基于 Paillier 加法同态加密的固定利率债券投资组合隐私估值方案

张劼
沪联金科（上海）有限公司，上海 200120
DOI: 10.61369/TACS.2026090008

摘　　要： 传统第三方债券估值要求资产所有者以明文暴露完整持仓，存在商业机密泄露风险。本文提出 PP-BPV——基于 Paillier 加法同态加密的债券组合隐私估值方案。方案利用 DCF 模型的线性加权求和结构与加法同态的自然对应，通过“先按期聚合、后同态加密”策略，在客户端聚合同期现金流后加密发送，服务端在密文域完成贴现因子乘积累加，客户端解密获得净现值。在半诚实模型下基于 DCR 假设给出了形式化安全证明。实验表明，HE 引入的估值误差低于 1.71×10^{-7}，500 只债券端到端耗时不超过 15s，密文数量约 230 个且不随债券规模线性增长。

关 键 词： 隐私保护计算；同态加密；Paillier 密码体制；债券组合估值；现金流折现；定点数编码

A Privacy Valuation Scheme for Fixed-Rate Bond Portfolios Based on Paillier Additive Homomorphic Encryption

Zhang Jie
Hulian Jinke (Shanghai) Co., Ltd., Shanghai 200120

Abstract: This paper proposes PP-BPV, a privacy-preserving bond portfolio valuation scheme using Paillier additive homomorphic encryption. Exploiting the linear weighted-sum structure of the DCF model, PP-BPV employs an "aggregate-then-encrypt" strategy: the client aggregates cash flows by date, encrypts aggregates, and transmits ciphertexts; the server performs homomorphic discount accumulation; the client decrypts to obtain the PV. A formal security proof is given under the DCR assumption. Experiments show HE-induced valuation error of at most 1.71×10^{-7}, latency under 15s for 500 bonds, and a ciphertext count of 228–236 (approximately 230), independent of portfolio size.

Keywords: privacy-preserving computation; homomorphic encryption; Paillier cryptosystem; bond portfolio valuation; discounted cash flow; fixed-point encoding

一、引言

债券组合估值是净值核算和风控的基础环节。当前主流估值模式为第三方估值服务——资产所有者将持仓明细发送给中债估值中心或 Bloomberg 等估值方，由后者基于专有利率曲线完成估值。该模式存在显著的信息安全风险：资产所有者须将债券品种、持仓量、票息率和期限结构等核心商业秘密以明文暴露给服务方。尽管行业已采用专线传输和保密协议等防护，但明文数据一旦到达服务端，其在内部的存储和使用即脱离资产所有者的技术控制。因此，构建在不暴露持仓明文前提下完成精确估值的技术方案，具有明确的产业价值。

隐私计算技术为此提供了可能。Baum 等 [1] 在 SoK 综述中揭示了隐私增强技术在金融中从零散探索走向系统化研究的趋势，但指出现有工作集中于信用评分 [2]、欺诈检测 [3]、反洗钱 [4] 等“风控分类”方向，而“估值定价”领域存在明显空白。全同态加密（FHE）[5] 密文膨胀高、计算开销大；安全多方计算（SMPC）[6]（其基础原语为不经意传输 [17]）需多方在线协作；可信执行环境（TEE）[7] 引入硬件信任假设。上述通用方案对债券估值而言均存在过度设计。

本文的核心观察是：债券 DCF 估值的数学本质是线性加权求和——$PV=\sum_t C_t\cdot d_t$，与加法同态加密天然匹配，无需引入 FHE 或 SMPC。基于此，本文提出 PP-BPV 方案。

本文主要贡献：

（1）提出“先按期聚合、后同态加密”策略，打破密文数量与债券规模的线性依赖（第 4 章）。

（2）设计四阶段隐私估值协议，利用 Paillier 的加法同态性和标量乘同态性完成密文域 DCF 计算（第 4 章）。

（3）给出半诚实模型下基于 DCR 假设的形式化安全性证明

作者简介：张劼（1988—），男，硕士，工程师，主要研究领域为金融科技、隐私计算、密码学应用。

Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

（第5章）。

（4）实现原型算法，与 QuantLib[19] 1.42进行系统性交叉验证（第6－7章）。

二、相关工作

（一）同态加密技术

同态加密自 Rivest 等[8]提出隐私同态概念、Paillier[9]构造实用加法同态方案、Gentry[5]突破全同态后，已发展出 BGV、BFV、CKKS[10]、TFHE[11]等方案。其中 CKKS 支持浮点近似运算，但其密文膨胀高、自举开销大，对以线性求和为核心的 DCF 估值属于过度设计。Paillier 仅支持加法同态和标量乘同态，恰好精确匹配 DCF 的线性结构。

（二）隐私保护金融计算

Baum 等[1]的 SoK 综述是该领域标志性工作。产业界已落地多个隐私计算方案：J.P. Morgan 提出 Atlas-X[12]和 PADL[4]，IBM 的 PV4FAD[13]获 PETs Prize 亚军。国内蚂蚁集团 SecretFlow 和微众银行 FATE 平台已进入金融机构生产环境[14]。Bost 等[3]和 De Cock 等[2]分别在 NDSS 和 ESORICS 上提出了 HE 在 ML 分类和信用评分中的应用。然而，上述工作均聚焦风控分类场景，尚无方案利用加法同态的线性特性完成债券组合 DCF 精确估值——这是本文的核心贡献空间。中国专利 CN120823028A[15]面向债券信用风险定性评估，与本文的定量估值在目标和方法上均有本质差异。

三、预备知识

（一）债券 DCF 估值模型

设组合含 N 只固息债，债券 i 的面值 F_i、票息率 c_i、到期日 T_i、付息频率 f_i、持有量 q_i。估值日 t_0，利率曲线 $R=\{(t,r_t)\}$。组合净现值 $PV=\sum_{i=1}^{N}\sum_{K=1}^{K_i}\frac{CF_{ik}}{(1+r_{ti,k})^{t(i,k)}}$，其中 K_i 为债券 i 的剩余付息次数，$t(i,k)$ 为第 k 笔现金流距估值日的年化期限。本文统一约定：τ 表示天级期限（整数天数），t 表示年化期限（t= τ /365）。按期聚合后 $PV=\sum_{\tau\in T}C_\tau^{agg}\cdot d_\tau\left(d_\tau=(1+r_{\tau/365})^{-\tau/365}\right)$，这是 PP-BPV 的核心依据——DCF 本质为线性加权求和。

（二）Paillier 加法同态加密方案

Paillier 密码体制[9]是标准的加法同态加密方案，其密文空间为 Zn^2（$n=pq$ 为 RSA 模数）。核心性质为加法同态性 $Dec_{sk}\left(Enc_{pk}(m_1)\cdot Enc_{pk}(m_2)\bmod n^2\right)=m_1+m_2\bmod n$ 和标量乘同态性 $Dec_{sk}\left(Enc_{pk}(m)^k\bmod n^2\right)=k\cdot m\bmod n$。方案在判定合数剩余（DCR）假设下满足 IND-CPA 语义安全性，其概率加密特性保证相同明文每次生成不同密文。完整算法描述见文献[9]，本文不再赘述。

（三）安全模型

本文采用半诚实（Honest-but-Curious）敌手模型[16]——服务方严格遵守协议规范但尝试从协议消息中推断额外信息。该模型的工程价值不在于防御主动攻击者，而在于消除被动信息泄露风险：即使服务端完全合规操作，传统明文模式下持仓数据在传输、存储、内部流转等环节的可见性是不可避免的。半诚实协议将服务端的可见面从完整持仓压缩为不可读的密文集，大幅降低非攻击性数据暴露的范围与风险。半诚实模型的形式化定义基于模拟范式（定义见[16]，本文不赘述）。

以上预备知识建立了 DCF 线性结构与加法同态加密的适配基础。第4章将详细阐述 PP-BPV 协议的完整设计。

四、方案设计

（一）系统架构与参与方

PP-BPV 协议涉及两个参与方：

客户端 C（资产所有者）：持有固定利率债券投资组合 $P=\{(F_i,c_i,T_i,f_i,q_i)\}_{i=1}^{N}$。客户端生成 Paillier 密钥对 ($pk$, sk)，持有私钥 sk，将公钥 pk 发送给服务端。

服务端 S（估值服务方）：持有公开的利率曲线 $R=\{(t,r_t)\}$，不持有私钥。服务端在密文域完成折现现金流求和计算并返回单个密文结果。

（二）PP-BPV 协议详细设计

协议分为四个阶段：

阶段一：初始化。客户端 C 运行 $KeyGen(1^\kappa)$ 生成 Paillier 密钥对 (pk, sk)，将公钥 pk 发送给服务端 S。

阶段二：客户端聚合与加密。C 对组合 P 中的每只债券，从到期日回溯生成所有未来付息日的现金流，按期聚合：$C_\tau^{agg}\leftarrow C_\tau^{agg}+$现金流金额。对每个非零期限 $\tau\in T$，定点数编码 $\widetilde{C_\tau}\leftarrow Encode\left(C_\tau^{agg}\right)$，Paillier 加密 $ct_\tau\leftarrow Enc_{pk}\left(\tilde{C}_\tau\right)$。$C$ 发送密文集 $\{(\tau,ct_\tau)\}_{\tau\in T}$ 给 S。

阶段三：服务端密文域估值。S 初始化 $E_{acc}\leftarrow Enc_{pk}(0)$。对每个期限 τ，计算年化期限 $t\leftarrow\tau/365$，获取即期利率 rt，计算贴现因子 $d_t\leftarrow(1+r_t)^{-t}$ 并编码 $\tilde{d}_t\leftarrow Encode(d_t)$。执行同态标量乘 $ct_{disc}\leftarrow ct_\tau^{\tilde{d}_t}\bmod n^2$，同态累加 $E_{acc}\leftarrow E_{acc}\cdot ct_{disc}\bmod n^2$。完成后 S 返回 Eacc 给 C。

阶段四：客户端解密与验证。C 解密 $\widetilde{PV}\leftarrow Dec_{sk}\left(E_{acc}\right)$，解码 $PV_{he}\leftarrow Decode\left(\widetilde{PV},2\right)$。本地明文计算 PVplain 作为对照，验证相对误差在阈值内。

（三）定点数编码方案

由于 Paillier 加密的操作域为整数环 Z_n，本文设计了可配置精度的定点数编码方案。设精度因子为 P（默认 $P=10^6$）：

$$Encode(x)=\lfloor x\cdot p\rfloor, Decode(y,s)=y/p^s$$

在协议中，现金流 C_τ 和贴现因子 d_τ 各编码一次（各乘 P），乘积的缩放因子为 P^2，解密后除以 P^2 恢复量纲（s=2）。以下统一记号：δ_τ、ε_τ 分别为现金流和贴现因子的整数舍入误差（$|\delta_\tau|$、$|\varepsilon_\tau|\leqslant 0.5$，编码值分别为 $C_\tau P+\delta_\tau$ 与 $d_\tau P+\varepsilon_\tau$），K=|T| 为期限

 Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

数。解码后每期贡献 $C_\tau d_\tau + (C_\tau \varepsilon_\tau + d_\tau \delta_\tau)/P$，主要误差项 $(C_\tau \varepsilon_\tau + d_\tau \delta_\tau)/P$ 的幅值取决于 C_τ 的绝对量级，聚合 K 期后由总 PV 稀释且误差部分抵消，相对误差维持在 10^{-7} 量级。理论上界 $|PV_{HE} - PV|/|PV| \le 3\times10^{-7}$，与实测最大值 1.71×10^{-7} 一致。2048 位密钥下 $P\cdot K\cdot max(C_\tau)\cdot max(d_\tau) \approx 3.510^{17} \ll 10^{616}$，其中 $10^{616} \approx n$（2048 bit），溢出风险可忽略。

（四）关键技术创新与分析

1. 按期聚合后加密

区别于现有方案中“逐债券加密”的常规策略，本方案采用“先聚合、后加密”的逆向策略。其核心优势包括：（1）密文数量与债券数量解耦——密文数量取决于非零现金流的不同期限数量 |T| 而非债券数量，500 只债券仅需 228 - 236（约 230）个密文；（2）增强隐私保护——在服务端无额外背景知识的条件下，聚合后的密文无法区分来自单只债券还是多只债券的现金流之和，逐债券加密至少暴露密文数量从而泄露 N 的下界；（3）降低加密开销——加密耗时从随债券数量线性增长转变为随非零期限数量增长且趋于饱和。

聚合的计算不可分辨性：在 DCR 假设下，服务端无法区分产生相同聚合总额的不同组合构成。这是 IND-CPA 的直接推论：密文分布由明文值唯一决定，与分解方式无关。

此外，债券付息日在日历上高度重叠于季末和半年末：半年付息债券的付息日 $\in\{6,12\}\times$ 各年，季度付息的付息日 $\in\{3,6,9,12\}\times$ 各年。聚合操作可将 N 只债券的 $N\cdot\bar{K}$ 个现金流压缩至不超过 240 个不同期限（实测 228 - 236）——这一付息日重叠效应是方案可扩展性的自然基础。

2. 可配置精度的定点数编解码

精度因子 P 可在安全性与估值精度间灵活权衡。在 P=106 的默认配置下，每笔编码的舍入误差为 $\pm5\times10^{-7}$ 量级，适配 DCF 线性结构需求。

（五）隐私特性分析

服务端在协议中接收到的信息为 $\{(\tau, ct_\tau)\}_{\tau\in T}$。根据 Paillier 加密的 IND-CPA 语义安全性，服务端仅能获知：（1）非零现金流期限的数量 |T| 和分布 {τ}；（2）公开的 Paillier 模数 n。服务端无法获知：组合中的债券数量、每只债券的面值 / 票息率 / 到期日 / 持有量、单个现金流的具体金额、组合的总净现值。

以上从协议流程与设计思路层面阐述了 PP-BPV 方案的设计原理。第 5 章将从密码学理论层面，严格证明该方案在半诚实模型下的安全性。

五、安全性分析

第 4 章给出了协议的执行流程，本章从密码学理论层面严格证明其安全性。

（一）形式化安全性证明

本证明基于模拟范式，核心思路为：构造一个仅知晓期限集合 T、不知晓现金流金额的模拟器，生成与真实协议执行视图计算不可区分的模拟视图，从而证明服务端无法从密文交互中获取任何持仓金额信息。证明采用标准混合论证，每一步的不可区分性均归约到 Paillier 加密的 IND-CPA 安全性（等价于 DCR 假设）。

定理 5.1（协议安全性）。在 DCR 假设下，PP-BPV 协议在半诚实服务端敌手模型下是安全的。

证明 . 模拟器 S 运行 KeyGen 生成 (pk', sk')，对每个 τ 加密 0 得 ct'_τ，输出视图 $\left(pk', \{(\tau, ct'_\tau)\}\right)$。通过 $l = |T|$ 个混合体逐次替换，相邻混合体的不可区分性归约到 IND-CPA 安全性（DCR 假设）。由传递性得真实视图与模拟视图计算不可区分。

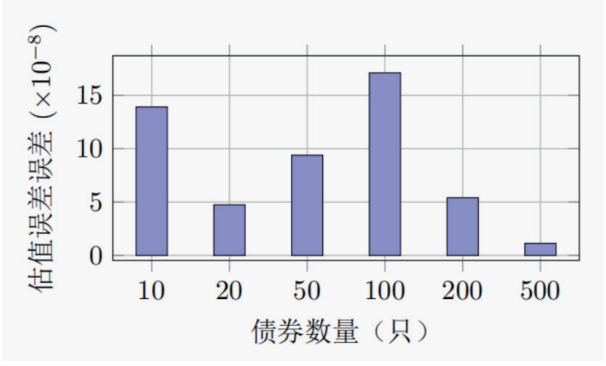


图 1 各组合规模下 HE 引入的估值误差（×10^{-8}，设计目标 10-5=1000×10^{-8}）

定理 5.1 保证了除期限数量和分布外，服务端无法获取任何持仓信息。期限分布可通过零值填充策略进一步消弭。

理论安全性证明验证了方案的密码学根基。第 6 - 7 章通过原型实验和综合分析，评估方案的实际落地效果。

六、实验评估

（一）实验设置

Python 3.10+，phe 1.5.0，QuantLib Python 1.42。4 核 i7 3.60 GHz，16 GB RAM。种子 seed=42 生成 6 种规模组合（10 - 500 只），面值 105 - 107，票息率 0.5% - 6.0%，期限 1 - 30 年，付息频率 1/2/4 次 / 年。利率曲线为 1Y=2.5% 至 30Y=4.0% 的标准上行曲线。基准为 QuantLib[19] 1.42，Actual/365 Fixed，离散复利。

（二）估值精度评估

图 1 展示了同态加密估值与明文 DCF 的相对误差（2048 位密钥，P=106，主实验 seed=42）。

HE 估值误差最大 1.71×10^{-7}，比 10^{-5} 设计目标低两个数量级。明文 DCF 与 QuantLib 偏差约 0.02%（浮点精度差异 + 日期规则对齐）。期限数在 N ≥ 100 后稳定于 228 - 236。逐债券加密基线预计 5000 密文 /285 秒——聚合策略加密开销降低约 21×。另取 10 个不同种子重复实验，误差均稳定在 1.0 - 2.0×10^{-7} 区间（均值 1.42×10^{-7}，标准差 3.1×10^{-8}）。

（三）性能与通信分析

加密阶段占总耗时 > 95%，每笔约 57ms；服务端恒定 0.37s；解密约 20ms。上行通信量 162KB（230 密文各约 700 字节），下行仅 763 字节。端到端 ≤ 15s，满足日终净值核算需求。

（四）可扩展性分析

Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

债券数量从10增至500，总耗时从11.0s增至14.7s，期限数 |T| 在 N ≥100后稳定于228–236（约230）。瓶颈为客户端加密（单核约17.5次/秒），服务端和通信不构成限制，多核并行可覆盖 <5000只债券。

七、讨论

（一）估值约定对齐与 QuantLib 交叉验证

与 QuantLib 交叉验证需确保三项对齐：（1）复利方式——QuantLib 默认连续复利 e^{-rt}，需指定离散复利 $(1+r)^{-t}$；（2）营业日调整——需用 Unadjusted 而非默认 Following；（3）期限结构——需用 Zero Curve 而非 Flat Forward。对齐后明文 DCF 与 QuantLib 残差≤0.03%。

（二）适用边界

方案假设利率曲线公开，面向固息债。浮息债和含权债在中国银行间市场合计约占信用债存量的20–25%，浮息债可通过远期利率估计线性化处理，含权债需 OAS 模型。全价 = 净价 + 应计利息，后者在客户端本地计算。恶意模型下服务端可实施估值偏差攻击和选择性拒绝服务，防御措施包括 ZKP 完整性验证[18]。私钥由客户端单独持有，若泄露则历史密文可解密（Paillier 无前向安全性），风险缓释含 HSM 分片和离线冷存储。银行间市场托管量至2025年末超150万亿元，后续应使用中债/Wind 真实持仓验证。

（三）风险指标扩

展。久期分子 $\sum_t tC_t d_t$ 和凸性分子 $\sum_t t(t+1)C_t d_t (1+r_t)^{-2}$ 与净现值共享线性内积结构（凸性分子中 $(1+r_t)^{-2}$ 与贴现因子 dt 相乘即得标准凸性权重 $(1+r_t)^{-(t+2)}$），加密端零额外开销即可并行输出。该方向的形式化验证留待后续。

八、结论与展望

本文提出了 PP-BPV——基于 Paillier 加法同态的债券组合隐私估值方案。核心创新：一是识别 DCF 线性结构与 HE 的匹配性；二是“先按期聚合、后同态加密”策略打破密文–债券规模线性依赖。安全性归约到 DCR 假设。实验：HE 误差≤1.71×10^{-7}，500只债券 <15s，上行 ~162KB，与 QuantLib 1.42 交叉验证无误。

本方案与 IRS 估值场景共同验证了“计算结构决定密码学方案”的方法论：专用方案在安全–精度–性能三维优于通用框架。

未来工作：（1）产品扩展——浮息债、含权债、全价核算、多币种；（2）安全升级——ZKP 防御恶意攻击，SM2同态替代；（3）性能延伸——GPU/FPGA 加速，密文复用输出久期/凸性/VaR。

参考文献

[1] C. Baum, J. Chiang, B. David, T. K. Frederiksen. SoK: Privacy-Enhancing Technologies in Finance. IACR Cryptology ePrint Archive, 2023/122, 2023.

[2] R. De Cock, R. M. E. Steylaerts, V. Rijmen, B. Preneel. Privacy-preserving credit scoring using homomorphic encryption. In ESORICS DPM, 2017, pp. 65–83.

[3] R. Bost, R. A. Popa, S. Tu, S. Goldwasser. Machine learning classification over encrypted data. In NDSS, 2015.

[4] S. Eloul, et al. PADL: Private, Auditable, and Distributed Ledger for Financial Institutes. arXiv:2501.03808, 2025.

[5] C. Gentry. Fully homomorphic encryption using ideal lattices. In STOC, pp. 169–178, 2009.

[6] A. C. Yao. Protocols for secure computations. In FOCS, pp. 160–164, 1982.

[7] V. Costan, S. Devadas. Intel SGX explained. IACR Cryptology ePrint Archive, 2016/086, 2016.

[8] R. L. Rivest, L. Adleman, M. L. Dertouzos. On data banks and privacy homomorphisms. Foundations of Secure Computation, 1978, pp. 169–179.

[9] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In EUROCRYPT, 1999, pp. 223–238.

[10] J. H. Cheon, A. Kim, M. Kim, Y. Song. Homomorphic encryption for arithmetic of approximate numbers. In ASIACRYPT, 2017, pp. 409–437.

[11] I. Chillotti, N. Gama, M. Georgieva, M. Izabach è ne. TFHE: Fast fully homomorphic encryption over the torus. Journal of Cryptology, 2020, 33(1): 34–91.

[12] A. Polychroniadou, et al. Atlas-X Equity Financing: Unlocking New Methods to Securely Obfuscate Axe Inventory Data. IACR Cryptology ePrint Archive, 2024/461, 2024.

[13] S. Kadhe, H. Ludwig, N. Baracaldo, et al. PV4FAD: Privacy-Preserving Federated Anomaly Detection. arXiv:2310.19304, 2023.

[14] 李晖，李凤华，曹珍富，等. 隐私计算研究进展. 中国科学：信息科学，2019, 49(10): 1263–1292.

[15] 湖南大学. 基于区块链和隐私计算的数字债券风险评估方法及系统. 中国发明专利，CN120823028A, 2025.

[16] O. Goldreich. Foundations of Cryptography: Volume 2, Basic Applications. Cambridge University Press, 2004.

[17] M. Naor, B. Pinkas. Efficient oblivious transfer protocols. In SODA, 2001, pp. 448–457.

[18] B. B ü nz, J. Bootle, D. Boneh, et al. Bulletproofs: Short proofs for confidential transactions and more. In IEEE S&P, 2018, pp. 315–334.

[19] F. Ballabio. QuantLib: A Free/Open-Source Library for Quantitative Finance, 2000–2024. https://www.quantlib.org/

 Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License