基于国密 SM2 的高效范围证明协议

林 超 黄欣沂 何德彪
(福建师范大学数学与信息学院 福州 350007)
(武汉大学国家网络安全学院 武汉 430072)

摘 要 在范围证明这类特殊的零知识证明协议中,证明者无需提供具体元素信息即可向验证者证明某一承诺的元素在指定集合内. 范围证明已被广泛应用于区块链、匿名证书、电子现金、群/环签名等需要身份/数据隐私保护的场景. 范围证明协议的设计方法包括平方分解(Square Decomposition)、签名基(Signature-based)、内积(Inner-product Argument)等,其中使用较为广泛的是 Camenisch 等在 ASIACRYPT 2008 会议上提出的签名基方法. 然而,Camenisch 等提出的范围证明协议不仅需要高耗时的双线性对运算,还涉及繁琐的证书管理,实用性还有待提高. 虽然何德彪等(专利申请公布号:CN110311776A)利用国密 SM9 数字签名算法设计新的协议,避免了证书管理,但仍需要双线性对运算,所以协议的计算开销还较高. 为了进一步减少计算量,丰富国产密码的应用,本文采用签名基方法,利用基于国密 SM2 的标识数字签名算法设计新的集合关系证明协议,有效解决证书管理和双线性对开销问题,在此基础上构造新的数值范围证明协议,支持更大范围的零知识证明. 为了证明所设计协议的安全性,本文先证明基于国密 SM2 的标识数字签名算法在自适应选择消息和身份攻击下具有存在不可伪造性(EUF-CMA-ID-A),在此基础上证明所设计协议满足完备性、可靠性和诚实验证者零知识性. 与 Camenisch 等和何德彪等提出的协议相比,在相同优化参数情况下,本文协议的主要通信带宽约为 1568 字节,分别减少了 41.66%和 78.12%;主要计算开销约为 491.5075 毫秒,分别减少了 85.93%和 85.85%. 这说明了本文设计的协议具有更强的实用性,更能满足前述场景的身份/数据隐私保护与有效性验证需求.

关键词 范围证明;零知识证明;Σ 协议;基于 SM2 的标识数字签名;证书管理
中图法分类号 TP311 **DOI 号** 10.11897/SP.J.1016.2022.00148

Efficient Range Proof Protocols Based on Chinese Cryptographic SM2

LIN Chao HUANG Xin-Yi HE De-Biao
(*College of Mathematics and Informatics, Fujian Normal University, Fuzhou* 350117)
(*School of Cyber Science and Engineering, Wuhan University, Wuhan* 430072)

Abstract Range proof is a special type of zero-knowledge proofs, among which a prover can prove to a verifier that the element of a commitment is within a specified range, but the prover does not need to tell the verifier the concrete information of this hiding element. Due to this special property, the range proof protocols have been widely applied in various scenarios especially those requiring security requirements of identity or data privacy protection (e.g. blockchain, anonymous certificates, electronic cash, group or ring signatures). Correspondingly, there are also many design methods of range proof protocols have been proposed recently, such as square decomposition method, signature-based method, inner-product argument method, and so forth, among which the signature-based method (proposed by Camenisch et al. in the conference of ASIACRYPT 2008) is one of the most widely used methods at present. However, the range proof

收稿日期:2020-11-18;在线发布日期:2021-04-25. 本课题得到国家重点研究开发计划项目(No. 2017YFB0802500)、国家自然科学基金项目(62032005, 61872089, 61932016, 61972294, 61772377, 61841701)、湖北省自然科学基金(2017CFA007)、福建省自然科学基金(2020J02016)资助. **林 超**,博士,讲师,主要研究领域为应用密码学、区块链隐私保护. E-mail:linchao91@fjnu.edu.cn. **黄欣沂(通信作者)**,博士,教授,主要研究领域为应用密码学、网络安全. Email:xyhuang81@gmail.com. **何德彪**,博士,教授,主要研究领域为应用密码学、密码协议、云计算安全.

protocols proposed by Camenisch et al. not only require a high time-consuming and costly bilinear pairing computation, but also involve a cumbersome certificate management overhead. This means that the utility of their proposed protocols still needs to be further improved. He et al. used the Chinese cryptographic SM9 digital signature algorithm to design two novel range proof protocols without the need of certificate managements, which have been applied for a patent in China (where the patent application publication number is No. CN110311776A). Nevertheless, their proposed protocols are still involved with the bilinear pairing operation, resulting in that their proposals also require a high computational cost. To further reduce the computational cost of existing range proof protocols and also enrich the applications of Chinese cryptographic algorithms, this paper also adopts the signature-based method, but uses an identity-based digital signature algorithm (constructed from the Chinese cryptographic SM2 algorithm) instead to propose a novel set membership protocol. This design can efficiently solve the issues of certificate management and bilinear pairing overhead at the same time. Moreover, we extend our designed set membership protocol to construct a novel numerical range proof protocol, so as to support a wider numerical range of zero-knowledge proofs. Also, in order to prove the security of our proposed two protocols, we first prove the security of the adopted identity-based digital signature algorithm, that is, this signature scheme is proven owning existential unforgery against adaptively chosen message and ID attacks (abbreviated as EUF-CM-ID-A). On basic of this security proof, we then demonstrate that our proposals own the security properties of completeness, special soundness and honest-verifier zero-knowledge. In comparison with Camenisch et al.'s and He et al.'s proposed protocols and using the same optimized parameters, the main communication overhead in our protocols is only about 1568 bytes which has reduced about 41.66% and 78.12% respectively, and the main computation cost in our protocols is only about 491.5075 milliseconds, which has saved about 85.93% and 85.85% respectively. This indeed demonstrates that our proposed protocols have the stronger utility comparing to the existing signature-based range proof protocols, and hence they are more suitable for satisfying requirements of identity or data privacy protection and validity verification in the aforementioned scenarios.

Keywords　range proof; zero-knowledge proof; Σ−protocol; identity-based SM2 digital signature; credential management

1　引　言

范围证明协议是一类特殊的零知识证明协议,分为集合关系证明和数值范围证明两种[1-2]. 集合关系证明可以让证明者在不提供具体元素情况下,使验证者相信某一承诺的元素在指定集合内. 数值范围证明可以让验证者相信该元素在指定数值范围内. 这意味着,知道被承诺元素 σ 的证明者可以通过零知识证明使验证者相信 σ 属于集合 Φ 或数值范围 $[a,b]$ (a,b 为大整数). 范围证明协议已广泛应用于区块链[3-4]、匿名证书[5]、电子现金[6-7]、群/环签名[8-9]等需要身份/数据隐私保护的场景.

范围证明协议的设计方法包括平方分解(Square Decomposition)、签名基(Signature-based)、内积(Inner-product Argument)等[10],其中使用较多的是 Camenisch 等[2]提出的签名基方法. 文献[2]的协议不仅涉及高耗时的双线性对运算(1次双线性对运算在移动终端的耗时约为 32 毫秒,是椭圆曲线标量乘运算的 9 倍左右[11]),而且涉及繁琐的证书管理①虽然何德彪等[12]利用国密 SM9 数字签名算法构造的协议避免了繁琐的证书管理,且与文献[2]中的协议具有同等安全性,但仍需要双线性对运算,难以支持物联网等资源受限的分布式场

① 基于 PKI 体系的密码系统需要 CA 维护证书撤销列表,用户数量指数增加,导致工作量巨大. 设计基于标识体系的范围证明协议可以避免繁琐的证书管理,还有助于物联网等资源受限的场景应用.

景. 这些不足限制了文献[2]和[12]设计的集合关系证明协议和范围证明协议的应用.

为了进一步减少计算量,丰富国产密码的应用,本文采用签名基方法,基于国密 SM2 设计新的集合关系证明协议,并在此基础上构造新的数值范围证明协议. 其中,协议所采用的签名算法是基于国密 SM2 的标识数字签名算法. 由于该标识签名算法的安全性目前尚未得到形式化安全性证明,所以在描述协议设计过程之后,本文先证明该标识数字签名算法满足抗自适应选择消息和身份攻击的存在不可伪造性(EUF-CM-ID-A),再证明本文设计协议的安全性. 由安全性证明与性能分析结果可知,本文协议不仅满足完备性、可靠性和诚实验证者零知识性,并且比文献[2]和[12]设计的协议拥有更好的性能. 在采用与文献[2]相同优化参数情况下,本文协议的主要通信开销约为 1568 字节,比文献[2]和[12]的协议分别减少 41.66%和 78.12%;主要计算开销约为 491.5075 毫秒,比文献[2]和[12]的协议分别减少 85.93%和 85.85%.

2 相关工作

1988 年,Brickell 等[1]最早提出范围证明的概念,即用户可以证明某离散对数值属于某一区间,但不泄露该值的其它信息. 虽然文献[1]设计的协议效率较高,但是只能支持比目标区间更大的范围证明,无法实现指定区间的范围证明. 为了证明电子现金支付系统中密态金额是非负的,Chan 等[13] 1998 年基于文献[1]提出安全性更高的协议. 但文献[13]的协议依赖于模数的未知性,验证者一旦知道生成元的阶数,可以利用模运算生成有效的证明,从而达到欺骗验证者的目的.

2000 年,Boudot 等[14]基于文献[13]与平方和分解方法构造了更加高效的范围证明,但仍无法支持指定区间的范围证明. 2003 年,Lipmaa[15]应用拉格朗日定理——任意正整数均可分解为 4 个整数的平方和,最早实现指定区间的范围证明. 但 Gorth 2005 年[16]指出,假如文献[15]中处理的元素形式如 $4n+1$,则通过三个整数的平方和分解方法可以得到相同结果,有效降低计算开销和通信代价. 平方和分解方法的不足是平方和分解耗时高达 $O(k^4)$(k 是元素的比特长度),远超过协议本身的执行时间[17].

签名基方法是范围证明协议的另外一类构造方法,最早是由 Camenisch 等[2] 2008 年提出的,其设计思路主要受到文献[18]中匿名认证协议的启发. 签名基方法分为初始化阶段和证明执行阶段:在初始化阶段,验证者计算集合或范围中各元素的数字签名并发送给证明者;在证明执行阶段,证明者先盲化承诺元素的数字签名,再与验证者执行 Σ 协议,在不泄露具体元素信息情况下,成功向验证者证明盲化数字签名的消息与承诺元素是相同的. 根据签名基的构造方式,Camenisch 等分别基于双线性群假设和离散对数假设构造了集合关系证明协议和数值范围证明协议. 2010 年,Chaabouni 等[19]采用新的数字分解方法实现指定区间的范围证明,可以提高文献[2]协议的效率,但该方法依赖的数字签名仍涉及双线性对运算,计算开销较大. 为了避免双线性对运算,Canard 等[20]结合 ElGamal 加密方案和明文等值判定方法替代 Boneh-Boyen 数字签名的验证计算,有效降低计算开销,但该方法仅在验证者数目小于 4 的时候有效. 何德彪等[12] 2019 年利用签名基构造方式,结合 SM9 数字签名设计新的集合关系证明协议和数值范围证明协议,有效避免繁琐的证书管理,但所设计协议仍涉及高耗时的双线性对运算,难以支持物联网等资源受限的分布式场景.

内积方法也是范围证明协议常用的构造方式. Bünz 等[21] 2018 年通过构造新的内积方法设计更加高效的范围证明协议(Bulletproofs),证明长度由线性增长降为对数级,但该方法需要消耗证明者较高的计算开销,且涉及公钥的操作数随电路大小增加而线性增加. 张凡等[22] 2020 年通过构造多项式承诺方案,结合向量积承诺方案提出效率更高的范围证明协议,但该协议需要更长的证明长度,且未解决公钥操作数线性增加的问题.

3 技术背景

本节介绍基于国密 SM2 的标识数字签名、零知识证明与 Σ 协议、集合关系证明与数值范围证明等相关基础知识的定义.

3.1 基于国密 SM2 的标识数字签名

SM2 椭圆曲线公钥密码算法是国家密码管理局颁布的椭圆曲线公钥密码算法(参见《SM2 椭圆曲线公钥密码算法》规范,国家密码管理局,2010 年 12 月[23]),算法确定了数据加密、数字签名、密钥交换等算法或协议. 基于国密 SM2 的标识数字签名算法[24]是根据 SM2 数字签名改造的标识密码算法,可以避免高耗时的双线性对运算,主要利用身份

标识生成用户私钥,其应用与管理不用依赖数字证书、证书库和密钥库,可用于身份认证、密钥交换、零知识证明等. 基于国密 SM2 的标识数字签名包括初始化、密钥解析、签名和验证 4 个算法:

初始化 (Setup):算法输入安全参数 λ,随机选取大素数 q,确定非奇异椭圆曲线 $E:y^2=x^3+ax+b(\mathrm{mod}\,q)$ ($a,b\in\mathbb{Z}_q^*$),在包含无穷远点和 E 的所有点中选取素数 n 阶循环群 $\mathbb{G}$ 和生成元 $P\in\mathbb{G}$. 随机选取 $x\in\mathbb{Z}_n^*$,计算 $P_{pub}=xP$,同时选取三个安全哈希函数:$\mathcal{H}_v:\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^v$、$\mathcal{H}_0:\{0,1\}^*\to\{0,1\}^{256}$ 和 $\mathcal{H}:\{0,1\}^*\times\{0,1\}^*\to\mathbb{Z}_n^*$. 算法输出系统主公钥 $mpk=(E,a,b,q,\mathbb{G}_1,n,P,P_{pub},\mathcal{H}_v,\mathcal{H}_0,\mathcal{H})$ 和主私钥 $msk=x$.

密钥解析 (Extract):算法输入系统主公钥 mpk、主私钥 x 和用户身份信息 ID_a,随机选取 $l\in\mathbb{Z}_n^*$,计算 $L=lP=(x_L,y_L)$、$h=\mathrm{H}(ID_a\,||\,L)$ 和 $d=l+xh(\mathrm{mod}\,n)$,算法输出用户的私钥 $sk=(L,d)$.

签名(Sign):算法输入系统主公钥 mpk、用户私钥 $sk=(L,d)$、用户身份标识 ID_a 和消息 m,计算 $Z_a=\mathcal{H}_0(ENTLA\,||\,ID_a\,||\,a\,||\,b\,||\,x_P\,||\,y_P\,||\,x_L\,||\,y_L)$ 和 $e=\mathcal{H}_v(Z_a\,||\,m)$,其中,$ENTLA$ 是 ID_a 的比特长度,(x_P,y_P) 和 (x_L,y_L) 分别是 P 和 L 的横纵坐标. 随机选取 $k\in\mathbb{Z}_n^*$,计算 $K=kP=(x_K,y_K)$ 和 $r=(e+x_K)(\mathrm{mod}\,n)$. 若 $r=0$ 或 $r+k=n$,则重新选取 k 再计算,否则计算 $s=(1+d)^{-1}(k-rd)(\mathrm{mod}\,n)$. 若 $s\neq0$,则输出消息 M 的签名 $\sigma=(L,r,s)$.

验证 (Verify):算法输入系统主公钥 mpk、用户身份信息 ID_a、消息 m 和待验证签名 $\sigma=(L,r,s)$,若 $r\notin\mathbb{Z}_n^*$,$s\notin\mathbb{Z}_n^*$,则输出 0,否则计算 $t=r+s(\mathrm{mod}\,n)$. 若 $t=0$,则输出 0,否则计算 $Z'_a=\mathcal{H}_0(ENTLA\,||\,ID_a\,||\,a\,||\,b\,||\,x_P\,||\,y_P\,||\,x_L\,||\,y_L)$、$e'=\mathcal{H}_v(Z'_a\,||\,m)$、$h'=\mathcal{H}(ID_a\,||\,L)$、$K'=sP+t(L+h'P_{pub})=(x'_K,y'_K)$ 和 $r'=(e'+x'_K)(\mathrm{mod}\,n)$. 若 $r'=r$,则输出 1,否则输出 0. 假如该算法最后输出 1,则说明签名有效,否则说明签名无效.

由于文献[24]未提供算法的形式化安全性证明,所以本文将在第 4.1 节证明该算法的安全性. 标识数字签名的标准安全模型[25-26]主要通过模拟伪造者$\mathcal{F}$和挑战者$\mathcal{C}$之间的交互游戏进行刻画,其中伪造者$\mathcal{F}$可以向挑战者$\mathcal{C}$询问以下谕言机:

$\mathcal{O}_{Setup}$:$\mathcal{C}$ 调用 Setup 算法生成参数(mpk,msk),并将 mpk 返回给$\mathcal{F}$;

$\mathcal{O}_{Extract}$:$\mathcal{C}$ 根据$\mathcal{F}$的请求身份 ID,利用主私钥 msk 运行 Extract 算法生成身份 ID 的私钥 sk,并将 sk 返回给$\mathcal{F}$;

$\mathcal{O}_{Hash}$:$\mathcal{C}$根据$\mathcal{F}$的请求数据计算哈希值,并将哈希值返回给$\mathcal{F}$;

$\mathcal{O}_{Sign}$:$\mathcal{C}$根据$\mathcal{F}$的请求身份 ID 和消息 m,利用主私钥 msk 运行 Sign 算法生成消息 m 的签名 σ,并将 σ 返回给$\mathcal{F}$.

$\mathcal{F}$自适应询问上述谕言机足够次数后输出 (ID^*,m^*,σ^*). 假如 $\mathrm{Verify}(mpk,ID^*,m^*,\sigma^*)=1$,$ID^*$ 未在 $\mathcal{O}_{Extract}$ 询问过,并且 (ID^*,m^*) 未在 $\mathcal{O}_{Sign}$ 询问过,则称$\mathcal{F}$伪造成功.

定义 1.　若$\mathcal{F}$在上述游戏中获胜的概率是可忽略的,则称标识数字签名算法在自适应选择消息和身份攻击下具有存在不可伪造性(Existential Unforgery on Adaptively Chosen Message and ID Attacks, EUF-CM-ID-A).

定义 2.　在定义 1 游戏中的 $\mathcal{O}_{Setup}$ 谕言机增加指定伪造身份 ID,并要求$\mathcal{F}$最后伪造指定 ID 的消息签名对. 若$\mathcal{F}$在修改后游戏获胜的概率是可忽略的,则称标识数字签名算法在自适应选择消息和指定身份攻击下具有存在不可伪造性(Existential Unforgery on Adaptively Chosen Message and Given ID Attacks, EUF-CM-GID-A).

3.2　零知识证明与 Σ 协议

假设交互协议 Π 包括证明者 P 和验证者 V 两个实体,P 可以让 V 相信二元关系 $R=\{(x,w)\}:\{0,1\}^*\times\{0,1\}^*$($x$ 和 w 分别指的是实例和证据),但存在错误概率 κ. 若协议 Π 满足完备性 (Completeness)①和可靠性 (Soundness)②,则称 Π 为知识证明系统 (Proof of Knowledge). 若 Π 还满足诚实验证者零知识性 (Honest-Verifier Zero-Knowledge)③,则称 Π 为交互式诚实验证者零知识证明系统[27][28]. Cramer 等[28]提出的标准技术可以将诚实验证者零知识证明系统转换成一般零知识证明系统,该技术尤其适用于 Σ 协议. 因为已有范围证明协议讨论的是诚实验证者零知识性,所以为了得到准确的分析与对比结果,本文同样讨论诚实验证者

① 完备性:对于任意的 $(x,w)\in R$,P 和 V 执行交互协议生成的证明 π 被 V 接受的概率为 1.

② 可靠性:假设恶意的证明者 P^* 能够以不可忽略的概率 ε 让 V 接受生成的证明 π^* ,则存在 PPT 的解析算法 E (称为 Extractor) 能以 $\varepsilon-\kappa$ 的概率解析得到 w^*,$s.t.$,$(x,w^*)\in R$.

③ 诚实验证者零知识性:对于任意的 $(x,w)\in\mathrm{R}$,存在 PPT 的仿真算法 S (称为 Simulator) 与 V 执行交互协议输出证明 π^*,令 P 与 V 执行交互协议输出证明 π,则 π^* 和 π 是不可区分的.

零知识性.

Σ协议[29]是一类交互式3次握手(3－move)零知识证明系统,假设证明者P和验证者V执行Σ协议得到结果(a,c,z),其中,(a,z)是证明者P利用私有证据信息w,根据V的挑战值c计算得到的证明. Σ协议满足完备性(Completeness)、特殊可靠性(Special Soundness)和特殊诚实验证者零知识性(Special Honest-Verifier Zero-Knowledge),其中,完备性是指,假设存在有效函数ϕ使得$\phi(a,a,c,z)=1$成立,则V接受(a,c,z);特殊可靠性是指,已知两组有效的(a,c,z),(a,c',z'),且$c\neq c'$,可恢复出P的证据信息w;特殊诚实验证者零知识性是指,已知V的挑战值c,存在概率多项式时间(Probabilistic polynomial time,PPT)仿真算法S可与V交互输出有效的(a,c,z),假设真实交互环境P与V输出(a',c',z'),则(a,c,z)与(a',c',z')具有不可区分性[29].

Σ协议可以通过Fiat-Shamir转换[30](安全哈希函数$\mathcal{H}$)得到非交互式实例. 同样针对上述的$R=\{(x,w)\}$,P计算a之后直接调用$c=\mathcal{H}(x,a)$得到挑战值c,再利用私有证据信息w计算得到z,最后直接将(x,a,c,z)发送给V. Fiat-Shamir转换得到的非交互式协议仍满足完备性、可靠性和零知识性[30].

3.3 集合关系证明与数值范围证明

集合关系证明是指通过零知识证明的方式证明某承诺的元素在集合内. 若定义承诺方案的生成算法、承诺算法和打开算法为Gen、Com和Open,则对于已知承诺C和集合Φ,可以将集合关系证明协议表示为$P\{(\sigma,\rho):C\leftarrow Com(\sigma;\rho)\wedge\sigma\in\Phi\}$. 其中,此类协议应用可采用任意具有完全隐藏性质的承诺方案[2-3]. 若上述集合关系证明中的集合Φ为连续的整数序列$\Phi=[\alpha,\beta]$,$\alpha,\beta\in\mathbb{N}$,则称该证明协议为数值范围证明协议.

签名基方法是一类常用的范围证明设计方法[2],包括初始化阶段和证明阶段. 在初始化阶段,验证者V计算集合Φ各元素的签名$(s_1,\ldots,s_{|\Phi|})$,并将这些签名发送给证明者P. 此后双方进入证明执行阶段,P先盲化承诺元素σ对应的签名值s_σ,再将盲化签名值发送给V;接着,P和V执行Σ协议证明盲化签名值的消息与承诺元素σ是一致的,从而完成范围证明.

4 协议设计

本节先利用基于国密SM2的标识数字签名设计新的集合关系证明协议,再扩展得到新的数值范围证明协议. 为了证明两个新设计协议的安全性,本节首先证明基于国密SM2的标识数字签名算法满足EUF-CM-ID-A,在此基础上证明所设计协议满足完备性、可靠性和诚实验证者零知识性. 虽然本节描述的两个协议均为交互式,但是它们可直接通过Fiat-Shamir转换[30]得到非交互式实例.

4.1 基于国密SM2的集合关系证明协议

本节结合基于国密SM2的标识数字签名算法提出新的集合关系证明协议(如图1所示),具体协议描述如下:

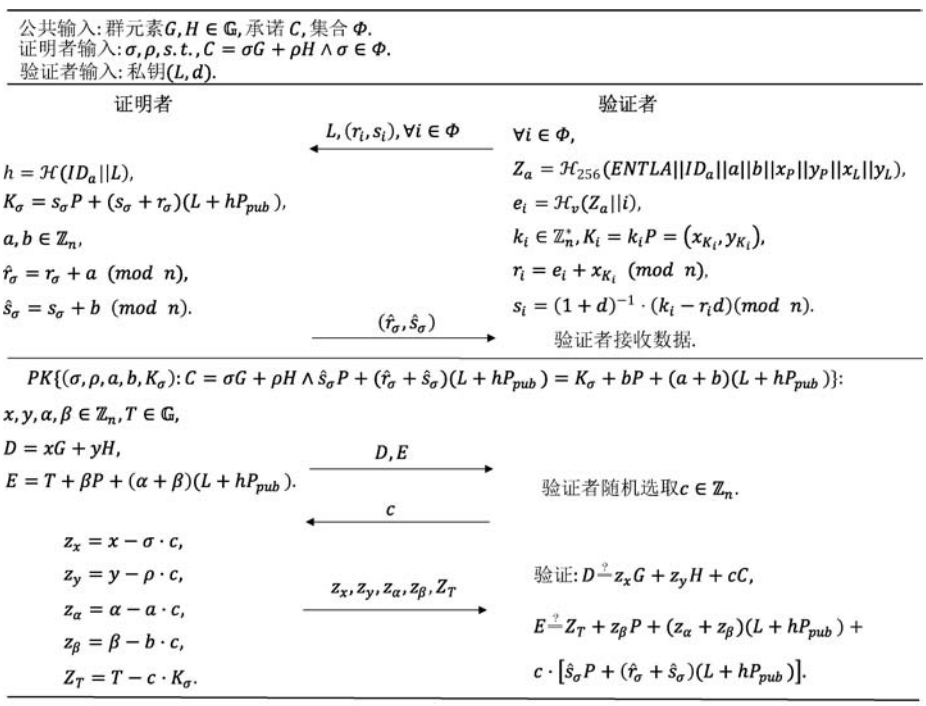

图1 基于国密SM2的集合关系证明协议设计

(1)系统建立:该阶段主要产生协议所需参数.输入安全参数 λ,随机选取大素数 q,确定非奇异椭圆曲线 $E:y^2=x^3+ax+b(mod\,q)$(其中,$a,b\in\mathbb{Z}_q^*$),在包含无穷远点的 E 所有点中选取素数 n 阶循环群 $\mathbb{G}$,并随机选取生成元 $G,H,P\in\mathbb{G}$. 接着,随机选取 $x\in\mathbb{Z}_n^*$ 并计算 $P_{pub}=xP$,同时选取三个安全哈希函数:$\mathcal{H}_v:\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^v$、$\mathcal{H}_0:\{0,1\}^*\to\{0,1\}^{256}$ 和 $\mathcal{H}:\{0,1\}^*\times\{0,1\}^*\to\mathbb{Z}_n^*$. 算法输出系统主公钥 $mpk=(E,a,b,q,\mathbb{G},n,P,P_{pub},\mathcal{H}_v,\mathcal{H}_0,\mathcal{H})$ 和主私钥 $msk=x$.

(2)初始化:该阶段产生承诺值 C 和关系集合 Φ 各个元素的基于国密的 SM2 标识签名 $(L,r_i,s_i),\forall i\in\Phi$. 具体过程如下:

1) 系统利用主公钥 mpk 和主私钥 msk 生成验证者私钥 (L,d),即随机选取 $l\in\mathbb{Z}_n^*$,计算 $L=lP=(x_L,y_L)$、$h=\mathcal{H}(ID_a\,||\,L)$ 和 $d=l+xh(mod\,n)$,并将 (L,d) 发送给验证者.

2) 证明者随机选取 $\rho\in Z_n^*$,计算承诺 $C=\sigma G+\rho H$,其中 σ 为证明者拥有的集合元素.

3) 验证者计算目标集合中 $|\Phi|$ 个元素的基于国密 SM2 标识数字签名 $(L,r_i,s_i):\forall i\in\Phi,Z_a=\mathcal{H}_0(ENTLA\,||\,ID_a\,||\,a\,||\,b\,||\,x_P\,||\,y_P\,||\,x_L\,||\,y_L)$、$e_i=\mathcal{H}_v(Z_a\,||\,i)$,并随机选取 $k_i\in\mathbb{Z}_n^*$ 计算 $K_i=k_iP=(x_{K_i},y_{K_i})$,$r_i=(e_i+x_{K_i})(mod\,n)$. 若 $r_i=0$ 或 $r_i+k_i=n$,则重新选取 k_i 再计算;否则计算 $s_i=(1+d)^{-1}(k_i-r_id)(mod\,n)$. 若 $s_i\neq0$,则输出签名 $(L,r_i,s_i),\forall i\in\Phi$.

4) 验证者将签名 $(L,r_i,s_i),\forall i\in\Phi$ 发送给证明者.

(3) 证明执行:证明者首先计算拥有元素对应签名的盲化值:假设拥有元素为 $\sigma\in\Phi$,证明者首先计算 $h=\mathcal{H}(ID_a\,||\,L)$,$K_\sigma=s_\sigma P+(s_\sigma+r_\sigma)(L+hP_{pub})$,然后随机选取 $a,b\in\mathbb{Z}_n^*$ 并计算 $\hat{r}_\sigma=r_\sigma+a$,$\hat{s}_\sigma=s_\sigma+b$. 证明者将 $(\hat{r}_\sigma,\hat{s}_\sigma)$ 发送给验证者. 接着,证明者和验证者执行 $\sum$ 协议 $PK\{(\sigma,\rho,a,b,K_\sigma):C=\sigma G+\rho H\ \wedge\ \hat{s}_\sigma P+(\hat{r}_\sigma+\hat{s}_\sigma)(L+hP_{pub})=K_\sigma+bP+(a+b)(L+hP_{pub})$,具体过程如下:

1) 证明者随机选取 $x,y,\alpha,\beta\in\mathbb{Z}_n^*,T\in\mathbb{G}$,计算中间数据 $D=xG+yH,E=T+\beta P+(\alpha+\beta)(L+hP_{pub})$,最后将 (D,E) 发送给验证者.

2) 验证者随机选取 $c\in\mathbb{Z}_n^*$,并将 c 发送给证明者.

3) 证明者先计算 $z_x=x-\sigma\cdot c,z_y=y-\rho\cdot c,z_\alpha=\alpha-a\cdot c,z_\beta=\beta-b\cdot c,Z_T=T-c\cdot K_\sigma$,再将 $(z_x,z_y,z_\alpha,z_\beta,Z_T)$ 发送给验证者.

4) 验证者验证等式 $D=z_xG+z_yH+cC$ 和 $E=Z_T+z_\beta P+(z_\alpha+z_\beta)(L+hP_{pub})+c\cdot[\hat{s}_\sigma P+(\hat{r}_\sigma+\hat{s}_\sigma)(L+hP_{pub})]$ 是否成立. 若成立,说明验证通过;否则,拒绝该证明.

下面通过两个引理证明基于国密 SM2 的标识数字签名算法满足 EUF-CM-ID-A.

引理 1. 如果存在具有自适应选择消息和身份攻击能力的 $\mathcal{F}_0$ 算法能够以时间 t_0 和概率 ε_0 成功伪造基于国密 SM2 的标识数字签名(假设 $\mathcal{F}_0$ 可成功破坏 EUF-CM-ID-A),那么存在具有自适应选择消息和指定身份攻击能力的 $\mathcal{F}_1$ 算法能够以时间 $t_1=t_0+q_Ht_H+q_Et_E+q_St_S$ 和概率 $\varepsilon_1=\varepsilon_0\cdot\left(1-\frac{1}{n}\right)\cdot\frac{1}{q_H}$ 成功伪造基于国密 SM2 的标识数字签名($\mathcal{F}_1$ 可以利用 $\mathcal{F}_0$ 成功破坏 EUF-CM-GID-A),其中 q_H,q_E,q_S 分别为 $\mathcal{F}_0$ 询问 $\mathcal{O}_H,\mathcal{O}_{Extract},\mathcal{O}_{Sign}$ 的最大次数,t_H,t_E,t_S 分别为 $\mathcal{F}_0$ 单次询问 $\mathcal{O}_H,\mathcal{O}_{Extract},\mathcal{O}_{Sign}$ 的时间,n 是循环群 $\mathbb{G}$ 的阶,并且 $\mathcal{F}_0$ 和 $\mathcal{F}_1$ 询问 $\mathcal{O}_H$、$\mathcal{O}_{\mathrm{Extract}}$ 和 $\mathcal{O}_{Sign}$ 的次数相同.

证明:已知主公钥 mpk、指定身份 ID、$\mathcal{O}_H$ 谕言机、$\mathcal{O}_{Extract}$ 谕言机和 $\mathcal{O}_{Sign}$ 谕言机,$\mathcal{F}_1$ 算法可以响应 $\mathcal{F}_0$ 算法的以下询问:

$\mathcal{O}'_{Setup}$:$\mathcal{F}_1$ 直接将 mpk 返回给 $\mathcal{F}_0$;

$\mathcal{O}'_{Extract}$:假如 $\mathcal{F}_0$ 询问的输入值为 $ID'_i=ID$,则游戏中止;否则,$\mathcal{F}_1$ 调用 $(L'_i,d'_i)=\mathcal{O}_{\mathrm{Extract}}(ID_i')$,并将 (L_i,d_i) 返回给 $\mathcal{F}_0$;

$\mathcal{O}'_H$:$\mathcal{F}_1$ 随机选取 $r\in\{1,2,\ldots,q_H\}$,令 $\mathcal{F}_0$ 和 $\mathcal{F}_1$ 询问 $\mathcal{O}_H$ 的第 i 个输入值分别为 (ID_i,L_i) 和 (ID'_i,L_i'),则 $ID'_i=ID_i,L'_i=L_i$. $\mathcal{F}_1$ 直接调用 $h'_i=\mathcal{O}_{\mathrm{H}}(ID'_i\,||\,L'_i)$ 并将 h'_i 返回给 $\mathcal{F}_0$;

$\mathcal{O}'_{Sign}$:假设 $\mathcal{F}_0$ 询问询问的输入值为 (ID'_i,m_i),则 $\mathcal{F}_1$ 调用 $\sigma_i=\mathcal{O}_{\mathrm{Sign}}(ID'_i,m_i)$,并将 (ID'_i,m_i,σ_i) 返回给 $\mathcal{F}_0$.

令 $\mathcal{F}_0$ 输出的有效消息签名对为 (ID^*,m^*,σ^*),若 $ID^*=ID$,则 $\mathcal{F}_1$ 输出 (ID^*,m^*,σ^*) 作为游戏结果;否则,攻击失败. 下面分析 $\mathcal{F}_1$ 成功攻击基于国密的 SM2 标识数字签名算法的概率:

由于 $\mathcal{O}'_H$、$\mathcal{O}'_{\mathrm{Extract}}$ 和 $\mathcal{O}'_{Sign}$ 三个谕言机与 $\mathcal{O}_{\mathrm{H}}$、$\mathcal{O}_{\mathrm{Extract}}$ 和 $\mathcal{O}_{Sign}$ 三个谕言机产生的分布具有不可区分性,故 $\mathcal{F}_0$ 从询问结果无法获取额外信息,即

$\Pr[Verify(mpk, ID^*, m^*, \sigma^*)=1]=\varepsilon_0$.

其中，Pr 是指概率. 因为 $\mathcal{O}'_{\mathrm{H}}$ 是随机谕言机（Random Oracle）①，所以 $\mathcal{F}_0$ 在不询问 $\mathcal{O}'_{\mathrm{H}}$ 情况下输出有效三元组 (ID^*, m^*, σ^*) 的概率是可忽略的，即

$$\Pr\begin{bmatrix} ID^*=ID_i, \exists i\in\{1,2,\cdots,q_H\} \mid \\ Verify(mpk, ID^*, m^*, \sigma^*)=1 \end{bmatrix}=1-\frac{1}{n}.$$

此外，r 是独立且随机选取的，这说明

$$\Pr[ID^*=ID_r \mid ID^*=ID_i, \exists i\in\{1,2,\cdots,q_H\}]=\frac{1}{q_H}.$$

综上可知，

$$\Pr\begin{bmatrix} ID^*=ID_r=ID \wedge Verify \\ (mpk, ID^*, m^*, \sigma^*)=1 \end{bmatrix}=\varepsilon_0\cdot\left(1-\frac{1}{n}\right)\cdot\frac{1}{q_H}.$$

所以，$\mathcal{F}_1$ 算法成功的概率为 $\varepsilon_1=\varepsilon_0\cdot\left(1-\frac{1}{n}\right)\cdot\frac{1}{q_H}$，时间为 $t_1=t_0+q_Ht_H+q_Et_E+q_St_S$.

引理 2. 如果存在具有自适应选择消息和指定身份攻击能力的 $\mathcal{F}_1$ 算法以时间 t_1 和概率 ε_1 成功伪造基于国密 SM2 的标识数字签名（假设 $\mathcal{F}_1$ 可成功破坏 EUF-CM-GID-A），那么存在具有自适应选择消息攻击能力的 $\mathcal{F}_2$ 算法能够以时间 $t_2=t_1+q_Ht_H+q_Et_E+q_St_S$ 和概率 $\varepsilon_2=\varepsilon_1$ 成功伪造 SM2 数字签名（$\mathcal{F}_2$ 可以利用 $\mathcal{F}_1$ 成功伪造 SM2 数字签名）.

证明：已知公钥 pk 和 $\mathcal{O}_{SM2-Sign}$ 谕言机，$\mathcal{F}_2$ 算法可以响应 $\mathcal{F}_1$ 算法的以下询问：

$\mathcal{O}'_{Setup}$：$\mathcal{F}_2$ 随机选取 $x'\in\mathbb{Z}_n^*$ 和用户身份 ID'，计算 $P'_{pub}=x'P$，将 P'_{pub} 和 ID' 返回给 $\mathcal{F}_1$；

$\mathcal{O}'_{Extract}$：令 $\mathcal{F}_1$ 询问的输入值为 ID_i，若 $ID_i\neq ID'$，则 $\mathcal{F}_2$ 随机选取 $l_i\in\mathbb{Z}_n^*$ 并计算 $L_i=l_iP$，$h_i=\mathcal{H}(ID_i\|L_i)$，$d_i=l_i+x'h_i(\mathrm{mod}n)$，并将 (L_i,d_i) 返回给 $\mathcal{F}_1$；否则，$\mathcal{F}_2$ 随机选取 $h_i\in\mathbb{Z}_n^*$，计算 $L_i=pk-h_i\cdot P'_{pub}$，令 $\mathcal{H}(ID_i\|L_i)=h'$，并将 L' 返回给 $\mathcal{F}_1$；此外，$\mathcal{F}_2$ 将 (h_i,ID_i,L_i) 保存在哈希值列表 HL 中；

$\mathcal{O}'_{H}$：令 $\mathcal{F}_1$ 询问的输入值为 (ID_i,L_i)，$\mathcal{F}_2$ 从列表 HL 读取 (h_i,ID_i,L_i)，并将 h_i 返回给 $\mathcal{F}_1$；

$\mathcal{O}'_{Sign}$：令 $\mathcal{F}_1$ 询问输入值为 (ID_i,m_i)，$\mathcal{F}_2$ 先计算 $Z_a=\mathcal{H}_0(ENTLA\|ID_i\|a\|b\|x_P\|y_P\|x_L\|y_L)$，再调用 $\sigma_i=\mathcal{O}_{SM2-Sign}(Z_a\|m_i)$，最后将 (ID_i,m_i,σ_i) 返回给 $\mathcal{F}_1$.

令 $\mathcal{F}_1$ 输出的有效消息签名对为 (ID',m',σ')，$\mathcal{F}_2$ 计算 $Z'_a=\mathcal{H}_0(ENTLA\|ID'\|a\|b\|x_P\|y_P\|x_{L'}\|y_{L'})$，然后直接将 $(Z'_a\|m',\sigma')$ 作为游戏结果. 由于游戏过程未出现中止情况，所以 $\mathcal{F}_2$ 算法成功的概率为 $\varepsilon_2=\varepsilon_1$，时间为 $t_2=t_1+q_Ht_H+q_Et_E+q_St_S$.

根据引理 1 和引理 2 可知，如果存在具有自适应选择消息和身份攻击能力的 $\mathcal{F}_0$ 算法以时间 t_0 和概率 ε_0 成功攻击基于国密 SM2 的标识数字签名算法，那么存在具有自适应选择消息攻击能力的 $\mathcal{F}_2$ 算法能够以时间 $t_2=t_0+2q_Ht_H+2q_Et_E+2q_St_S$ 和概率 $\varepsilon_2=\varepsilon_0\cdot\left(1-\frac{1}{n}\right)\cdot\frac{1}{q_H}$ 成功伪造 SM2 数字签名. 但 Zhang 等在文献[23]中证明 SM2 数字签名算法对于自适应选择消息攻击的概率多项式时间敌手是存在不可伪造的，即满足 EUF-CMA（Existential Unforgeability-Chosen Message Attacks），产生矛盾. 因此，基于国密 SM2 的标识数字签名算法满足 EUF-CM-ID-A.

定理 1. 若基于国密 SM2 的标识数字签名算法满足 EUF-CM-ID-A，则图 1 的集合关系证明协议是零知识证明协议，即满足完备性、可靠性和诚实验证者零知识性.

证明：完备性. 通过验证下列等式可验证协议的完备性：

$$\begin{aligned} D&=z_xG+z_yH+cC\\ &=(x-\sigma\cdot c)G+(y-\rho\cdot c)H+c(\sigma G+\rho H)\\ &=xG+yH=D,\\ E&=Z_T+z_\beta P+(z_\alpha+z_\beta)(L+hP_{pub})\\ &\quad+c\cdot[\hat{s}_\sigma P+(\hat{r}_\sigma+\hat{s}_\sigma)(L+hP_{pub})]\\ &=T-c\cdot K_\sigma+(\beta-b\cdot c)P\\ &\quad+(\alpha+\beta-a\cdot c-b\cdot c)(L+hP_{pub})\\ &\quad+c\cdot[K_\sigma+bP+(a+b)(L+hP_{pub})]\\ &=T+\beta P+(\alpha+\beta)(L+hP_{pub})=E. \end{aligned}$$

可靠性. 由零知识证明的可解析性（Extraction）可知，若存在恶意的证明者 P* 能够以 ε 的概率让 V 接受生成的证明，则存在 PPT 的解析算法 E 能够以 $O(\varepsilon)$ 的概率计算得到证据 $(\sigma,\rho,a,b,K_\sigma)$. 令 E 输出 $\{L,(r_i,s_i)_{i=1}^{|\Phi|},(\hat{r}_\sigma,\hat{s}_\sigma),D,E,c,c',z_x,z'_x,z_y,z'_y,z_\alpha,z'_\alpha,z_\beta,z'_\beta,Z_T,Z'_T\}$，通过下列计算可以解析得到证据：$t=(c'-c)^{-1}$，$\sigma=(z_x-z'_x)\cdot t$，$\rho=(z_y-z'_y)\cdot t$，$a=(z_\alpha-z'_\alpha)\cdot t$，$b=(z_\beta-z'_\beta)\cdot t$，$K_\sigma=t\cdot(Z_T-Z'_T)$.

因为 n 是素数，所以 $(c'-c)$ 在 $\mathbb{Z}_n$ 上存在逆元，可利用扩展欧几里德算法求解 $t=(c'-c)^{-1}$. 若 $\sigma\notin\Phi$，则说明 P* 能够以 $O(\varepsilon)$ 的概率成功伪造基

① 本引理证明过程中，$\mathcal{F}_1$ 算法根据均匀分布（Uniform）、可解析性（Extractability）和可编程性（Programmability）三个性质控制哈希函数的输出值，所以 $\mathcal{O}'_{\mathrm{H}}$ 是随机谕言机.

于国密 SM2 的标识数字签名. ε 必须是可忽略的,否则与基于国密 SM2 的标识数字签名算法是 EUF-CM-ID-A 产生矛盾.

诚实验证者零知识性. 为了证明图 1 的协议满足诚实验证者零知识性,构造表 1 的仿真器 Sim 以模拟与诚实验证者 V* 的所有交互操作. 由于参数 $a,b \in \mathbb{Z}_n^*$ 是随机选取的,且承诺方案具有完全隐藏性质,所以 Sim 的前两步操作是完全盲化的,即 V* 或其他 PPT 攻击者无法从拦截的消息 $(\hat{r}_\sigma,\hat{s}_\sigma)$ 恢复出 (r_σ,s_σ). 此外,由于第 3～5 步的 Σ 协议满足特殊诚实验证者零知识性,所以能有效防止证据泄露. 综上可见,所设计的集合关系证明满足诚实验证者零知识性.

表 1　集合关系证明协议的仿真器 Sim

1. Sim 向 V^* 请求集合中各元素的签名 $\{L,(r,s_i)_{i=1}^{|\Phi|}\}$.
2. Sim 随机选取 $a,b \in \mathbb{Z}_n^*$ 以计算 $\hat{r}_\sigma = r_\sigma + a, \hat{s}_\sigma = s_\sigma + b$,将 $(\hat{r}_\sigma,\hat{s}_\sigma)$ 发给 V^*.
3. Sim 随机选取 $x,y,\alpha,\beta \in \mathbb{Z}_n^*, T \in \mathbb{G}$,计算中间数据 $D=xG+yH, E=T+\beta P+(\alpha+\beta)(L+hP_{pub})$,并将 D,E 发给 V^*.
4. Sim 接收到 V^* 发送的挑战值 $c \in \mathbb{Z}_n^*$.
5. Sim 计算 $z_x=x-\sigma\cdot c, z_y=y-\rho\cdot c, z_\alpha=\alpha-a\cdot c, z_\beta=\beta-b\cdot c, Z_T=T-c\cdot K_\sigma$,并将 $(z_x,z_y,z_\alpha,z_\beta,Z_T)$ 发送给 V^*.

4.2　基于国密 SM2 的数值范围证明协议

为了扩展到集合大小更大的关系证明,实现大整数的数值范围证明,本节利用上述设计的集合关系证明协议设计新的数值范围证明协议,成功地将上述的 $\sigma \in \Phi$ 扩展至 $\sigma \in [0,u^l)$. 与文献[2]的思路一样,先将元素 σ 表示成 u 进制形式 $\sigma=\sum_{j=0}^{l-1}\sigma_j \cdot u^j$,其中,$l$ 为系数个数,再利用所设计的集合关系证明协议证明元素 σ 的各个系数 σ_j 均满足 $\sigma_j \in [0,u-1]$. 由于 $[0,u-1]$ 各元素的签名可以重复使用,验证者仅需发送一次区间 $[0,u-1]$ 各元素的签名 $\{L,(r_i,s_i)_{i=0}^{u-1}\}$ 给证明者. 同时,为了降低证明者的计算开销,要求验证者将随机生成的点 $K_i (i \in \mathbb{Z}_u)$ 一起发送给证明者,证明者无需重新计算即可直接使用 K_i 执行后续证明操作. 因为验证者只需在初始化阶段发送 $(K_i,r_i,s_i)_{i=0}^{u-1}$ 给证明者,所以发送 $K_i (i \in \mathbb{Z}_u)$ 所增加的通信开销可以被接受. 具体的数值范围证明协议设计过程如图 2 所示,其中,PK 是指 P 和 V 执行相关的 Σ 协议.

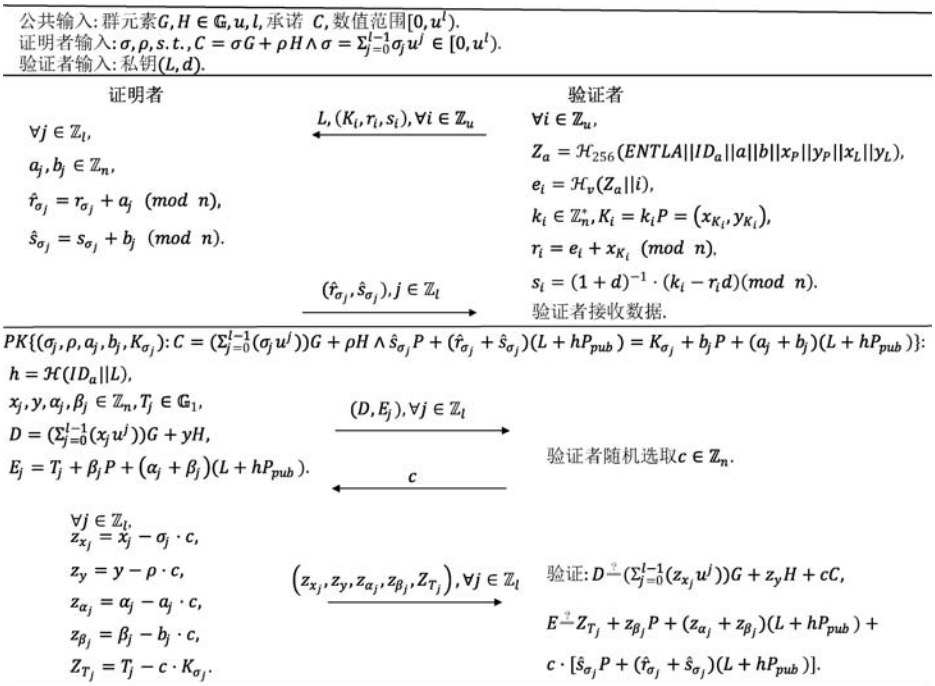

图 2　支持 $[0,u^l)$ 的基于国密 SM2 的数值范围证明协议设计

定理 2. 若基于国密 SM2 的标识数字签名算法满足 EUF-CM-ID-A，则图 2 的数值范围证明协议是零知识证明协议，即满足完备性、可靠性和诚实验证者零知识性.

证明(概要). 基于国密 SM2 的标识数字签名算法的数值范围证明协议的完备性验证方式与定理 1 类似，在此不再详述. 与前面所述的集合关系证明协议一样，所设计的数值范围证明协议的可靠性主要依赖于知识证明协议的可解析性. 关于诚实验证者零知识性，同样可以构造与表 1 类似的仿真器，由仿真器相关步骤的完全盲化性与所采用 Σ 协议的特殊诚实验证者零知识性可以证明所设计的数值范围证明协议具有诚实验证者零知识性.

备注 1. 上述基于国密 SM2 的标识数字签名算法的数值范围证明协议不仅支持 $\sigma \in [0,u^l)$ 形式的数值范围证明，还可以扩展成一般形式 $[\alpha,\beta](\alpha,\beta \in \mathbb{N})$ 的数值范围证明. 主要采用文献[2]提到的民间换算技术 (Folklore Reguction Technology)：如果 $u^{l-1}<\beta<u^l$，那么将 $\sigma \in [\alpha,\beta]$ 等价为 $\sigma-\beta+u^l \in [0,u^l] \wedge \sigma-\alpha \in [0,u^l)$. 如果 $\alpha+u^{l-1}<\beta$，那么将 $\sigma \in [\alpha,\beta]$ 等价为 $\beta-\sigma \in [0,u^{l-1}] \vee \sigma-\alpha \in [0,u^{l-1})$.

5 性能分析

本节主要比较文献[2]、[12]以及本文所设计协议的通信代价和计算开销. 令 $|\Phi|$ 表示集合关系证明中的集合大小，u 和 l 分别表示 u 进制和系数个数. 为了达到 $\lambda=128$ 的安全等级，采用 $\mathbb{F}_{256}$ 上的 Barreto-Naehrig (BN) 曲线[31]进行测试评估. 因此，$\mathbb{G}_1$，$\mathbb{G}_2$，$\mathbb{G}_T$ 和 $\mathbb{Z}_n$ 上的元素长度分别为 64 字节、128 字节、384 字节和 32 字节.

5.1 通信代价分析

为了得到合理的通信开销比较结果，分别统计文献[2]、[12]以及本文所设计协议的通信代价情况(如表 2 所示). 与文献[2]和[12]的协议相比，本文设计的两种协议在通信带宽方面具有明显优势. 据文献[2]提到，系统最优参数为 $u=57$ 和 $l=5$，所以在初始化阶段，文献[2]和[12]的协议分别消耗通信带宽 3712 字节和 27360 字节，而本文协议消耗 7360 字节；在证明阶段，文献[2]和[12]的协议分别消耗通信带宽 2688 字节和 7168 字节，而本文协议仅需消耗通信带宽 1568 字节. 可见，与文献[2]和[12]的协议相比，本文协议在初始化阶段仍消耗较多带宽，由于初始化阶段只执行一次，该代价可以被接受；但在证明阶段的通信带宽分别可节省约 41.66%和 78.12%的通信带宽.

5.2 计算开销分析

为了比较文献[2]、[12]的协议和本文所设计协议的计算开销，本文首先在 PC 端测试协议相关运算的耗时情况，其中 PC 端平台相关参数为 Dell 牌

表 2 通信代价分析对比(单位：字节)

协议	阶段	文献[2]	文献[12]	本文
集合关系证明	初始化	$(\lvert\Phi\rvert+1)\lvert\mathbb{G}_1\rvert=64\lvert\Phi\rvert+64$	$\lvert\Phi\rvert(\lvert\mathbb{Z}_n\rvert+\lvert\mathbb{G}_1\rvert)=96\lvert\Phi\rvert$	$2\lvert\Phi\rvert\lvert\mathbb{Z}_n\rvert+\lvert\mathbb{G}_1\rvert=64\lvert\Phi\rvert+64$
	证明执行	$4\lvert\mathbb{Z}_n\rvert+2\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_T\rvert=640$	$10\lvert\mathbb{Z}_n\rvert+7\lvert\mathbb{G}_1\rvert+2\lvert\mathbb{G}_T\rvert=1536$	$7\lvert\mathbb{Z}_n\rvert+3\lvert\mathbb{G}_1\rvert=416$
数值范围证明	初始化	$(u+1)\lvert\mathbb{G}_1\rvert=64u+64$	$u\lvert\mathbb{Z}_n\rvert+u\lvert\mathbb{G}_1\rvert+u\lvert\mathbb{G}_T\rvert=480u$	$(u+1)\lvert\mathbb{G}_1\rvert+2u\lvert\mathbb{Z}_n\rvert=128u+64$
	证明执行	$(2l+2)\lvert\mathbb{Z}_n\rvert+(l+1)\lvert\mathbb{G}_1\rvert+l\lvert\mathbb{G}_T\rvert=512l+128$	$(8l+2)\lvert\mathbb{Z}_n\rvert+(6l+1)\lvert\mathbb{G}_1\rvert+2l\lvert\mathbb{G}_T\rvert=1408l+128$	$(2l+1)\lvert\mathbb{G}_1\rvert+(5l+2)\lvert\mathbb{Z}_n\rvert=288l+128$

电脑、Windows 7 操作系统、i5－4210U 1.70－GHz 处理器、4 GB 内存. 通过 PC 端上的 Miracl 库 10000 次测试取平均值得到各运算运行时间，相应的符号定义和运行时间如表 3 所示.

先统计两种对比协议涉及的运算类型和次数，再结合表 3 的各运算耗时情况计算得到各阶段各角色的计算开销(如表 4 所示). 当系统参数取到最优值 $u=57$ 和 $l=5$ 时，在初始化阶段，文献[2]和[12]的协议耗时分别为 516.0833 毫秒和 2977.6743 毫秒，本文协议耗时为 505.7346 毫秒；在证明阶段，文献[2]和[12]的协议耗时分别为 3493.8969 毫秒和 3474.4492 毫秒，本文协议的耗时为 491.5075 毫秒. 可见，与文献[2]和[12]的协议相比，本文协议的计算开销有较大改进，其中在证明阶段分别降低

约 85.93%和 85.85%. 这主要是因为本文设计的两个协议均不涉及高耗时的双线性对运算. 此外,本文所设计的协议与文献[12]的协议一样,避免了 PKI 体系下巨大的证书管理开销,可见其实用性更强.

表 3　符号定义和耗时情况(单位:毫秒)

符号	描述	时间
T_{g1sm}	群 $\mathbb{G}_1$ 上的点乘运算	8.8517
T_{g2sm}	群 $\mathbb{G}_2$ 上的点乘运算	19.731
T_{pa}	群 $\mathbb{G}_1$ 上的点加运算	0.0811
T_h	安全哈希算法	0.0006
T_{bp}	群 $\mathbb{G}_T$ 上的双线性对运算	119.3940
T_{ebp}	群 $\mathbb{G}_T$ 上的模幂运算	50.3876
T_{mbp}	群 $\mathbb{G}_T$ 上的模乘运算	0.5946
T_{mi}	域 $\mathbb{Z}_n^*$ 上的模逆运算	0.0471
T_{mm}	域 $\mathbb{Z}_n^*$ 上的模乘运算	0.0097

6　结　论

本文结合 Camenisch 等[2]提出的签名基构造方法,利用基于国密 SM2 的标识数字签名算法设计更加高效的集合关系证明协议和范围证明协议. 本文先证明基于国密 SM2 的标识数字签名算法的安全性,再进一步证明设计的两个协议满足零知识证明协议的完备性、可靠性和诚实验证者零知识性. 通过与文献[2]和[12]所设计协议的性能对比,说明本文设计的协议在避免繁琐的证书管理基础上,进一步降低了通信带宽和计算开销. 因此,本文协议具有更强的实用性,更能满足区块链、匿名证书、电子现金、群/环签名等场景的隐私保护需求.

表 4　计算开销分析对比(单位:毫秒)

协议	阶段	角色	文献[2]	文献[12]	本文
集合关系证明	初始化	验证者	$(\lvert\Phi\rvert+1)T_{g1sm}+\lvert\Phi\rvert T_{mi}$ $=8.8988\lvert\Phi\rvert+8.8517$	$\lvert\Phi\rvert(T_{ebp}+T_h+T_{g1sm})$ $=59.2399\lvert\Phi\rvert$	$(\lvert\Phi\rvert+1)T_h+$ $\lvert\Phi\rvert(T_{g1sm}+2T_{mm})+T_{mi}=8.8717$ $\lvert\Phi\rvert+0.0477$
	证明执行	证明者	$3T_{g1sm}+2T_{bp}+T_{mbp}$ $+2T_{ebp}+3T_{mm}+T_{pa}$ $=366.8231$	$14T_{g1sm}+T_{g2sm}+T_{bp}+3T_{mbp}+$ $4T_{ebp}+9T_{mm}+8T_{pa}+T_h=$ 467.1197	$11T_{g1sm}+6T_{mm}$ $+7T_{pa}+T_h=97.9952$
		验证者	$3T_{g1sm}+3T_{bp}+2T_{mbp}$ $+3T_{ebp}+2T_{pa}=537.2513$	$12T_{g1sm}+2T_{bp}+3T_{mbp}+4T_{ebp}$ $+9T_{pa}=549.0725$	$9T_{g1sm}+4T_{mm}$ $+8T_{pa}=80.3529$
数值范围证明	初始化	验证者	$(u+1)T_{g1sm}+uT_{mi}$ $=8.8988u+8.8517$	$u(T_{ebp}+T_h+T_{g1sm})$ $=59.2399u$	$uT_{g1sm}+T_{mi}+2uT_{mm}$ $+(u+1)T_h$ $=8.8717u+0.0477$
	证明执行	证明者	$(l+2)T_{g1sm}+(l+1)T_{bp}$ $+lT_{mbp}+2lT_{ebp}$ $+(3l+1)T_{mm}+T_{pa}$ $=229.7257l+137.1882$	$(12l+2)T_{g1sm}+2lT_{mbp}+3lT_{ebp}$ $+10lT_{mm}+6lT_{pa}=259.156l$ $+17.7034$	$(4l+2)T_{g1sm}+4lT_{pa}$ $+(5l+1)T_{mm}+1T_h$ $=35.7797l+17.7137$
		验证者	$3T_{g1sm}+(2l+1)T_{bp}$ $+2lT_{mbp}+3lT_{ebp}$ $+lT_{mm}+2T_{pa}$ $=417.7048l+119.5562$	$(9l+3)T_{g1sm}+(l+1)T_{bp}+3lT_{mbp}$ $+4lT_{ebp}+lT_{mm}+(7l+2)T_{pa}$ $=402.9709l+146.1113$	$(6l+3)T_{g1sm}+$ $(6l+2)T_{pa}+4lT_{mm}=53.6356l+$ 26.7173

参　考　文　献

[1] Brickell E, Chaum D, Damgård I, van de Graaf J. Gradual and verifiable release of a secret//Proceedings of the Conference on the Theory and Application of Cryptographic. Santa Barbara, USA, 1987: 156-166

[2] Camenisch J, Chaabouni R, Shelat A. Efficient protocols for set membership and range proofs//Proceedings of the Advances in Cryptology. Melbourne, Australia, 2008: 234-252

[3] Fuchsbauer G, Orrù M, Seurin Y. Aggregate cash systems: a cryptographic investigation of mimblewimble//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Darmstadt, Germany, 2019: 657-689

[4] Zhu L, Gao F, Shen M, Li Y, Zhen B, Mao L. Survey and privacy preserving techniques for blockchain technology. Journal of Computer Research and Development, 2017, 54 (10): 2170-2186(in Chinese)

(祝烈煌，高峰，沈蒙，郑宝昆，毛洪亮，吴震. 区块链隐私保护研究综述. 计算机研究与发展，2017，54 (10)：2170-2186)

[5] Camenisch J，Lysyanskaya A. An efficient system for non-transferable anonymous credentials with optional anonymity revocation//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Innsbruck，Austria，2001：93-118

[6] Boudot F，Traoré J. Efficient publicly verifiable secret sharing schemes with fast or delayed recovery//Proceedings of the International Conference on Information and Communications Security，Sydney，Australia，1999：87-102

[7] Peng B，Hong F，Cui G. Divisible e-cash based on signatures of zero-knowledge proof and strong-rsa problem. Journal on Communications，2006，27 (7)：12-19
(彭冰，洪帆，崔国华. 基于零知识证明签名和强 RSA 问题的可分电子现金. 通信学报，2006，27 (7)：12-19)

[8] Li K，Yang R，Ho Au M，Xu Q. Practical range proof for cryptocurrency monero with provable security//Proceedings of the International Conference on Information and Communications Security. Beijing，China，2017：255-262

[9] Sun S，Ho Au M，Liu J，Yuen T. RingCT 2.0：a compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero//Proceedings of the European Symposium on Research in Computer Security. Oslo，Norway，2017：456-474

[10] Deng C，Fan J，Zhen W，Luo Y，Zheng Y，Li Y，Ding J. A survey on range proof and its applications on blockchain//Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. Guilin，China，2019：1-8

[11] Abbasinezhad-Mood D，Nikooghadam M. An anonymous ecc-based self-certified key distribution scheme for the smart grid. IEEE Transactions on Industrial Electronics，2018，65 (10)：7996-8004

[12] He D，Lin C，Xie X，Li S，S L. Data processing methods，devices，computer equipment and storage media，China，October 08，2019. Patent Application Publication：No. CN110311776A(in Chinese)
(何德彪，林超，谢翔，李升林，孙立林. 数据处理方法、装置、计算机设备和存储介质，中国，2019 年 10 月 08 日. 专利申请公布号：CN110311776A)

[13] Chan A，Frankel Y，Tsiounis Y. Easy come-easy go divisible cash//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Espoo，Finland，1998：561-575

[14] Boudot F. Efficient proofs that a committed number lies in an interval//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Bruges，Belgium，2000：431-444

[15] Lipmaa H. On diophantine complexity and statistical zero-knowledge arguments//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Taipei，China，2003：398-415

[16] Groth J. Non-interactive zero-knowledge arguments for voting//Proceedings of the International Conference on Applied Cryptography and Network Security. New York，USA，2005：467-482

[17] Rabin M，Shallit Jeffery. Randomized algorithms in number theory. Communications on Pure and Applied Mathematics，2010，39(S1)：S239-S256

[18] Teranishi I，Sako K. K-times anonymous authentication with a constant proving cost//Proceedings of the International Workshop on Public Key Cryptography. New York，USA，2006：525-542

[19] Chaabouni R，Lipmaa H，Shelat A. Additive combinatorics and discrete logarithm based range protocols//Proceedings of the 15th Australasian Conference on Information Security and Privacy. Sydney，Australia，2010：336-351

[20] Canard S，Coisel I，Jambert A，Traoré J. New results for the practical use of range proofs//Proceedings of the EuroPKI：European Public Key Infrastructure Workshop. Egham，UK，2013：47-64

[21] Bünz B，Bootle J，Boneh D，Poelstra A，Wuille P，Maxwell G. Bulletproofs：short proofs for confidential transactions and more//Proceedings of the IEEE Symposium on Security and Privacy. San Francisco，USA，2018：315-334

[22] Zhang F，Gao S，Zeng Z，Liu Z. An efficient scheme of range proofs. Journal of Cryptologic Research，2020，7(2)：197-211(in Chinese)
(张凡，高胜，曾志强，刘喆. 一种高效的范围证明方案. 密码学报，2020，7(2)：197-211)

[23] Zhang Z，Yang K，Zhang J，Chen C. Security of the sm2 signature scheme against generalized key substitution attacks//Proceedings of the International Conference on Research in Security Standardisation. Tokyo，Japan，2015：140-153

[24] He D，Zhang J，Chen B，Zhang Y. An identity-based digital signature method and system based on SM2，China，November 13，2018. Patent Application Publication：No. CN10880-9658A(in Chinese)
(何德彪，张佳妮，陈泌文，张宇波. 一种基于 SM2 的身份基的数字签名方法与系统，中国，2018 年 11 月 13 日. 专利申请公布号：CN108809658A)

[25] Shamir A. Identity-based cryptosystems and signature schemes//Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques. Santa Barbara，USA，1984：47-53

[26] Cha J，Cheon J. An identity-based signature from gap diffie-hellman groups//Proceedings of the International Workshop on Public Key Cryptography. Miami，USA，2003：18-30

[27] Bellare M，Goldreich O. On defining proofs of knowledge//Proceedings of the Annual International Cryptology Conference. California，USA，1992：390-420

[28] Cramer R，Damgård I，MacKenzie P. Efficient zero-knowledge proofs of knowledge without intractability assump-

tions//Proceedings of the International Workshop on Public Key Cryptography. Melbourne, Australia, 2000: 354-372

[29] Damgård I. On Σ-protocols. Lecture Notes, University of Aarhus, Department for Computer Science, 2002

[30] Faust S, Kohlweiss M, Marson G, Venturi D. On the non-malleability of the Fiat-Shamir transform//Proceedings of the International Conference on Cryptology in India. Kolkata, India, 2012: 60-79

[31] Barreto P, Naehrig M. Pairing-friendly elliptic curves of prime order//Proceedings of the International Workshop on Selected Areas in Cryptography. Kingston, Canada, 2005: 319-331

LIN Chao, Ph. D., lecturer. His research interests include applied cryptography and blockchain privacy protection.

HUANG Xin-Yi, Ph. D., professor. His research interests include applied cryptography and network security.

HE De-Biao, Ph. D., professor. His research interests include applied cryptography, cryptographic protocols, and cloud computing security.

Background

Range proof, as a special type of zero knowledge proofs, has attracted many researchers especially when the blockchain emerges. It can be applied into different scenarios for protecting privacy, such as blockchain, anonymous certificate, electronic cash systems, group/ring signature scheme, and so forth. Camenisch et al.'s (ASIACRYPT 2008) proposal is one of widely used range proof protocols, but which requires high time-consuming bilinear pairing computations and cumbersome certificate managements. Although He et al. adopted SM9 digital signature algorithm to construct novel protocols without the need of complex certificate managements, their proposal is still faced with the intractable bilinear pairing operation.

Our work in this paper enriches research on bilinear pairing-free and identity-based range proof protocols. Specifically, on basis of the signature-based method, we adopt an identity-based digital signature algorithm based on Chinese cryptographic SM2 to construct two protocols (i. e. set membership protocol and range proof protocol). We also prove the security of adopted identity-based digital signature algorithm, which is also of independent interests. Through the comparative performance analysis with Camenisch et al.'s and He et al.'s protocols, we prove that our proposed protocols can reduce the communication overhead about 41.66% and 78.12% respectively, and save the computation cost about 85.93% and 85.85% respectively. This undoubtedly demonstrates the utility of our proposals.

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0802500, in part by the National Natural Science Foundation of China under Grants 62032005, 61872089, 61932016, 61972294, 61772377, and 61841701, in part by the Natural Science Foundation of Hubei Province of China under Grant 2017CFA007, in part by the Natural Science Foundation of Fujian Province under Grant 2020J02016.