

基于明文长度的椭圆曲线密码密文构建方法

张希栋, 佟为明*, 王铁成, 金显吉

(哈尔滨工业大学 电气工程及自动化学院, 哈尔滨 150001)

(*通信作者电子邮箱 jzzxdy@126.com)

摘要:针对存储椭圆曲线密码加密生成的密文与明文相比需要的存储空间较多的问题,提出了一种基于明文长度的构建椭圆曲线密码密文的方法。首先,该方法通过分析椭圆曲线密码加密运算流程,推导出明文椭圆曲线点的数量决定存储密文椭圆曲线点需要的存储空间。其次,该方法融合明文分割和明文组合的加密模式,建立了信息加密模型;在建立的模型中针对明文分割和明文组合信息加密模式,设计出能够生成最小数量明文椭圆曲线点的明文分割算法和明文组合算法。最后,该方法计算出存储密文椭圆曲线点需要的存储空间,并通过分析决定存储空间需求的影响因素,给出减少生成密文椭圆曲线点数量的解决途径。分析和示例计算表明,与加密单个字符方式相比,应用基于明文分割信息加密模式,存储密文椭圆曲线点占用的存储空间减少了88.2%;应用基于明文组合信息加密模式,存储密文椭圆曲线点占用的存储空间减少了90.2%。研究结果表明,提出的加密方法能够有效地减少生成密文椭圆曲线点的数量,降低存储密文椭圆曲线点对硬件存储空间的需求。

关键词:椭圆曲线密码机制;有限域算术;椭圆曲线算术;存储空间

中图分类号: TP309.7; TP391 **文献标志码:** A

Cipher texts generation method in elliptic curve cryptography based on plaintext length

ZHANG Xidong, TONG Weiming*, WANG Tiecheng, JIN Xianji

(School of Electrical Engineering and Automation, Harbin Institute of Technology, Harbin Heilongjiang 150001, China)

Abstract: Since the space for saving cipher texts is more than that for saving plaintexts in elliptic curve cryptography encrypting process, a method of generating cipher texts which utilized elliptic curve cryptography based on plaintext length was proposed. Firstly, by analyzing encrypting operation process of elliptic curve encryption, it was deduced that the space for cipher texts of elliptic curve points was decided by the number of plaintexts in elliptic curve points. Secondly, by fusing the encrypting patterns based on segmentation and combination plaintexts, an encrypting model was constructed, and plaintext segmentation algorithm and plaintext combination algorithm were put forward to generate the minimum number of elliptic curve points. Finally, the demanded space for saving cipher texts in elliptic curve points was calculated, and the solutions for reducing the number of cipher texts in elliptic curve points were given. By the analysis and calculation, it is shown that the space of cipher text elliptic curve points decreases 88.2% by segmentation plaintexts and decreases 90.2% by combination plaintexts. The results show the method can decrease the number of cipher texts in elliptic curve points and the storage space demand for hardware.

Key words: elliptic curve cryptography; finite field arithmetic; elliptic curve arithmetic; storage space

0 引言

在信息安全技术领域,椭圆曲线密码机制(Elliptic Curve Cryptography, ECC)具有较强的单位数据安全性,即ECC通过选取相对长度较小的密钥,具有较强的加密安全性^[1-2],并且计算ECC的数学基础主要为基于有限域算术运算,容易通过计算机的硬件和软件计算完成^[3-4],因此ECC已成为国内外研究人员在该领域研究的热点问题^[5-6]。

在椭圆曲线密码加密机制中,需要使用明文嵌入椭圆曲线算法^[7],将明文映射为椭圆曲线上的点,再对映射到椭圆曲线上的点进行椭圆曲线算术运算,产生新的椭圆曲线点作

为密文^[8]。在椭圆曲线密码加密系统中,如何将明文嵌入到椭圆曲线中是加密信息要解决的首要问题。目前有相关文献对此进行研究,主要包括设计和改进明文嵌入椭圆曲线算法等内容。如文献[8]主要研究了明文嵌入椭圆曲线算法的设计和运算过程,将每个明文字符分别映射为椭圆曲线上的点;文献[9-10]主要研究了明文嵌入椭圆曲线的改进算法及计算方法。

在上述研究明文嵌入椭圆曲线算法的文献中,文献[8]的研究结果是将整个明文字段内的字符分别映射成椭圆曲线上的点,将导致加密生成的密文数量较多。在文献[9-10]的相关研究中,研究人员未考虑两种情形:1)要加密的明文

收稿日期:2015-05-05;修回日期:2015-06-25。 基金项目:国家自然科学基金资助项目(51077015)。

作者简介:张希栋(1971-),男,辽宁凌海人,高级工程师,博士研究生,主要研究方向:电力系统通信、信息安全; 佟为明(1964-),男,黑龙江牡丹江人,教授,博士生导师,博士,主要研究方向:电力系统通信、现场总线、信息安全、工业控制网络安全; 王铁成(1954-),男,黑龙江哈尔滨人,教授,博士生导师,博士,主要研究方向:电机与电器、电机驱动控制; 金显吉(1982-),男,辽宁朝阳人,博士,主要研究方向:电力系统网络通信、集成系统信息安全。

字段数量较多;2)计算中表示明文的数较大,超出有限域计算范围。在上述两种情形下,如何将明文映射成较少数量的椭圆曲线点,控制生成的密文数量,是应用椭圆曲线密码技术完成信息加密过程要解决的重要问题。为此,本文通过分析明文嵌入椭圆曲线算法,研究基于明文长度的信息加密模式,提出能够降低明文嵌入为椭圆曲线点数量的加密信息方法,减少生成密文椭圆曲线点的数量,以降低存储密文对系统硬件资源的占用。

1 椭圆曲线密码加密运算分析

1.1 素数域椭圆曲线

椭圆曲线密码加密主要基于有限域椭圆曲线上点的算术运算完成。以素数域为例,计算用的椭圆曲线由式(1)~(2)^[11]给出。

设 p 为素数,模 p 的全体余数集合 $\{0,1,\dots,(p-1)\}$ 关于模 p 的加法和乘法构成一个 p 阶素数有限域,用 F_p 表示。定义在素数域 F_p 上的椭圆曲线^[11]由式(1)确定的曲线给出:

$$y^2 = x^3 + ax + b \quad (1)$$

其中: $a, b \in F_p, (4a^3 + 27b^2) \bmod (p) \neq 0, x, y \in F_p$ 。

满足式(1)的数对 (x, y) 为式(1)确定的曲线上的点,同时规定存在一个无穷远点 ∞ 也是式(1)确定的曲线上的点^[11]。因此,素数域 F_p 上的椭圆曲线为式(1)确定的曲线上的点的集合 $E(F_p)$:

$$E(F_p) = \{(x, y) \in F_p \cup \infty\} \quad (2)$$

1.2 加密计算流程

椭圆曲线密码加密计算的运算过程主要包括两个层次:1)对明文进行有限域算术运算,将明文映射为有限域椭圆曲线上的点,即为明文嵌入素数域椭圆曲线算术运算;2)在椭圆曲线上,应用椭圆曲线加密算法,对表示明文的点进行椭圆曲线算术运算生成密文,即为素数域椭圆曲线点的算术运算。依据上述椭圆曲线密码加密算术运算层次,本文中将明文嵌入为椭圆曲线上的点规定为明文椭圆曲线点;将椭圆曲线上由椭圆曲线密码加密生成并隐含明文消息的密文对应的点规定为密文椭圆曲线点。

1) 明文嵌入素数域椭圆曲线算术运算。

计算明文嵌入为素数域椭圆曲线上的点,实质上是基于明文的素数域算术运算。计算明文嵌入椭圆曲线的算法主要有确定性算法和概率算法两种,其中明文嵌入椭圆曲线概率算法应用较为普遍,具有普适性^[9],最典型的概率算法是Koblitz算法^[12]。基于Koblitz概率算法的明文嵌入素数域椭圆曲线的主要计算流程为:

①将明文 m 用数 w_m 表示, w_m 的数值包括 $w_m \leq p-1$ 或 $w_m \geq p$ 两种情形之一。

②若 $w_m \leq p-1$,选择正整数 k, j ,且满足条件 $0 \leq j \leq k-1$ 和 $kw_m + j \in F_p$ 。

③对每个 j ,通过式(3)计算 x_j ,并将其代入式(1),直至计算出 $E(F_p)$ 上的第一个点 P_{kw_m+j} ,即为明文 m 嵌入在 $E(F_p)$ 上的点。

$$x_j = kw_m + j \quad (3)$$

④在解密计算过程,应用椭圆曲线上明文 m 对应的明文椭圆曲线点坐标 x_j ,计算明文 w_m :

$$w_m = \lfloor x_j/k \rfloor \quad (4)$$

其中: $\lfloor x_j/k \rfloor$ 为计算 x_j/k 的底函数。

⑤若 $w_m \geq p$,则数 w_m 不在有限域 F_p 上,要将明文 m 切割成明文字段,要求表示每个明文字段的数都在有限域 F_p 上,再应用计算流程中步骤2)和3)将每个明文字段分别嵌入为椭圆曲线上的点。

在明文嵌入为椭圆曲线的计算流程中,明文 m 嵌入为 $E(F_p)$ 上的点的数量由数 w_m 决定。在 $w_m \leq p-1$ 情形,明文 m 嵌入为 $E(F_p)$ 上一个确定的点;在 $w_m \geq p$ 情形,明文 m 嵌入为 $E(F_p)$ 上的点的数量等于将明文 m 切割成的明文字段数量。

2) 素数域椭圆曲线点的算术运算。

应用椭圆曲线密码对明文椭圆曲线点进行加密计算,主要基于Elgmal椭圆曲线密码加密机制进行^[11],如文献[13]提出的椭圆曲线混合密码算法,对明文 m 加密的主要算术运算过程为:

$$C_1 = P_m + wQ_2 \quad (5)$$

其中: C_1 为文献[9]提出的混合密码算法中计算的密文椭圆曲线点, P_m 为明文椭圆曲线点, w 为文献[13]提出的混合密码算法计算过程生成的参数, Q_2 为报文接收方的公钥。

式(5)表示的明文椭圆曲线点加密运算,与明文嵌入椭圆曲线算术运算中 $w_m \leq p-1$ 的情形相对应,通过明文 m 嵌入为椭圆曲线 $E(F_p)$ 上的一个确定的点 P_m ,建立了明文椭圆曲线点与密文椭圆曲线点的一对一的对应关系。

对于上述明文嵌入椭圆曲线算术运算中 $w_m \geq p$ 情形,将每个明文字段分别映射为椭圆曲线上的点,计算映射的密文椭圆曲线点为:

$$C_i = E_n(P_m^i, Q_2) \quad (6)$$

其中: P_m^i 表示由明文切割成的第 i 个明文字段计算出的明文椭圆曲线点, E_n 表示基于Elgmal加密机制的椭圆曲线加密算法, C_i 表示由明文椭圆曲线点 P_m^i 加密计算出的密文椭圆曲线点。同样在每个明文椭圆曲线点 P_m^i 和密文椭圆曲线点 C_i 之间建立一对一的对应关系。

式(5)~(6)给出的计算过程实质为椭圆曲线算术运算过程,加密计算出的密文为椭圆曲线上确定的点,明文椭圆曲线点的数量控制加密计算出的密文椭圆曲线点的数量。

1.3 密文存储空间

加密计算出的密文椭圆曲线点以坐标的形式存储在硬件内。本文中,将存储密文椭圆曲线点需要硬件资源提供的最小存储容量规定为密文存储空间。为了降低密文存储空间,减少存储密文椭圆曲线点对硬件资源的占用,采用椭圆曲线点压缩方法存储密文椭圆曲线点^[14]。如密文椭圆曲线点 C_1 用坐标表示为 (x', y') ,压缩过程为:

$$\text{Point-Compress}(C_1) = (x', y' \bmod 2) \quad (7)$$

其中: $\text{Point-Compress}(C_1)$ 为文献[14]给出的点压缩运算函数。

压缩密文由密文椭圆曲线点 C_1 的坐标 x' 和坐标 y' 的最低有效位表示,用二进制数形式表示为 $x'_{l'-2} \dots x'_1 x'_0 y'_0$,其中 l' 为压缩后密文的二进制位数:

$$l' = \lceil \lg x' \rceil + 1 \quad (8)$$

其中: $\lceil \lg x' \rceil$ 为计算 $\lg x'$ 的顶函数,用于计算 x' 的二进制位数。

在素数域 F_p 上, x' 最大值为 $p-1$,由此计算压缩密文的

最大二进制位数 l'_{\max} :

$$l'_{\max} = \lceil \lg(p-1) \rceil + 1 \quad (9)$$

依据式(9),在硬件内存储单个密文椭圆曲线点,要求硬件资源提供的密文存储空间至少能够存储 l'_{\max} 位的信息量,因此存储单个密文椭圆曲线点需要的密文存储空间由式(10)给出。

$$M_c = \lceil l'_{\max}/8 \rceil = \lceil (\lceil \lg(p-1) \rceil + 1)/8 \rceil \quad (10)$$

其中: M_c 表示密文存储空间,单位为 B。

根据式(10)给出的密文存储空间计算结果,在硬件内存储单个密文椭圆曲线点,需要的密文存储空间由椭圆曲线点压缩后密文的最大二进制位数 l'_{\max} 决定。

2 加密方法的提出

2.1 加密模型构建

通过分析椭圆曲线密码加密运算流程,降低生成的密文椭圆曲线点数量,能够减少存储密文椭圆曲线点占用的密文存储空间。为此,本文提出构建椭圆曲线密码信息加密模型。本文中,将椭圆曲线密码加密过程中依据需要加密明文的二进制位数大小,生成最低数量密文椭圆曲线点的实施模式规定为椭圆曲线密码信息加密模式。提出的椭圆曲线密码信息加密模型包括两种信息加密模式:

1) 要加密的明文为单个明文字段,在 $w_m \leq p-1$ 时,直接应用明文嵌入椭圆曲线算法,将明文映射为椭圆曲线上一个确定的点;在 $w_m \geq p$ 时,采用合适的方式分割明文,使计算生成的密文椭圆曲线点数量最少,即为基于明文分割的信息加密模式。

2) 要加密的明文包含多个明文字段,采用合适的方式组合明文,同样使计算生成的密文椭圆曲线点数量最少,即为基于明文组合的信息加密模式。

基于明文分割的信息加密模式由图1(a)给出,基于明文组合的信息加密模式由图1(b)给出。

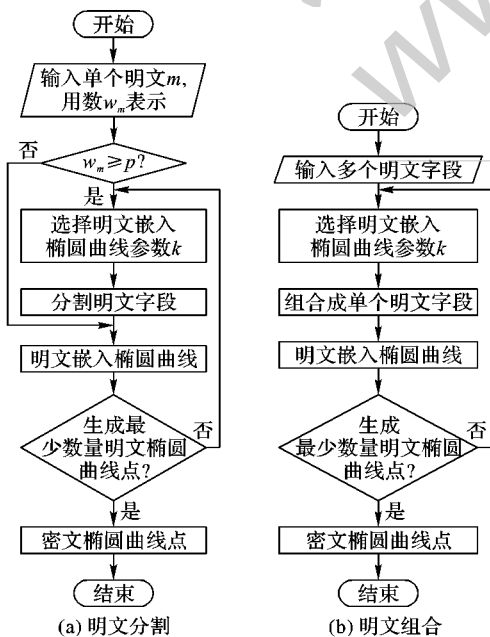


图1 基于明文分割和明文组合椭圆曲线密码信息加密模式

基于明文分割/组合的信息加密模式主要包括三个层次的计算环节: 1) 选择明文嵌入椭圆曲线参数; 2) 分割/组合

明文字段,生成明文椭圆曲线点; 3) 计算出密文椭圆曲线点。其中,如何选择合适的明文嵌入椭圆曲线参数,使通过分割明文和组合明文后生成的明文椭圆曲线点的数量最小,是上述信息加密模式要解决的关键问题,因此有必要设计一种能够解决该问题的最小数量明文椭圆曲线点生成算法。

2.2 算法设计

2.2.1 明文分割算法

明文分割算法为在基于明文分割椭圆曲线密码信息加密模式下能够生成最小数量明文椭圆曲线点的解决方法,对应加密单个明文字段的情形,相当于明文嵌入椭圆曲线算术运算中数 $w_m \geq p$ 的场景,算法运算流程如下:

1) 依据数 w_m 的二进制位数分割,计算出分割后的明文字段数 n' :

$$n' = \lceil \lg w_m \rceil / \lceil \lg w' \rceil \quad (11)$$

其中: $\lceil \lg w_m \rceil$ 为计算数 w_m 的二进制位数的顶函数, $\lceil \lg w' \rceil$ 用于计算分割的单个明文字段对应的数 w' 的二进制位数。

2) 确定分割的单个明文字段嵌入椭圆曲线要满足的条件,由式(12)~(13)给出,其中式(13)为嵌入椭圆曲线过程数 kw' 的二进制位数要满足的条件。

$$kw' \leq p-1 \quad (12)$$

$$\lceil \lg kw' \rceil \leq \lceil \lg(p-1) \rceil \quad (13)$$

其中: $\lceil \lg(p-1) \rceil$ 为数 $p-1$ 的二进制位数, $\lceil \lg kw' \rceil$ 为数 kw' 的二进制位数:

$$\lceil \lg kw' \rceil = \lceil \lg k \rceil + \lceil \lg w' \rceil - 1 \quad (14)$$

其中: $\lceil \lg k \rceil$ 为数 k 的二进制位数。

3) 由式(11)、式(13)和式(14)计算出分割后的明文字段最小数量 n'_{\min} :

$$n'_{\min} = \lceil \lceil \lg w_m \rceil / (\lceil \lg(p-1) \rceil - \lceil \lg k \rceil + 1) \rceil \quad (15)$$

2.2.2 明文组合算法

明文组合算法为在基于明文组合椭圆曲线密码信息加密模式下能够生成最小数量明文椭圆曲线点的解决方法,对应加密多个不同种类明文字段的情形,采用明文字段组合方式,如要加密的明文字段数量为 n'' ,算法流程如下:

1) 计算个 n'' 明文字段的总长度 l'' :

$$l'' = \sum_{i=1}^{n''} \lceil \lg w_i \rceil \quad (16)$$

其中: $\lceil \lg w_i \rceil$ 为第 i 个字段的二进制位数。

2) 计算由明文字段组合方式构成单个字段的二进制位数。

首先,使用字符级联的方式构成明文字段。如 j 个明文字段能够通过字符级联的方式构成一个明文字段,用表达式(17)表示:

$$m_j \leftarrow m_j^1 \parallel m_j^2 \parallel \cdots \parallel m_j^{i'} \parallel \cdots \parallel m_j^j \quad (17)$$

其中: “ \parallel ” 为字符串级联符号, $m_j^{i'}$ 为第 i' 个明文字段, m_j 为 j 个明文字段级联后生成的一个明文字段。

其次,计算组合成的单个明文字段长度要满足的条件,由式(18)~(19)给出:

$$\lceil \lg kw_j^{i'} \rceil = \lceil \lg k \rceil + \lceil \lg w_j^{i'} \rceil - 1 \quad (18)$$

$$\lceil \lg kw_j^{i'} \rceil \leq \lceil \lg(p-1) \rceil \quad (19)$$

其中数 $w_j^{i'}$ 表示明文字段 m_j 。

最后,计算组合成的单个明文字段最大长度 l''_{\max} :

$$l''_{\max} = \lceil \lg(p-1) \rceil - \lceil \lg k \rceil + 1 \quad (20)$$

3) 计算组合后生成明文字段的最小数量,由式(21)给出。

$$n''_{\min} = \lceil l''/l''_{\max} \rceil = \left\lceil \frac{\sum_{i=1}^{n''} \lceil \lg w_i \rceil}{\lceil \lg(p-1) \rceil - \lceil \lg k \rceil + 1} \right\rceil \quad (21)$$

由上述计算得出,在基于明文分割和明文组合算法的信息加密模式下,能够确定出生成明文椭圆曲线点的最小数量。

2.3 密文存储空间计算示例

2.3.1 计算依据

由于密文椭圆曲线点与明文椭圆曲线点存在一对一的对应关系,通过计算生成的明文椭圆曲线点的数量,确定生成的密文椭圆曲线点的数量,因而能够计算出存储密文椭圆曲线点需要的密文存储空间。依据明文椭圆曲线点的数量,在基于明文分割的信息加密模式下,存储密文椭圆曲线点需要的最小密文存储空间 M'_c 由式(22)给出;在基于明文组合的加密模式下,存储密文椭圆曲线点需要的最小密文存储空间 M''_c 由式(23)给出。

$$M'_c = M_c n'_{\min} \quad (22)$$

$$M''_c = M_c n''_{\min} \quad (23)$$

2.3.2 计算示例

为验证提出的信息加密模式在节省占用硬件存储空间方面的效果,对比文献[8]中分别加密单个明文字符的信息加密模式,应用示例计算密文存储空间。

计算示例使用的输入参数包括:1)使用美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)推荐的素数域 F_p 上的随机椭圆曲线 P-192,素数域 F_p 的阶 p 为 $2^{192} - 2^{64} - 1$;2)基于明文分割加密模式使用的单个明文字段为一个字符串,字符串长度为 32 B;3)基于明文组合加密模式使用 20 个字符串,每个字符串对应一个明文字段,每个字符串长度为 32 B;4)两种信息加密模式使用的明文嵌入椭圆曲线参数 k 取值为 1024。

与文献[4]中分别加密单个明文字符的加密模式相比,依据式(22)计算基于明文分割加密模式下的密文存储空间,计算结果由表1给出;再依据式(23)计算基于明文组合加密模式下的密文存储空间,计算结果如表2所示。

表1 加密单个明文字符与明文分割加密模式需要的密文存储空间

模式	字符串数量	单个字符串长度/B	单个密文椭圆曲线点占用存储空间/B	密文椭圆曲线点数量	密文存储空间/B
加密单个字符模式	1	32	25	17	425
明文分割加密模式	1	32	25	2	50

表2 加密单个明文字符与明文组合加密模式需要的密文存储空间

模式	字符串数量	单个字符串长度/B	单个密文椭圆曲线点占用存储空间/B	密文椭圆曲线点数量	密文存储空间/B
加密单个字符模式	20	32	25	41	1025
明文组合加密模式	20	32	25	4	100

3 结果分析

1) 明文嵌入椭圆曲线参数影响密文椭圆曲线点生成数量。

在基于明文分割的信息加密模式中,由式(15)和式(22)得出,明文嵌入椭圆曲线参数 k 的二进制位数 $\lceil \lg k \rceil$ 直接决定分割明文生成的最小明文椭圆曲线点数量,控制生成的密文椭圆曲线点的数量。明文分割信息加密模式通过减少参数 k 的二进制位数 $\lceil \lg k \rceil$,能够降低在存储密文椭圆曲线点占用的密文存储空间。

在基于明文组合的信息加密模式中,由式(21)和式(23)得出,参数 k 的二进制位数 $\lceil \lg k \rceil$ 直接控制组合明文生成的最小明文椭圆曲线点数量,决定生成的密文椭圆曲线点的数量。同样通过减少参数 k 的二进制位数 $\lceil \lg k \rceil$,明文组合信息加密模式能够降低存储密文椭圆曲线点需要的密文存储空间。

因此,在上述信息加密模式中,选择具有较少二进制位数的参数 k ,能够直接增加通过明文组合生成的单个明文字段的二进制位数,减少最终计算生成的密文椭圆曲线点数量,降低存储密文椭圆曲线点对硬件资源存储空间的需求。

2) 两种信息加密模式影响最小密文存储空间需求。

由表1计算结果得出,应用基于明文分割信息加密模式加密单个明文字段,需要的密文存储空间与文献[4]采用的加密模式相比减少 88.2%。由表2计算结果得出,与文献[4]

采用的加密模式相比,应用基于明文组合信息加密模式加密多个明文字段,需要的密文存储空间减少 90.2%。因此,提出的信息加密模式能够明显节省密文存储空间。

4 结语

基于上述分析和计算结果,提出的椭圆曲线密码加密方法与文献[4]加密方式相比,能够明显地减少椭圆曲线密码加密生成的密文椭圆曲线点数量,节省密文存储空间;提出的椭圆曲线密码信息加密模式,通过选取适当的明文嵌入素数域椭圆曲线参数 k ,减少参数 k 的二进制位数 $\lceil \lg k \rceil$,能够进一步减少存储密文椭圆曲线点占用的硬件资源。

此外,本项目提出的信息加密方法研究内容中未涉及计算效率方面的问题,在后续研究中对此将展开深入分析和研究。

参考文献:

- [1] WANG C. A research on the securities of elliptic curve cryptosystems [D]. Wuhan: Wuhan University, 2002: 46-52. (汪朝晖. 椭圆曲线密码的安全性研究[D]. 武汉: 武汉大学, 2002: 46-52.)
- [2] WANG Z, CHEN J, TU H, et al. Efficient implementation of elliptic curve cryptosystem over prime fields [J]. Journal of Wuhan University: Natural Science Edition, 2004, 50(3): 335-338. (汪朝晖, 陈建华, 涂航, 等. 素域上椭圆曲线密码的高效实现[J]. 武汉大学学报: 理学版, 2004, 50(3): 335-338.)

(下转第 2876 页)

- [9] ALI A, LUDWIG S, RAN O F. A cognitive trust-based approach for Web service discovery and selection[C]// Proceedings of the 3rd European Conference on Web Services. New York: ACM Press, 2005: 38–49.
- [10] BILLHARDT H, HERMOSO R, OSSOWSKI S. Trust-based service provider selection in open environments[C]// Proceedings of the 22nd Annual ACM Symposium on Applied Computing. New York: ACM Press, 2007: 1375–1380.
- [11] JIE Z, ROBIN C. Trusting advice from other buyers in e-marketplaces: the problem of unfair ratings[C]// Proceedings of the 8th International Conference on Electronic Commerce. New York: ACM Press, 2006: 225–234.
- [12] SHENG G, WEN T, GUO Q, *et al.* Trustworthy Web service recommendation based on collaborative filtering[J]. Journal of Northeastern University: Natural Science, 2013, 34(6): 806–809. (盛国军, 温涛, 郭权, 等. 基于协同过滤的可信 Web 服务推荐[J]. 东北大学学报: 自然科学版, 2013, 34(6): 806–809.)
- [13] ZHANG P, CHEN E, LI B. Web services trust computation based on social network dynamic feedback[J]. Pattern Recognition and Artificial Intelligence, 2013, 26(4): 337–343. (张佩云, 陈恩红, 李波. 基于社会网络动态反馈的 Web 服务信任度计算[J]. 模式识别与人工智能, 2013, 26(4): 337–343.)
- [14] LONG J, YUAN X, GUI W. A policy for the trusted QoS evaluation and service selection with environment aware[J]. Chinese Journal of Electronics, 2012, 40(6): 1133–1140. (龙军, 袁鑫攀, 桂卫华. 基于环境感知的可信 QoS 评价与服务选取策略[J]. 电子学报, 2012, 40(6): 1133–1140)
- [15] GOLBECK J. Generating predictive movie recommendations from trust in social networks[C]// Proceedings of the 4th International Conference on Trust Management. Berlin: Springer-Verlag, 2006: 93–104.
- [16] SENSOY M, YOLUM P. Ontology-based service representation and selection[J]. IEEE Transactions on Knowledge and Data Engineering, 2007, 19(8): 1102–1115.
- [17] WANG Y, VASSILEVA J. A review on trust and reputation for Web service selection[C]// Proceedings of 27th International Conference on Distributed Computing Systems Workshops. Piscataway: IEEE Press, 2007: 25–29.
- [18] LIU Y, ZHENG X, CHEN D. Trustworthy services discovery based on trust and recommendation relationships[J]. Systems Engineering—Theory and Practice, 2012, 32(12): 2789–2795. (刘迎春, 郑小林, 陈德人. 基于信任和推荐关系的可信服务发现[J]. 系统工程理论与实践, 2012, 32(12): 2789–2795.)
- [19] LIU X, GUI W, PAN D, *et al.* A method of QoS trustworthiness evaluation based on D-S evidence theory[J]. Journal of Harbin Institute of Technology, 2013, 45(3): 96–101. (刘昕民, 桂卫华, 潘迪宏, 等. 一种基于 D-S 证据理论的 QoS 可信度评估方法[J]. 哈尔滨工业大学学报, 2013, 45(3): 96–101.)
- [20] JOSANG A, ISMAIL R, BOYD C. A survey of trust and reputation systems for online service provision[J]. Decision Support Systems, 2007, 43(2): 618–644.
- [21] XU F, LYU J. Reputation-based recommender discovery approach for service selection[J]. Journal of Software, 2010, 21(2): 388–400. (徐峰, 吕建. 面向可信服务选取的基于声誉的推荐者发现方法[J]. 软件学报, 2010, 21(2): 388–400.)

(上接第 2866 页)

- [3] SHEN C, ZHANG H, FENG D, *et al.* Overview of information security [J]. Science in China, Series E: Information Science, 2007, 37(2): 129–150. (沈昌祥, 张焕国, 冯登国, 等. 信息安全综述[J]. 中国科学, E 辑: 信息科学, 2007, 37(2): 129–150.)
- [4] BATINA L, BERNAORS S, PRENEEL B, *et al.* Hardware architectures for public key cryptography [J]. VLSI Journal, 2003, 34(12): 1–64.
- [5] BATINA S, PRENEEL L, VANDEWALLE B, *et al.* Hardware implementation of an elliptic curve processor over $GF(p)$ [C]// ASPAC 2003: Proceedings of the 14th IEEE International Conference on Application—Specific Systems, Architectures and Processors. Piscataway: IEEE Press, 2003: 433–443.
- [6] ZHANG L, SHEN J, ZHAO L. Security enhanced elliptic curve cryptosystem approach [J]. Journal of Xi'an Jiaotong University, 2001, 35(10): 1038–1042. (张龙军, 沈钧毅, 赵霖. 椭圆曲线密码体制安全性研究[J]. 西安交通大学学报, 2001, 35(10): 1038–1042.)
- [7] LIU F, ZHANG J. An algorithm of plaintext embedding in elliptic curve [J]. Journal of Jinan University: Natural Science, 2005, 19(4): 333–334. (刘峰, 张建中. 一种明文嵌入到椭圆曲线上的混合算法[J]. 济南大学学报: 自然科学版, 2005, 19(4): 333–334.)
- [8] ZHANG J. Design and implementation of plaintext embedding in elliptic curve cryptosystem [J]. Journal of Zhengzhou University of Light Industry: Natural Science, 2009, 24(6): 97–99. (张静. 椭圆曲线密码系统中明文嵌入算法的设计与实现[J]. 郑州轻工业学院学报: 自然科学版, 2009, 24(6): 97–99.)
- [9] LI G. Research on plaintext embedment in elliptic curves [J]. Journal of Jiangxi Normal University: Natural Sciences, 2007, 31(2): 127–130. (李国敬. 椭圆曲线中明文嵌入问题研究[J]. 江西师范大学学报: 自然科学版, 2007, 31(2): 127–130.)
- [10] HOU A, GAO B, XIN X. An improved algorithm and its implementation for the embedding of plaintext into elliptic curve [J]. Computer Application and Software, 2008, 25(7): 58–59. (侯爱琴, 高宝建, 辛小龙. 明文嵌入椭圆曲线的改进算法及实现[J]. 计算机应用与软件, 2008, 25(7): 58–59.)
- [11] HANKERSON D, MENEZES A, VANSTONE S. Guide to elliptic curve cryptography [M]. ZHANG H. translated. Beijing: Publishing House of Electronics Industry, 2005: 71–73. (HANKERSON D, MENEZES A, VANSTONE S. 椭圆曲线密码学导论[M]. 张焕国, 译. 北京: 电子工业出版社, 2005: 71–73.)
- [12] KOBLITZ N. A course in number theory and cryptography [M]. 3rd ed. Berlin: Springer-Verlag, 1994: 79–180.
- [13] TONG W, ZHANG X, LI Z, *et al.* A hybrid cryptography algorithm for data concentrator communication message based on elliptic curve cryptography [J]. Automation of Electric Power Systems, 2014, 38(4): 86–91. (佟为明, 张希栋, 李中伟, 等. 基于椭圆曲线密码的数据集中器通信报文混合密码算法[J]. 电力系统自动化, 2014, 38(4): 86–91.)
- [14] STINSON D R. Cryptography theory and practice [M]. 3rd ed. FENG D, translated. Beijing: Publishing House of Electronics Industry, 2009: 206–207. (STINSON D R. 密码学原理与实践[M]. 3 版. 冯登国, 译. 北京: 电子工业出版社, 2009: 206–207.)