三中间值，用所述第二寄存器中的数据作为底数、所述第三中间值作为指数进行幂运算并用运算结果更新所述第五寄存器中的数据；

[0081] 第十二运算更新单元，用于对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第三寄存器中的数据；

[0082] 第十三运算更新单元，用于用所述第一预设值作为底数进行3次幂运算得到第四中间值，用所述第二寄存器中的数据作为底数、所述第四中间值作为指数进行幂运算并用运算结果更新所述第五寄存器中的数据；

[0083] 第十四运算更新单元，用于对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并将运算结果存储到所述第一寄存器中；

[0084] 第十五运算更新单元，用于用所述第六寄存器中的数据作为底数、所述第一预设值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据；

[0085] 第十六运算更新单元，用于对所述第四寄存器中的数据与所述第三寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据；

[0086] 第十七运算更新单元，用于对所述第五寄存器中的数据进行逆元计算并用计算结果更新所述第五寄存器中的数据；

[0087] 第十八运算更新单元，用于用所述第一预设值作为底数进行2次幂运算得到第五中间值，用所述第六寄存器中的数据作为底数、所述第五中间值作为指数进行幂运算并用运算结果更新所述第三寄存器中的数据。

[0088] 进一步地，所述第三计算更新模块包括：

[0089] 第十九运算更新单元，用于对所述第六寄存器中的数据进行逆元计算并用计算结果更新所述第六寄存器中的数据；

[0090] 第二十运算更新单元，用于用所述第四寄存器中的数据作为底数、所述第一预设值作为指数进行幂运算并用运算结果更新所述第四寄存器中的数据；

[0091] 第二十一运算更新单元，用于对所述第四寄存器中的数据进行逆元计算并用计算结果更新所述第四寄存器中的数据。

[0092] 进一步地，所述第四计算更新模块包括：

[0093] 第二十二运算更新单元，用于对所述第二寄存器中的数据进行逆元计算并用计算结果更新所述第二寄存器中的数据；

[0094] 第二十三运算更新单元，用于对所述第六寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据；

[0095] 第二十四运算更新单元，用于对所述第六寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

[0096] 第二十五运算更新单元，用于对所述第七寄存器中的数据与所述第七寄存器中的数据进行12次域乘法运算并用运算结果更新所述第七寄存器中的数据；

[0097] 第二十六运算更新单元，用于对所述第七寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据；

[0098] 第二十七运算更新单元，用于对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

[0099] 第二十八运算更新单元，用于对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

[0100] 第二十九运算更新单元，用于对所述第三寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据。

[0101] 进一步地，所述第五计算更新模块包括：

[0102] 第三十运算更新单元，用于对所述第四寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

[0103] 第三十一运算更新单元，用于对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

[0104] 第三十二运算更新单元，用于对所述第四寄存器中的数据与所述第四寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

[0105] 第三十三运算更新单元，用于对所述第四寄存器中的数据与所述第二寄存器中的

数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据。

[0106] 进一步地，所述第六计算更新模块包括：

[0107] 第三十四运算更新单元，用于对所述第四寄存器中的数据与所述第一寄存器中的数据进行12次域乘法运算并用运算结果更新所述第四寄存器中的数据；

[0108] 第三十五运算更新单元，用于对所述第五寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第五寄存器中的数据；

[0109] 第三十六运算更新单元，用于对所述第四寄存器中的数据与所述第五寄存器中的数据进行12次域乘法运算并用运算结果更新所述第二寄存器中的数据，将所述第二寄存器中的数据作为线性对运算结果进行保存。

[0110] 本发明与现有技术相比，具有用下优点：本发明技术方案应用于解密、签名等过程，通过对线性对运算进行拆分，大大减少了运算时间，进一步地提高使用本发明技术方案的各种安全应用的效率。

附图说明

[0111] 图1为本发明实施例一提供的一种在嵌入式系统中加快线性对运算的实现方法流程图；

[0112] 图2和图3为本发明实施例二提供的一种在嵌入式系统中加快线性对运算的实现方法流程图；

[0113] 图4为本发明实施例三提供的一种在嵌入式系统中加快线性对运算的实现装置方框图。

具体实施方式

[0114] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0115] 实施例一

[0116] 本发明实施例一提供了一种在嵌入式系统中加快线性对运算的实现方法，如图1所示，包括：

[0117] 步骤S1：协处理器获取第一预设值、第二预设值、获取第一数据组；分配第一寄存器、第二寄存器、第三寄存器、第四寄存器、第五寄存器、第六寄存器、第七寄存器，并将第一数据组存储到第二寄存器中；

[0118] 具体的，本实施例中的第一数据组为12维数据；

[0119] 步骤S2：协处理器对第二寄存器中的数据和第一预设值进行计算并将计算结果存储到第六寄存器中，对第二寄存器中的数据进行计算并将计算结果存储到第四寄存器中，对第四寄存器中的数据、第二寄存器中的数据和第一预设值进行计算并用计算结果更新第六寄存器中的数据；

[0120] 具体的，在本实施例中，步骤S2包括：

[0121] 步骤S2-1：协处理器用第一预设值作为底数进行6次幂运算得到第一中间值，将第

二寄存器中的数据作为底数、第一中间值作为指数进行幂运算并将运算结果存储到第六寄存器中;对第二寄存器中的数据进行逆元计算并将计算结果存储到第四寄存器中;

[0122] 步骤S2-2:协处理器对第六寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第六寄存器中的数据;

[0123] 步骤S2-3:协处理器用第一预设值作为底数进行2次幂运算得到第二中间值,用第六寄存器中的数据作为底数、第二中间值作为指数进行幂运算并用运算结果更新第四寄存器中的数据;

[0124] 步骤S2-4:协处理器对第六寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第二寄存器中的数据;

[0125] 步骤S2-5:协处理器用第二寄存器中的数据作为底数、第二预设值作为指数进行幂运算并用运算结果更新第四寄存器中的数据;

[0126] 步骤S2-6:协处理器用第四寄存器中的数据作为底数、第二预设值作为指数进行幂运算并用运算结果更新第六寄存器中的数据;

[0127] 步骤S3:协处理器对第六寄存器中的数据、第二预设值和第一预设值进行计算并将计算结果存储到第五寄存器中,根据第五寄存器中的数据更新第三寄存器中的数据;

[0128] 具体的,在本实施例中,步骤S3包括:

[0129] 步骤S3-1:协处理器用第六寄存器中的数据作为底数、第二预设值作为指数进行幂运算并用运算结果更新第三寄存器中的数据;

[0130] 步骤S3-2:协处理器用第三寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新第五寄存器中的数据;

[0131] 步骤S3-3:协处理器对第三寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第三寄存器中的数据;

[0132] 步骤S4:协处理器对第三寄存器中的数据进行计算并将计算结果存储到第七寄存器中,对第五寄存器中的数据、第二寄存器中的数据、第一预设值进行计算并用计算结果更新第三寄存器中的数据;

[0133] 具体的,在本实施例中,步骤S4包括:

[0134] 步骤S4-1:协处理器对第三寄存器中的数据进行逆元计算并用计算结果更新第七寄存器中的数据;

[0135] 步骤S4-2:协处理器用第二寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新第三寄存器中的数据;

[0136] 步骤S4-3:协处理器用第一预设值作为底数进行2次幂运算得到第三中间值,用第二寄存器中的数据作为底数、第三中间值作为指数进行幂运算并用运算结果更新第五寄存器中的数据;

[0137] 步骤S4-4:协处理器对第三寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第三寄存器中的数据;

[0138] 步骤S4-5:协处理器用第一预设值作为底数进行3次幂运算得到第四中间值,用第二寄存器中的数据作为底数、第四中间值作为指数进行幂运算并用运算结果更新第五寄存器中的数据;

[0139] 步骤S4-6:协处理器对第三寄存器中的数据与第五寄存器中的数据进行12次域乘

法运算并将运算结果存储到第一寄存器中；

[0140] 步骤S4-7：协处理器用第六寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新第三寄存器中的数据；

[0141] 步骤S4-8：协处理器对第四寄存器中的数据与第三寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0142] 步骤S4-9：协处理器对第五寄存器中的数据进行逆元计算并用计算结果更新第五寄存器中的数据；

[0143] 步骤S4-10：协处理器用第一预设值作为底数进行2次幂运算得到第五中间值，用第六寄存器中的数据作为底数、第五中间值作为指数进行幂运算并用运算结果更新第三寄存器中的数据；

[0144] 步骤S5：协处理器更新第六寄存器中的数据，对第六寄存器中的数据和第一预设值进行计算并用计算结果更新第四寄存器中的数据；

[0145] 具体的，在本实施例中，步骤S5包括：

[0146] 步骤S5-1：协处理器对第六寄存器中的数据进行逆元计算并用计算结果更新第六寄存器中的数据；

[0147] 步骤S5-2：协处理器用第四寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新第四寄存器中的数据；

[0148] 步骤S5-3：协处理器对第四寄存器中的数据进行逆元计算并用计算结果更新第四寄存器中的数据；

[0149] 步骤S6：协处理器对第六寄存器中的数据、第四寄存器中的数据和第七寄存器中的数据进行计算并用计算结果更新第五寄存器中的数据；

[0150] 具体的，在本实施例中，步骤S6包括：

[0151] 步骤S6-1：协处理器对第二寄存器中的数据进行逆元计算并用计算结果更新第二寄存器中的数据；

[0152] 步骤S6-2：协处理器对第六寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0153] 步骤S6-3：协处理器对第六寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0154] 步骤S6-4：协处理器对第七寄存器中的数据与第七寄存器中的数据进行12次域乘法运算并用运算结果更新第七寄存器中的数据；

[0155] 步骤S6-5：协处理器对第七寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0156] 步骤S6-6：协处理器对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0157] 步骤S6-7：协处理器对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0158] 步骤S6-8：协处理器对第三寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0159] 步骤S7：协处理器更新第四寄存器中的数据，对第四寄存器中的数据和第二寄存

器中的数据进行计算并用计算结果更新第五寄存器中的数据；

[0160] 具体的，在本实施例中，步骤S7包括：

[0161] 步骤S7-1：协处理器对第四寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0162] 步骤S7-2：协处理器对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0163] 步骤S7-3：协处理器对第四寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0164] 步骤S7-4：协处理器对第四寄存器中的数据与第二寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0165] 步骤S8：协处理器根据第四寄存器中的数据和第一寄存器中的数据更新第四寄存器中的数据，对第五寄存器中的数据和第四寄存器中的数据进行计算得到线性对运算结果并保存；

[0166] 具体的，在本实施例中，步骤S8包括：

[0167] 步骤S8-1：协处理器对第四寄存器中的数据与第一寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0168] 步骤S8-2：协处理器对第五寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0169] 步骤S8-3：协处理器对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第二寄存器中的数据，将第二寄存器中的数据作为线性对运算结果进行保存。

[0170] 本发明实施例中的线性对运算结果应用在各种安全应用(密码服务、电子邮件安全、智能终端保护、物联网安全、云存储安全等)中，参与使用私钥进行解密或使用私钥进行签名的过程。本发明实施例通过对线性对运算进行拆分，大大减少了运算时间，进一步地提高使用本发明技术方案的各种安全应用的效率。

[0171] 实施例二

[0172] 本发明实施例二提供了一种在嵌入式系统中加快线性对运算的实现方法，如图2和图3所示，包括：

[0173] 步骤101：协处理器获取第一预设值、第二预设值、获取第一数据组；分配第一寄存器、第二寄存器、第三寄存器、第四寄存器、第五寄存器、第六寄存器、第七寄存器，并将第一数据组存储到第二寄存器中；

[0174] 在本实施例中，第一数据组为12维256bit的数据，例如为$f(a_0,,,,,,,,,,,,a_{11})$；

[0175] 步骤102：协处理器用第一预设值作为底数进行6次幂运算得到第一中间值，将第二寄存器中的数据作为底数、第一中间值作为指数进行计算并将计算结果存储到第六寄存器中；对第二寄存器中的数据进行逆元计算并将计算结果存储到第四寄存器中；

[0176] 步骤103：协处理器对第六寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第六寄存器中的数据；

[0177] 步骤104：协处理器用第一预设值作为底数进行2次幂运算得到第二中间值，用第六寄存器中的数据作为底数、第二中间值作为指数进行幂运算并用运算结果更新第四寄存

器中的数据；

[0178] 步骤105：协处理器对第六寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第二寄存器中的数据；

[0179] 步骤106：协处理器用第二寄存器中的数据作为底数、第二预设值作为指数进行幂运算并用运算结果更新第四寄存器中的数据；

[0180] 步骤107：协处理器用第四寄存器中的数据作为底数、第二预设值作为指数进行幂运算并用运算结果更新第六寄存器中的数据；

[0181] 步骤108：协处理器用第六寄存器中的数据作为底数、第二预设值作为指数进行幂运算并用运算结果更新第三寄存器中的数据；

[0182] 步骤109：协处理器用第三寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新第五寄存器中的数据；

[0183] 步骤110：协处理器对第三寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第三寄存器中的数据；

[0184] 步骤111：协处理器对第三寄存器中的数据进行逆元计算并用计算结果更新第七寄存器中的数据；

[0185] 步骤112：协处理器用第二寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新第三寄存器中的数据；

[0186] 步骤113：协处理器用第一预设值作为底数进行2次幂运算得到第三中间值，用第二寄存器中的数据作为底数、第三中间值作为指数进行幂运算并用运算结果更新第五寄存器中的数据；

[0187] 步骤114：协处理器对第三寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第三寄存器中的数据；

[0188] 步骤115：协处理器用第一预设值作为底数进行3次幂运算得到第四中间值，用第二寄存器中的数据作为底数、第四中间值作为指数进行幂运算并用运算结果更新第五寄存器中的数据；

[0189] 步骤116：协处理器对第三寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并将运算结果存储到第一寄存器中；

[0190] 步骤117：协处理器用第六寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新第三寄存器中的数据；

[0191] 步骤118：协处理器对第四寄存器中的数据与第三寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0192] 步骤119：协处理器对第五寄存器中的数据进行逆元计算并用计算结果更新第五寄存器中的数据；

[0193] 步骤120：协处理器用第一预设值作为底数进行2次幂运算得到第五中间值，用第六寄存器中的数据作为底数、第五中间值作为指数进行幂运算并用运算结果更新第三寄存器中的数据；

[0194] 步骤121：协处理器对第六寄存器中的数据进行逆元计算并用计算结果更新第六寄存器中的数据；

[0195] 步骤122：协处理器用第四寄存器中的数据作为底数、第一预设值作为指数进行幂

运算并用运算结果更新第四寄存器中的数据；

[0196] 步骤123：协处理器对第四寄存器中的数据进行逆元计算并用计算结果更新第四寄存器中的数据；

[0197] 步骤124：协处理器对第二寄存器中的数据进行逆元计算并用计算结果更新第二寄存器中的数据；

[0198] 步骤125：协处理器对第六寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0199] 步骤126：协处理器对第六寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0200] 步骤127：协处理器对第七寄存器中的数据与第七寄存器中的数据进行12次域乘法运算并用运算结果更新第七寄存器中的数据；

[0201] 步骤128：协处理器对第七寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0202] 步骤129：协处理器对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0203] 步骤130：协处理器对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0204] 步骤131：协处理器对第三寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0205] 步骤132：协处理器对第四寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0206] 步骤133：协处理器对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0207] 步骤134：协处理器对第四寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0208] 步骤135：协处理器对第四寄存器中的数据与第二寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0209] 步骤136：协处理器对第四寄存器中的数据与第一寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0210] 步骤137：协处理器对第五寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0211] 步骤138：协处理器对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第二寄存器中的数据，将第二寄存器中的数据作为线性对运算结果进行保存。

[0212] 本发明实施例中的线性对运算结果应用在各种安全应用(密码服务、电子邮件安全、智能终端保护、物联网安全、云存储安全等)中，参与使用私钥进行解密或使用私钥进行签名的过程。本发明实施例通过对线性对运算进行拆分，大大减少了运算时间，进一步地提高使用本发明技术方案的各种安全应用的效率。

[0213] 实施例三

[0214] 本发明实施例三提供了一种在嵌入式系统中加快线性对运算的实现装置，该装置设置在协处理器中，如图4所示，本实施例的装置包括：

[0215] 获取分配存储模块401，用于获取第一预设值、第二预设值、获取第一数据组；分配第一寄存器、第二寄存器、第三寄存器、第四寄存器、第五寄存器、第六寄存器、第七寄存器，并将第一数据组存储到第二寄存器中；第一数据组为12维数据；

[0216] 计算存储更新模块402，用于对第二寄存器中的数据和第一预设值进行计算并将计算结果存储到第六寄存器中，对第二寄存器中的数据进行计算并将计算结果存储到第四寄存器中，对第四寄存器中的数据、第二寄存器中的数据和第一预设值进行计算并用计算结果更新第六寄存器中的数据；

[0217] 第一计算更新模块403，用于对第六寄存器中的数据、第二预设值和第一预设值进行计算并将计算结果存储到第五寄存器中，根据第五寄存器中的数据更新第三寄存器中的数据；

[0218] 第二计算更新模块404，用于对第三寄存器中的数据进行计算并将计算结果存储到第七寄存器中，对第五寄存器中的数据、第二寄存器中的数据、第一预设值进行计算并用计算结果更新第三寄存器中的数据；

[0219] 第三计算更新模块405，用于更新第六寄存器中的数据，对第六寄存器中的数据和第一预设值进行计算并用计算结果更新第四寄存器中的数据；

[0220] 第四计算更新模块406，用于对第六寄存器中的数据、第四寄存器中的数据和第七寄存器中的数据进行计算并用计算结果更新第五寄存器中的数据；

[0221] 第五计算更新模块407，用于更新第四寄存器中的数据，对第四寄存器中的数据和第二寄存器中的数据进行计算并用计算结果更新第五寄存器中的数据；

[0222] 第六计算更新模块408，用于根据第四寄存器中的数据和第一寄存器中的数据更新第四寄存器中的数据，对第五寄存器中的数据和第四寄存器中的数据进行计算得到线性对运算结果并保存。

[0223] 进一步地，本实施例的计算存储更新模块402包括：

[0224] 第一计算存储单元，用于用第一预设值作为底数进行6次幂运算得到第一中间值，将第二寄存器中的数据作为底数、第一中间值作为指数进行幂运算并将运算结果存储到第六寄存器中；对第二寄存器中的数据进行逆元计算并将计算结果存储到第四寄存器中；

[0225] 第一运算更新单元，用于对第六寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第六寄存器中的数据；

[0226] 第二运算更新单元，用于用第一预设值作为底数进行2次幂运算得到第二中间值，用第六寄存器中的数据作为底数、第二中间值作为指数进行幂运算并用运算结果更新第四寄存器中的数据；

[0227] 第三运算更新单元，用于对第六寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第二寄存器中的数据；

[0228] 第四运算更新单元，用于用第二寄存器中的数据作为底数、第二预设值作为指数进行幂运算并用运算结果更新第四寄存器中的数据；

[0229] 第五运算更新单元，用于用第四寄存器中的数据作为底数、第二预设值作为指数进行幂运算并用运算结果更新第六寄存器中的数据。

[0230] 进一步地，本实施例的第一计算更新模块403包括：

[0231] 第六运算更新单元，用于用第六寄存器中的数据作为底数、第二预设值作为指数进行幂运算并用运算结果更新第三寄存器中的数据；

[0232] 第七运算更新单元，用于用第三寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新第五寄存器中的数据；

[0233] 第八运算更新单元，用于对第三寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第三寄存器中的数据。

[0234] 进一步地，本实施例的第二计算更新模块404包括：

[0235] 第九运算更新单元，用于对第三寄存器中的数据进行逆元计算并用计算结果更新第七寄存器中的数据；

[0236] 第十运算更新单元，用于用第二寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新第三寄存器中的数据；

[0237] 第十一运算更新单元，用于用第一预设值作为底数进行2次幂运算得到第三中间值，用第二寄存器中的数据作为底数、第三中间值作为指数进行幂运算并用运算结果更新第五寄存器中的数据；

[0238] 第十二运算更新单元，用于对第三寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第三寄存器中的数据；

[0239] 第十三运算更新单元，用于用第一预设值作为底数进行3次幂运算得到第四中间值，用第二寄存器中的数据作为底数、第四中间值作为指数进行幂运算并用运算结果更新第五寄存器中的数据；

[0240] 第十四运算更新单元，用于对第三寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并将运算结果存储到第一寄存器中；

[0241] 第十五运算更新单元，用于用第六寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新第三寄存器中的数据；

[0242] 第十六运算更新单元，用于对第四寄存器中的数据与第三寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0243] 第十七运算更新单元，用于对第五寄存器中的数据进行逆元计算并用计算结果更新第五寄存器中的数据；

[0244] 第十八运算更新单元，用于用第一预设值作为底数进行2次幂运算得到第五中间值，用第六寄存器中的数据作为底数、第五中间值作为指数进行幂运算并用运算结果更新第三寄存器中的数据。

[0245] 进一步地，本实施例的第三计算更新模块405包括：

[0246] 第十九运算更新单元，用于对第六寄存器中的数据进行逆元计算并用计算结果更新第六寄存器中的数据；

[0247] 第二十运算更新单元，用于用第四寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新第四寄存器中的数据；

[0248] 第二十一运算更新单元，用于对第四寄存器中的数据进行逆元计算并用计算结果更新第四寄存器中的数据。

[0249] 进一步地，本实施例的第四计算更新模块406包括：

[0250] 第二十二运算更新单元，用于对第二寄存器中的数据进行逆元计算并用计算结果更新第二寄存器中的数据；

[0251] 第二十三运算更新单元，用于对第六寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0252] 第二十四运算更新单元，用于对第六寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0253] 第二十五运算更新单元，用于对第七寄存器中的数据与第七寄存器中的数据进行12次域乘法运算并用运算结果更新第七寄存器中的数据；

[0254] 第二十六运算更新单元，用于对第七寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0255] 第二十七运算更新单元，用于对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0256] 第二十八运算更新单元，用于对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0257] 第二十九运算更新单元，用于对第三寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据。

[0258] 进一步地，本实施例的第五计算更新模块407包括：

[0259] 第三十运算更新单元，用于对第四寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0260] 第三十一运算更新单元，用于对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0261] 第三十二运算更新单元，用于对第四寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0262] 第三十三运算更新单元，用于对第四寄存器中的数据与第二寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据。

[0263] 进一步地，本实施例的第六计算更新模块408包括：

[0264] 第三十四运算更新单元，用于对第四寄存器中的数据与第一寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据；

[0265] 第三十五运算更新单元，用于对第五寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据；

[0266] 第三十六运算更新单元，用于对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第二寄存器中的数据，将第二寄存器中的数据作为线性对运算结果进行保存。

[0267] 本发明实施例中的线性对运算结果应用在各种安全应用(密码服务、电子邮件安全、智能终端保护、物联网安全、云存储安全等)中，参与使用私钥进行解密或使用私钥进行签名的过程。本发明实施例通过对线性对运算进行拆分，大大减少了运算时间，进一步地提高使用本发明技术方案的各种安全应用的效率。

[0268] 用上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明公开的技术范围内，可轻易想到的变化或替换，

都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该用权利要求的保护范围为准。

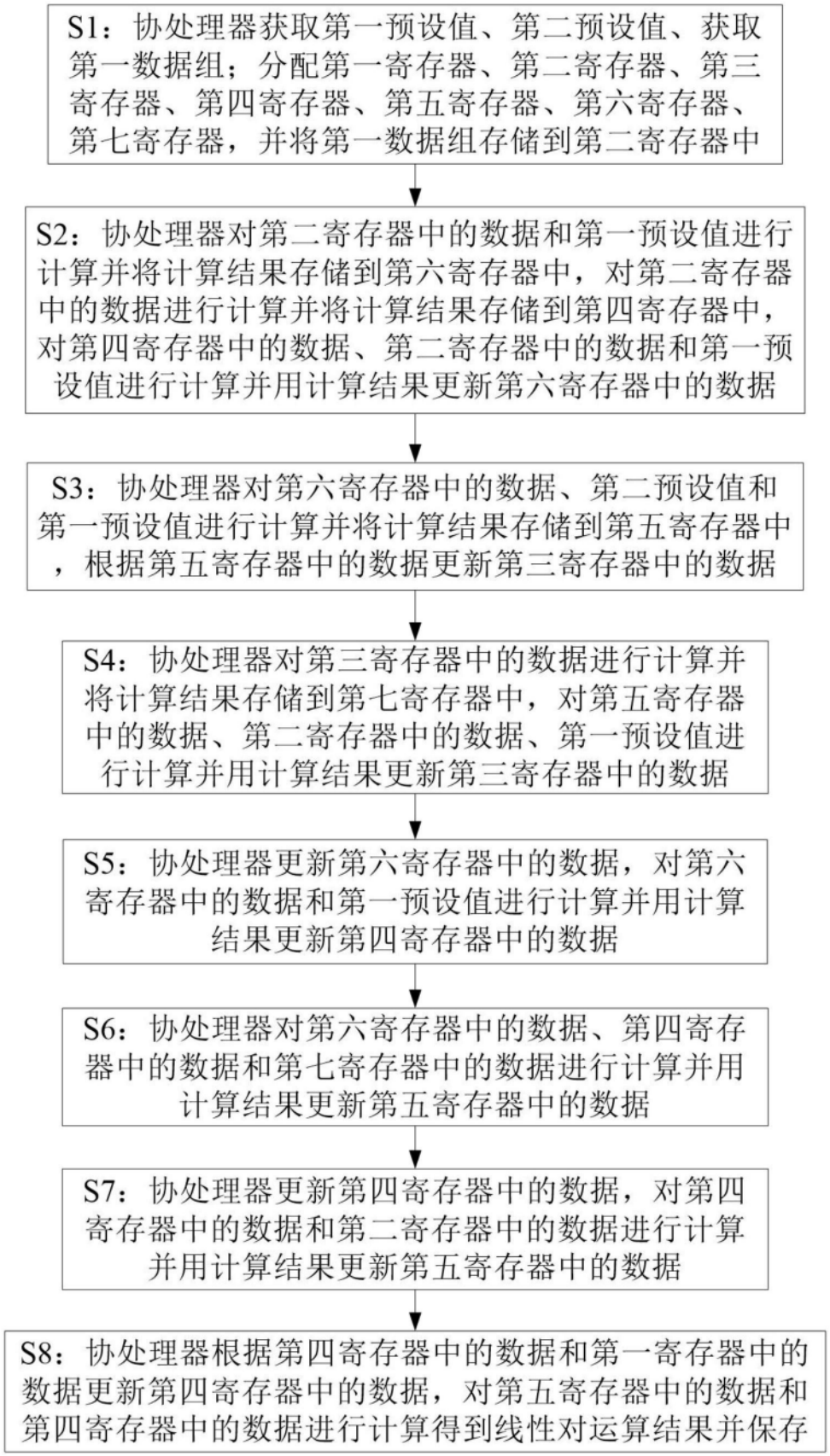

S1：协处理器获取第一预设值、第二预设值、获取第一数据组；分配第一寄存器、第二寄存器、第三寄存器、第四寄存器、第五寄存器、第六寄存器、第七寄存器，并将第一数据组存储到第二寄存器中
S2：协处理器对第二寄存器中的数据和第一预设值进行计算并将计算结果存储到第六寄存器中，对第二寄存器中的数据进行计算并将计算结果存储到第四寄存器中，对第四寄存器中的数据、第二寄存器中的数据和第一预设值进行计算并用计算结果更新第六寄存器中的数据
S3：协处理器对第六寄存器中的数据、第二预设值和第一预设值进行计算并将计算结果存储到第五寄存器中，根据第五寄存器中的数据更新第三寄存器中的数据
S4：协处理器对第三寄存器中的数据进行计算并将计算结果存储到第七寄存器中，对第五寄存器中的数据、第二寄存器中的数据、第一预设值进行计算并用计算结果更新第三寄存器中的数据
S5：协处理器更新第六寄存器中的数据，对第六寄存器中的数据和第一预设值进行计算并用计算结果更新第四寄存器中的数据
S6：协处理器对第六寄存器中的数据、第四寄存器中的数据和第七寄存器中的数据进行计算并用计算结果更新第五寄存器中的数据
S7：协处理器更新第四寄存器中的数据，对第四寄存器中的数据和第二寄存器中的数据进行计算并用计算结果更新第五寄存器中的数据
S8：协处理器根据第四寄存器中的数据和第一寄存器中的数据更新第四寄存器中的数据，对第五寄存器中的数据和第四寄存器中的数据进行计算得到线性对运算结果并保存

图1


101：协处理器获取第一预设值、第二预设值、获取第一数据组；分配第一寄存器、第二寄存器、第三寄存器、第四寄存器、第五寄存器、第六寄存器、第七寄存器，并将第一数据组存储到第二寄存器中
102：协处理器用第一预设值作为底数进行6次幂运算得到第一中间值，将第二寄存器中的数据作为底数、第一中间值作为指数进行计算并将计算结果存储到第六寄存器中；对第二寄存器中的数据进行逆元计算并将计算结果存储到第四寄存器中
103：协处理器对第六寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第六寄存器中的数据
104：协处理器用第一预设值作为底数进行2次幂运算得到第二中间值，用第六寄存器中的数据作为底数、第二中间值作为指数进行幂运算并用运算结果更新第四寄存器中的数据
105：协处理器对第六寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第二寄存器中的数据
106：协处理器用第二寄存器中的数据作为底数、第二预设值作为指数进行幂运算并用运算结果更新第四寄存器中的数据
107：协处理器用第四寄存器中的数据作为底数、第二预设值作为指数进行幂运算并用运算结果更新第六寄存器中的数据
108：协处理器用第六寄存器中的数据作为底数、第二预设值作为指数进行幂运算并用运算结果更新第三寄存器中的数据
109：协处理器用第三寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新第五寄存器中的数据
110：协处理器对第三寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第三寄存器中的数据
111：协处理器对第三寄存器中的数据进行逆元计算并用计算结果更新第七寄存器中的数据
112：协处理器用第二寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新第三寄存器中的数据
113：协处理器用第一预设值作为底数进行2次幂运算得到第三中间值，用第二寄存器中的数据作为底数、第三中间值作为指数进行幂运算并用运算结果更新第五寄存器中的数据
114：协处理器对第三寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第三寄存器中的数据
115：协处理器用第一预设值作为底数进行3次幂运算得到第四中间值，用第二寄存器中的数据作为底数、第四中间值作为指数进行幂运算并用运算结果更新第五寄存器中的数据
116：协处理器对第三寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并将运算结果存储到第一寄存器中
117：协处理器用第六寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新第三寄存器中的数据
118：协处理器对第四寄存器中的数据与第三寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据
119：协处理器对第五寄存器中的数据进行逆元计算并用计算结果更新第五寄存器中的数据
120：协处理器用第一预设值作为底数进行2次幂运算得到第五中间值，用第六寄存器中的数据作为底数、第五中间值作为指数进行幂运算并用运算结果更新第三寄存器中的数据

图2

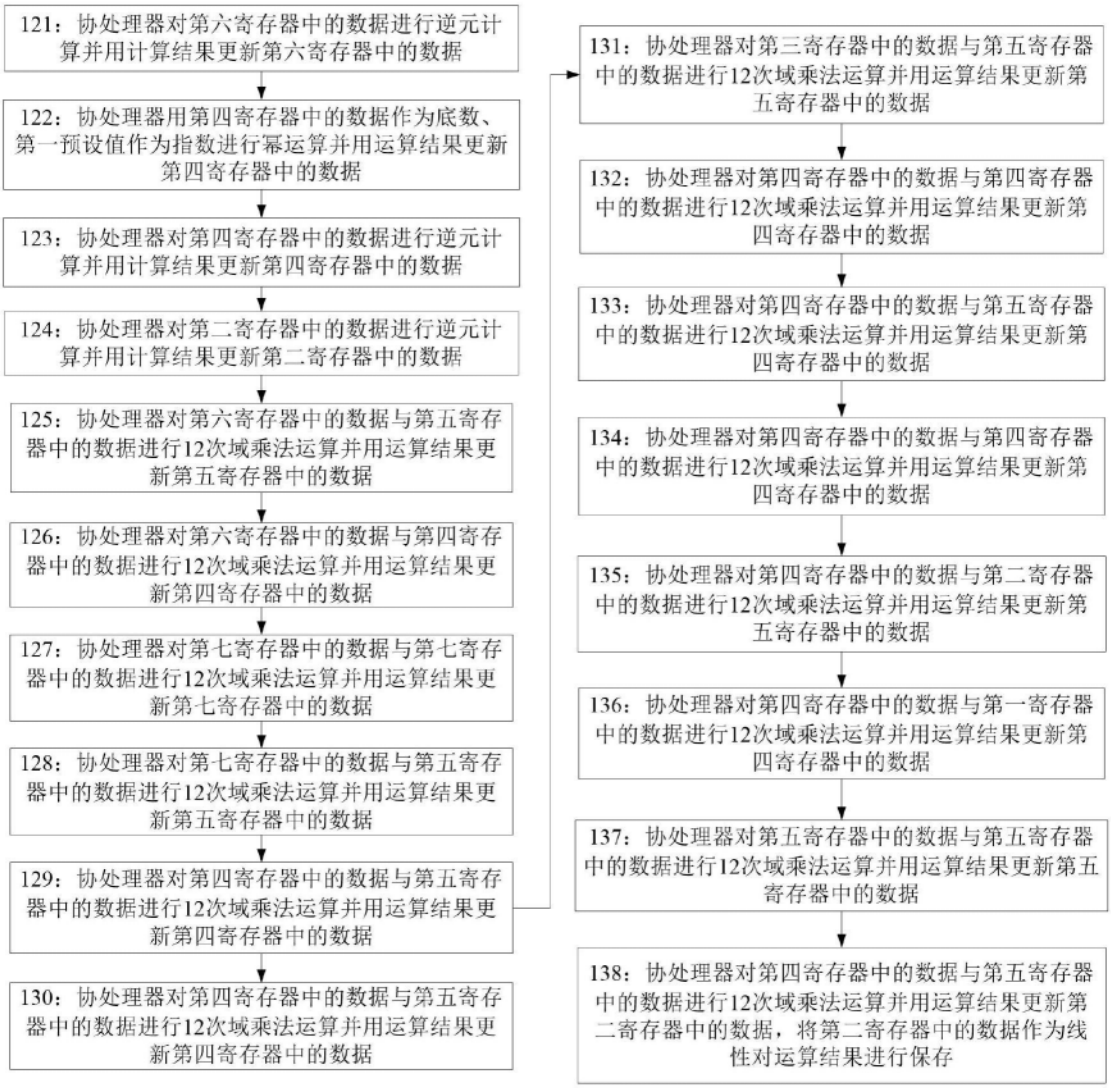

121：协处理器对第六寄存器中的数据进行逆元计算并用计算结果更新第六寄存器中的数据
122：协处理器用第四寄存器中的数据作为底数、第一预设值作为指数进行幂运算并用运算结果更新第四寄存器中的数据
123：协处理器对第四寄存器中的数据进行逆元计算并用计算结果更新第四寄存器中的数据
124：协处理器对第二寄存器中的数据进行逆元计算并用计算结果更新第二寄存器中的数据
125：协处理器对第六寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据
126：协处理器对第六寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据
127：协处理器对第七寄存器中的数据与第七寄存器中的数据进行12次域乘法运算并用运算结果更新第七寄存器中的数据
128：协处理器对第七寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据
129：协处理器对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据
130：协处理器对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据
131：协处理器对第三寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据
132：协处理器对第四寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据
133：协处理器对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据
134：协处理器对第四寄存器中的数据与第四寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据
135：协处理器对第四寄存器中的数据与第二寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据
136：协处理器对第四寄存器中的数据与第一寄存器中的数据进行12次域乘法运算并用运算结果更新第四寄存器中的数据
137：协处理器对第五寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第五寄存器中的数据
138：协处理器对第四寄存器中的数据与第五寄存器中的数据进行12次域乘法运算并用运算结果更新第二寄存器中的数据，将第二寄存器中的数据作为线性对运算结果进行保存

图3


一种在嵌入式系统中加快线性对运算的实现装置
获取分配存储模块401
计算存储更新模块402
第一计算更新模块403
第二计算更新模块404
第三计算更新模块405
第四计算更新模块406
第五计算更新模块407
第六计算更新模块408

图4