北京航空航天大學

BEIHANG UNIVERSITY

第三十三届“冯如杯”竞赛主赛道项目论文模板

——基于 Latex 的论文模板

摘要

本 Latex 模板是北京航空航天大学大学第三十三届“冯如杯”竞赛主赛道论文模板，由北京航空航天大学校团委基于 GitHub 用户 ***Somedaywilldo*** 与 ***cpfy*** 的成果迭代开发而来。在此由衷感谢所有开发者对本模板的贡献与对“冯如杯”竞赛的大力支持。

摘要内容包括：“摘要”字样，摘要正文，关键词。在摘要的最下方另起一行，用显著的字符注明文本的关键词。

摘要是论文内容的简短陈述，应体现论文工作的核心思想。摘要一般约 500 字。摘要内容应涉及本项科研工作的目的和意义、研究思想和方法、研究成果和结论。

关键词是为用户查找文献，从文中选取出来用来揭示全文主题内容的一组词语或术语，应尽量采用词表中的规范词（参照相应的技术术语标准）。关键词一般为 3 到 8 个，按词条的外延层次排列。关键词之间用逗号分开，最后一个关键词后不打标点符号。

关键词：关键词 1，关键词 2，关键词 3，关键词 4，关键词 5

Abstract

This Latex template for the 33rd Fengru Cup Competition of Beihang University, is developed by Communist Youth League Committee of BUAA iteratively based on the contribution of GitHub users ***Somedaywilldo*** and ***cpfy***. Here, we would like to thank all the developers for their contributions to this template and for their support of the Fengru Cup Competition.

The abstract includes: the word "Abstract", the body of the abstract, and the keywords. On a separate line at the bottom of the abstract, indicate the key words of the text in prominent characters.

The abstract is a short statement of the content of the paper and should reflect the core ideas of the paper work. The abstract is usually about 500 words. The abstract should cover the purpose and significance of this scientific work, research ideas and methods, research results and conclusions.

Keywords are a set of words or terms selected from the text to reveal the subject content of the whole text for the user to find the literature, and the standardized words in the word list (refer to the corresponding technical terminology standards) should be used as much as possible. The keywords are usually 3 to 8, arranged according to the level of extensibility of the words. The keywords are separated by commas, and no punctuation marks are used after the last keyword.

Keywords: Keywords 1, Keywords 2, Keywords 3, Keywords 5, Keywords 6

目录

一、简介

第三十三届“冯如杯”主赛道论文一律由在计算机上输入、排版、定稿后转成 PDF 格式，在集中申报时通过网络上传。**论文封面及全文中不能出现作者姓名、学院、专业、指导老师的相关信息**。包括 5 个部分, 顺序依次为:

- 封面（中文）
- 中文摘要、关键词 (中文、英文)
- 主体部分
- 结论
- 参考文献

二、论文的书写规范

论文正文部分需分章节撰写，每章应另起一行。章节标题要突出重点，简明扼要、层次清晰。字数一般在 15 字以内，不得使用标点符号。标题中尽量不采用英文缩写词，对必须采用者，应使用本行业的通用缩写词。层次以少为宜，根据实际需要选择。三级标题的层次按章（如“一、”）、节（如“(一)”）、条（如“1.”）的格式编写，各章题序的阿拉伯数字用 Times New Roman 体。

（一）字体和字号

论文题目：二号，华文中宋体加粗，居中。

副标题：三号，华文新魏，居右（可省略）。

章标题：三号，黑体，居中。

节标题：四号，黑体，居左。

条标题：小四号，黑体，居左。

正文：小四号，中文字体为宋体，西文字体为 Times New Roman 体，首行缩进，两端对齐。

页码：五号 Times New Roman 体，数字和字母

（二）页边距及行距

学术论文的上边距：25mm；下边距：25mm；左边距：30mm；右边距 20mm。章、节、条三级标题为单倍行距，段前、段后各设为 0.5 行（即前后各空 0.5 行）。正文为 1.5

倍行距，段前、段后无空行（即空 0 行）。

（三）页眉

页眉内容为北京航空航天大学第三十三届“冯如杯”竞赛主赛道参赛作品，内容居中。页眉用小五号宋体字，页眉标注从论文主体部分开始（引言或第一章）。请注意论文封面无页眉。

（四）页码

论文页码从“主体部分（引言、正文、结论）”开始，直至“参考文献”结束，用五号阿拉伯数字连续编码，页码位于页脚居中。**封面、题名页不编页码**。

摘要、目录、图标清单、主要符号表用五号小罗马数字连续编码，页码位于页脚居中。

（五）图、表及其附注

图和表应安排在正文中第 1 次提及该图、表的文字的下方，当图或表不能安排在该页时，应安排在该页的下一页。

1. 图

图题应明确简短，**用五号宋体加粗**，数字和字母为**五号 Times New Roman 体加粗**，图的编号与图题之间应空半角 2 格。图的编号与图题应置于图下方的居中位置。图内文字为 **5 号宋体**，数字和字母为 **5 号 Times New Roman 体**。曲线图的纵横坐标必须标注“量、标准规定符号、单位”，此三者只有在不必要注明（如无量刚等）的情况下方可省略。坐标上标注的量的符号和缩略词必须与正文中一致。

2. 表

表的标号应采用从 1 开始的阿拉伯数字编号，如：“表 1”、“表 2”、……。表编号应一直连续到附录之前，并与章、节和图的编号无关。只有一幅表，仍应标为“表 1”。表题应明确简短，用**五号宋体加粗**，数字和字母为**五号 Times New Roman 体加粗**，表的编号与表题之间应空半角 2 格。表的编号与表头应置于表上方的居中位置。表内文字为 **5 号宋体**，数字和字母为 **5 号 Times New Roman 体**。

3. 附注

图、表中若有附注时，附注各项的序号一律用“附注 + 阿拉伯数字 + 冒号”，如：“附注 1：”。

附注写在图、表的下方，一般采用 5 号宋体。

4. 参考文献

凡有直接引用他人成果（文字、数字、事实以及转述他人的观点）之处，均应加标注说明列于参考文献中，以避免论文抄袭现象的发生。

标注格式：引用参考文献标注方式应全文统一，标注的格式为 [序号]，放在引文或转述观点的最后一个句号之前，所引文献序号用小 4 号 Times New Roman 体、以上角标形式置于方括号中，如“……成果”[1]。

三、原理与算法

基于零知识范围证明的的位置隐私保护系统改进实际上是围绕 GPS 上的零知识范围证明展开的。这是改进的新系统的技术核心，只要能实现这一点，整体的系统便能搭建起来。为了使系统的针对目标更加清晰，我们定义如下问题场景: 证明方在拥有一个隐藏的用户 GPS 坐标和一个公开的参考点 GPS 坐标的基础上，向验证方证明用户 GPS 坐标在参考点 GPS 坐标的一定范围内，但这个过程不会透露用户 GPS 坐标的具体信息。在以下两章中，我们将介绍该问题的解决方案和相应的技术原理。

（一）基于哈达玛积的问题转化

观察问题场景，我们发现其中涉及两个 GPS 坐标：隐藏的用户 GPS 坐标和公开的参考点 GPS 坐标，分别记作 $S(x_1, y_1)$ 和 $P(x_2, y_2)$。考虑到实际生活场景中的 GPS 坐标往往是经纬度形式，因此这两个坐标同样采用经纬度形式。同时为了兼顾一定的准确性，在经纬度精度上，本文选取 4 位小数作为参考样例, 即 x_1,x_2,y_1,y_2 均为五位小数。此时最大误差大概是在 5 米左右。当然，如果需要让结果进一步精确，仍可以进一步调整精度。

要判断坐标 S 是否在坐标 P 的一定范围内，我们可以参考平面中心圆模型。通过判断两者间的距离 R 是否处于一定数值范围内，即可检验坐标间关系是否满足要求。为了使问题更加明确，本文中用符号 l_{min},l_{max} 分别来表示距离的下界和上界, 且均为整数。其中整数的选取主要为了更好地运用零知识范围证明。实际应用中，l_{min},l_{max} 应根据具体需求进行一定的变化。基于以上定义，我们将问题转化为：用户 GPS 坐标在参考点 GPS 坐标的一定范围内等价于检验以下公式

$$l_{\text{min}} < d_{SP} \leq l_{\text{max}} \tag{1}$$

其中 d_{SP} 代表坐标 S 和 P 之间的距离，数值选取小数点后 5 位。而要得出 d_{SP} 的

具体数值，我们需要利用坐标 $S(x_1, y_1)$ 和 $P(x_2, y_2)$ 进行如下公式计算:

$$\begin{cases} S' = (R\cos x_1 \cos y_1, R\sin x_1 \cos y_1, R\sin y_1), \\ P' = (R\cos x_2 \cos y_2, R\sin x_2 \cos y_2, R\sin y_2), \\ d_{SP} = R\arccos[\cos(x_1 - x_2)\cos y_1 \cos y_2 + \sin y_1 \sin y_2]. \end{cases} \tag{2}$$

其中 S' 和 P' 分别代表经纬度坐标 $S(x_1, y_1)$ 和 $P(x_2, y_2)$ 在三维直角坐标系下对应坐标，R 代表地球的半径。这样就可以进行 d_{SP} 和 L 的比较了。

但是，我们采用的零知识范围证明适用于任意整数范围，而非任意实数范围。并且零知识范围证明主要是对向量进行操作，而非直接的数值。因此我们不仅需要将 d_{SP} 进行整数化处理，还要进一步将其转化为进制形式来形成对应向量。下面介绍解决方案。

首先，将 d_{SP},$l_{\min}$,$l_{\max}$ 乘以 10^5, 进一步得到 D_{SP},$L_{\min}$,$L_{\max}$ 这样我们不仅保留了小数部分，避免了直接去除小数部分带来的误差，同时完成了取整。不过值得注意，乘以 10 的几次方主要取决于应用需求和相关参数的精度选取。

接着, 取满足 $u^{n-1} < L_{\max} \leq u^n$ 的 u 和 n, 对 D_{SP},$L_{\min}$,$L_{\max}$,$D_{SP} - L_{\min}$,$D_{SP} - L_{\max} + u^n$ 分别进行进制转化，得到向量 v,a,b,c,d。本文中以二进制作为参考样例。进一步计算以下内积关系，以证明 $L_{\min} < D_{SP} \leq L_{\max}$:

$$\begin{cases} \langle v \odot (v - 1^m), r\rangle = 0 \\ \langle c \odot (c - 1^m), r\rangle = 0 \\ \langle d \odot (d - 1^m), r\rangle = 0 \\ \langle c, r_{[:m-n]} || 0^n\rangle = 0 \\ \langle d, r_{[:m-n]} || 0^n\rangle = 0 \\ \langle v - a - c, 2^m\rangle = 0 \\ \langle v - b + bi(2^n) - d, 2^m\rangle = 0 \end{cases} \tag{3}$$

以上运算基于一个足够大的有限域 $\mathbb{F}$ 的。参数 m 大小为 $|\mathbb{F}|$, 参数 r 是验证方随机选取的一个挑战值。$\odot$ 表示哈达玛积, 即 $a \odot b = (a_1, \ldots, a_k) \odot (b_1, \ldots, b_k) = (a_1 b_1, \ldots, a_k b_k)$。$bi()$ 表示将数转化为二进制的向量。以上的七个公式就是零知识范围证明实际上的证明对象，至此问题已经转化完成，接下去的流程就是零知识范围证明了。其中的具体原理，详见下一章关于零知识范围证明的介绍。

（二）范围证明的理论基础

1. 默克尔树

默克尔树[1]（Merkle Tree or Hash Tree）是一棵用哈希值搭建起来的树，树的所有节点都存储了哈希值。整棵树包含根节点、中间节点和叶节点。树采取自下而上的生成方式，叶节点经哈希运算得到哈希值，而其余节点的哈希值均由其子节点的哈希值经哈希计算得到。默克尔树的具体结构见图 1。

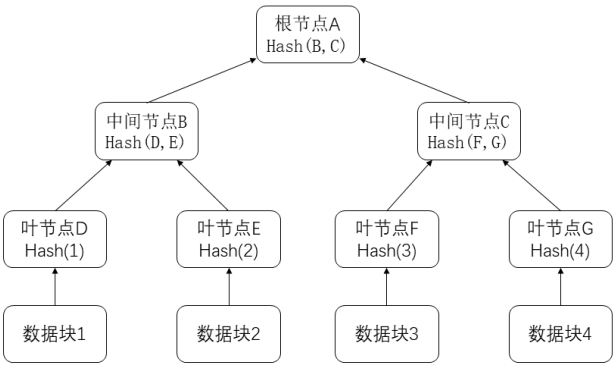

图 1 默克尔树结构图

基于哈希函数的防碰撞特性（Collision resistance）、隐藏性 (Hiding) 和谜题友好性（Puzzle friendly），对默克尔树的任意局部修改，都会对根节点和路径上的中间节点产生影响。默克尔树的这个特性提供了一种很好的检测数据是否被篡改的方法。在本文中，我们使用具有抗碰撞特性和不可逆特性的哈希函数来构造默克尔树，进而利用构造的树来完成对向量的承诺，并通过次线性尺度的证明来开放树的多处索引。对向量 v 的承诺包含以下三种算法，即承诺操作（Commit）、开放操作（Open）、验证操作（Verify）：

- $\text{root}_v \leftarrow \text{MT.Commit}(v)$
- $(\{v_i\}_{i\in\mathcal{I}}, \pi_{\mathcal{I}}^v) \leftarrow \text{MT.Open}(\mathcal{I}, v)$
- $\{1, 0\} \leftarrow \text{MT.Verify}(\text{root}_v, \mathcal{I}, \{v_i\}_{i\in\mathcal{I}}, \pi_{\mathcal{I}}^v)$

2. 里得 · 所罗门编码

里得 · 所罗门编码[2] [3]（Reed-Solomon Code, RS Code）是一种编码方式，用其编码的码字是域上某个特定单变量多项式的一组函数值，表示成向量的形式。因此，在本文中我们使用 RS Code 来编码向量。

用抽象代数的模型来定义，选择一个 q 阶的有限域 $\mathbb{F}$，作为编码的字母表。再选择 $\mathbb{F}$ 的一个陪集 L，所选择的特定单变量多项式成为编码多项式（encoding polynomial），且度小于 $\rho \cdot |L|$，其中 $\rho \in (0,1)$ 称为编码率，用这样的多项式编码出的向量表示为 $\mathrm{RS}[L,\rho] \in \mathbb{F}^{|L|}$。

具体而言，编码的过程如下：设插值集 $H = \{\xi_1, \cdots, \xi_{|H|}\}$，估值集 $L = \{\eta_1, \cdots, \eta_{|L|}\}$，且 $|L| > |H|$，被编码的向量设为 $v \in \mathbb{F}^{|H|}$。首先，找到预设的度的编码多项式 $\hat{p}$，使得 $\hat{p}|_H = \{\hat{p}(\xi_1), \cdots, \hat{p}(\xi_{|H|})\} = v$。然后计算 $\hat{p}$ 在 L 上的估值（Evaluation），得到码字 $\hat{p}|_L$。计算估值和插值的算法使用快速傅里叶变换（Fast Fourier Transform, FFT）和其逆变换（Inverse FFT, IFFT）。

3. 诚实验证方前提的零知识证明

零知识证明（Zero-Knowledge Argument of Knowledge, ZKAoK）是一种验证协议，在其中证明方（Prover）不提供任何有关某个论断的有用信息，而能使验证方（Verifier）验证该论断为正确的。这项协议技术在信息安全及密码学等领域应用广泛。“诚实验证方前提（Honest Verifier）”意为验证方是正确遵循协议进行验证的。

用计算复杂度理论（Computational Complexity Theory）的模型定义，零知识证明是一个用于证明 NP（Non-deterministic Polynomial）二元关系 $\mathcal{R}$ 的算法三元组 $(\mathcal{G}, \mathcal{P}, \mathcal{V})$。其中 $\mathcal{G}$ 表示公共参数生成算法，设其输出为 pp；$\mathcal{P}$ 和 $\mathcal{V}$ 分别表示非确定多项式时间（Probabilistic Polynomial Time, PPT）的证明算法和验证算法。

诚实验证方前提的零知识证明[2]具有以下条件需要满足：

- **完备性（*Completeness*）**：即正确的论断都可以被证明为正确。假设 λ 为私有参数，对于每个 $\mathcal{G}$ 的输出 $\mathrm{pp} \leftarrow \mathcal{G}(1^\lambda)$，每个 $\mathcal{R}$ 中的元素 (x, ω)，以及字母表上任意字符串 $z \in \{0,1\}^*$，有：

$$\Pr[\langle \mathcal{P}(\omega), \mathcal{V}(z)(\mathrm{pp}, x) = 1 \rangle] = 1 - \mathrm{negl}(\lambda)$$

  其中 Pr 表示概率，negl(λ) 表示当 λ 足够大时，可以忽略不计的量。

- **正确性（*Soundness*）**：即被证明的论断大都是正确的，只有极小的可能出错。对于每个 $\mathcal{G}$ 的输出 $\mathrm{pp} \leftarrow \mathcal{G}(1^\lambda)$，每个不在 $\mathcal{R}$ 中的元素 (x, ω)，以及字母表上任意字符串 $z \in \{0,1\}^*$，有：

$$\Pr[\langle \mathcal{P}^*(\omega), \mathcal{V}(z)(\mathrm{pp}, x) = 1 \rangle] \leq \mathrm{negl}(\lambda)$$

其中 $\mathcal{P}^*$ 表示任意的 PPT 证明方。

- **零知识性（*Zero-knowledge*）**：即 $\mathcal{P}$ 和 $\mathcal{V}$ 之间的对话可以只依据公开信息被完全模拟。对于每个 $\mathcal{G}$ 的输出 $\text{pp}\leftarrow \mathcal{G}(1^\lambda)$，任意的诚实的 PPT 验证方 $\mathcal{V}$，每个 $\mathcal{R}$ 中的元素 (x,ω) 和任意字母表上的字符串 $z\in\{0,1\}^*$，存在一个 PPT 模拟机 $\mathcal{S}$，使得：

$$\{\langle\mathcal{P}(\omega),\mathcal{V}(z)\rangle(\text{pp},x)\}\overset{c}{\approx}\{\mathcal{S}^{\mathcal{V}}(\text{pp},x,z)\}$$

其中 $\mathcal{S}^{\mathcal{V}}$ 表示多项式空间下给定 $\mathcal{V}$ 的模拟机，$\overset{c}{\approx}$ 表示两者在计算上不可区分（Computationally indistinguishable）。

- **知识论证性（*Argument of knowledge*）**：即所有论证的证明都不会是不合法的。对于每个 $\mathcal{G}$ 的输出 $\text{pp}\leftarrow \mathcal{G}(1^\lambda)$，任意的 $x,z\in\{0,1\}^*$，对于所有恶意的 PPT 证明方 $\mathcal{P}^*$，存在一个可预期多项式时间的抽取机 $\mathcal{E}$，使得：

$$\Pr[\langle\mathcal{P}^*(\omega),\mathcal{V}(z)\rangle(\text{pp},x)=1\wedge((x,\omega)\notin\mathcal{R})|_{\omega\leftarrow\mathcal{E}^{\mathcal{P}^*}(\text{pp},x)}]\leq\text{negl}(\lambda)$$

其中 $\mathcal{E}^{\mathcal{P}^*}$ 表示抽取机对 $\mathcal{P}^*$ 的任意性及整个运行过程都具有访问权限。

4. 交互式谕示机证明

交互式谕示机证明[4] [5]（Interactive Oracle Proof, IOP）是一种证明系统模型，在其中验证方可以通过谕示机概率性地问询证明方所持有的关于被证明的论断的有效信息，但由于是概率性地问询，所以验证方并不能得到证明方的全部信息。

同样，使用计算复杂度理论的模型来定义，IOP 是证明 k 轮 NP 二元关系的算法三元组 $(\mathcal{G},\mathcal{P},\mathcal{V})$，其中 $\mathcal{G}$ 表示公共参数生成算法，设其输出为 pp；$\mathcal{P}$ 和 $\mathcal{V}$ 分别表示 PPT 证明算法和验证算法。具体而言，一个 k 轮的 IOP 包含 k 轮的交互（interaction）。在第 i 轮（$0<i\leq k$），验证方向证明方均匀且随机地发送消息 m_i，且验证方能够通过谕示机得到以 m_i 为输入的输出，证明方需返回 π_i 给验证方。在最后一轮，验证方得到了证明方返回的 k 个位置的信息 $\pi=(\pi_1,\cdots,\pi_k)$，并且需决定接受或拒绝证明方的证明（Proof）。

交互式谕示机证明[6]具有以下条件需要满足：

- **完备性（*Completeness*）**：对于每个 $\text{pp}\leftarrow\mathcal{G}(1^\lambda)$ 以及 $(x,\omega)\in\mathcal{R}$，有：

$$\Pr[\langle\mathcal{P}(\omega),\mathcal{V}^\pi\rangle(\text{pp},x)=1]=1$$

其中 $\mathcal{V}^{\pi}$ 表示 $\mathcal{V}$ 可以访问谕示 π。

- **正确性（*Soundness*）**：对于每个 pp$\leftarrow \mathcal{G}(1^{\lambda})$，每个 PPT 的 $\mathcal{P}^{*}$ 以及 $(x,\omega)\notin\mathcal{R}$，有：

$$\Pr[\langle\mathcal{P}^{*}(\omega),\mathcal{V}^{\pi}\rangle(\text{pp},x)=1]\leq \text{negl}(\lambda)$$

在本文中，主要涉及两种类型的 IOP，分别是 *RS-IOP* 和 *IOP of proximity*，前者即使用里德-所罗门码（Reed-Solomon code）的 IOP，后者指对于正确性的条件，允许证明方的秘密和合法证据之间具有微小的差距（proximity）。

5. 单变量求和校验协议

单变量求和校验协议（Univariate Sum-check Protocol）主要应用于有限域上的多项式求和问题。首先，假设有两个乘法群 $H,L\subset\mathbb{F}$ $(|L|>|H|)$，一个小于 $k(k>|H|)$ 阶的单变量多项式 $f(\cdot)$，以及一个被声明（claimed）的和 μ。在已有假设上，单变量求和校验协议的作用就是证明 $\sum_{a\in H}f(a)=\mu$。

在实际操作中，证明方需要将 $f(x)$ 利用带余除法唯一地转化为 $x\cdot\hat{p}(x)+\zeta+\hat{Z_H}(x)\hat{h}(x)$，其中除式为 $\hat{Z_H}(x)$，代表 H 上的“消失”多项式（Vanishing polynomial），满足 $\forall a\in H,\ \hat{Z_H}(a)=0$。接着，基于对 $\hat{f}|_L$ 和 $\hat{h}|_L$ 的谕示机访问，验证方可以验证是否有 $\hat{p}|_L\in\text{RS}(L,\frac{|H|-1}{|L|})$ 以及 $\hat{h}|_L\in\text{RS}(L,\frac{|L|-|H|}{|L|})$，其中：

$$\hat{p}(x)=\frac{|H|\cdot\hat{f}(x)-\mu-|H|\cdot\hat{Z_H}(x)\hat{h}(x)}{x} \tag{4}$$

以上采用 RS 编码的 IOP 满足正确性和完备性[6]，当我们将它转换为一个标准 IOP 时，它仍然是在检验谕示 $\hat{f}|_L,\hat{h}|_L,\hat{p}|_L$ 是否为具有相应度的界限的 RS 码。而这个过程可以通过下面的低度检测协议来完成。

6. 低度检测和 FRI

给定度 $k_1,\cdots,k_t$，码字 $\hat{v}_1|_L,\cdots,\hat{v}_t|_L$，其中 L 为一个乘法陪集，低度检测协议允许验证方借助对这些码字的谕示机访问来检验以下语句是否成立：

$$\forall j\in\{0,\cdots,t\},\ \hat{v}_j|_L\in\text{RS}[L,\frac{k_j}{|L|}] \tag{5}$$

公式（5）用于检测编码给定码字的编码多项式的度是否低于给定的度。

在本文中，我们的低度检测协议选取快速 Reed-Solomon 交互式谕示机邻近证明[7]（Fast Reed-Solomon Interactive Oracle Proof of Proximity, Fast RS IOPP, FRI）。给定

对证明方消息 l 处取值的谕示机访问，该 FRI 是具有完整性（Completeness）和正确性（Soundness）容错率为 $O(\frac{L}{\mathbb{F}}) + \text{negl}(l,k)$ 的 IOPP，其中 $l = O(\lambda), k = \max\{k_1, \cdots, k_t\}$。

总的来说，用于实现单变量求和校验的 FRI 协议可以表示为：

$$\langle \text{FRI}.\mathcal{P}(\hat{f}, \hat{h}, \hat{p}, \text{FRI}.\mathcal{V}^{\hat{f}|_L, \hat{h}|_L, \hat{p}|_L}) \rangle (k, k-|H|, |H|-1) \tag{6}$$

7. 向量内积论证

向量内积论证（Inner Product Arguments, IPA），是一证明手段，即给出两个向量 $\vec{a}, \vec{b}$ 的承诺（commitment），其中 $\vec{a}, \vec{b}$ 属于 $\mathbb{F}^n$，$\mathbb{F}$ 为域，可以证明这两个被承诺的向量的内积等于某一公开的标量，而不需要揭示这两个向量的具体取值。

在信息安全领域，常见的承诺方式有皮特森哈希值（Pedersen hash）或者 RS 编码，在本文中采用后者。

向量内积论证可以用于证明单变量多项式在某点处的值。首先将多项式 $\hat{f} = f_0 + f_1 x + \cdots + f_n x^n$ 表示为向量 $\vec{f} = (f_0, f_1, \cdots, f_n)$ 注意到：

$$\hat{f}(s) = (\vec{f}, (1, s, \cdots, s^n)) \tag{7}$$

公式（7）表明计算等价于两个向量的内积，因此可转化为向量内积论证。

（三）基于交互式谕示机证明的零知识范围证明

1. 批处理向量内积论证

为了实现批处理 IPA（Batch Inner Product Argument, B-IPA），我们考虑单变量求和校验协议的一个性质：无论多个多项式的阶数是否相同，单变量求和校验协议都支持校验每一个一元多项式的和[6]。此性质为构造一个校验编码向量间内积关系的 IPA 提供了一种可能，其中编码向量来自于不同阶数的编码多项式。

特别地，将阶数分别为 $k_1, ..., k_t$ 的秘密编码多项式设为 $\hat{v}_1, ..., \hat{v}_t$。再将阶数分别为 $k_{t+1}, ..., k_{2t}$ 的公开多项式设为 $\hat{r}_1, ..., \hat{r}_t$。假定证明方 $\mathcal{P}$ 想要证明对于任意 $j \in \{1, \cdots, t\}$，都满足 $\sum_{a \in H} \hat{v}_j(a) \cdot \hat{r}_j(a) = y_j$。实现过程中，证明方 $\mathcal{P}$ 首先需要用默克尔树生成对 $(\hat{v}_1|_L, ..., \hat{v}_t|_L)$ 的承诺，并将其发送给验证方 $\mathcal{V}$。接着，验证方选择随机 t 个元素 $\beta_1, ..., \beta_t$，设 $\hat{q} = \sum_{j=1}^{t} \beta_j \hat{v}_j \cdot \hat{r}_j$。最后证明方 $\mathcal{P}$ 和验证方 $\mathcal{V}$ 使用单变量求和校验协议来证明以下等式成立：

$$\sum_{a \in H} \hat{q}(a) = \sum_{a \in H} \sum_{j=1}^{t} \beta_j \hat{v}_j(a) \cdot \hat{r}_j(a) = \sum_{j=1}^{t} \beta_j y_j \tag{8}$$

除此之外，批处理 IPA 的正确性容错率（Soundness error）仅取决于 t 个项中最大的阶数 $k_{\max}$，$k_{\max} = \max\{k_i + k_{t+i}\}_{1\le i\le t}$。

基于此，我们给出**批处理内积关系（*Batch inner product relation*）**的定义：设二元关系 $\mathcal{R}_{\text{B-IPA}}$ 为所有 (x,ω) 的集合，其中：

$$x = (\mathbb{F}, H, L, \{k_j\}_{1\le j\le 2t}, \{\hat{r}_j\}_{1\le j\le t}, \{y_j\}_{1\le j\le t})$$
$$\omega = \{\hat{v}_j\}_{1\le j\le t}$$

且有公式（8）成立。

接下来验证该批处理 IPA 的正确性、完备性以及知识论证性：

- **批处理 IPA 的完备性（*B-IPA Completeness*）**：考虑 $\hat{q}$ 的变换，设对 $j \in \{1,\cdots,t\}$，有 $\sum_{a\in H}\beta_j v_j(a) r_j(a) = \beta_j y_j$，那么公式（8）成立。这符合单变量和校验的二元关系形式。因此，批处理 IPA 有着与单变量和校验协议相同的完备性。

- **批处理 IPA 的正确性（*B-IPA Soundness)*）**：可以考虑以下两种发生错误的情形：

  情形一. 假设由于随机的线性选择组合，非法的单变量和校验关系恰好成立。我们假设 $\forall j \in \{1,\cdots,t\}, \sum_{a\in H}\hat{v}_j(a)\cdot\hat{r}_j(a) = y'_j$，且对于 $\{1,\cdots,t\}$ 的某个子集 Q，有 $\forall q \in Q, y_q \neq y'_q$。简便起见，不妨设 $t \in Q$。验证方随机选择 t-1 个元素 $\beta_1,\cdots,\beta_{t-1}$，则 $\sum_{j=1}^{t}\beta_j y_j = \sum_{j=1}^{t}\beta_j y'_j$ 当且仅当：

$$\beta_t = \frac{\beta_1(y'_1 - y_1) + \cdots + \beta_{t-1}(y'_{t-1} - y_{t-1})}{y_t - y'_t} \tag{9}$$

  公式（9）发生的可能性仅为 $1/|\mathbb{F}|$，而实际选用的有限域大小往往很大，因此概率可忽略不计。

  情形二. 假设变量和校验关系是非法的，即公式（8）不成立。那么批处理 IPA 正确性的错误有以下三种可能：

  （1）若 RS 编码的 IOP 非法，则正确性取决于单变量和校验协议，故具有正确性。

  （2）若 FRI 非法，则正确性错误的上界为 $\epsilon_{FRI} = \mathcal{O}(|L|/|\mathrm{F}|) + negl(\ell, k_{max}/|L|)$。

  （3）若默克尔树的根不正确或任意验证路径不正确，由于哈希函数的防碰撞性质，正确性错误的上界为 $negl(\lambda)$。

- **批处理 IPA 的知识论证性（*B-IPA Knowledge Argument)*）**：批处理 IPA 是基于随机谕示机模型的一种知识论证。对于任意 PPT 对手 $\mathcal{P}^*$，总存在一个 PPT 抽取机 $\mathcal{E}$

使得：给定 $\mathcal{P}^*$ 的随机访问带，对每个由 $\mathcal{P}^*$ 生成的陈述：

$$x = (\mathbb{F}, H, L, \{k_j\}_{j\in[2t]}, \{\hat{r_j}\}_{j\in[t]}, \{y_j\}_{j\in[t]}) \tag{10}$$

有以下的概率为 negl(λ)：

$$\Pr\left[\begin{array}{c} \text{root}^* \leftarrow \mathcal{P}^*(1^\lambda, x), \langle \mathcal{P}^*, \mathcal{V}\rangle(\text{pp,x}) = 1, \{\hat{v}_j\}_{1\le j\le t} \leftarrow \mathcal{E}(1^\lambda, x) : \\ \text{MT.Commit}(\mathbb{V}|_L) \neq \text{root}^* \vee (x, \{\hat{v}_j\}_{1\le j\le t}) \notin \mathcal{R}_{\text{B-IPA}} \end{array}\right] \tag{11}$$

批处理 IPA 的知识论证属性来源于默克尔树的可抽取性。给定默克尔树树根和足够多的验证通路，总存在一个高效的方法能够抽取默克尔树上所有被承诺的叶节点。一旦这些叶节点被成功提取，就能通过 IFFT 算法获取满足 $|L| > k_{\max}$ 的秘密多项式，进而实现知识论证的属性[4] [2]。

图 2 展示了在批处理 IPA 中，证明方与验证方进行交互、证明方向验证方证明 $(x, \omega) \in \mathcal{R}_{\text{B-IPA}}$ 的流程。

其中 $\mathbb{V}|_L \in \mathbb{F}^{t\times|L|}$ 表示矩阵 $(a_{ij})_{t\times|L|} = (\hat{v}_i|_L[j])$。MT.Commit($\mathbb{V}|_L$) 表示将矩阵 $\mathbb{V}|_L$ 的每一列放入默克尔树的叶节点。

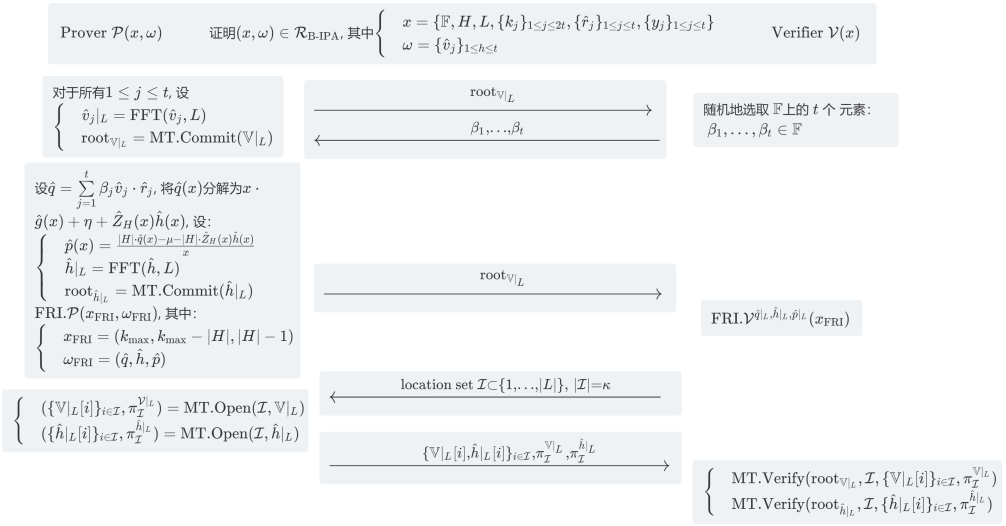

图 2：批处理向量内积论证（Batch IPA）$\langle \text{IPA}_B.\mathcal{P}(\omega), \text{IPA}_B.\mathcal{V}\rangle(x)$

2. 对于 $[0, u^{n-1}]$ 的范围证明

为了证明上界为 u^m（即 u 进制展开为 m 位）的秘密值 V 在范围 $[0, 2^n - 1]$ 中 $(n < m)$，只需要满足以下等式：

$$\begin{aligned} &v \odot (v - 1^m) \odot \cdots \odot (v - u^m) = 0^m, \\ &v \odot (1^{m-n} || 0^n) = 0^m. \end{aligned} \tag{12}$$

其中 $v = (v_0, v_1, \ldots, v_{m-1}), V = \sum_{j=0}^{m} v_j u^j$。进一步地，相当于证明：

$$\begin{aligned} &\langle v \odot (v - 1^m) \odot \cdots \odot (v - u^m), r \rangle = 0, \\ &\langle v, r_{[:m-n]} || 0^n \rangle = 0. \end{aligned} \tag{13}$$

经理论计算，对于验证方选取的任意 $r \in \mathbb{F}$，公式（13）非法成立，即出现正确性错误的概率为 $1/\mathbb{F}$。

对于公式（13），可以利用批处理 IPA 来证明，即输入设为：

$$\begin{aligned} &x = (\mathbb{F}, H, L, (u|H| - (u-1)), |H|, |H|, |H|, (\hat{r}, \hat{s}), (0,0)), \\ &\omega = (\hat{w}, \hat{v}) \end{aligned} \tag{14}$$

基于此，我们给出**范围关系（*Range relation*）**的定义：设二元关系 $\mathcal{R}_{\text{RP}}$ 为所有 (x, ω) 的集合，其中：

$$x = (\mathbb{F}, H, L, m, n, [0, u^n - 1]),\ \omega = V.$$

且有秘密值 V 满足 $V \in [0, u^n - 1]$ 成立。

图（3）展示了在 RP 中，证明方与验证方进行交互、证明方向验证方证明 $(x, \omega) \in \mathcal{R}_{\text{RP}}$ 的流程。其中 $\mathbb{F}$ 是一个有限域，L, H 是 $\mathbb{F}$ 的乘法陪集。秘密值 V 满足 $V \in [0, u^n - 1]$。

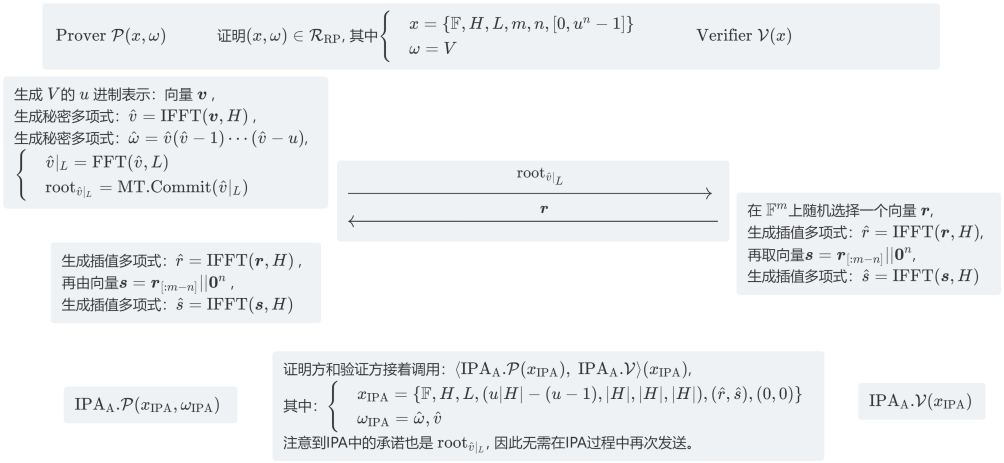

图 3：范围证明（Range Proof）$\langle\mathbf{RP}.\mathcal{P}(\omega),\mathbf{RP}.\mathcal{V}\rangle(x)$

3. 批处理范围证明

基于前述的批处理 IPA，我们可以构建一个证明多个秘密值在各自对应范围内的证明。假设我们要证明秘密值 $V_1,...,V_t$ 分别处于对应范围 $[0,u_1^{n_1}-1],...,[0,u_t^{n_t}-1]$，那么对于任意 $j\in\{1,\ldots,t\}$, 都有如下公式：

$$\begin{aligned} &v_j\odot(v_j-1^m)\odot\cdots\odot(v_j-u_j^m)=0^m,\\ &v_j\odot(1^{m-n_j}||0^{n_j})=0^m \end{aligned} \tag{15}$$

其中 $m\geq\max\{n_1,...,n_t\}$。进一步转换上述公式，可以推出：对于任意 $j\in\{1,\cdots,t\}$, 都有如下公式：

$$\begin{aligned} &\langle v_j\odot(v_j-1^m)\odot...\odot(v_j-u_j^m),r\rangle=0,\\ &\langle v_j,(r^{m-n_j}||0^{n_j})\rangle=0 \end{aligned} \tag{16}$$

对于公式（16），可以利用批处理 IPA 来证明，即输入设为：

$$\begin{aligned} &x=(\mathbb{F},H,L,\{k_j\}_{j\in[4t]},\{\hat{r}_j\}_{j\in[2t]},\{y_j\}_{j\in[2t]}),\\ &w=\hat{w}_1,...,\hat{w}_t,\hat{v}_1,...,\hat{v}_t, \end{aligned} \tag{17}$$

其中一些变量满足如下关系:

$$\begin{aligned}
\{k_j\}_{j\in[t]} &= \underbrace{u_1|H| - (u_1 - 1), ..., t_t|H| - (u_t - 1)}_{t}, \\
\{k_j\}_{j\in[t+1,4t]} &= \underbrace{|H|, ..., |H|}_{3t}, \\
\{\hat{r}_j\}_{j\in[2t]} &= \underbrace{\hat{r}, ..., \hat{r}}_{t}, \underbrace{\hat{s}_1, ..., \hat{s}_t}_{t}, \\
\{y_j\}_{j\in[2t]} &= \underbrace{0, ..., 0}_{2t}.
\end{aligned} \tag{18}$$

其中对任意 $j \in \{1, \cdots, t\}$, $\hat{s}_j$ 和 $\hat{v}_j$ 是 $r^{m-n_j}||0^{n_j}, v_j$ 的编码多项式, 以及 $\hat{w}_j = \hat{v}_j(\hat{v}_j - 1) \cdots (\hat{v}_j - u_j)$。

4. 对于任意范围的范围证明

考虑到实际整数范围证明往往是任意整数, 我们需要进一步拓宽前述范围证明的通用性。为了实现这一点，我们需要利用前述的对范围 $[0, u^n - 1]$ 的范围证明。假设要验证秘密值 $V \in [A, B - 1]$, 其中 A, B 均为任意整数。收到 Camenisch[8] 等人的启发，我们首先将这个问题进行如下转化:

$$V - A \in [0, u^n - 1] \wedge V - B + u^n \in [0, u^n - 1] \tag{19}$$

其中 $u^{n-1} < B < u^n$。基于新的公式，我们成功将任意整数范围的证明转化到了范围 $[0, u^n - 1]$ 的证明上，从而我们可以利用前述的对范围 $[0, u^n - 1]$ 的范围证明来实现任意范围的范围证明。

在任意范围的证明流程中，验证方不采用基于秘密值 V 的向量 v 的询问，而是直接让证明方通过 IPA 证明 $V - A = C$ 和 $V - B + u^n = D$。由于此处 IPA 不止一个，因此我们可以引入批处理 IPA 来加快处理过程。实际上，任意范围的范围证明可以简单看作基于批处理 IPA 的多个任意基底范围证明的有效融合。

5. 补充零知识性

前述的范围证明实际上并不是零知识性的，它存在两个层面的知识泄露:

- 问询环节: 在验证者打开默克尔树的承诺时, 其可见 l 个 $\mathbb{V}|_L$ 的估值。而这些估值与秘密向量 $\{v_j\}_{1\le j\le t}$ 相关，因而会泄露 $\{V_j\}_{1\le j\le t}$ 的部分信息。
- PRI 协议环节: 在验证方借助 $O(\log|L|)$ 轮对码字 $\hat{v}_1|_L, \cdots, \hat{v}_L|_L$ 的谕示机访问时,

验证方可以根据这些已得的信息获取额外的其他信息。

因此，我们采取与张、谢等人[2]相似的处理。

对于第一个知识泄露，我们使证明者采取以下措施：选择一个度为 l 的随机多项式 $\hat{\delta}_j$，利用其掩盖 $\hat{v}_j$，即 $\hat{v}'_j = \hat{v}_j + \hat{Z}_H \cdot \hat{\delta}_j$，其中 $\hat{Z}_H$ 是陪集 H 上的“消失”多项式，即对 $\forall h \in H, \hat{Z}_H(h) = 0$.

对于第二个知识泄露，我们使证明者采取同样的措施，即使用随机多项式 $\hat{\gamma}$ 来掩盖秘密多项式 $\hat{v}$，并控制 $\hat{\gamma}$ 的度在 $(u_{\max}+1)|H| + u_{\max}(l-1)$。基于以上处理，我们给出批处理的零知识范围证明的流程，如图（4）所示。

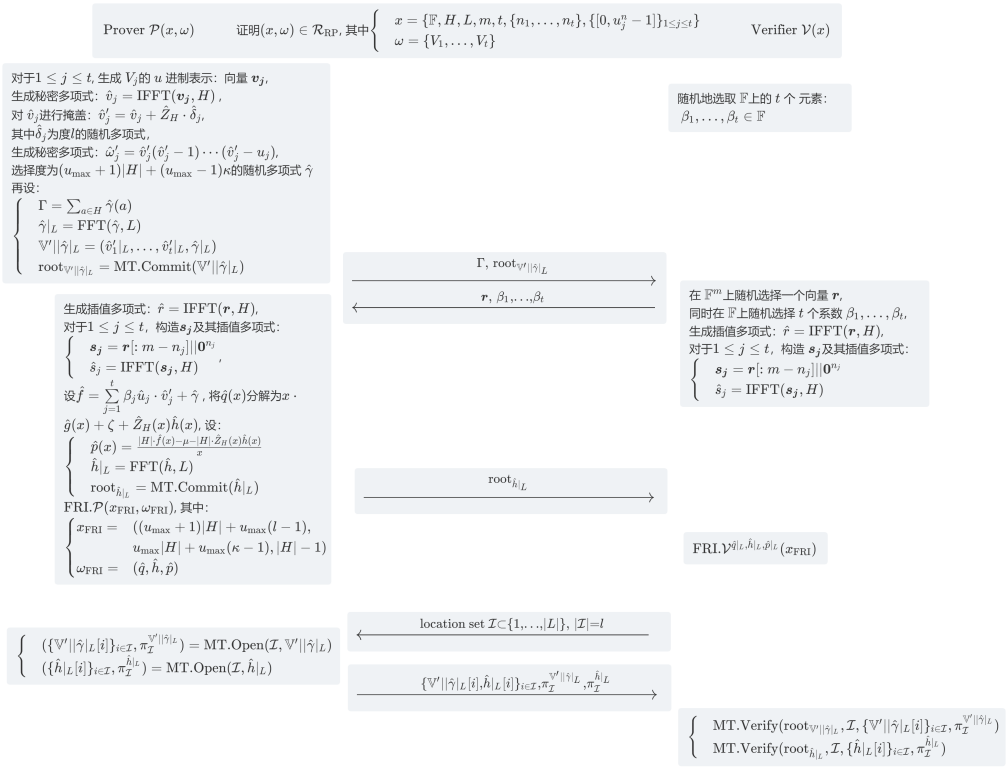

图 4：零知识范围证明（Zero-Knowledge Range Proof）$\langle \mathbf{RP_{zk}}.\mathcal{P}(\omega), \mathbf{RP_{zk}}.\mathcal{V}\rangle(x)$

可以证明，以上流程具有完备性（Completeness）、正确性（Soundness）、知识论证性（Argument of knowledge）、诚实验证者前提的零知识性（Honest-verifier zero knowledge）。

四、图表模板

图表示例展示如下：

图 5 example_caption

(a) 示意图 1

(b) 示意图 2

(c) 示意图 3

图 6 一行三张子图并排示意

表 2 三线表使用示例

方法	表头 1	表头 2	表头 3	表头 4
方法 1	数据	数据	数据	数据
方法 2	数据	数据	数据	数据

结论

论文的结论单独作为一章，但不加章号。

注意: 文件大小不超过 5M。

(a) 示意图 1

(b) 示意图 2

(c) 示意图 3

(d) 示意图 4

图 7 2*2 四张子图示意

参考文献

[1] MERKLE, R.C. *A certified digital signature*[M]//CRYPTO 1989. Springer, 1989: 218–-238.

[2] ZHANG X T Z Y S D, J. *Transparent polynomial delegation and its applications to zero knowledge proof* [M]//SP 2020. IEEE, 2020: 859–-876.

[3] BHADAURIA F Z H C V M X T Z Y, R. *Ligero++: A new optimized sublinear IOP* [M]//CCS 2020. ACM, 2020: 2025–-2038.

[4] BEN-SASSON C A S N, E. *Interactive oracle proofs*[M]//TCC 2016-B. 2016: 31–-60.

[5] REINGOLD R G R R, O. *Constant-round interactive proofs for delegating computation* [M]//STOC 2016. ACM, 2016: 49-–62.

[6] BEN-SASSON C A R M S N V M W N, E. *Aurora: Transparent succinct arguments for R1CS*[M]//EUROCRYPT 2019. Springer, 2019: 103–-128.

[7] BEN-SASSON B I H Y R M, E. *Fast reed-solomon interactive oracle proofs of proximity* [M]//ICALP 2018. 2018: 14:1–-14:17.

[8] CAMENISCH C R S A, J. *Efficient protocols for set membership and range proofs*[M]// ASIACRYPT 2008. Springer, 2008: 234–-252.