计算机应用
Journal of Computer Applications
ISSN 1001-9081,CN 51-1307/TP

《计算机应用》网络首发论文

题目：基于区块链的电子医疗记录安全共享
作者：林超，何德彪，黄欣沂
收稿日期：2021-11-09
网络首发日期：2022-01-17
引用格式：林超，何德彪，黄欣沂．基于区块链的电子医疗记录安全共享[J/OL]．计算机应用. https://kns.cnki.net/kcms/detail/51.1307.TP.20220115.1014.002.html

网络首发：在编辑部工作流程中，稿件从录用到出版要经历录用定稿、排版定稿、整期汇编定稿等阶段。录用定稿指内容已经确定，且通过同行评议、主编终审同意刊用的稿件。排版定稿指录用定稿按照期刊特定版式（包括网络呈现版式）排版后的稿件，可暂不确定出版年、卷、期和页码。整期汇编定稿指出版年、卷、期、页码均已确定的印刷或数字出版的整期汇编稿件。录用定稿网络首发稿件内容必须符合《出版管理条例》和《期刊出版管理规定》的有关规定；学术研究成果具有创新性、科学性和先进性，符合编辑部对刊文的录用要求，不存在学术不端行为及其他侵权行为；稿件内容应基本符合国家有关书刊编辑、出版的技术标准，正确使用和统一规范语言文字、符号、数字、外文字母、法定计量单位及地图标注等。为确保录用定稿网络首发的严肃性，录用定稿一经发布，不得修改论文题目、作者、机构名称和学术内容，只可基于编辑规范进行少量文字的修改。

出版确认：纸质期刊编辑部通过与《中国学术期刊（光盘版）》电子杂志社有限公司签约，在《中国学术期刊（网络版）》出版传播平台上创办与纸质期刊内容一致的网络版，以单篇或整期出版形式，在印刷出版之前刊发论文的录用定稿、排版定稿、整期汇编定稿。因为《中国学术期刊（网络版）》是国家新闻出版广电总局批准的网络连续型出版物（ISSN 2096-4188，CN 11-6037/Z），所以签约期刊的网络版上网络首发论文视为正式出版。

网络首发时间：2022-01-17 15:03:59
网络首发地址：https://kns.cnki.net/kcms/detail/51.1307.TP.20220115.1014.002.html

Journal of Computer Applications ISSN 1001-9081
计算机应用 CODEN JYIIDU http://www.joca.cn

文章编号:1001-9081(****)**-0000-00 doi:10.11772/j.issn.1001-9081.2021111895

基于区块链的电子医疗记录安全共享

林超[1]，何德彪[2*]，黄欣沂[1]

(1.福建师范大学 计算机与网络空间安全学院 福州 350007；
2. 武汉大学 国家网络安全学院 武汉 430072
(*通信作者电子邮箱 hedebiao@163.com)

摘 要: 针对电子医疗记录 (EMR) 共享面临的数据提供商集权化、患者数据管理显被动、互操作效率低、恶意传播等问题，提出一种基于区块链的电子医疗记录安全共享方法。首先，基于商用密码(SM2)数字签名算法提出一种更加安全高效的泛指定验证者签名证明(UDVSP)方案；然后，设计具有上传、验证、检索、撤销等功能的智能合约；其次，构造基于区块链的电子医疗记录安全共享系统；最后，通过安全性分析和性能分析论证 UDVSP 方案和共享系统的可行性。安全性分析结果表明，所设计的 UDVSP 方案满足可证明安全性。性能评估结果表明，与现有常用的 UDVSP/UDVS 方案(包括 UDVSP-1、UDVSP-2、UDVS-1 和 UDVS-2)相比，节省至少 87.42%的计算开销和 93.75%的通信代价。区块链智能合约原型系统的仿真结果进一步论证了共享系统的安全性和高效性。

关键词: 电子医疗记录；区块链；SM2 数字签名算法；泛指定验证者签名证明；数据共享

中图分类号:TP309.2 **文献标志码：A**

Blockchain-based electronic medical record secure sharing

LIN Chao[1], HE De-Biao[2*], HUANG Xin-Yi[1]

(1. College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350007, China;
2. School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China)

Abstract: To solve various issues faced by Electronic Medical Record (EMR) sharing, such as centralized data provider, passive patient data management, low interoperability efficiency, and malicious dissemination, a blockchain-based EMR secure sharing method was proposed. Firstly, the commercial cryptography SM2 digital signature algorithm was utilized to propose a more secure and efficient Universal Designated Verifier Signature Proof (UDVSP) scheme. Then, a smart contract with functionalities of uploading, verification, retrieval, and revocation was designed. Next, a blockchain-based EMR secure sharing system was constructed. Finally, security analysis and performance analysis were given to demonstrate the feasibility of UDVSP scheme and sharing system. Security analysis shows that the proposed UDVSP is probably secure. Performance analysis shows that comparing with existing UDVSP/UDVS scheme (including UDVSP-1,UDVSP-2,UDVS-1 and UDVS-2), the proposed UDVSP scheme saves the computation cost at least 87.42% and communication overhead at least 93.75%. The prototype of blockchain smart contract further demonstrates the security and efficiency of sharing system.

Keywords: electronic medical record; blockchain; SM2 digital signature algorithm; universal designated verifier signature proof; data sharing

0 引言

随着互联网技术和电子程序的快速发展，传统的纸质健康档案系统逐渐向功能完备的数字化基础设施转变[1]。电子医疗记录 (Electronic Medical Records，EMR) 将在不远的将来充斥整个世界。研究电子医疗记录共享技术有助于提高医疗保健服务质量、促进生物医学发现和降低医疗成本[2][3]。虽然目前已有众多电子医疗记录共享方案，但这些方案面临数据提供商集权化、患者数据管理显被动、互操作效率低等问题，难以广泛应用。尤其在实际的就诊过程中，患者不局限于特定的医院和医生，可能会去不同的诊所或医院找不同医生进行医疗观察/治疗，或者从一家医院转到另一家医院。

收稿日期: 2021-11-09; **修回日期**:2021-12-18; **录用日期**: 2022-01-05。
基金项目: 国家自然科学基金项目 (62102089)；中央高校基本科研业务费专项资金 (2042021kf1030)。
作者简介: 林超(1991—)，男，福建平和，讲师，博士，CCF 会员，主要研究方向：应用密码学与区块链；何德彪(1980—)，男，山东聊城，教授，博士，CCF 会员，主要研究方向：应用密码学、安全协议、云计算安全；黄欣沂(1981—)，男，江苏仪征，教授，博士，CCF 会员，主要研究方向：应用密码学、网络安全。

区块链是一种分布式账本技术，因具有公开验证、不可篡改、可编程等特点[4][5]，可解决上述问题。目前已有多种方案[3][6][7]尝试利用区块链实现电子医疗记录管理与共享，这些方案的通用架构主要包含医生（或医疗机构）、患者、区块链三种角色 (图 1)，其中医生负责生成/发布患者的电子医疗记录到区块链，患者可以从链上检索电子医疗记录并向其他医生/医疗机构展示。为了节省区块链存储代价，部分方案将原始电子医疗记录存储在云端，仅将哈希值、索引、时间戳等摘要信息记录到区块链。

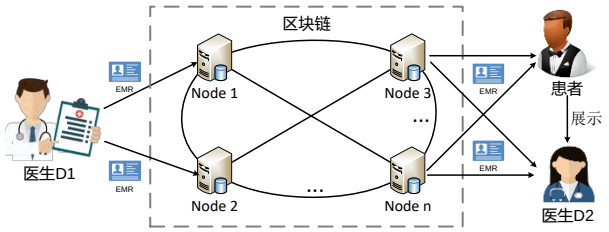

图 1 基于区块链的电子医疗记录共享通用架构
Fig. 1 Typical architecture of blockchain-based EMR sharing

在现有基于区块链的电子医疗记录共享系统中，患者的电子医疗记录容易检索和共享，有效提升了电子医疗记录的互操作性，同时保证了患者对自身数据的拥有权与使用权。然而，这些系统将面临电子医疗记录隐私泄露问题。一方面，区块链的公开透明性导致任意实体均可获取链上的电子医疗记录；另一方面，共享后的电子医疗记录易被恶意传播。由于加密技术或访问控制技术可有效解决第一个问题[8][9]，所以本文主要关注如何保护电子医疗记录共享后的隐私。

据相关电子医疗记录管理要求，每份电子医疗记录需要包含数字签名信息，保障电子医疗记录的真实性、不可抵赖性和完整性。这也是电子医疗记录易被恶意传播的主要原因。泛指定验证者签名证明 (Universal Designated Verifier Signature Proof, UDVSP) [10]可以解决这个问题，同时保障区块链中电子医疗记录的可验证性和隐私保护。假设指定者 (患者 Alice) 从签名者 (医生 D1) 获得新的电子医疗记录。Alice 可以在不提供电子医疗记录签名的情况下，让指定验证者 (医生 D2) 相信电子医疗记录内容，并且医生 D2 无法让其他人相信这份电子医疗记录的内容。本文将 UDVSP 应用于区块链场景的电子医疗记录共享，医生 D1 先利用盲化因子对电子医疗记录进行处理，再将盲化电子医疗记录上传到区块链，患者可利用盲化因子生成证明，完成电子医疗记录的指定验证者展示。

由于现有的 UDVSP 方案[10][11]均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[12])，这将阻碍 UDVSP 在电子医疗记录共享、电子投票、匿名证书、收入汇总管理等领域的应用。因此，本文先基于商用密码 SM2 数字签名算法提出一种安全高效的 UDVSP 方案，再设计基于区块链的电子医疗记录安全共享系统。由安全性分析与性能评估结果可知，本文设计的 UDVSP 方案是可证明安全的，且无需高耗时的双线性对运算，比现有方案节省至少 87.42%的计算开销和 93.75%的通信代价。因此，基于本文的 UDVSP 构建的系统实用性更强。

1 相关工作

本节介绍泛指定验证者签名 (证明) 和基于区块链的电子医疗记录共享的相关工作。

1.1 泛指定验证者签名 (证明)

Steinfeld 等[13]2003 年最早提出泛指定验证者签名的概念。这种特殊签名允许指定者 (也称签名拥有者) 在不泄露签名情况下，让指定验证者相信他/她拥有这个签名。因此，泛指定验证者签名能够有效阻止指定验证者恶意传播签名，适用于电子医疗记录、收入汇总等场景，提供隐私保护功能。

为了实现可证明安全，Zhang 等[14] 2005 年利用 SDH (Strong Diffie-Hellman) 问题设计泛指定验证者签名 (Universal Designated Verifier Signature, UDVS)方案，Huang 等[15] 2008 年利用 GBDH (Gap Bilinear Diffie-Hellman) 问题设计 UDVS 方案.文献[14]和文献[15]的方案计算开销较大，难以广泛应用。为了提高效率，Lin 等[16]2013 年基于 BIDH (Bilinear Inverse Diffie-Hellman) 问题设计两种更加高效的 UDVS 方案，但这两种方案的验证部分仍涉及双线性对运算，效率有待提高。在安全性提升方面，Rastegari 等[17]2019 年提出了标准模型下安全的 UDVS 方案。此外，国内外学者还研究基于标识/无证书的 UDVS 方案[18][19][20]，并将 UDVS 与传递签名[21][22]、内容提取签名[23]等其他特殊签名相结合，实现隐私保护。

上述 UDVS 方案存在公钥初始化问题，指定验证者需要事先利用签名拥有者的系统参数生成公私钥信息，同时申请公钥证书[10]。这在实际生活中极其不便，尤其指定验证者一般已经在不同的系统参数下生成公私钥信息和申请公钥证书.为了验证某实体的签名拥有权，需要更换系统参数重新生成公私钥并申请公钥证书，为验证者带来不便。

Baek 等[10] 2005 年提出泛指定验证者签名证明 (UDVSP)，这是 UDVS 的一种变形，不仅具有 UDVS 的可验证性与隐私保护功能，还有效解决 UDVS 面临的公钥初始化问题。文献[10]基于 BLS (Boneh-Lynn-Shacham) 签名和 BB (Boneh-Boyen) 签名提出两种 UDVSP 方案，但这两种方案均涉及高耗时的双线性对运算，难以支持移动终端或其他轻量级场景。Chen 等[11]2009 年提出基于标识的 UDVSP 方案，可以避免繁琐的公钥证书管理，但也涉及高耗时的双

线性对运算。据调查，目前尚未有无需双线性对运算的UDVSP方案在国内外刊物上公开发表。

1.2 基于区块链的电子医疗记录共享

为了满足医疗领域面临的身份验证、互操作性、数据共享、隐私保护等需求，国内外学者利用区块链技术提出了一系列解决方案。Mettler[24] 2016年利用以太坊设计一种电子医疗记录共享网络基础设施，实现患者与医生之间无缝共享患者的电子医疗记录，但无法保证电子医疗记录被恶意修改和滥用。Yue 等[9] 2016年利用区块链技术提出一套医疗数据网关 (Healthcare Data Gateways, HDG) 系统，主要在统一数据模式下存储和组织电子医疗数据，支持患者拥有、控制和共享自身电子医疗记录。虽然HDG系统尝试在提供数据隐私保护的同时实现数据安全共享，但无法支持用户自定义共享电子医疗数据和数据共享后的隐私保护。

Azaria 等[8]2016年结合云存储和区块链提出具有认证、保密、可靠、共享等特点的Medrec模型。虽然Medrec可以保障患者和医生之间的数据互操作性，但存在电子医疗数据共享后隐私泄露问题。Roehrs 等[25] 2017年为了实现物理健康记录 (Physical Health Record) 的分发性和互操作性，提出了支持跨卫生组织的健康记录统一视图模型。虽然这种模型可以解决电子医疗记录与物理健康记录之间的差异性问题，但存在数据共享范围受限、隐私泄露隐患等不足。薛腾飞等[26] 2017年利用区块链和代理重加密技术提出新的医疗数据共享模型，可以解决各医疗机构间数据共享难题，但存在数据共享复杂和隐私泄露问题。

2018年，Liu 等[3]结合区块链技术、密文策略属性基加密 (Ciphertext-Policy Attribute-Based Encryption, CPABE) 和内容提取签名 (Content Extraction Signature)，提出一种具有隐私保护功能的电子医疗记录共享方案。Wu 等[27] 2019年引入数据掩码技术和星际文件系统 (Inter Planetary File System)，设计了高效的区块链电子医疗记录共享模型。2020年，Li 等[28]设计新的基于区块链的电子医疗纪录共享系统，解决了相互信任问题和电子医疗记录存储/共享安全问题。

上述基于区块链的电子医疗记录共享系统虽然能够解决一些访问控制、数据存储、身份隐私等安全问题，但均未考虑电子医疗记录共享后的隐私泄露问题。本文主要解决该问题，既实现数据有效性验证，又防止数据被恶意传播。

2 技术背景

本节介绍相关符号、系统模型、SM2 数字签名算法、泛指定验证者签名证明等基础知识的定义。

2.1 符号定义

本文主要涉及符号及定义如下：

- λ：系统参数；
- q：λ 比特的大素数；
- E：非奇异椭圆曲线 $y^2 = x^3 + ax + b\left(mod\ q\right)$，$a,b \in \mathbb{Z}_q^*$；
- $\mathbb{G}$：素数 n 阶的加法循环群；
- $\mathcal{H}$：安全哈希函数 $\mathcal{H}:\{0,1\}^* \times \{0,1\}^* \to \mathbb{Z}_n^*$；
- $\{A_i\}_{i=1}^t$：集合 $\{A_1, A_2 \ldots, A_t\}$；
- $out \leftarrow \mathrm{A}(in)$：算法 A 输入 in，输出 out；
- $\mathcal{PPT}$：概率多项式时间。
- P：交互证明中的证明者。
- V：交互证明中的验证者。

2.2 系统模型

基于区块链的电子医疗记录安全共享系统主要包括医生、患者、区块链三种角色 (图 2)。

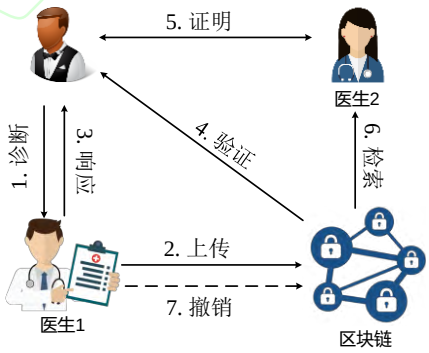

图 2 系统模型

Fig. 2 System model

医生：本角色主要为患者诊断服务，是电子医疗记录的生成者。收到患者的门诊请求后 (步骤 1)，医生为患者诊断生成电子医疗记录，然后将电子医疗记录盲化处理后上传到区块链 (步骤 2)，再将盲化因子返回给患者 (步骤 3)。此外，本角色在提供诊断服务时，可要求患者提供过往电子医疗记录 (步骤 5)，并从区块链检索相关数据进行验证 (步骤 6) 。

患者：本角色是电子医疗记录的拥有者，在接受医生诊断后获取电子医疗记录的相关证明凭证 (即前述的盲化因子)，利用此凭证验证电子医疗记录的有效性 (步骤 4)。在更换其他医生时，患者可提供过往电子医疗记录获取更准确、更高效的医疗服务，但为了避免电子医疗记录被恶意传播，患者不直接提供电子医疗记录，而是利用盲化处理的电子医疗记录和盲化因子向新医生证明 (步骤 5) 。

区块链：本角色是分布式账本，用于维护患者的盲化电子医疗记录列表，提供电子医疗记录的上传 (步骤 2)、验证 (步骤 4)、检索 (步骤 6)、撤销 (步骤 7) 服务。此角色主要分为公有链和联盟链，其中公有链允许任何实体共同维护账本，而联盟链仅由授权节点维护账本。在系统实现部分，本文将采用智能合约实现上述功能。

系统需要满足以下性质：

完备性 (Completeness)：本性质用于保障系统的正确性/可靠性。有效盲化因子生成的电子医疗记录拥有证明可被验证通过。假设用户没有盲化因子，将无法生成有效的电子医疗记录拥有证明。

不可链接性 (Unlinkability)：本性质用于保障系统的数据隐私。任意的 $\mathcal{PPT}$ 敌手无法从盲化电子医疗记录中恢复得到原始电子医疗记录。此外，任意的 $\mathcal{PPT}$ 敌手无法将同一原始电子医疗记录生成的两个不同的盲化电子医疗记录进行关联。

兼容性 (Compatibility)：本性质用于保障系统的实用性。要求系统实现不会受限于区块链的类型，也就是既能支持以太坊等公有链，也能支持超级账本等联盟链。

2.3 SM2 数字签名算法

国家密码管理局 2010 年颁布的 SM2 数字签名算法，已成为国际标准数字签名 ISO/IEC 14888-3 和国家商用密码公钥算法标准 GM/T 000.3-2012[29]。该算法包括初始化 (Setup)、密钥生成 (Key Generation, KGen)、签名 (Sign) 和验证 (Verify) 四个算法：

初始化 (Setup)：算法输入安全参数 λ，随机选取大素数 q，确定椭圆曲线 $E: y^2 = x^3 + ax + b (\mathrm{mod}\ q)$ (其中，$a, b \in \mathbb{Z}_q^*$)，在 E 所有点 (包含无穷远点) 中选取素数 n 阶循环群 $\mathbb{G}$ 以及生成元 $G \in \mathbb{G}$.选取安全哈希函数 $\mathcal{H}: \{0,1\}^* \to \mathbb{Z}_n^*$ 。算法输出系统参数 $pp = (E, a, b, q, \mathbb{G}, n, G, \mathcal{H})$。

密钥生成 (KGen)：算法输入系统参数 pp，随机选取 $d \in \mathbb{Z}_n^*$，计算 $P = dG$，算法输出私钥 $sk = d$ 和公钥 $pk = P$ 。

签名 (Sign)：算法输入系统参数 pp、私钥 $sk = d$ 和消息 m 。随机选取 $k \in \mathbb{Z}_n^*$，计算 $K = kG = (x_K, y_K)$、$e = \mathcal{H}(m)$ 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 $s \neq 0$，则输出消息 m 和签名 $\sigma = (r, s)$ 。

验证 (Verify)：算法输入系统参数 pp、用户公钥 $pk = P$、消息 m 和待验证签名 $\sigma = (r, s)$，若 $r, s \notin \mathbb{Z}_n^*$，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 $e' = \mathcal{H}(m)$、$K' = sG + tP = (x_K^{'}, y_K^{'})$ 和 $r' = (e' + x_K^{'}) (\mathrm{mod}\ n)$ 。若 $r' = r$，则输出 1 表示签名有效，否则输出 0 表示无效。

SM2 数字签名算法满足正确性、自适应选择攻击存在不可伪造性 (Existential UnForgeability on adaptively Chosen Message Attacks, EUF-CMA) 和抗密钥替换攻击[29] 。

2.4 泛指定验证者签名证明

UDVSP 可以保证签名拥有者 Alice 在不提供真实签名 σ 情况下，让 Bob 相信自己拥有签名 σ，但 Bob 无法让其他人相信 Alice 拥有签名 σ 。UDVSP 方案包括初始化 (Udvsp Setup, USetup)、密钥生成 (Udvsp Key Generation, UKGen)、签名 (Udvsp Sign, USign)、验证 (Udvsp Verify, UVerf)、转换 (Udvsp Transform, UTran)、交互证明 (Udvsp Interactively Verify, UIVerf) 六个算法：

初始化 (USetup)：算法输入安全参数 λ，输出系统参数 pp 。

密钥生成 (UKGen)：算法输入系统参数 pp，输出公私钥对 (pk, sk)。

签名 (USign)：算法输入系统参数 pp、私钥 sk 和消息 m，输出的签名 σ 。

验证 (UVerf)：算法输入系统参数 pp、公钥 pk、消息 m 和待验证签名 σ，输出 1 表示签名有效，否则输出 0。

转换 (UTran)：算法输入系统参数 pp、公钥 pk、消息 m 和签名 σ，输出转换签名 $\hat{\sigma}$ 和转换密钥 sk 。

交互验证 (UIVerf)：交互式验证协议由签名拥有者 Alice 和指定验证者 Bob 执行。Alice 和 Bob 共同输入系统参数 pp、签名者公钥 pk、消息 m 和转换签名 $\hat{\sigma}$，Alice 额外输入转换密钥 sk 。Alice 的目标是证明 $\hat{\sigma}$ 由有效签名 σ 生成。此协议输出 1 表示 Bob 接受证明，否则输出 0。

上述 USetup 由系统管理员执行，UKGen 和 USign 算法由签名者执行，UVerf 和 UTran 算法由签名拥有者执行。此外，UDVSP 需要满足“USign 与 UVerf 一致”、“UTran 与 UIVerf 一致”两种一致性要求。“USign 与 UVerf 一致”是指 USign 算法生成的 (m, σ) 能够通过 UVerf 的验证；

“UTran 与 UIVerf 一致”是指 UTran 生成的转换签名 $\hat{\sigma}$ 和转换密钥 sk 能够通过 UIVerf 的验证。

此外，UDVSP 需要满足 EUF-CMA 和抗冒充攻击 (Resistance-IMpersonation, R-IM) 两类安全性。EUF-CMA 与数字签名的不可伪造性保持一致。假设 UDVSP = (USetup, UKGen, USign, UVerf, UTran, UIVerf)，$\mathrm{USign}(sk,\cdot)$ 为签名谕言机，则对于伪造者 $\mathcal{F}$，构造以下实验：

$\mathbf{Exp}_{\mathrm{UDVSP},\mathcal{F}}^{UF-CMA}(\lambda)$:

$(pk,sk)\leftarrow \mathrm{UKGen}(1^{\lambda})$;

$(m^{*},\sigma^{*})\leftarrow \mathcal{F}^{\mathrm{USign}(sk,\cdot)}(pk)$;

若 $1\leftarrow \mathrm{UVerf}(pk,m^{*},\sigma^{*})$ 且 m^{*} 未在 $\mathrm{USign}(sk,\cdot)$ 询问过，则输出 1，否则输出 0。

令 $\mathcal{F}$ 攻破 UDVSP 的不可伪造性的优势为

$$\mathbf{Adv}_{\mathrm{UDVSP},\mathcal{F}}^{UF-CMA}(\lambda)=\Pr\left[\mathbf{Exp}_{\mathrm{UDVSP},\mathcal{F}}^{UF-CMA}(\lambda)=1\right]。$$

定义 1. 当且仅当 $\mathbf{Adv}_{\mathrm{UDVSP},\mathcal{F}}^{UF-CMA}(\lambda)$ 对于所有 $\mathcal{PPT}$ 伪造者 $\mathcal{F}$ 可忽略，UDVSP 满足 EUF-CMA 。

R-IM 是指 UDVSP 能够保证没有签名的敌手无法冒充诚实的签名拥有者。这个性质可分为抗类型 1 冒充攻击 (R-IM-TYPE-1)和抗类型 2 冒充攻击 (R-IM-TYPE-2)：

R-IM-TYPE-1：拥有有效转换签名的敌手扮演恶意指定验证者，与诚实签名拥有者执行自适应的 UIVerf 交互。敌手目标是冒充签名拥有者与其他诚实指定验证者成功交互。假设 Type-1 敌手 $\mathcal{A}$ 包含 $\hat{\mathrm{V}}$ (恶意指定验证者) 和 $\hat{\mathrm{P}}$ (恶意签名拥有者) 两个子算法，P 为诚实的签名拥有者。函数 Conv_{UIVerf} 返回 UIVerf 算法的交互脚本和随机值 $(T,r^{\hat{V}})\leftarrow \mathrm{Conv}_{UIVerf}[\mathrm{P}(sk)\leftrightarrow\hat{\mathrm{V}}](pk,\hat{\sigma},m)$，UIVerf 中 P 和 $\hat{\mathrm{V}}$ 的最大交互次数为 $p(\lambda)$。构造以下实验：

$\mathbf{Exp}_{\mathrm{UDVSP},\mathcal{A}}^{R-IM-TYPE-1}(\lambda)$:

$(pk,sk)\leftarrow \mathrm{UKGen}(1^{\lambda});m\leftarrow\{0,1\}^{*}$;

$\sigma\leftarrow \mathrm{USign}(sk,m);(\hat{\sigma},sk)\leftarrow \mathrm{UTran}(pk,\sigma)$;

$T_i\leftarrow \mathrm{Conv}_{UIVerf}\left[\mathrm{P}(sk)\leftrightarrow\hat{\mathrm{V}}\right](pk,\hat{\sigma},m),i\le p(\lambda)$;

$b\leftarrow \mathrm{UIVerf}\left[\hat{\mathrm{P}}\left(\left(\mathrm{T_i},\mathrm{r_i}^{\hat{V}}\right)_{i=1}^{p(\lambda)}\right)\leftrightarrow\mathrm{V}\right](pk,\hat{\sigma},m)$

Return b。

令敌手 $\mathcal{A}$ 攻破 UDVSP 的 R-IM-TYPE-1 优势为

$$\mathbf{Adv}_{\mathrm{UDVSP},\mathcal{A}}^{R-IM-TYPE-1}=\Pr\left[\mathbf{Exp}_{\mathrm{UDVSP},\mathcal{A}}^{R-IM-TYPE-1}(\lambda)=1\right]。$$

定义 2. 当且仅当 $\mathbf{Adv}_{\mathrm{UDVSP},\mathcal{A}}^{R-IM-TYPE-1}$ 对于所有 $\mathcal{PPT}$ 敌手 $\mathcal{A}$ 可忽略，UDVSP 满足 R-IM-TYPE-1。

R-IM-TYPE-2：敌手 $\mathcal{A}$ 直接忽略拥有的转换签名，并自适应地生成新的转换签名，然后冒充签名拥有者与诚实的指定验证者进行 UIVerf 交互。构造以下实验：

$\mathbf{Exp}_{\mathrm{UDVSP},\mathcal{A}}^{R-IM-TYPE-2}(\lambda)$:

$(pk,sk)\leftarrow \mathrm{UKGen}(1^{\lambda});m\leftarrow\{0,1\}^{*}$;

$\left(\hat{\sigma}',sk'\right)\leftarrow \mathcal{A}(pk,m)$:

$b\leftarrow \mathrm{UIVerf}\left[\mathcal{A}\left(sk'\right)\leftrightarrow\mathrm{V}\right](pk,\hat{\sigma},m)$

Return b。

令敌手 $\mathcal{A}$ 攻破 UDVSP 的 R-IM-TYPE-2 优势为

$$\mathbf{Adv}_{\mathrm{UDVSP},\mathcal{A}}^{R-IM-TYPE-2}=\Pr\left[\mathbf{Exp}_{\mathrm{UDVSP},\mathcal{A}}^{R-IM-TYPE-2}(\lambda)=1\right]。$$

定义 3. 当且仅当 $\mathbf{Adv}_{\mathrm{UDVSP},\mathcal{A}}^{R-IM-TYPE-2}$ 对于所有 $\mathcal{PPT}$ 敌手 $\mathcal{A}$ 可忽略，UDVSP 满足 R-IM-TYPE-2。

3 协议设计

本节先利用 SM2 数字签名算法设计 UDVSP 方案，再设计智能合约，最后构造系统。

3.1 基于 SM2 数字签名算法的 UDVSP

基于 SM2 数字签名算法设计的 UDVSP，可以避免双线性对运算，有效提升性能。本文设计的 UDVSP 包括 USetup、UKGen、USign、UVerf、UTran 和 UIVerf 六个算法：

初始化 (USetup)：算法输入安全参数 λ，输出 SM2 数字签名算法的系统参数 $pp=(E,a,b,q,\mathbb{G},n,G,\mathcal{H})$。

密钥生成 (UKGen)：算法输入系统参数 pp，随机选取 $d\in\mathbb{Z}_n^{*}$，计算 $P=dG$，输出私钥 $sk=d$、公钥 $pk=P$。

签名 (USign)：算法输入系统参数 pp、私钥 $sk=d$ 和消息 m。随机选取 $k\in\mathbb{Z}_n^{*}$，计算 $K=kG=(x_K,y_K)$，$e=\mathcal{H}(m)$ 和 $r=(e+x_K)(mod\ n)$。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 $s\neq 0$，则输出消息 m 和签名 $\sigma=(r,s)$。

验证 (UVerify)：算法输入系统参数 pp、用户公钥 $pk=P$、消息 m 和待验证签名 $\sigma=(r,s)$，若 $r,s\notin\mathbb{Z}_n^*$，则输出 0，否则计算 $t=r+s\pmod n$。若 $t=0$，则输出 0，否则计算 $e'=\mathcal{H}(m)$、$K'=sG+tP=\left(x_K^{'},y_K^{'}\right)$ 和 $r'=\left(e'+x_K^{'}\right)\pmod n$。若 $r'=r$，则输出 1 表示签名有效，否则输出 0 表示无效。

转换 (UTran)：算法输入系统参数 pp、公钥 $pk=P$、消息 m 和签名 $\sigma=(r,s)$，随机选取 $a,b\in\mathbb{Z}_n^*$ 并计算 $e=\mathcal{H}(m),\hat{r}=r+a-e(\bmod n),\hat{s}=s+b(\bmod n)$，输出转换签名 $\hat{\sigma}=(\hat{r},\hat{s})$ 和转换密钥 $tk=(a,b)$。

交互证明 (UIVerf)：签名拥有者 P 与指定验证者 V 执行以下交互：

1) P 首先计算 $K=sG+(r+s)P$，然后随机选取 $\alpha,\beta\in\mathbb{Z}_n^*,R\in\mathbb{G}$，计算 $D=R+\beta G+\alpha P+\beta P$。最后，P 将 D 发送给 V。

2) V 随机选取 $c\in Z_n^*$ 并将 c 返回给 P。

3) P 计算 $Z_K=R-cK$，$z_a=\alpha-c\cdot a(\bmod n)$，$z_b=\beta-c\cdot b(\bmod n)$，并将 (Z_K,z_a,z_b) 发送给 V。

4) V 接受到 (Z_K,z_a,z_b) 后，计算 $e'=\mathcal{H}(m)$，$D=Z_K+z_bG+z_aP+z_bP+c(\hat{s}G+\hat{r}P+e'P+\hat{s}P)$。若 $D'=D$，则输出 1 表示接受，否则输出 0。

SM2 数字签名的正确性保证了 UDVSP 的“USign 与 UVerf 一致”，以下论证“UTran 与 UIVerf 一致”，其中 $e'=\mathcal{H}(m),\hat{r}=r+a-e(\bmod n),\hat{s}=s+b(\bmod n)$：

$$\begin{aligned}D'&=Z_K+z_bG+z_aP+z_bP+c(\hat{s}G+\hat{r}P+e'P+\hat{s}P)\\&=(R-cK)+(\alpha-c\cdot a)G+(\alpha-c\cdot a)P+(\beta-c\cdot b)P\\&\quad+c(K+bG+aP+bP)=R+\beta G+\alpha P+\beta P=D。\end{aligned}$$

3.2 智能合约设计

系统需要提供盲化电子医疗记录的上传、验证、检索、撤销等服务，本文利用智能合约进行实现。当且仅当盲化电子医疗记录被上传到智能合约，患者才能利用盲化因子提供有效的电子医疗记录证明，同时要求仅有授权的医生才能够上传/撤销盲化电子医疗记录。本文的智能合约主要包括 Upload、Check、Get、Revoke 四个算法 (算法 1)。

算法 1 - Smart Contract on EMRList：

输入: Function name, invoked parameters

输出: Setting up functions:

```
address[n] doctorList; % 定义授权医生列表
structure BEMR      % 定义数据结构体
  uint256 br; % 一部分盲化电子医疗记录
  uint256 bs; % 另一部分盲化电子医疗记录
FUNCTION EMRList(address[20] doctor)
% 构造函数，智能合约部署时自动执行
  FOR(i = 0; i < doctor.length; i++)
    doctorList =doctor[i];
  ENDFOR
  mapping(uint256=> BEMR) emrMap;
FUNCTION Upload(br, bs) returns (address)
% 授权医生调用该算法上传盲化电子医疗记录
  require(msg.sender ∈ doctorList); % 权限判断
  index = H(br, bs); % 计算索引值
  emrMap[index].br = br;
  emrMap[index].bs = bs;
  RETURN index;
FUNCTION Check(br, bs) returns (bool)
% 调用该算法可判断盲化电子医疗记录是否上传
  index = H(br, bs); % 计算索引值
  IF (emrMap[index].br = br && emrMap[index].bs =
bs ) RETURN true;
  ELSE RETURN false;
  ENDIF
FUNCTION view Get(index) returns (uints256[2])
% 调用该算法可检索盲化电子医疗记录.
  br = emrMap[index].br;
  bs = emrMap[index].bs;
  RETURN (br, bs);
FUNCTION Revoke(br, bs)
% 授权医生可调用该算法撤销盲化电子医疗记录
  require(msg.sender ∈ doctorList); % 权限判断
  index = H(br, bs); % 计算索引值
  emrMap[index].br = null;
  emrMap[index].bs = null;
```

3.3 系统设计

在上述的 UDVSP = (USetup, UKGen, USign, UVerf, UTran, UIVerf)和智能合约 EMRList = (Upload, Check, Get, Revoke) 的基础上，下面介绍系统设计。

初始化阶段：系统管理员调用 USetup 算法生成系统参数 pp，并部署前述的智能合约到区块链，获取智能合约地址 $scid$。系统管理员公布 $(pp,scid)$，便于医生和患者后续调用密码算法和合约算法。此外，医生调用 UKGen 算法生成私钥 $sk=d$ 和公钥 $pk=P$。

记录生成阶段：患者到医院就诊，医生 D1 为患者诊断并生成电子医疗记录：通过私钥 sk 调用 USign 算法生成 $\left(m,\sigma=\left(r,s\right)\right)\leftarrow \mathrm{USign}\left(pp,sk,m\right)$，其中 m 是患者的诊断相关信息。然后，医生 D1 调用 UTran 算法生成 $\left(\hat{\sigma}=\left(\hat{r},\hat{s}\right),tk=\left(a,b\right)\right)\leftarrow \mathrm{UTran}\left(pp,pk,m,\sigma\right)$。接着，医生 D1 调用合约 $scid$ 的 Upload 算法，将 $\hat{\sigma}$ 上传到区块链，获得索引信息 $index$。最后，医生 D1 将转换密钥 tk、诊断消息 m 和索引信息 $index$ 通过安全信道发送给患者.患者调用合约 $scid$ 的 Get 算法获取盲化电子医疗记录 $\hat{\sigma}$，利用转换密钥恢复得到 σ，并调用 UVerf 算法验证 σ 的有效性。

展示阶段：假设患者到其他医院就诊，医生 D2 为其提供诊断服务。为了提高就诊效率和准确性，同时保护电子医疗记录的隐私，患者可以向指定医生 D2 展示电子医疗记录。因此，患者与医生 D2 共同执行 UIVerf 交互协议，其中医生 D2 调用合约 $scid$ 的 Get($index$)获取盲化电子医疗记录，若 UIVerf 最终输出 1 表示医生 D2 相信患者确实拥有电子医疗记录 (m,σ)。由于 UIVerf 交互协议不会泄露原始电子医疗记录(m,σ)，并且 UDVSP 具有隐私保护功能，所以避免了(m,σ)被医生 D2 恶意传播。

撤销阶段：假如患者想要撤销某一条原始电子医疗记录，可向授权医生发起请求。授权医生调用合约 $scid$ 的 Revoke 算法，删除指定的盲化电子医疗记录。患者、医生或其他实体可调用合约 $scid$ 的 Check 算法，判断盲化电子医疗记录是否被撤销。

4 安全性分析

为了分析系统的安全性，本文首先证明 UDVSP 的安全性。由于 UDVSP 的 EUF-CMA 与 SM2 数字签名算法的 EUF-CMA 保持一致，所以本文主要分析 UDVSP 的 R-IM-TYPE-1 (定理 1) 和 R-IM-TYPE-2 (定理 2)。

定理 1 若 UDVSP 的 UIVerf 交互式协议满足诚实验证者零知识性 (Honest-verifier Zero-knowledge)，则 UDVSP 具有 R-IM-TYPE-1 的性质。

证明：本文首先构造模拟器 Sim (算法 2) 证明 UDVSP 的 UIVerf 协议满足诚实验证者零知识性。Sim 首先获取有效的消息签名对 $\left(m,\sigma=\left(r,s\right)\right)$，模拟与诚实验证者 V 的所有交互。由于步骤 1 和 2 的随机数 $a,b\in\mathbb{Z}_n^*$，所以 Sim 的前两个步骤具有完全的盲性，验证者 V 和其他敌手无法从转换签名 $\left(\hat{r},\hat{s}\right)$ 恢复得到原始签名 $\left(r,s\right)$。此外，步骤 3-5 是 Σ 协议，满足特殊诚实验证者零知识性，有效防止转换密钥 $\left(a,b\right)$ 被泄露。因此，UDVSP 的 UIVerf 协议满足诚实验证者零知识性。

算法 2-UIVerf 协议的模拟器 Sim：

1. Sim 向签名者请求签名 $(m,\sigma=(r,s))$。

2. Sim 随机选取 $a,b\in\mathbb{Z}_n^*$ 并计算 $e=\mathcal{H}(m)$, $\hat{r}=r+a-e(\mathrm{mod}\,n)$, $\hat{s}=s+b(\mathrm{mod}\,n)$，发送 $(\hat{r},\hat{s})$ 给 V。

3. Sim 随机选取 $\alpha,\beta\in\mathbb{Z}_n^*,R\in\mathbb{G}$，计算 $D=R+\beta G+\alpha P+\beta P$，并将 D 发送给 V。

4. Sim 接收到 V*发送的挑战值 $c\in\mathbb{Z}_n^*$。

5. Sim 计算 $Z_K=R-cK$, $z_a=\alpha-c\cdot a(\mathrm{mod}\,n)$, $z_b=\beta-c\cdot b(\mathrm{mod}\,n)$，并将 $\left(Z_K,z_a,z_b\right)$ 发送给 V。若存在 $\mathcal{PPT}$ 冒充者 $\mathcal{A}=(\hat{V},\hat{P})$ 成功破坏 UDVSP 的 R-IM-TYPE-1，则 $\mathcal{A}$ 可以获取 $\left(a,b\right)$ 的相关信息来与其他指定验证者成功交互。这将违背 UDVSP 中 UIVerf 的诚实验证者零知识性。因此，UDVSP 具有 R-IM-TYPE-1 的性质。

定理 2 若 SM2 数字签名算法具有 EUF-CMA 的性质，则 UDVSP 具有 R-IM-TYPE-2 的性质。

证明：假设存在算法 $\mathcal{A}$ 成功破坏 UDVSP 的 R-IM-TYPE-2 性质，则存在算法 $\mathcal{B}$ 可以利用 $\mathcal{A}$ 的能力成功破坏 SM2 数字签名算法的 EUF-CMA。算法 $\mathcal{B}$ 已知 $(E,a,b,q,\mathbb{G},n,G,\mathcal{H},P)$ ($P=dG,\mathcal{H}:\{0,1\}^*\rightarrow\mathbb{Z}_n^*$)，目标是输出一组有效的消息签名对。

首先 $\mathcal{B}$ 将 $\left(E,a,b,q,\mathbb{G},n,G,\mathcal{H},P\right)$ 发送给 $\mathcal{A}$，并调用 $\mathcal{A}$ 获取 m 的转换签名 $\hat{\sigma}=\left(\hat{r},\hat{s}\right)$。然后 $\mathcal{B}$ 与 $\mathcal{A}$ 执行 UIVerf 的步骤 1 得到 D，$\mathcal{B}$ 随机选取 $c\in\mathbb{Z}_n^*$ 返回给 $\mathcal{A}$。最后，$\mathcal{A}$ 返回 $\left(Z_K,z_a,z_b\right)$，$\mathcal{B}$ 计算 $e'=\mathcal{H}(m)$ 并验证 $D=Z_K+z_bG+z_aP+z_bP+c\left(\hat{s}G+\hat{r}P+e'P+\hat{s}P\right)$ 是否成立。若不成立，则 $\mathcal{B}$ 终止当前交互，否则 $\mathcal{B}$ 以新的 $c'\in\mathbb{Z}_n^*$ 重新调用 $\mathcal{A}$，$\mathcal{B}$ 得到新的证明值 $\left(Z_K^{'},z_a^{'},z_b^{'}\right)$。若 $D'=Z_K^{'}+z_b^{'}G+z_a^{'}P+z_b^{'}P+c'\left(\hat{s}G+\hat{r}P+e'P+\hat{s}P\right)$，则 $\mathcal{B}$ 可计算 $a=\left(z_a-z_a^{'}\right)\cdot\tau(\mathrm{mod}\,n)$、$b=(z_b-z_b^{'})\cdot\tau(\mathrm{mod}\,n)$、$K=\tau(Z_K-Z_K^{'})$。其中 $\tau=\left(c'-c\right)^{-1}$，可调用扩展欧几里得算法求解。$\mathcal{B}$ 利用 $\left(a,b\right)$ 恢复得到 $\sigma=\left(r,s\right)$，最后输出伪造的消息签名对

(m,σ)。这与 SM2 数字签名算法的 EUF-CMA 相矛盾，所以 UDVSP 具有 R-IM-TYPE-2 的性质。

在上述基础上，本文进一步分析系统的完备性、不可链接性和兼容性。

完备性：系统的完备性一方面是因为 UDVSP 的“UTran 与 UIVerf 一致”，另一方面是转换密钥仅患者和医生可知，其他人无法生成有效的盲化电子医疗记录证明。

不可链接性：系统利用转换密钥隐藏原始电子医疗记录，由于 UDVSP 具有 R-IM-TYPE-1 和 R-IM-TYPE-2 性质，没有 $\mathcal{PPT}$ 敌手能够从盲化电子医疗记录中恢复得到原始电子医疗记录。此外，智能合约仅存储盲化电子医疗记录，假如 $\mathcal{PPT}$ 敌手未拥有转换密钥，则无法将盲化电子医疗记录链接到同一原始电子医疗记录。

兼容性：在系统设计中，主要利用区块链智能合约进行实现，所以任何支持智能合约功能的区块链均适用，例如：支持 Solidity 语言的公有链以太坊和支持 Go 语言的联盟链超级账本。

5 性能评估

本节从燃气(Gas)消耗、计算开销和通信代价讨论系统性能。

燃气消耗：为评估系统的燃气消耗，本文采用以太坊测试平台 Remix (https://remix.ethereum.org/)实现。Remix 采用编译器 (0.4.23+commit.124ca40d.Emscripten.clang)、语言 (Solidity)、以太坊虚拟机(Ethereum Virtual Machine, EVM)版本 (默认)、部署环境 (Javascript 虚拟机)、功能插件 (调试器、部署/运行、Solidity 编译器、Solidity 静态分析)。

在上述配置的 Remix 中编译和部署智能合约代码，得到图 3 的燃气消耗情况。其中，据 CoinMarketCap 2021 年 7 月 26 日行情，1 Ether 约等于 2000 美元 (United States of America Dollar, USD)，最高燃气限制设为 3,000,000 gas，每个燃气设为 2 GWei (约为 0.006 Ether 和 12 USD)。合约部署 Deploy 消耗交易燃气最多，约为 3.2080 USD (其中包含执行燃气 1.2936 USD)，其余的 Upload、Check、Get 和 Revoke 算法消耗的交易燃气均小于 0.45 USD，尤其是 Check、Get 和 Revoke 仅消耗 Gas 分别为 0.1117 USD、0.1110 USD 和 0.1268 USD。由于 Deploy 仅需执行一次，而其余算法在系统中需要重复调用，所以上述的交易燃气消耗情况合理，满足实际应用需求。

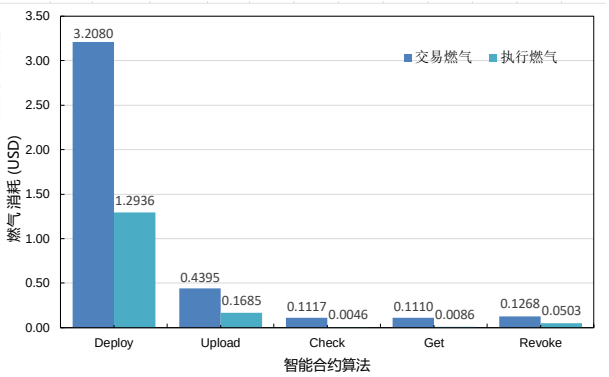

图 3 智能合约算法的燃气消耗情况

Fig. 3 Gas cost of smart contract algorithms

计算开销与通信代价：系统的计算开销与通信代价主要由 UDVSP 方案引起，所以本文首先理论分析 UDVSP 的计算开销与通信代价。同时，分析对比本文的 UDVSP 与现有常用的 UDVSP/UDVS 方案 (包括 UDVSP-1[10]、UDVSP-2[10]、UDVS-1[15]和 UDVS-2[17])。其中，本文将 UDVS 的两个密钥生成算法统一为 UKGen 算法，且通信代价部分主要考虑 UIVerf 交互协议的通信代价。从理论分析对比结果 (表 1) 可知，本文 UDVSP 的计算开销和通信代价均比现有方案更优，主要是因为本文的 UDVSP 避免了高耗时的双线性对运算和全域哈希函数计算。

为了分析实际性能，本文进一步在个人电脑端评估各项密码操作耗时。采用的配置为：处理器 (i7-9750H 2.59 GHZ)、内存 (16 GB)、操作系统 (Windows 10)、密码算法库 (Miracl 库 7.0 版本)、椭圆曲线 (BLS)，配有嵌入度为 24 的 Ate 双线性对，安全等级可达 256 比特)。因此，$\mathbb{Z}_n,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T$ 的元素长度分别为 64 字节、160 字节、640 字节和 1920 字节。根据各项密码操作测试结果 (表 2)，可以分析对比实际计算开销和通信代价。从表 3 可以看出，本文 UDVSP 的 UKGen 算法、USign 算法、UVerf 算法、UTran 算法和 UIVerf 算法的耗时分别为 35.3111 毫秒、35.3971 毫秒、70.7993 毫秒、0.0138 毫秒和 496.6129 毫秒，带宽为 128 字节。与现有方案相比，本文 UDVSP 的计算开销至少降低 87.42%，通信代价至少降低 93.75%。说明本文 UDVSP 方案构建的系统实用性更强。

表 1 理论性能分析对比结果

Tab. 1 Theoretical performance comparison results

方案	计算开销					通信代价
	UKGen	USign	UVerf	UTran	UIVerf	UIVerf
UDVSP-1[10]	T_{g1sm}	$T_{\text{h2p}}+T_{\text{g1sm}}$	$2T_{\text{bp}}+T_{\text{h2p}}$	T_{g1sm}	$2T_{\text{bp}}+T_{\text{mm}}+T_{\text{ma}}$ $+2T_{\text{ebp}}+T_{\text{mbp}}+T_{\text{h2p}}$	$\lvert\mathbb{G}_T\rvert+2\lvert\mathbb{Z}_n\rvert$

UDVSP-2[10]	$2T_{\text{g2sm}}$	$T_{\text{g1sm}}+T_{\text{mi}}$ $+T_{\text{mm}}+2T_{\text{ma}}$	$2T_{\text{bp}}+2T_{\text{g2sm}}$ $+2T_{\text{g2pa}}$	T_{g1sm}	$2T_{\text{bp}}+2T_{\text{g2sm}}+2T_{\text{g2pa}}$ $+T_{\text{ebp}}+T_{\text{mm}}+T_{\text{ma}}$ $+2T_{\text{ebp}}+T_{\text{mbp}}$	$\lvert\mathbb{G}_T\rvert+2\lvert\mathbb{Z}_n\rvert$
UDVS-1[15]	$4T_{\text{g1sm}}$	$3T_{\text{g1sm}}+$ $2T_{\text{g1pa}}+T_{\text{mm}}$	$T_{\text{g1sm}}+T_{\text{g1pa}}$ $+3T_{\text{bp}}+T_{\text{mbp}}$	$2T_{\text{g1sm}}+T_{\text{mm}}$ $+3T_{\text{g1pa}}+T_{\text{bp}}$	$T_{\text{g1sm}}+T_{\text{g1pa}}+2T_{\text{bp}}$ $+T_{\text{mbp}}+2T_{\text{ebp}}$	$\lvert\mathbb{G}_T\rvert+\lvert\mathbb{G}_1\rvert$
UDVS-2[17]	$2T_{\text{g1sm}}$	$5T_{\text{g1sm}}+3T_{\text{g1pa}}$	$2T_{\text{g1sm}}+3T_{\text{g1pa}}$ $+3T_{\text{bp}}+T_{\text{mbp}}$	T_{bp}	$2T_{\text{g1sm}}+3T_{\text{g1pa}}+$ $2T_{\text{bp}}+T_{\text{mbp}}+2T_{\text{ebp}}$	$\lvert\mathbb{G}_T\rvert+\lvert\mathbb{G}_1\rvert$
本文 UDVSP	T_{g1sm}	$T_{\text{g1sm}}+T_{\text{mi}}+T_{\text{h}}$ $+2T_{\text{mm}}+2T_{\text{ma}}$	$2T_{\text{g1sm}}+T_{\text{g1pa}}$ $+2T_{\text{ma}}+T_{\text{h}}$	$3T_{\text{ma}}+T_{\text{h}}$	$14T_{\text{g1sm}}+13T_{\text{g1pa}}+$ $7T_{\text{mm}}+3T_{\text{ma}}+T_{\text{h}}$	$2\lvert\mathbb{Z}_n\rvert$

表 2　符号定义和耗时情况

Tab. 2 Notations and time cost

符号	描述	时间/ms
T_{g1sm}	群 $\mathbb{G}_1$ 上的点乘运算	35.3111
T_{g2sm}	群 $\mathbb{G}_2$ 上的点乘运算	206.575
T_{g1pa}	群 $\mathbb{G}_1$ 上的点加运算	0.165954
T_{g2pa}	群 $\mathbb{G}_2$ 上的点加运算	206.575
T_{h}	安全哈希函数	0.00576
T_{h2p}	全域哈希函数	17.1464
T_{bp}	群 $\mathbb{G}_T$ 上的双线性对运算	820.32
T_{ebp}	群 $\mathbb{G}_T$ 上的模幂运算	689.273
T_{mbp}	群 $\mathbb{G}_T$ 上的模乘运算	2.05855
T_{mi}	域 $\mathbb{Z}_n^*$ 上的模逆运算	0.05023
T_{mm}	域 $\mathbb{Z}_n^*$ 上的模乘运算	0.01231
T_{ma}	域 $\mathbb{Z}_n^*$ 上的模加运算	0.00271

表 3　实际性能对比结果

Tab. 3 Empirical performance comparison results

方案	计算开销/ms					通信代价/Byte
	UKGen	USign	UVerf	UTran	UIVerf	UIVerf
UDVSP-1[10]	35.3111	52.4575	1657.7864	35.3111	3038.4060	2048
UDVSP-2[10]	413.1500	35.3791	2055.0557	35.3111	4124.9480	2048
UDVS-1[15]	141.2444	106.2775	2498.4960	891.4524	3056.7220	2080
UDVS-2[17]	70.6222	178.4542	2534.1390	820.3200	3092.3650	2080
本文 UDVSP	35.3111	35.3971	70.7993	0.0138	496.6129	128

6 结论

虽然泛指定验证者签名证明 (UDVSP) 可以解决现有基于区块链的电子医疗记录共享系统面临的恶意传播问题，但现有的 UDVSP 方案均涉及高耗时的双线性对运算。本文先利用 SM2 数字签名算法设计一种更加安全高效的 UDVSP 方案，再构建基于区块链的电子医疗记录安全共享系统。为了说明 UDVSP 方案和共享系统具有实用性，本文首先证明本文 UDVSP 的安全性，然后在此基础上分析系统的安全性，最后通过性能对比和仿真结果进行论证。

参考文献

[1] TAMERSOY A, LOUKIDES G, NERGIZ M E, et al. Anonymization of longitudinal electronic medical records[J]. IEEE Transactions on Information Technology in Biomedicine, 2012, 16(3): 413-423.

[2] OHNO-MACHADO L. Sharing data from electronic health records within, across, and beyond healthcare institutions: Current trends and perspectives[J]. Journal of the American Medical Informatics Association, 2018, 25(9): 1113-1113.

[3] LIU J, LI X, YE L, et al. BPDS: A blockchain based privacy-preserving data sharing for electronic medical records[C].// Proceedings of the 2018 IEEE Global Communications Conference, Piscataway: IEEE, 2018: 1-6.

[4] LIN C, HE D, HUANG X, et al. BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0[J]. Journal of Network and Computer Applications, 2018, 116: 42-52.

[5] 祝烈煌，高峰，沈蒙，等. 区块链隐私保护研究综述[J]. 计算机研究与发展，2017, 54(10): 2170-2186. (ZHU L H, GAO F, SHEN M, et al. Survey and privacy preserving techniques for blockchain technology[J]. Journal of Computer Research and Development, 2017, 54(10): 2170-2186.)

[6] DUBOVITSKAYA A, XU Z, RYU S, et al. Secure and trustable electronic medical records sharing using blockchain[C]. Proceedings of the 2017 American Medical Informatics Association Annual Symposium, USA: AMIA, 2017: 650.

[7] USMAN M, QAMAR U. Secure electronic medical records storage and sharing using blockchain technology[J]. Procedia Computer Science, 2020, 174: 321-327.

[8] AZARIA A, EKBLAW A, VIEIRA T, et al. Medrec: Using blockchain for medical data access and permission management[C].// Proceedings of the 2nd International Conference on Open and Big Data, Piscataway: IEEE, 2016: 25-30.

[9] YUE X, WANG H, JIN D, et al. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control[J]. Journal of Medical Systems, 2016, 40(10): 1-8.

[10] BAEK J, SAFAVI-NAINI R, SUSILO W. Universal designated verifier signature proof (or how to efficiently prove knowledge of a signature)[C].// Proceedings of the 11th International Conference on the Theory and Application of Cryptology and Information Security, Cham: Springer, 2005: 644-661.

[11] CHEN X, CHEN G, ZHANG F, et al. Identity-based universal designated verifier signature proof system[J]. International Journal of Network Security, 2009, 8(1): 52–58.

[12] ABBASINEZHAD-MOOD D, NIKOOGHADAM M. An anonymous ecc-based self-certified key distribution scheme for the smart grid[J]. IEEE Transactions on Industrial Electronics, 2018, 65(10): 7996-8004.

[13] STEINFELD R, BULL L, WANG H, et al. Universal designated-verifier signatures[C].// Proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security, Cham: Springer, 2003: 523-542.

[14] ZHANG R, FURUKAWA J, IMAI H. Short signature and universal designated verifier signature without random oracles[C].// Proceedings of the 3rd International Conference on Applied Cryptography and Network Security, Cham: Springer, 2005: 483-498.

[15] HUANG X, SUSILO W, MU Y, et al. Secure universal designated verifier signature without random oracles[J]. International Journal of Information Security, 2008, 7(3): 171-183.

[16] LIN H Y. Secure universal designated verifier signature and its variant for privacy protection[J]. Information Technology and Control, 2013, 42(3): 268-276.

[17] RASTEGARI P, BERENJKOUB M, DAKHILALIAN M, et al. Universal designated verifier signature scheme with non-delegatability in the standard model[J]. Information Sciences, 2019, 479: 321-334.

[18] SEO S H, HWANG J Y, CHOI K Y, et al. Identity-based universal designated multi-verifiers signature schemes[J]. Computer Standards & Interfaces, 2008, 30(5): 288-295.

[19] CAO F, CAO Z. An identity based universal designated verifier signature scheme secure in the standard model[J]. Journal of Systems and Software, 2009, 82(4): 643-649.

[20] CHANG T Y. An ID-based multi-signer universal designated multi-verifier signature scheme[J]. Information and Computation, 2011, 209(7): 1007-1015.

[21] HOU S, HUANG X, LIU J K, et al. Universal designated verifier transitive signatures for graph-based big data[J]. Information Sciences, 2015, 318: 144-156.

[22] LIN C, WU W, HUANG X, et al. A new universal designated verifier transitive signature scheme for big graph data[J]. Journal of Computer and System Sciences, 2017, 83(1): 73-83.

[23] WANG M, ZHANG Y, Ma J, et al. A universal designated multi verifiers content extraction signature scheme[J]. International Journal of Computational Science and Engineering, 2020, 21(1): 49-59.

[24] METTLER M. Blockchain technology in healthcare: The revolution starts here[C].// Proceedings of the 18th International Conference on E-health Networking, Applications and Services, Piscataway: IEEE, 2016: 1-3.

[25] ROEHRS A, DA COSTA C A, DA ROSA RIGHI R. OmniPHR: A distributed architecture model to integrate personal health records[J]. Journal of Biomedical Informatics, 2017, 71: 70-81.

[26] 薛腾飞, 傅群超, 王枞, et al. 基于区块链的医疗数据共享模型研究[J]， 自动化学报，2017, 43(9): 1555-1562. (XUE T F, FU Q C, WANG C, et al. A medical data sharing model via blockchain[J]. Acta Automatica Sinica, 2017, 43(9): 1555-1562.)

[27] WU S H, DU J. Electronic medical record security sharing model based on blockchain[C].// Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, New York: ACM, 2019: 13-17.

[28] LI L, YUE Z X, WU G Q: Electronic Medical Record Sharing System Based on Hyperledger Fabric and InterPlanetary File System[C].// Proceedings of the 5th International Conference on Compute and Data Analysis, New York: ACM, 2021: 149-154.

[29] ZHANG Z, YANG K, ZHANG J, et al. Security of the SM2 signature scheme against generalized key substitution attacks[C].// Proceedings of the 2nd International Conference on Research in Security Standardisation, Cham: Springer, 2015: 140-153.

This work is partially supported by the National Natural Science Foundation of China (62102089), the Fundamental Research Funds for the Central Universities (2042021kf1030).

LIN Chao, born in 1991, Ph.D., lecturer. His research interests include applied cryptography and blockchain privacy protection.
HE Debiao, born in 1980, Ph.D., professor. His research interests include applied cryptography, cryptographic protocols, and cloud computing security.

HUANG Xinyi, born in 1981, Ph.D., professor. His research interests include applied cryptography and network security.