

基于批量签名思想的可截取签名构造

唐紫鑫^{1,2}, 黄欣沂^{1,2}

(1. 福建师范大学数学与信息学院, 福建 福州 350007;
2. 福建省网络安全与密码技术重点实验室, 福建 福州 350007)

摘要: 根据批量签名的思想, 将 Waters 数字签名方案批量化, 进而构造可截取签名。所构造的方案是 Steinfeld、Bull、Zheng (ICISC 2001) 提出的 RSAProd 方案的改进, 以较长的截取签名长度为代价节省整体的运算时间, 并证明所构造方案在适应性选择消息攻击下具有不可伪造性和隐私性。

关键词: 可截取签名; Waters 数字签名; 批量签名; RSAProd 方案

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018102

Construction of the content extraction signature scheme based on the thought of the batch scheme

TANG Zixin^{1,2}, HUANG Xinyi^{1,2}

1. School of Mathematics and Information, Fujian Normal University, Fuzhou 350007, China
2. Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou 350007, China

Abstract: The Waters scheme was transformed into the content extraction signature scheme at the bridge of the thought from the batch signature scheme. The proposed scheme is improved by the RSAProd scheme, presented by Steinfeld, Bull, Zheng (ICISC 2001). The operation time is saved in every stage at the slight sacrifice of the length of extraction signatures. The security was proved that the proposed scheme is existentially unforgeable under chosen message attacks while the privacy is maintained.

Key words: content extraction signature, Waters scheme, batch signature, RSAProd scheme

1 引言

数据和信息之间是相互联系的。数据是反映客观事物属性的记录, 是信息的具体表现形式^[1]。数据经过加工处理之后, 就成为信息; 而信息需要经过数字化转变成数据才能存储和传输^[1]。数据不仅是用户的隐私, 更是互联网财富的源泉。众多科研机构、研究人员将问题与生活实际联系起来时, 数据提供着必不可少的支撑。在数据驱

动型经济背景下, 企业的决策和国家的发展战略制定都需要以数据为依据, 各大企业乃至世界各国陷入一场前所未有的数据争夺战。数据安全问题的保障、隐私数据的保护也成为数据争夺战中应当考虑的重要问题。

数字签名^[2]是保证数据安全的核心技术之一, 在电子政务、电子商务、医疗数据、电子现金等领域有广泛的用途。数字签名可提供数据内容的完整性和数据源的真实性检测。

收稿日期: 2018-10-25; 修回日期: 2018-11-20

通信作者: 黄欣沂, xyhuang81@yahoo.com

基金项目: 国家自然科学基金资助项目 (No.61822202, No.61872089)

Foundation Item: The National Natural Science Foundation of China (No.61822202, No.61872089)

数字签名的标准安全要求是在自适应选择消息攻击下满足 EUF-CMA 安全——存在不可伪造性 (existential unforgeability under adaptive chosen message attacks)^[3]。EUF-CMA 安全的含义：已知签名者的公钥，PPT (probability polynomial-time) 攻击者通过适应性询问获得需要的有效消息签名对后，能为某个新消息计算出有效签名的概率是可以忽略的。若数字签名方案满足此标准安全要求，则该数字签名有效并能让消息接收者相信收到的消息是完整的且未被恶意篡改，同时消息的来源是相应公钥的持有者。经典数字签名方案有 ElGamal^[4-5]、DSA、ECDSA^[6]、RSA-FDH^[7] 和 Schnorr^[8] 签名等。

尽管数字签名方案的标准安全要求能够满足数据认证的基本要求，却也阻碍了签名持有者对已签名数据的合理操作。

为了满足相应的实际需求，Steinfeld、Bull、Zheng (ICISC 2001) 提出可截取签名 (CES, content extraction signature)^[9]。截取中“截”意味着删除，“取”作提取之意。在不与初始签名人进行交互的情况下，可截取签名允许签名的持有者将可以公开进行验证的数据提取出来组成新数据，并根据初始签名计算出对新数据的签名。换言之，可截取签名允许签名的持有者对删除敏感数据后的新数据集生成新的签名。

由于相对数字签名所拥有的此种特殊功能，可截取签名的应用场景相当广泛。本文以电子病历为例阐述可截取签名的功能。假设研究所 C 为研究某种疾病的治疗方案，需要征集广大患者的病历。以患者 B 为例，设 B 可提供就诊医院 A 签发的电子病历。电子病历通常记录着患者的姓名、性别、身份证号、家庭地址、联系电话、病史和诊疗记录 (包括病情描述和处方) 等相关信息。但是 B 不愿向研究所透露身份证号、家庭地址、联系电话等信息。如果 A 直接用普通数字签名算法对病历签名，那么 B 无法对病历进行删改以保护隐私信息，从而 B 可能拒绝 C 的请求。可截取签名则较好地解决此类问题。若 A 在签名阶段使用可截取签名对病历签名，则 B 可以对病历进行适当的操作，再提供给 C。相比普通数字签名，可截取签名最大的优势在于支持删除操作，且不

需要私钥即可通过初始数据和初始签名计算出新的数字签名，并证实所保留数据的真实性。自提出以来，国内外学者对可截取签名进行了大量深入的研究。

文献[10]将可截取签名应用于以数字图书馆为典型代表的环境，提出采用分级群组策略的可截取签名方案，这是对文献[9]提出的可截取签名的直接应用。文献[11]提出新的基于身份的可截取签名方案，该方案不需要对每个子消息进行签名，这提高了签名效率，且能够防止私钥产生机构伪造签名。文献[12]提出一种满足强安全性、基于离散对数困难问题的可截取签名方案，此方案还包含身份信息，指数计算较少，相应地减少了计算量。文献[13]的方案基于 FDH-RSA 签名方案改进，在保持原方案安全性能不变的基础上，优化截取文档的结构，解决了截取后文档存在的板式凌乱问题。文献[14]提出一种能把密钥泄露带来的损失减小到最低的可截取签名方案。文献[15]提出一种细粒度的访问控制，在加密数据的同时把符合属性的子消息传送给用户，对存储中访问控制的问题进行细化，提高消息的利用率。文献[16]则将截取消息分为必须截取和可选截取两部分，允许对部分消息进行统一签名和验证。这些重要研究在文献[9]的基础上从不同角度继承和发展，丰富了可截取签名的研究。

上述应用方案的改进与文献[9]中提出的 CV (commit vector)、HT (hash tree)、RSA 积 (RSAP, RSAProd)、MERP (multi-exponent RSAProd) 4 种方案联系密切。CV 方案基于向量承诺设计，用 n 个签名取代一个签名。方案以 n 个承诺为代价，只要能减少承诺的计算量，那么签名的计算量也会相应减少。但提取子消息的随机值和删除的子消息的承诺值使签名长度很长，与子消息的数量呈线性关系。为了减少删除的子消息的承诺值造成的签名冗长，改进的 HT 方案巧妙地使用抗碰撞的散列函数构造二叉树，将数据存储在二叉树中，减少了签名长度，然而计算量仍很大。RSAP 方案的构造基于 RSA 签名的同态性质，因而验证者只需验证 RSA 签名的乘积模 N 的值是否等于散列值乘积的签名模 N 的值。因此，方案减少了传送给验证者的签名长度，缺点在于没有减少签名

者与数据持有者之间所传递签名的长度。而 MERP 方案对这个缺点进行了改进,节省了签名者的计算量但失去了快速验证的性质。这几个方案的设计目标都是既能快速签名又能快速验证的可截取签名,且都是基于批量签名^[17]设计的。

批量签名的概念由 Fiat 于 1989 年提出,能够用一次签名对若干个不同消息签名,并且可以对每一条消息进行独立验证。此后,批量签名得到广泛的应用和发展,其中影响很大的工作之一是文献[18]提出的基于树结构的批量签名算法。此结构与任何可证明安全的数字签名进行结合都可以得到安全的批量签名方案。文献[9]中的 HT 方案所用的树结构便是根据树结构的批量签名改造而来。不同之处在于,文献[18]的方案不能满足可截取签名隐私性的要求,于是文献[9]中的一个方案运用向量承诺^[19]的隐藏性保证隐私性,此即为 HT 方案奠定基础的 CV 方案。文献[9]中的 RSAP 方案具有批量验证的性质,但是不能批量签名。MERP 方案应用文献[17]中的 Fiat 变换进行多指数 RSA 批量化,使方案具有批量签名的性质,但失去快速验证的性质。另外,文献[13]也引入批量签名的思想,改进了签名和认证部分。由此,将批量签名改进成可截取签名是构造可截取签名值得研究的一个方向,改进的过程中关键在于如何在保护数据隐私性的同时使计算量和签名长度同时达到最优。

本文从 Waters 签名方案^[20]着手,先把数字签名批量化,构造批量化的 Waters 签名,再将批量签名转化为可截取签名(称之为基于 Waters 签名方案的可截取签名 WCES)。此方案为可截取签名的构造提供了较为一般的方法,与其他可截取签名方案进行横纵向对比,说明此方案运行速度较快。

2 预备知识

2.1 双线性对

设 G 和 G_1 分别是素数 p 阶乘法群, g 为群 G 的生成元,映射 $\hat{e}: G \times G \rightarrow G_1$ 具有以下性质。

1) 双线性: 若 $\forall a, b \in \mathbb{Z}$, 有 $\hat{e}(g^a, g^b) = \hat{e}(g^b, g^a) = \hat{e}(g, g)^{ab}$ 。

2) 非退化性: 若 $\forall a, b \in G$, 使 $\hat{e}(a, b) \neq 1$,

其中, 1 为 G_1 的单位元。

3) 可计算性: 存在多项式时间算法计算 $\hat{e}(g^a, g^b)$ 。

2.2 困难假设

在循环群 G 中定义计算性 DH 假设 (CDH, computational Diffie-Hellman)。简单地说, CDH 假设表示以下问题是困难的: 对于任意生成元 $g \in G$, 已知 $g^a, g^b \in G$ (a, b 均是随机选取的指数), 输出 $g^{ab} \in G$, 将此假设正式化如下列定义。

定义 1^[21] 群 G 中的 CDH 问题是困难的, 对任意多项式时间算法 A , 以下概率可忽略。

$$\Pr[params \leftarrow G(1^k); \\ a, b \leftarrow \mathbb{Z}_q : A(params, g^a, g^b) = g^{ab}]$$

2.3 数字签名

定义 2^[21] 数字签名方案包括 3 个多项式算法 ($KeyGen, Sign, Verify$)。

1) 随机的密钥生成算法 ($KeyGen$): 输入安全参数 1^k , 输出公私钥对 (pk, sk) 。记作

$$(pk, sk) \leftarrow KeyGen(1^k)$$

2) 签名算法 ($Sign$): 输入私钥 sk 和消息 m , 输出消息 m 的签名 σ 。记作

$$\sigma \leftarrow Sign(sk, m)$$

3) 确定性的验证算法 ($Verify$): 输入公钥 pk , 消息 m 和待验证的签名 σ , 输出 0 或 1。如果 σ 是 m 的有效签名, 则输出 1, 否则输出 0。记作

$$\{0, 1\} \leftarrow Verify(pk, m, \sigma)$$

定义 3^[21] (CMA 实验) 数字签名方案需要满足的安全性质是在自适应选择消息攻击下具有存在不可伪造性。本文用挑战者 C 和攻击者 A 之间的实验来描述不可伪造性。

初始化: C 运行密钥生成算法 $KeyGen(1^k)$ 获得公私钥对 (pk, sk) , 并将 pk 传送给 A 。

询问: A 可以通过访问签名预言机 $Sign$ 的方式向挑战者询问至多 q 个消息的签名。

对每个消息 $m_i (i = 1, 2, \dots, q)$, C 运行签名算法 $Sign(sk, m_i)$, 并将算法的输出 (m_i, σ_i) 返回给 A 。本文用 Q 表示 A 向预言机询问过的消息集合 $Q = \{m_1, m_2, \dots, m_n\}$ 。

输出伪造: 在完成所有消息询问后, 设 A 输

出伪造的消息签名对是 (m^*, σ^*) 。若此消息签名对满足条件 $Verify(pk, m^*, \sigma^*) = 1$ 且 $m^* \notin Q$ ，则 A 攻击成功。

在选择消息攻击下，如果任意的概率多项式敌手 A 攻击成功的概率是可忽略的，则称签名方案 $(KeyGen, Sign, Verify)$ 具有存在不可伪造性。

2.4 Waters 签名方案

定义 4^[21] Waters 签名方案包括 3 个多项式时间算法。

1) 密钥生成算法：输入安全参数 1^k ，计算参数 $params = (\mathcal{G}, \mathcal{G}_1, q, g, \hat{e}) \leftarrow G(1^k)$ ；随机选择 $a \leftarrow \mathbb{Z}_q$ 并设 $g_1 := g^a$ ；选择随机数 $g_2, u_0, \dots, u_k \leftarrow \mathcal{G}$ ；输出公钥 $(params, g_1, g_2, u_0, \dots, u_k)$ ，私钥 g_2^a 。

设 $H(m) = u_0 \prod_{i=1}^k u_i^{m_i}$ ，其中， $m = m_1 m_2 \dots m_k \in \{0, 1\}^k$ 。

2) 签名算法：给定消息 $m \in \{0, 1\}^k$ ，输入签名者所选随机数 $r \in \mathbb{Z}_q$ ，输出签名 $(g_2^a H(m)^r, g^r)$ 。

3) 验证算法：输入消息 m 和对应签名 (σ_1, σ_2) ，检查 $\hat{e}(g, \sigma_1) = \hat{e}(\sigma_2, H(m)) \hat{e}(g_1, g_2)$ 是否成立，如若成立，则输出 1，否则输出 0。

定理 1^[21] 如果群 $\mathcal{G}$ 中的 CDH 问题是困难的，那么 Waters 签名方案在适应性选择消息攻击下满足存在不可伪造性。

2.5 批量签名

对很多消息同时签名时，批量签名能够用一次签名完成对若干个不同的消息签名，并且可以对每一条消息进行独立验证^[17]，从而批量对消息签名大大提高了效率。

批量签名应用非常广泛，能用于电子商务、电子现金等领域。因其应用领域的相似性，可考虑转化为可截取签名。与批量签名不同的是，可截取签名可将待签名消息做适当处理以保护隐私信息。

2.6 可截取签名

由于普通的数字签名不允许对数据进行任何修改，为了让签名持有者能够从初始数字签名计算出截取签名（对删除隐私信息后的数据生成的签名），一种简易的方法是签名者 A 把消息划分为若干子消息，逐个对子消息进行签名，并把所有子消息的签名传送给签名的使用者 B 。 B 保留

需要的子消息，并从得到的签名中挑选对应的子消息的签名组成的集合作为截取消息的签名。这是可截取签名的一种经典设计思路。验证者能够对此签名集合中的每一签名逐个验证。但如果签名者不能对消息的截取进行控制，将容易导致消息被恶意截取以致消息泄露。为此，文献[9]在可截取签名中引入可截取访问规则（CEAS, content extraction access structure），使签名者能够通过 CEAS 控制消息 M 的截取，从而有效阻止消息被恶意截取进而泄露隐私。

本文用消息 $M = \{m_1, m_2, \dots, m_n\}$ 表示由 n 个子消息组成的原消息。新消息 $M' = \{m_1', m_2', \dots, m_n'\}$ 。

$CI(M')$ 表示保留消息编号的集合。为保证签名者对原消息 M 的截取方式具有完全控制权，CEAS 对每个子消息段规定必须保留和可保留 2 种方式，分别用 1 和 0 表示。故 CEAS 是由若干个向量组成的，每一个向量代表一个可截取规则。截取者根据 CEAS 选择的截取子集 X 确定 $CI(M')$ 以及 M' 。其中， M' 中的子消息数量、排列位置必须和 M 中的子消息保持一致。若 M 中子消息 m_i 的编号在 $CI(M')$ 中，则 M' 中的 $m_i' = m_i$ ，否则，用符号“?” 替换 m_i 。如果截取方式合法，则表示为 $CI(M') \in CEAS$ 。

例如，设任意消息 $M = \{m_1, m_2, m_3, m_4, m_5, m_6\}$ ，不妨设 $CEAS = \{(1, 1, 0, 0, 0, 0), (1, 0, 1, 0, 0, 0)\}$ 。若 $X = (1, 1, 0, 0, 0, 0) \in CEAS$ ，则 $CI(M') = \{1, 2\}$ 和对应的 $M' = \{m_1, m_2, ?, ?, ?, ?\}$ 是合法的； $CI(M') = \{1, 2, 3\}$ 和对应的 $M' = \{m_1, m_2, m_3, ?, ?, ?\}$ 也是合法的。但是， $CI(M') = \{1, 3\}$ 和对应的 $M' = \{m_1, ?, m_3, ?, ?, ?\}$ 是不合法的，因为没有保留必须保留的消息 m_2 ； $CI(M') = \{1, 2, 3\}$ 和对应的 $M' = \{m_1, m_2, m_3, ?, ?\}$ 也是不合法的，因为 M' 和 M 中子消息数量不一致。

定义 5^[9] 可截取签名包括 4 个多项式算法 $CES = (Gen, Sig, Ext, Ver)$ 。

1) 密钥生成算法 (Gen)：输入安全参数 1^k ，输出公私钥对 (pk, sk) 。记作

$$(pk, sk) \leftarrow Gen(1^k)$$

2) 签名算法 (Sig)：输入私钥 sk 、 M 和可截取访问规则 $CEAS$ ，输出可截取签名 σ_F 。记作

$$(M, \sigma_F) \leftarrow Sig(sk, M, CEAS)$$

3) 截取算法 (Ext)：输入公钥 pk 、 M 、可

截取签名 σ_F 和截取子集 X ，输出截取签名 σ_E 。
记作

$$(M', \sigma_E) \leftarrow \text{Ext}(pk, M, \sigma_F, X)$$

4) 验证算法 (Ver): 输入公钥 pk 、消息 M 和签名 σ ，输出 0 或者 1。如果 σ 是 M 的有效签名，输出 1，否则输出 0。记作

$$\{0, 1\} \leftarrow Ver(pk, M, \sigma)$$

可截取签名的正确性要求：可截取签名 (CES) 需要满足下述一致性条件。

(签名算法的正确性要求) 对任意的安全参数 1^k ，任意的公私钥对 $(pk, sk) \leftarrow Gen(1^k)$ 、 $CEAS$ 、 M 和 $(M, \sigma_F) \leftarrow Sig(sk, M, CEAS)$ ，必须能够通过算法 Ver 的验证，即 $Ver(pk, M, \sigma_F) = 1$ 。

(验证算法的正确性要求) 对任意的安全参数 1^k ，任意的公私钥对 $(pk, sk) \leftarrow Gen(1^k)$ 、 $CEAS$ 、 M 、 $(M, \sigma_F) \leftarrow Sig(sk, M, CEAS)$ 、截取子集 $X \in CEAS$ 和 $(M', \sigma_E) \leftarrow Ext(pk, M, \sigma_F, X)$ ，必须能够通过算法 Ver 的验证，即 $Ver(pk, M', \sigma_E) = 1$ 。

可截取签名的安全模型包括不可伪造性和隐私性两部分。

CES 不可伪造性指除了按照可截取访问规则生成原签名消息的子消息之外，攻击者不能再对其他消息产生有效的可截取签名。

假设概率多项式算法能够以自适应选择消息的方式攻击可截取签名方案 (Gen, Sig, Ext, Ver) ，可以用挑战者 C 和伪造者 F 之间的实验描述可截取签名方案的不可伪造性。

C 运行 $Gen(1^k)$ 获得公私钥对 (pk, sk) ，并将公钥 pk 传送给 F 。

F 可以自适应地访问签名预言机。 F 以 $(M_i, CEAS_i)$ 向预言机进行至多 q 次询问， C 运行签名算法 $Sig(sk, M_i, CEAS_i)$ 并返回有效的消息签名对 (M_i, σ_i) 给 F 。本文用 M 表示 F 向预言机询问过的消息集合 $M = \{M_1, M_2, \dots, M_q\}$ 。

最终 F 输出伪造的消息签名对 (M^*, σ^*) 。

挑战者运行验证算法，如果下列条件成立，那么 F 伪造成功：

1) $Ver(pk, M^*, \sigma^*) = 1$ ；

2) 若 F 伪造的消息 M^* 不是曾经询问过的消息 M_i 的子集，则 F 伪造了一个新的有效消息，或

者， M^* 是 M_i 的子集但伪造的消息中保留的消息不满足相应截取规则，即 $CI(M^*) \notin CEAS_i$ 。

在适应性选择消息攻击下，如果对任意的概率多项式伪造者 F 在实验中获胜的概率是可忽略的，那么称可截取签名方案 (Gen, Sig, Ext, Ver) 在适应性选择消息攻击下满足存在不可伪造性。

隐私性是指已知截取消息和截取签名，攻击者不能知道被删除消息的内容。

假设概率多项式算法能够以自适应选择消息的方式攻击可截取签名方案 (Gen, Sig, Ext, Ver) ，可以用挑战者 F 和区分者 D 之间的实验描述可截取签名方案的隐私性。

实验主要包括 2 个阶段：在询问阶段中， D 可以自适应请求询问 Sig 预言机，询问阶段结束后， D 向 C 提出挑战 (M_0, M_1) ，作为回应， C 产生随机数 $c \in \{0, 1\}$ ，筛选出 M_0 和 M_1 其中一个，并对随机筛选出的消息计算截取签名返回给 D 。在猜测阶段， D 仍然可询问 Sig 预言机，最后给出猜测值 c' 。

初始化： F 运行 $Gen(1^k)$ 获得公私钥对 (pk, sk) ，并将公钥 pk 传送给 D 。

询问阶段： D 可以自适应地询问签名预言机 Sig 。 D 以 $(M_i, CEAS_i)$ 向预言机进行至多 q 次询问，然后 C 运行 $Sig(sk, M_i, CEAS_i)$ 并返回有效的消息签名对 (M_i, σ_i) 给 D 。本文用 M 表示 D 向预言机询问过的消息集合 $M = \{M_1, M_2, \dots, M_q\}$ 。

D 自适应地选择合法的签名，利用截取算法 Ext 计算得到截取签名。

挑战阶段：询问阶段结束后， D 输出 2 个消息 (M_0, M_1) ，它们除了在位置 i^* 处的子消息不同外，在其他位置的子消息是相同的。即 $M_0[i] = M_1[i], i \neq i^*$ 。这组消息分别在位置 i^* 上有着对应的消息 M_0 和 M_1 ，即 $M_0[i^*] = M_0$ ， $M_1[i^*] = M_1$ 。同时， D 对 2 个消息选择相同的 $CEAS^*$ ，且 D 可选择待保留消息编号的集合 $X^* \in CEAS^*, i^* \notin X^*$ 。

作为回应， C 利用产生的随机数 $c \in \{0, 1\}$ ，筛选出 M_0 和 M_1 其中一个，选出的消息设为 M^* ，即 $M^* = M_c$ 。根据 D 选择的 $CEAS^*$ 以及 $X^* \in CEAS^*$ ， C 依次计算

$$\sigma_F^* \leftarrow Sig(sk, M^*, CEAS^*)$$

$$\sigma_E^* \leftarrow \text{Ext}(pk, M^*, \sigma_F^*, X^*)$$

最终将计算结果 σ_E^* 返回给 $\mathcal{D}$ 。

猜测阶段：收到 $\mathcal{C}$ 返回的签名后， $\mathcal{D}$ 仍然可以询问 Sig ，最后给出猜测值 c' 。

猜测值：最后 $\mathcal{D}$ 输出猜测的值 c' ，如果 $c' = c$ 且 $i^* \notin X^*$ ，那么 $\mathcal{D}$ 区分成功。

在适应性选择消息攻击下，设区分者 $\mathcal{D}$ 区分成功的概率为 $\Pr[c' = c]$ ，定义 $\mathcal{D}$ 能区分成功的优势为 $\text{Adv}_{\mathcal{D}, \text{CES}}^{\text{CMA}, pk}$ ，那么 $\text{Adv}_{\mathcal{D}, \text{CES}}^{\text{CMA}, pk} = \Pr[c' = c] - \frac{1}{2}$ 。

如果对于任意的概率多项式区分者 $\mathcal{D}$ 而言，该优势都是可忽略的，则可截取签名方案 $(\text{Gen}, \text{Sig}, \text{Ext}, \text{Ver})$ 在选择消息攻击下满足隐私性。

2.7 弱序 CES 不可伪造性

定义 6^[9] 对于能访问 CES 签名预言机的任意攻击者 $\mathcal{A}$ ，如果 $\mathcal{A}$ 产生有效的消息签名对 (M, σ) 是不可行的，则称可截取签名方案 CES 具有弱序 CES 不可伪造性 (WO-UF)，其中有效的消息签名对 (M, σ) 满足下列条件：

1) 签名 σ 是消息 M 的有效签名；

2) 消息 M 包含某个位置 i 上的子消息，此子消息不同于所有向 CES 签名预言机询问过的消息位置 i 处的子消息。

定义 7^[9] (不可伪造变换 $T_{\text{wo}}(\bullet)$) 变换 $T_{\text{wo}}(\bullet)$ 将任何 CES 方案 $\text{CES}_1 = (\text{Gen}_1, \text{Sig}_1, \text{Ext}_1, \text{Ver}_1)$ 作为输入，都可以将其转化为新方案，即 $\text{CES}_2 = T_{\text{wo}}(\text{CES}_1) = (\text{Gen}_2, \text{Sig}_2, \text{Ext}_2, \text{Ver}_2)$ 。

引理 1^[9] 变换 $T_{\text{wo}}(\bullet)$ 将任何具有弱序不可伪造性的方案 CES_1 转化为 $\text{CES}_2 = T_{\text{wo}}(\text{CES}_1)$ ，使方案 CES_2 具备完整的 CES 存在不可伪造性。具体以公式表示为

$$\begin{aligned} \text{Insec}_{\text{CES}_2}^{\text{CES-UF}}(t, q_s, n, l) &\leq \\ \text{Insec}_{\text{CES}_1}^{\text{WO-UF}}(t', q'_s, n', l') &+ \frac{q_s(q_s - 1)}{2^{l_{\text{tag}} + 1}} \end{aligned} \quad (1)$$

t 是攻击者最大运行时间， q_s 是询问签名预言机的最大次数， n 是询问子消息的个数， l 是签名长度，且 $t' = t, q'_s = q_s, n' = n, l' = l + l_{\text{CEAS}} + l_{\text{tag}} + \log(n)$ 。

另外，定义 $\text{Insec}_{\text{CES}_2}^{\text{CES-UF}}(t, q_s, n, l) = \max_{A \in \text{AS}_{RP}} \text{Succ}_{A, \text{CES}_2}^{\text{CES-UF}}$ ，将攻击成功的最大概率考虑为不安全性。其中，资源参数 $RP = (t, q_s, n, l)$ ， $A \in \text{AS}_{RP}$ 是所有攻击者的集合。

3 批量化 Waters 数字签名方案

本节呈现由数字签名到批量签名的转换过程。

3.1 方案描述

定义 8 批量化 Waters 数字签名方案包括 3 个多项式算法。

1) 密钥生成算法 (KeyGen)：输入安全参数 1^k ，确定参数组 $\text{params} = (\mathcal{G}, \mathcal{G}_1, q, g, \hat{e}) \leftarrow G(1^k)$ 。 $|\mathcal{G}| = |\mathcal{G}_1| = q$ ，且 q 是一个大素数。 $\mathcal{G}$ 和 $\mathcal{G}_1$ 的生成元是 g 。随机选择 $a \leftarrow \mathbb{Z}_q$ 并设 $g_1 := g^a$ 。选择随机数 $g_2, u_0, \dots, u_k \leftarrow \mathcal{G}$ 。

输出公钥 $(\text{params}, g_1, g_2, u_0, \dots, u_k)$ ，私钥 g_2^a 。

2) 签名生成算法 (Sign)：输入待签名的消息 M （按需被分为 n 个子消息）和私钥 g_2^a ，签名过程如下。

① 计算每个子消息的散列值 $H(m_i) = u_0$

$$\prod_{j=1}^k u_j^{m_{ij}}, \quad m_i = m_{i1}m_{i2} \cdots m_{in} \in \{0, 1\}^k.$$

② $H(m) = H(H(m_1) \| H(m_2) \| \cdots \| H(m_n))$ 。

③ 签名者选择随机数 $r \in \mathbb{Z}_q$ ，计算消息 M 签名 $(\sigma_1, \sigma_2) = (g_2^a H(m)^r, g^r)$ 。

④ 输出消息 M 的批量签名 $((\sigma_1, \sigma_2), H(m), h_1, h_2, \dots, h_n), h_i = H(m_i)$ 。

3) 签名验证算法 (Verify)：输入公钥 $(\text{params}, g_1, g_2, u_0, \dots, u_k)$ 、消息 M 和对应的签名 (σ_1, σ_2) 。验证过程如下。

① 验证 $h_i = H(m_i), i = 1, 2, \dots, n$ 。

② 检查 $\hat{e}(g, \sigma_1) = \hat{e}(\sigma_2, H(m)) \cdot \hat{e}(g_1, g_2)$ 是否成立。若成立，则输出 1，否则输出 0。

3.2 方案安全性分析

定理 2 如果 Waters 方案在适应性选择消息攻击下满足存在不可伪造性，那么批量化的 Waters 方案是安全的。

说明 $((\sigma_1, \sigma_2), H(m), h_1, h_2, \dots, h_n), h_i = H(m_i))$ 是消息 M 的批量签名，则对每一个消息，都可以考虑单独的 Waters 签名。因此接下来只需考虑单个 Waters 签名的伪造。假设存在敌手攻破批量签名，敌手每选择一个消息，能产生相应的 Waters 签名，最终对一个新消息 $\tilde{m}$ 形成批量签名。

因此，本文将问题归结为，在适应性选择消

息攻击下对 Waters 签名方案的攻击。而由定理 1 知 Waters 签名方案在适应性选择消息攻击下具有存在不可伪造性, 可证批量化的 Waters 签名的安全性。

4 基于 Waters 签名方案的可截取签名

4.1 方案描述

定义 9 基于 Waters 签名方案的可截取签名 (WCES) 包括 4 个多项式算法。

1) 密钥生成算法 (*Gen*): 输入安全参数 1^k , 由此确定参数组 $params = (\mathcal{G}, \mathcal{G}_1, q, g, \hat{e}) \leftarrow G(1^k)$ 。 $|\mathcal{G}| = |\mathcal{G}_1| = q$, 且 q 是一个大素数。 $\mathcal{G}$ 和 $\mathcal{G}_1$ 的生成元是 g 。随机选择 $a \leftarrow \mathbb{Z}_q$ 并设 $g_1 := g^a$ 。选择随机数 $g_2, u_0, \dots, u_k \leftarrow \mathcal{G}$ 。

输出公钥 $(params, g_1, g_2, u_0, \dots, u_k)$, 私钥 g_2^a 。

2) 签名生成算法 (*Sig*): 输入待签名的消息 M (按需被分为 n 个子消息)、可截取访问规则 CEAS 和私钥 g_2^a 。定义 T 为 CEAS 标记, 在签名过程中随机选取。签名过程如下。

① 对 M 的每个子消息 m_i , 附上可截取访问规则 CEAS, CEAS 标记 T , 消息长度 n , 消息编号 i , 即 $m_i \leftarrow (CEAS, T, n, i, M_i)$, 其中 M' 对应于消息 m_i , 且 $M_i = (m_{i1} m_{i2} \dots m_{in}), m_{ij} \in \{0, 1\}^k$ 。

② 计算子消息散列值 $H(m_i) \leftarrow u_0 \prod_{j=1}^k u_j^{m_{ij}}$ 。

③ 签名者选择随机数 $r \in \mathbb{Z}_q$, 计算每个子消息的签名 $(\sigma_{i1}, \sigma_2) = (g_2^a H(m_i)^r, g^r)$ 。

④ 输出 $\sigma_F \leftarrow (CEAS, T, \langle (\sigma_{i1}, \sigma_2) \rangle_{i \in [n]})$ 。

3) 签名截取算法 (*Ext*): 输入消息 M 、可截取访问规则 CEAS 和可截取签名 σ_F , 截取者执行如下过程: 首先截取者验证收到的签名是否有效, 若有效, 则执行下列步骤, 否则返回失败。

删除相应子消息的签名, 截取过程如下。

① 根据签名者指定的可截取访问规则 CEAS 构造截取子集 X 。

② 根据截取子集, 生成保留的消息集合 M' 。

③ 取出保留消息对应的签名 $\langle (\sigma_{i1}, \sigma_2) \rangle_{i \in X}$ 。

④ 输出 $\sigma_E \leftarrow (CEAS, T, M', \langle (\sigma_{i1}, \sigma_2) \rangle_{i \in X})$ 。

4) 签名验证算法 (*Ver*): 输入公钥 $(params, g_1, g_2, u_0, \dots, u_k)$ 、消息 M' 和对应的签名 σ_E , 验证者执行如下过程。

① 令 $X' \leftarrow CI(M')$, 签名者首先验证 $X' \in CEAS$ 是否成立, 若成立, 则执行下列步骤, 否则返回失败。

② 对每个子消息 $m_i, i \in X'$, 计算 $H(m_i)$ 。

③ 计算 $H(m) \leftarrow \prod_{i \in X'} H(m_i)$ 。

④ 检查 $\prod_{i \in X'} \hat{e}(g, \sigma_{i1}) = \hat{e}(\sigma_2, H(m)) \cdot \hat{e}(g_1, g_2)$

是否成立。若成立, 则算法输出 1, 否则输出 0。

4.2 方案正确性分析

该方案的正确性包括以下两部分。

1) (签名算法的正确性要求) 对任意的安全参数 1^k , 任意的公钥 $(params, g_1, g_2, u_0, \dots, u_k)$ 、私钥 g_2^a 、可截取访问规则 CEAS、CEAS 标记 T 、消息 M , $m_i \leftarrow (CEAS, T, n, i, M_i)$, 计算每个子消息的散列值, 生成签名 $(\sigma_{i1}, \sigma_2) \leftarrow (g_2^a H(m_i)^r, g^r)$, 则 $\sigma_F \leftarrow (CEAS, T, \langle (\sigma_{i1}, \sigma_2) \rangle_{i \in [n]})$ 必须能够通过算法 *Ver* 的验证, 即 $Ver(pk, M, \sigma_F) = 1$ 满足

$$\begin{aligned} \prod_{i \in X'} \hat{e}(g, \sigma_{i1}) &= \prod_{i \in X'} \hat{e}(g, g_2^a H(m_i)^r) \\ &= \hat{e}(g, g_2^a) \hat{e}(g, H(m_1)^r) \hat{e}(g, g_2^a) \\ &\quad \hat{e}(g, H(m_2)^r) \dots \hat{e}(g, g_2^a) \hat{e}(g, H(m_n)^r) \\ &= \hat{e}(g^a, g_2) \hat{e}(g^r, H(m_1)) \hat{e}(g^a, g_2) \\ &\quad \hat{e}(g^r, H(m_2)) \dots \hat{e}(g^a, g_2) \hat{e}(g^r, H(m_n)) \\ &= \hat{e}(g_1, g_2) \hat{e}(\sigma_2, H(m_1)) \hat{e}(g_1, g_2) \\ &\quad \hat{e}(\sigma_2, H(m_2)) \dots \hat{e}(g_1, g_2) \hat{e}(\sigma_2, H(m_n)) \\ &= \hat{e}(\sigma_2, H(m)) \hat{e}(g_1, g_2) \end{aligned} \quad (2)$$

2) (验证算法的正确性要求) 对任意的安全参数 1^k , 任意的公钥 $(params, g_1, g_2, u_0, \dots, u_k)$ 、私钥 g_2^a 、可截取访问规则 CEAS、CEAS 标记 T 、消息 M' , 生成签名 $(\sigma_{i1}, \sigma_2) \leftarrow (g_2^a H(m_i)^r, g^r)$ 、进而构成 $\sigma_F \leftarrow (CEAS, T, \langle (\sigma_{i1}, \sigma_2) \rangle_{i \in [n]})$, 且对任意的截取子集 $X \in CEAS$ 和 $(M', \sigma_E) \leftarrow Ext(pk, M, \sigma_F, X)$, 必须能够通过算法 *Ver* 的验证, 即 $Ver(pk, M', \sigma_E) = 1$, 且当 $n = len(M')$ 时, 式(2)成立。

4.3 方案安全性分析

定理 3 1) 如果标准的数字签名 Waters 方案在适应性选择消息攻击下满足存在不可伪造性, 则 WCES 方案具有 CES 存在不可伪造性, 满足

$$\begin{aligned} Insec_{WCES}^{CES-UF}(t, q_s, n, l) &\leq \\ Insec_{Waters}^{CMA}(t[F], q_s[F], l[F]) &+ \frac{q_s(q_s - 1)}{2^{l_{aug} + 1}} \end{aligned} \quad (3)$$

其中, t 是攻击者最大运行时间, q_s 是询问签名预言机的最大次数, n 是询问子消息的个数, l 是签名长度。

2) WCES 方案具有 CES 隐私性 (完善且无条件的), 即 $Insec_{WCES}^{CES-PR}(\infty, n, l) = 0$ 。

证明 1) 首先, 方案 WCES 将一般性安全加强变换 $T_{WO}(\bullet)$ (定义 7) 作用于简易的 $WCES_1$ 方案转化而来, 即 $WCES = T_{WO}(WCES_1)$, 其中, 简易的 $WCES_1$ 方案中签名的子消息不包括 $(CEAS, n, T)$ 。

应用引理 1, 有

$$Insec_{WCES}^{CES-UF}(t, q_s, n, l) \leq Insec_{WCES_1}^{WO-UF}(t', q'_s, n', l') + \frac{q_s(q_s - 1)}{2^{\log^{+1}}} \quad (4)$$

其中, $t' = t, q'_s = q_s, n' = n, l' = l + l_{CEAS} + l_{tag} + \log(n)$ 。

要表示攻击 WCES 方案成功的概率与攻击 Waters 方案成功的概率的关系, 只需证明

$$Insec_{WCES_1}^{WO-UF}(t', q'_s, n', l') \leq Insec_{Waters}^{CMA}(t[F], q_s[F], l[F]) \quad (5)$$

其中, $t[F] = t' + O(q'_s n'), q_s[F] = (q'_s + 1)n', n' = n, l[F] = l' + \log(n')$ 。

令攻击 A_1 在 $WO-UF$ 下攻击签名方案 $WCES_1 = (Gen_1, Sig_1, Ext_1, Ver_1)$, 攻击者 A_2 在 CMA 下攻击签名方案 $Waters = (KeyGen, Sign, Verify)$ 。根据对 A_1 的攻击限制攻击者 A_2 成功的概率。

A_2 调用 CMA 实验, 输入 Waters 方案的公钥 $(params, g_1, g_2, u_0, \dots, u_k)$ 和安全参数 1^k , 其中 $params = (\mathcal{G}, \mathcal{G}_1, q, g, \hat{e}) \leftarrow G(1^k)$, 随机选择 $a \leftarrow \mathbb{Z}_q$ 并设 $g_1 := g^a$, 选择随机数 $g_2, u_0, \dots, u_k \leftarrow \mathcal{G}$, 相应的私钥是 g_2^a 。 A_2 能询问 Waters 方案签名预言机 S 。

初始化: 输入 1^k , $(params, g_1, g_2, u_0, \dots, u_k)$, A_2 运行 A_1 , 其中 A_1 作为 A_2 的子程序。

询问: 当 A_1 向预言机 Sig_1 做出第 j 个 CES 询问 $(CEAS_j, M_j)$, A_2 使用询问预言机 S 返回的结果通过模拟 Sig_1 算法做出回答。

令 $n_j = \text{len}(M_j)$ 。对任意的 $i \in [n_j]$, A_2 定义消息 $\bar{M}_j[i] = (i, M_j[i])$, 且向签名预言机 S 询问此消息的签名 $\bar{\sigma}_j[i]$ 。最终, A_2 设置模拟的签名为 $\sigma_j = (\langle \bar{\sigma}_j \rangle)_{i \in [n_j]}$ 。假设 A_2 保存此询问记录。

输出: A_1 终止询问并输出伪造的消息签名对

(M^*, σ^*) , 其中 $H(M^*) = \prod_{i \in X} H(M^*[i])$, $\sigma^* = (\sigma^*[1], \sigma^*[2]) = (g_2^a H(M^*)^r, g^a)$ 。

令 $n^* = \text{len}(M^*)$ 且 $X^* = CI(M^*)$ 。 A_2 搜索存储的询问记录, 试图寻找位置 (设单个消息截取满足截取规则) $i^* (\in X^*)$ 处的子消息满足

$$M^*[i^*] \neq M_j[i^*], \forall j \in [q_s]$$

如果 A_2 找到这样的一个位置 i^* , 则对每个 $i \in X^* - \{i^*\}$, 向签名预言机 S 对消息 $\bar{M}^*[i] = (i, M^*[i])$ 进行询问, 获得签名

$$(\sigma^*[i], \sigma^*[2]) = (g_2^a \cdot H(\bar{M}^*[i])^r, g^a)$$

经计算得

$$\bar{\sigma}^* = (g_2^a \cdot H(\bar{M}^*[i])^r, g^a)$$

最终, A_2 输出的伪造消息签名对是 $(\bar{M}^*[i^*], \bar{\sigma}^*[i^*])$ 。

至此完成 A_2 的描述, A_2 的资源参数可以从上述描述中得到验证。为了证明此论点, 还需要描述 A_2 在选择消息攻击下攻击成功的概率。

使用 $\Pr[\cdot]_{\text{exp}}$ 表示实验 exp 的概率;

CES 方案 $WCES_1$ (在 $WO-UF$ 下) 和 Waters 方案 (在 CMA 下) 的攻击实验分别记作 w_1 和 w 。

定义以下事件。 Succ_1 表示 A_1 在 $WO-UF$ 意义下攻击成功。 Succ_1 意味着 $(\bar{M}^*, \bar{\sigma}^*)$ 能通过方案 $WCES_1$ 的验证算法 (称此事件为 Valid_1), 且存在 $i^* (\in X^*)$ 满足 $M^*[i^*] \neq M_j[i^*], \forall j \in [q_s]$ (称此事件为 NewM_1)。事件 Succ_2 表示 A_2 在 CMA 意义下攻击成功。 Succ_2 意味着 $(\bar{M}^*, \bar{\sigma}^*)$ 能通过方案 Waters 的验证算法 (称此事件为 Valid_2), 且消息 $\bar{M}^*$ 从未询问过签名预言机 S (称此事件为 NewM_2)。

下面证明如果 Succ_1 发生, 则 Succ_2 也发生。因为 A_2 在攻击实验 $\text{exp}.w$ 中模拟 A_1 的视图, 如同在攻击实验 w_1 , 所以事件 Succ_2 在 2 个实验中有相同的概率, 因此有 $\text{Succ}_{A_2, \text{Waters}}^{CMA}(k) \geq \text{Succ}_{A_1, \text{WCES}}^{CES-UF}(k)$ 。

这包含要证的式子。

为了完成证明, 还需证 Succ_1 包含 Succ_2 。首先 Succ_1 包含 Valid_1 , 事件 Succ_1 表示 A_1 成功攻破方案 $WCES_1$, 则伪造的消息签名对是一个有效的 Waters 签名, 同时 Valid_2 发生。下面说明 NewM_2 发生。因为 Succ_1 发生, 则 NewM_1 发生, 即

$M^*[i^*] \neq M_j[i^*], \forall j \in [q_s], \bar{M}^*[i^*] \neq \bar{M}_j[i^*], \forall j \in [q_s]$, 且 A_2 对预言机 S 的其他询问 (即 $\bar{M}^*[i]$ 和 $\bar{M}_j[i]$, $i \neq i^*, \forall j \in [q_s]$) 均和伪造的消息 $\bar{M}^*[i^*]$ 有着不同前缀)。所以 $Succ_1$ 发生, 伪造的消息不会询问过预言机 S 。此即 $NewM_2$ 发生。

2) 此可截取签名的隐私性是显然的, 因为截取签名统计上独立于删除的子消息。

4.4 效率分析

本节对基于 Waters 签名方案的可截取签名的算法复杂度进行分析。

纵向上, 由于 WCES 方案可视为文献[2]提出的 RSAP 方案的平行改进, 因此将其与 RSAP 方案进行比较, 符号说明如表 1 所示, 比较结果如表 2 所示。

由表 1 可得, 由于 Waters 签名方案运算速度的优越性, WCES 方案在空间复杂度与 RSAP 方

案相近的情况下, 能够保持时间复杂度较优。

横向上, 文献[13]提出的方案改进的可截取签名方案 (IRSAP, Improved RSAP) 以及文献[9]中的 HT 方案都是应用批量签名思想对可截取签名进行的改进, 其中, IRSAP 也是根据 RSAP 方案改进而来, 因而可考虑与 CEAS 方案进行对比分析, 如表 3 所示, 符号说明也如表 1 所示。

从表 3 可看出, IRSAP 的算法复杂度略高于 RSAP 方案。HT 方案引入批量签名的思想固然提高了签名速度, 签名长度亦相应减少, 但其算法复杂度很大程度上依赖于数字承诺的应用。可见 WCES 乃折中有有效的改进。

5 结束语

本文主要呈现可截取签名较为一般的构造方

表 1

符号说明

符号	符号说明	符号	符号说明
n	原消息中子消息的数目	T_{Ext}^{Waters}	截取签名所用时间
m	截取消息中子消息的数目	T_{Prod_H}	计算散列值乘积的时间
T_S^{RSA}	执行一次 RSA 签名所需时间	l_S^{RSA}	RSA 签名长度
T_S^{Waters}	执行一次 Waters 签名所需时间	l_S^{Waters}	Waters 签名长度
T_S	执行一次签名所需时间	l_{tag}	CES-tag 长度
T_C	执行一承诺所需时间	l_n	消息的个数为 n
T_H	计算一次散列函数所需时间	l_{CEAS}	CEAS 编码长度
N	RSA 中模数因子	l_m	子消息长度, 假设每个子消息等长
T_{Prod}^{RSA}	一次求积模 N 所需时间	l_i	子消息编码长度
T_V^{RSA}	执行一次 RSAP 方案验证算法时间	l_H	散列值长度 $l_H = l_{tag} + l_{CEAS} + l_m + l_n + l_i$
T_V^{Waters}	执行一次 Waters 方案验证算法时间	l_C	承诺的长度
T_V	执行一次签名验证算法所需时间	$f(m, n)$	$\min\left(mlb\left(\frac{n}{m}\right), n-m\right)$

表 2

2 种方案算法复杂度纵向比较

方案	签名时间	截取时间	验证时间	签名长度	截取长度
RSAP	$n(T_H(l_H) + T_S^{RSA})$	T_{Prod}^{RSA}	$mT_H(l_H) + T_{Prod}^{RSA} + T_V^{RSA}$	$l_{tag} + l_{CEAS} + nl_S^{RSA}$	$l_{tag} + l_{CEAS} + l_S^{RSA}$
WCES	$n(T_H(l_H) + T_S^{Waters})$	T_{Ext}^{Waters}	$mT_H(l_H) + T_{Prod_H} + T_V^{Waters}$	$l_{tag} + l_{CEAS} + nl_S^{Waters}$	$l_{tag} + l_{CEAS} + ml_S^{Waters}$

表 3

3 种方案算法复杂度横向比较

方案	签名时间	截取时间	验证时间	签名长度	截取长度
WCES	$n(T_H(l_H) + T_S^{Waters})$	T_{Ext}^{Waters}	$mT_H(l_H) + T_{Prod_H} + T_V^{Waters}$	$l_{tag} + l_{CEAS} + nl_S^{Waters}$	$l_{tag} + l_{CEAS} + ml_S^{Waters}$
IRSAP	$n(T_H(l_H) + T_S^{RSA}) + T_{batch}$	T_{Prod}^{RSA}	$mT_H(l_H) + T_{Prod}^{RSA} + T_V^{RSA} + T_{batch}$	$l_{tag} + l_{CEAS} + nl_S^{RSA} + l_{batch}$	$l_{tag} + l_{CEAS} + l_S^{RSA} + l_{batch}$
HT	$T_S(l_H) + 3nT_C(l_m)$	$T_{Ext}^{HT} + 3nT_C(l_m)$	$T_V(l_H) + (2n+m)T_C(l_m)$	$l_S + l_r$	$l_S + ml_r + f(m, n)l_C$

法。根据批量签名的思想, 将 Waters 数字签名方案批量化, 进而改进为可截取签名。所构造的方案可视为 RSAP 方案的平行改进, 以较长的截取签名长度为代价节省整体的运算时间。通过与其他方案的横向对比说明了所构造方案的优点。并证明所构造方案在适应性选择消息攻击下具有不可伪造性和隐私性。

本文的构造是根据批量签名中批量验证的思想降低各个算法的时间复杂度, 但所需传递的签名长度有待进一步优化。文献[9]所提出的 MERP 方案应用批量签名中一次签名的优点缩短签名长度, 提高截取者与验证者的传递效率, 不足之处是失去快速验证的性质, 使验证效率略低。因此, 构造时间复杂度和空间复杂度同时较低的可截取签名是一个值得挑战的研究问题。

参考文献:

- [1] 中兴通讯学院. 对话多媒体通信[M]. 北京: 人民邮电出版社, 2010.
ZTE UNIVERSITY. Talk to multimedia communication[M]. Beijing: Posts and Telecom Press, 2010.
- [2] RIVEST R L, SHAMIR A, ADLEMAN L A. Method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.
- [3] GOLDWASSER S, MICALI S, RIVEST R L. A digital signature scheme secure against adaptive chosen-message attacks[J]. Siam Journal of Computing, 1988, 17(2): 281-308.
- [4] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[C]//Workshop on the Theory and Application of Cryptographic Techniques (Eurocrypt 1984). 1984: 10-18.
- [5] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Trans inf theory, 1984, 31(4): 469-472.
- [6] STANDARDS N I O. Digital signature standard (DSS)[J]. Federal Information Processing Standards Publication 186-2, 2000, 25.
- [7] BELLARE M, ROGAWAY P. The exact security of digital signatures-how to sign with RSA and rabin[C]//International Conference on Theory and Application of Cryptographic Techniques. 1996: 399-416.
- [8] SCHNORR C P. Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4(3): 161-174.
- [9] STEINFELD R, BULL L, ZHENG Y. Content extraction signatures[C]//The International Conference on Information Security and Cryptology (ICISC 2001). 2001: 285-304.
- [10] BULL L, SQUIRE D M G, ZHENG Y. A hierarchical extraction policy for content extraction signatures[J]. International Journal on Digital Libraries, 2004, 4(3): 208-222.
- [11] 蓝才会, 王彩芬. 基于身份的可截取签名方案[J]. 计算机应用, 2007, 27(10): 2456-2458.
- LAN C H, WANG C F. ID-based content extraction signature[J]. Journal of Computer Applications, 2007.
- [12] 曹素珍, 王彩芬. 基于离散对数问题的可截取签名方案[J]. 计算机工程, 2013, 39(4): 132-136.
- CAO S Z, WANG C F. Content extraction signature scheme based on DLP[J]. Computer Engineering, 2013, 39(4): 132-136.
- [13] 李旭, 杜小妮, 王彩芬, 等. 基于 RSA 的可截取签名改进方案[J]. 计算机工程与应用, 2014, 50(24): 96-99.
- XU L I, XIAONI D U, WANG C, et al. Improved scheme of content extraction signatures based on RSA[J]. Computer Engineering & Applications, 2014.
- [14] WANG C, LI Y, HUANG S Y, et al. A new forward secure content extraction signature scheme[C]//International Conference on Fuzzy Systems and Knowledge Discovery. 2016: 1698-1702.
- [15] 王彩芬, 徐婷, 张玉磊, 等. 基于可截取签名和属性加密的云存储访问控制方案[J]. 计算机工程与科学, 2015, 37(2): 238-244.
- WANG C F, TING X U, ZHANG Y L, et al. An access control scheme in cloud storage based on content extraction signature and attribute encryption[J]. Computer Engineering & Science, 2015.
- [16] 王敏, 马金花, 刘江华, 等. 两类可截取签名方案的改进[J]. 网络与信息安全学报, 2017, 3(4): 69-77.
- WANG M, MA J H, LIU J H, et al. The two improvements of the content extraction signature [J]. Chinese Journal of Network and Information Security, 2017, 3(4): 69-77.
- [17] FIAT A. Batch RSA[J]. Journal of Cryptology, 1997, 10(2): 75-88.
- [18] PAVLOVSKI C J, BOYD C. Efficient batch signature generation using tree structures[C]//International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC 1999). 1999: 70-77.
- [19] CATALANO D, FIORE D. Vector commitments and their applications[M]//Public-Key Cryptography-PKC 2013. Springer Berlin Heidelberg, 2013: 55-72.
- [20] WATERS B. Efficient identity-based encryption without random oracles[J]. Eurocrypt, 2005, 2004(2004): 114-127.
- [21] KATZ J. Digital signatures[M]. Springer US, 2010: 127-128.

[作者简介]



唐紫鑫 (1993-), 男, 湖南株洲人, 福建师范大学硕士生, 主要研究方向为密码学 and 信息安全。



黄欣沂 (1981-), 男, 江苏仪征人, 福建师范大学教授、博士生导师, 主要研究方向为密码学 and 信息安全。