

两类可截取签名方案的改进

王敏^{1,2}, 马金花^{1,2}, 刘江华^{1,2}, 伍玮^{1,2}

(1. 福建师范大学数学与计算机科学学院, 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: 结合批签名中统一签名的思想, 分别提出基于承诺方案和基于 RSA 这 2 类可截取签名的改进方案。改进方案中对部分消息进行统一处理, 提高了签名和验证效率。在随机预言模型下, 证明所提改进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; 批签名; 承诺方案; RSA; 随机预言模型

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00162

Two improved content extraction signature schemes

WANG Min^{1,2}, MA Jin-hua^{1,2}, LIU Jiang-hua^{1,2}, WU Wei^{1,2}

(1. School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007, China;
2. Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou 350007, China)

Abstract: Motivated by the idea of batch signatures, two variants of content extraction signature schemes based on commit vector and RSA respectively were presented. In the proposed schemes, the efficiency of signing and verification were improved by unifying certain message. The analysis show that the proposed schemes are existentially unforgeable under chosen message attacks in the random oracle model.

Key words: content extraction signature, batch signature, commit vector, RSA, random oracle model

1 引言

随着计算机和网络技术的迅速发展, 人类社会已经步入信息化时代。信息化让人的生活变得更加方便、快捷, 同时也带来了一系列信息安全隐患。数字签名^[1]是保障信息安全的基本技术之一, 解决了身份认证、数据完整性验证、不可抵赖等问题。在电子政务和电子商务系统化的今天, 数字签名技术应用极为广泛。普通数字签名的安全性要求具有访问签名预言机能力的适应性选择消息攻击者不能成功伪造一个新消息的有效

签名。虽然该安全要求能防止伪造数据, 却阻碍了签名持有人对已签名数据的合理操作。例如, 某学校给学生 Bob 签发一份(电子)大学毕业证, 该电子文档记录了 Bob 的姓名、年龄、家庭地址等详细信息, Bob 在求职时需要将这份电子文档作为申请材料的一部分发给应聘公司。为了保护个人隐私, Bob 希望在文档中隐藏家庭地址等敏感信息。如果学校用普通数字签名算法对毕业证进行签名, 那么该签名只能证实完整毕业证的有效性, 而无法证实删除敏感信息后文档的真实性。为了解决上述问题, Steinfeld 等^[2]最早提出了可

收稿日期: 2017-01-16; 修回日期: 2017-03-04。通信作者: 伍玮, 4787674@qq.com

基金项目: 国家自然科学基金资助项目(No.61402110, No.61472083); 福建师范大学校创新团队基金资助项目(No.IRTL1207)

Foundation Items: The National Natural Science Foundation of China (No.61402110, No.61472083), The Innovation Team of Fujian Normal University (No.IRTL1207)

截取签名 (CES, content extraction signatures) 的概念, 并给出了具体的实现方案。不同于传统的数字签名方案^[3-6], 在不与原始签名人交互的情况下, 可截取签名, 允许签名持有人根据需要从已签的原消息中截取出需要的消息段, 并为截取出的消息段计算有效签名, 证明截取出的消息段的真实性。鉴于这些优点, 国内外学者对可截取签名进行了大量深入研究。

文献[7]通过在 XML 签名规范中引入可截取签名功能, 实现了 XML 签名^[8]可截取的扩展。文献[9]在文献[2]的基础上, 提出采用分级群组策略的可截取签名方案。在该方案中, 作者设计了一种可有效应用于数字图书馆等环境中多级信息的内容截取访问结构。文献[10]结合文献[11], 提出了基于身份的可截取门限签名方案, 该方案能够实现签名的截取和门限恢复等功能。文献[12]首次提出了批签名的概念, 允许签名者实现消息的统一签名和验证, 可有效提高签名和验证效率, 但该方案限制了签名消息的数量。为了克服这个缺点, 文献[13]提出了基于二叉树的 Bi-tree 批签名方案, 该方案还可以将普通的签名算法转换成批签名。通过结合可截取签名和属性加密, 文献[14]提出一种细粒度的访问控制, 在数据加密的同时还能把符合属性的子消息发送给相应的用户, 对云存储中访问控制的问题进行细化, 提高了消息的利用率。此外, 文献[15]提出的可截取签名方案解决了截取后文档存在板式凌乱的问题, Wang 等^[16]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等。

文献[2]中提出的基于承诺方案的可截取签名方案实现了对消息的一次签名, 但签名中包括了所有子消息的承诺值及其对应的随机数, 导致签名较长。本文借鉴批签名^[12]中统一签名的思想, 对该方案进行改进, 在不改变原方案安全性和一次签名的基础上, 减少承诺值和随机数的数量, 缩短签名长度, 提高签名的通信效率。此外, 文献[2]中提出的基于 RSA 的可截取签名方案缩短了签名长度, 但签名者仍然需要对每个子消息进行签名, 导致方案的计算量较大。为了降低计算量, 本文结合批签名^[12]对该方案进行改进, 允许对部分消息进行统一签名和验证, 从而提高了

方案的效率。

2 可截取签名

本节介绍可截取签名的相关知识, 包括截取规则和相关符号的定义、可截取签名的定义和安全模型。

2.1 可截取签名的定义

由于普通数字签名不允许对消息进行任何修改, 为了让签名持有人能够获得已签名消息中部分消息的签名, 一种直接的方法是签名者 Alice 首先把消息划分为若干子消息, 然后对每个子消息进行签名, 并把所有子消息的签名发给 Bob。Bob 对消息进行截取, 保留需要的子消息, 并从得到的签名中挑选对应的子消息签名作为截取消息的签名。虽然验证者能够对这个签名进行验证, 但签名者不能对消息的截取进行控制, 容易导致消息的恶意截取。为了解决这些问题, 文献[2]在可截取签名中引入内容截取访问结构 CEAS, 使签名者能够通过 CEAS 控制消息 M 的截取, 从而阻止恶意截取。

$CEAS \subset \Gamma$ 定义为子消息编码的集合, 且规定签名持有人必须截取 CEAS 中对应的所有子消息, 并把 CEAS 中对应的所有消息称为必选消息, 如 $M = (m_1, m_2, m_3, m_4, m_5, m_6)$, $CEAS = \{2, 4, 6\}$ 。若 $CI(M') = \{1, 2, 4, 6\}$, 有 $M' = (m_1, m_2, *, m_4, *, m_6)$, 因此 $CEAS \subset CI(M')$ 表示截取方式是合法的; 若 $CI(M') = \{4, 6\}$, 有 $M' = (*, *, *, m_4, *, m_6)$, 因此 $CEAS \not\subset CI(M')$ 表示截取方式是非法的。假设用 $M = (m_1, m_2, \dots, m_n)$ 表示由 n 个子消息构成的消息, $M[i]$ 表示消息 M 中的第 i 个子消息, 用 Γ 表示所有子消息编码的集合, 即 $\Gamma = \{1, 2, \dots, n\}$ 。截取子集 $CI(M')$ 中存放需要截取的子消息编码。 M' 表示根据 $CI(M')$ 得到的截取消息, 即子消息的集合, 其中不需要截取的子消息用空白来标记, 用 * 表示空白子消息。

Steinfeld 等^[2]提出的可截取签名方案由 4 个多项式时间算法组成, 即 $CES = (GK, Sig, Ext, Ver)$, 具体如下。

密钥生成算法 GK: 输入安全参数 k , 输出公钥 pk 和私钥 sk 。

签名算法 Sig: 输入私钥 sk 、消息 M 和内容

截取访问结构 $CEAS$, 输出消息 M 的全局签名 σ_F 。

截取算法 Ext : 输入公钥 pk 、消息 M 、全局签名 σ_F 和截取子集 X , 输出截取签名 σ_E 。

验证算法 Ver : 输入公钥 pk 、截取后的消息 M' 、内容截取访问结构 $CEAS$ 和截取签名 σ_E , 若签名有效, 则输出 Acc , 否则输出 Rej 。

可截取签名的功能要求如下。

1) 可截取: 在不与原始签名者交互的情况下, 签名持有人可根据原消息中的一部分, 从给定的原消息签名中得到截取后消息的可公开验证签名。

2) 效率: 方案的通信开销或计算开销比简单的多次签名更高效。

2.2 可截取签名的安全模型

引理 1 如果没有攻击者, A 能够在概率多项式时间内, 在游戏 $Game1$ 中以不可忽略的概率获胜, 则称可截取签名方案在适应性选择消息攻击下具有 CES 不可伪造性。

挑战者 C 和攻击者 A 之间的游戏 $Game1$ 定义如下。

1) 挑战者 C 运行 GK 算法, 得到公私钥对 (pk, sk) , 并把公钥 pk 发给攻击者 A 。

2) 攻击者 A 可适应性地选择 k 个消息 $(CEAS_1, M_1), (CEAS_2, M_2), \dots, (CEAS_k, M_k)$, 向签名预言机询问, 询问 k 次后得到 k 个 CES 签名。

3) 攻击者 A 根据得到的 k 个 CES 签名, 计算消息 $(M^*, CEAS^*)$ 的 CES 签名 σ_E^* , A 把 σ_E^* 发给 C 。

4) 挑战者 C 运行 $Ver(pk, M^*, \sigma_E^*)$ 算法, 如果输出 Acc 且 $M^* \not\subset M_i (1 \leq i \leq k)$ 或 $CEAS^* \not\subset CI(M^*)$, 那么 A 获胜; 否则, A 失败。

引理 2 如果没有攻击者, A 能够在概率多项式时间内, 在游戏 $Game2$ 中以不可忽略的优势 Adv_A 获胜, 则称可截取签名方案在适应性选择消息攻击下具有 CES 隐私性。

挑战者 C 和攻击者 $A = (A_{find}, A_{guess})$ 之间的游戏 $Game2$ 定义如下。

1) 挑战者 C 运行 $GK(k)$ 算法, 得到公私钥对 (pk, sk) , 并把 (pk, sk) 发给攻击者 A 。

2) 攻击者 A 运行 $A_{find}(k, sk)$ 算法, 得到 $(s, M, M_0, M_1, i^*, CEAS^*, X^*)$, 其中, 消息 M_0 和 M_1 除

了 i^* 位置上对应的子消息不同外, 其他完全相同, 即对 $i \neq i^*$ 满足 $M[i] = M_0[i] = M_1[i]$ 。

3) 挑战者 C 随机选择一个比特 $b \in \{0, 1\}$, 同时设 $M^* = M_b$, 依次运行签名算法 $Sig(sk, M^*, CEAS^*)$ 和截取算法 $Ext(pk, M^*, \sigma_F^*, X^*)$ 分别得到 σ_F^* 和 σ_E^* , C 把 σ_E^* 发给 A 。

4) 攻击者 A 运行 $A_{guess}(s, \sigma_E^*)$ 算法, 输出 $b' \in \{0, 1\}$ 。如果 $b' = b$ 并且 $i^* \notin X^*$, 那么 A 获胜; 否则, A 失败。

定义 A 在游戏中的优势 $Adv_A = |p - \frac{1}{2}|$, 其中 p 表示 A 在游戏中获胜的概率。

3 基于承诺方案的可截取签名的改进方案

本节介绍所提基于承诺的可截取签名改进方案的基本定义, 包括方案具体步骤的描述、正确性分析、安全性分析以及效率分析。

3.1 方案描述

该方案是在 Steinfeld 等^[2]提出的基于承诺方案的可截取签名的基础上, 结合批签名的思想, 统一计算部分消息的承诺值, 从而提高了方案的效率。方案具体步骤描述如下。

1) 密钥生成算法 GK

① 输入安全参数 k , 承诺方案的密钥生成算法输出签名的公私钥对 (sk_s, pk_s) , 承诺方案的初始化算法输出方案参数字符串 sp 。

② 返回私钥 $sk = sk_s$ 和公钥 $pk = (pk_s, sp)$ 。

2) 签名算法 Sig

签名者给出截取规则 $CEAS$, 对长度为 n 的消息 M 的签名如下。

① 对必选子消息 $i \in CEAS$, 计算必选承诺值 $c_{CEAS} = C(\langle M[i] \rangle_{i \in CEAS}; r_{CEAS})$; 对非必选子消息 $i \in \Gamma \setminus CEAS$, 计算 $c[i] = C(M[i]; r[i])$ 。

② 对所有承诺值的串联签名 $\sigma_c = S(sk_s, (CEAS, c_{CEAS} \parallel \langle c[i] \rangle_{i \in \Gamma \setminus CEAS}))$ 。

③ 返回全局签名 $\sigma_F = (CEAS, \sigma_c, r_{CEAS} \parallel \langle r[i] \rangle_{i \in \Gamma \setminus CEAS})$ 。

3) 截取算法 Ext

① 截取者根据消息 M 和截取规则 $CEAS$, 给出截取子集 $CI(M')$, 假设 $X = CI(M')$ 。

② 根据截取子集 $CI(M')$, 得到截取消息 $M' = \{M[i] | i \in CI(M')\}$ 。

③ 对未截取的子消息 $i \in \Gamma \setminus X$ ，计算 $c[i] = C(M[i]; r[i])$ 。

④ 返回截取签名 $\sigma_E = (CEAS, \sigma_c, r_{CEAS} \parallel \langle r[i] \rangle_{i \in X \setminus CEAS}, \langle c[i] \rangle_{i \in \Gamma \setminus X})$

4) 验证算法 Ver

① 验证者收到截取签名 σ_E 、截取消息 M' ，假设 $X' = CI(M')$ 。

② 验证 $CEAS \subset CI(M')$ 是否成立，若不成立，返回验证失败。

③ 对必选子消息 $i \in CEAS$ ，计算必选消息散列值 $c_{CEAS} = C(\langle M'[i] \rangle_{i \in CEAS}; r_{CEAS})$ 。对非必选的截取子消息 $i \in X' \setminus CEAS$ ，计算 $c[i] = C(M'[i]; r[i])$ 。

④ 执行 $d_s = V(pk_s, (CEAS, c_{CEAS} \parallel \langle c[i] \rangle_{i \in \Gamma \setminus CEAS}, \sigma_c))$ ，若 $d_s = Acc$ ，返回验证成功；否则，返回验证失败。

3.2 方案的正确性分析

该方案的正确性包括以下2个部分。

1) 截取者对全局签名 σ_F 的正确性验证。

① 对必选子消息 $i \in CEAS$ ，计算必选承诺值 $c_{CEAS} = C(\langle M[i] \rangle_{i \in CEAS}; r_{CEAS})$ ；对非必选子消息 $i \in \Gamma \setminus CEAS$ ，计算 $c[i] = C(M[i]; r[i])$ 。

② 计算 $d_s = V(pk_s, (CEAS, c_{CEAS} \parallel \langle c[i] \rangle_{i \in \Gamma \setminus CEAS}, \sigma_c))$ ，得到 d_s 的值。

2) 验证者对截取签名 σ_E 的正确性验证。

① 验证 $CEAS \subset CI(M')$ 是否成立，若成立，则继续下面的步骤；否则返回失败。

② 对必选子消息 $i \in CEAS$ ，计算必选消息散列值 $c_{CEAS} = C(\langle M'[i] \rangle_{i \in CEAS}; r_{CEAS})$ 。对非必选的截取子消息 $i \in X' \setminus CEAS$ ，计算 $c[i] = C(M'[i]; r[i])$ 。

③ 计算 $d_s = V(pk_s, (CEAS, c_{CEAS} \parallel \langle c[i] \rangle_{i \in \Gamma \setminus CEAS}, \sigma_c))$ ，得到 d_s 的值。

3.3 方案的安全性分析

定理 1 如果标准数字签名 DS 在适应性选择消息攻击下满足不可伪造性，且承诺方案 CM 满足弱捆绑性，则本文提出的可截取签名改进方案满足 CES 不可伪造性。

证明 原命题的逆否命题可等价于：如果存在一个攻击者 A_{CES} 能够在概率多项式时间内，以不可忽略的概率在 $Game1$ 中获胜；那么也存在另外一个攻击者 A_{sig} （或 A_{com} ）可以利用 A_{CES} 在概率多项式时间内，以不可忽略的概率成功攻破标准数字签名的不可伪造性（或承诺方案

的弱捆绑性）。

1) 攻击者 A_{sig} 的攻击过程定义。

攻击目标：攻击者 A_{sig} 能够根据 A_{CES} 伪造出的 CES 签名对 (M^*, σ^*) ，得到给定公钥 pk_s 下有效的 DS 签名对 $(M^*, \bar{\sigma}^*)$ 。

准备阶段：攻击者 A_{sig} 首先得到承诺方案 CM 的承诺参数 sp ，设 $pk = (pk_s, sp)$ 。 A_{sig} 调用攻击者 A_{CES} ，并把 (k, pk) 作为 A_{CES} 的输入。

询问阶段：攻击者 A_{CES} 可适应性选择 k 个消息 $(CEAS_1, M_1), (CEAS_2, M_2), \dots, (CEAS_k, M_k)$ 向预言机询问。例如询问第 j ($1 \leq j \leq k$) 个消息 $(CEAS_j, M_j)$ 的 CES 签名， A_{sig} 通过模拟签名算法来回答 A_{CES} ，假设 $n_j = \text{len}(M_j)$ 表示 M_j 中子消息的数目。首先， A_{sig} 计算 M_j 中所有子消息的承诺值，即

$$\begin{cases} c_{CEAS_j} = C(\langle M_j[i] \rangle_{i \in CEAS_j}; r_{CEAS_j}), i \in CEAS_j \\ c_j[i] = C(M_j[i]; r_j[i]), i \in [n_j] \setminus CEAS_j \end{cases}$$

然后，攻击者 A_{sig} 向签名预言机询问消息 $(CEAS_j, c_{CEAS_j} \parallel \langle c_j[i] \rangle_{i \in [n_j] \setminus CEAS_j})$ 的 DS 签名 $\bar{\sigma}_j$ ，最后，攻击者 A_{sig} 返回 $(CEAS_j, M_j)$ 的 CES 签名 $\sigma_j = (CEAS_j, \bar{\sigma}_j, r_{CEAS_j} \parallel \langle r_j[i] \rangle_{i \in [n_j] \setminus CEAS_j})$ 给 A_{CES} 。

攻击阶段：询问结束后， A_{CES} 得到伪造的 CES 签名对 (M^*, σ^*) 。假设 $n^* = \text{len}(M^*)$ ， $X^* = CI(M^*)$ ，则 $\sigma^* = (CEAS^*, \bar{\sigma}^*, r_{CEAS^*} \parallel \langle r^*[i] \rangle_{i \in [n^*] \setminus CEAS^*}, \langle c^*[i] \rangle_{i \in [n^*] \setminus X^*})$ ， A_{sig} 对得到的 CES 签名对 (M^*, σ^*) 进行验证。 A_{sig} 计算消息 M^* 中所有子消息的承诺值，即

$$\begin{cases} c_{CEAS^*} = C(\langle M^*[i] \rangle_{i \in CEAS^*}; r_{CEAS^*}), i \in CEAS^* \\ c^*[i] = C(M^*[i]; r^*[i]), i \in [X^*] \setminus CEAS^* \\ c^*[i] = c^*[i], i \in [n^*] \setminus X^* \end{cases}$$

串联所有承诺值得到 $c^* = c_{CEAS^*} \parallel \langle c^*[i] \rangle_{i \in [n^*] \setminus CEAS^*}$ 。如果 $V(pk, M^*, \sigma^*) = Acc$ （其中 $M^* = (CEAS^*, c^*)$ ），则 A_{CES} 成功伪造了 CES 签名对 (M^*, σ^*) ，即 A_{sig} 成功伪造 DS 签名对 $(M^*, \bar{\sigma}^*)$ 。至此， A_{sig} 构造完毕。

2) 攻击者 $A_{com} = (A_1, A_2)$ 的攻击过程定义。

攻击目标：攻击者 A_{com} 能够根据 A_{CES} 伪造出的有效 CES 签名对 (M^*, σ^*) ，找到承诺碰撞对 $(M^*[\alpha], r^*[\alpha])$ 和 $(M_\beta[\alpha], r_\beta[\alpha])$ ，满足 $C(M^*[\alpha]; r^*[\alpha]) = C(M_\beta[\alpha]; r_\beta[\alpha])$ 且 $M^*[\alpha] \neq M_\beta[\alpha]$ 。

准备阶段： A_1 首先得到承诺方案 CM 的承诺参数 sp ，设 $pk = (pk_s, sp)$ 。 A_1 随机选取编码对 $(\beta, \alpha) \in [k] \times [n]$ ，其中 k 是向预言机询问的次数， n 是子消息的数目。 A_1 调用攻击者 A_{CES} ，并把 (k, pk) 作为 A_{CES} 的输入。

询问阶段：攻击者 A_{CES} 可适应性选择 k 个消息 $(CEAS_1, M_1), (CEAS_2, M_2), \dots, (CEAS_k, M_k)$ 向预言机询问。例如，询问第 j ($1 \leq j \leq k$) 个消息 $(CEAS_j, M_j)$ 的 CES 签名， A_1 通过模拟签名算法来回答 A_{CES} 。当 $j = \beta$ ， A_1 首先输出 $(s, M_\beta[\alpha])$ ；然后随机选取 $\bar{r}$ ，计算 $\bar{c} = (M_\beta[\alpha]; \bar{r})$ 。最后调用 A_2 ，并将 $(s, \bar{c}, \bar{r})$ 作为 A_2 的输入， A_2 令 $r_\beta[\alpha] = \bar{r}$ ， $c_\beta[\alpha] = \bar{c}$ ， A_{CES} 的第 β 次签名询问结束。 A_{CES} 的其他的签名询问同 A_{sig} 。

攻击阶段：询问结束后， A_{CES} 得到伪造的 CES 签名对 (M^*, σ^*) 。因此 A_2 也能成功找到 $(M_\beta[\alpha], r_\beta[\alpha])$ 的承诺碰撞对 $(M^*[\alpha], r^*[\alpha])$ 满足 $C(M^*[\alpha]; r^*[\alpha]) = c_\beta[\alpha] = C(M_\beta[\alpha]; r_\beta[\alpha])$ 且 $M^*[\alpha] \neq M_\beta[\alpha]$ 。至此， A_{com} 构造完毕。

综上所述，攻击者 A_{sig} 或 A_{com} 可以利用 A_{CES} 在概率多项式时间内，以不可忽略的概率成功伪造目标，即证明原命题成立。

3.4 效率分析

本节对 2 种方案的复杂度进行分析，用 CV 表示 Steinfeld 等^[2]提出的基于承诺方案的可截取签名方案，用 ACV 表示本文提出的改进方案，符号说明如表 1 所示。

表 1	符号说明
符号	符号说明
n	原消息中子消息的数目
m	截取消息中子消息的数目
m_{CEAS}	必选子消息的数目
T_C	计算一次承诺值所需时间
T_S^{CV}	执行一次签名所需时间
T_V^{CV}	执行一次验证所需时间
l_c	承诺值长度
l_r	承诺值对应随机字符串的长度
l_s^{CV}	签名长度
l_T	$CES - Tags$ 长度
l_m	子消息长度（假设每个子消息等长）
l_{CEAS}	$CEAS$ 编码长度
l_{seq}	子消息编码 i 长度

1) 2 种方案的时间复杂度分析。

①签名时间：消息 M 签名时，CV 方案需要分别计算每个子消息的承诺值（即 $c[i] = C(M[i]; r[i])$ ， $i \in \Gamma$ ），并对所有承诺值的串联进行签名（即 $\sigma_c = S(sk_s, (CEAS, \langle c[i] \rangle_{i \in \Gamma}))$ ），因此 CV 方案的签名时间为 $nT_C(l_m) + T_S^{CV}(l_{CEAS} + nl_c)$ ；而 ACV 方案统一计算必选消息的承诺值，签名时间为 $(n - m_{CEAS} + 1)T_C(l_m) + T_S^{CV}(l_{CEAS} + (n - m_{CEAS} + 1)l_c)$ 。

②截取时间：2 种方案都需要计算未截取部分子消息的承诺值（即 $c[i] = C(M[i]; r[i])$ ， $i \in \Gamma \setminus X$ ），截取时间均为 $(n - m)T_C(l_m)$ 。

③验证时间：CV 方案需要分别计算每个截取子消息的承诺值（即 $c[i] = C(M[i]; r[i])$ ， $i \in X$ ），验证时间为 $mT_C(l_m) + T_V^{CV}(l_{CEAS} + nl_c)$ ；而 ACV 方案统一计算必选消息的承诺值，验证时间为 $(m - m_{CEAS} + 1)T_C(l_m) + T_V^{CV}(l_{CEAS} + (n - m_{CEAS} + 1)l_c)$ 。

2) 2 种方案的空间复杂度分析。

①签名长度：CV 方案签名者生成的签名 $\sigma_F = (CEAS, \sigma_c, \langle r[i] \rangle_{i \in \Gamma})$ 的长度包括 $CEAS$ 编码长度、承诺值的签名长度 l_s 和 n 个消息段随机数的长度 nl_r ，因此签名长度为 $l_{CEAS} + l_s + nl_r$ ；ACV 方案中减少了 $m_{CEAS} - 1$ 个随机数，故签名长度为 $l_{CEAS} + l_s + (n - m_{CEAS} + 1)l_r$ 。

②截取签名长度：CV 方案中截取签名 $\sigma_E = (CEAS, \sigma_c, \langle r[i] \rangle_{i \in X}, \langle c[i] \rangle_{i \in \Gamma \setminus X})$ 的长度包括了 $CEAS$ 编码长度、承诺值的签名长度 l_s 、 m 个消息段随机数的长度 ml_r 和 $n - m$ 个承诺值的长度 $(n - m)l_r$ ，因此签名长度为 $l_{CEAS} + l_s + ml_r + (n - m)l_c$ ；ACV 方案中减少了 $m_{CEAS} - 1$ 个随机数，故签名长度为 $l_{CEAS} + l_s + (m - m_{CEAS} + 1)l_r + (n - m)l_c$ 。

根据上面的分析，2 种方案的时间和空间复杂度的比较如表 2 所示。

从表 2 可以看出，改进方案中把消息 M 分成必选子消息 $\{M[i] | i \in CEAS\}$ 和非必选子消息 $\{M[i] | i \in \Gamma \setminus CEAS\}$ 这 2 个部分分别处理，统一计算 m_{CEAS} 个必选子消息的承诺值，减少了 $m_{CEAS} - 1$ 个承诺值。随着必选子消息数目 m_{CEAS} 的增加，承诺值和随机数的数目也逐渐减少。因此，在不改变原方案一次签名和安全性的基础上，减少承诺值和随机数的数量，缩短签名长度，提高了签名的通信效率。

表 2

2 种方案复杂度比较

方案	时间复杂度			空间复杂度	
	签名时间	截取时间	验证时间	签名长度	截取长度
CV	$nT_C(l_m) + T_S^{CV}(l_{CEAS} + nl_C)$	$(n-m)T_C(l_m)$	$mT_C(l_m) + T_V^{CV}(l_{CEAS} + nl_C)$	$l_{CEAS} + l_s + nl_r$	$l_{CEAS} + l_s + ml_r + (n-m)l_C$
ACV	$(n-m_{CEAS}+1)T_C(l_m) + T_S^{CV}(l_{CEAS} + (n-m_{CEAS}+1)l_C)$	$(n-m)T_C(l_m)$	$(m-m_{CEAS}+1)T_C(l_m) + T_V^{CV}(l_{CEAS} + (n-m_{CEAS}+1)l_C)$	$l_{CEAS} + l_s + (n-m_{CEAS}+1)l_r$	$l_{CEAS} + l_s + (m-m_{CEAS}+1)l_r + (n-m)l_C$

4 基于 RSA 可截取签名的改进方案

本节介绍所提基于 RSA 可截取签名改进方案的基本定义, 包括方案具体步骤的描述、正确性分析、安全性分析以及效率分析。

4.1 方案描述

该方案是在 Steinfeld 等^[2]提出的基于 RSA 可截取签名方案的基础上, 结合批签名^[12]中统一签名的思想, 对部分消息进行统一签名和验证。方案具体步骤描述如下。

1) 密钥生成算法 GK

①随机选取 2 个长度为 $\frac{k}{2}$ 的大素数 p 和 q ,

并计算 $N = pq$, $\phi = (p-1)(q-1)$ 。

②随机选取整数 e 满足 $\gcd(e, \phi) = 1$, 计算 $d = e^{-1} \bmod \phi$ 。

③返回私钥 $sk = (N, e, d)$ 和公钥 $pk = (N, e)$ 。

2) 签名算法 Sig

对长度为 n 的消息 M 的签名如下。

① 签名者给出截取规则 $CEAS$, 同时随机产生一个固定长度的 $CEAS$ 标记 T 。

② 对必选子消息 $i \in CEAS$, 计算必选消息散列值 $h_{CEAS} = H(CEAS, T, n, \langle i \parallel M[i] \rangle_{i \in CEAS})$ 和必选消息签名 $\sigma_{CEAS} = h_{CEAS}^d$; 对非必选子消息 $i \in \Gamma \setminus CEAS$, 分别计算 $h[i] = H(CEAS, T, n, i \parallel M[i])$ 和子消息签名 $\sigma[i] = h[i]^d$ 。

③ 返回全局签名 $\sigma_F = (CEAS, T, \sigma_{CEAS} \parallel \langle \sigma[i] \rangle_{i \in \Gamma \setminus CEAS})$ 。

3) 截取算法 Ext

①根据消息 M 和截取规则 $CEAS$, 截取者给出截取子集 $CI(M')$, 假设 $X = CI(M')$ 。

②根据截取子集 $CI(M')$, 得到截取消息 $M' = \{M[i] | i \in CI(M')\}$ 。

③对非必选的截取子消息 $i \in X \setminus CEAS$, 计

算 $\sigma = \sigma_{CEAS} \prod_{i \in X \setminus CEAS} \sigma[i] \pmod{N}$ 。

④返回截取签名 $\sigma_E = (CEAS, T, \sigma)$ 。

4) 验证算法 Ver

①验证者收到截取签名 σ_E 、截取子集 $CI(M')$, 假设 $X' = CI(M')$ 。

②验证 $CEAS \subset CI(M')$ 是否成立, 若不成立, 返回验证失败。

③对必选子消息 $i \in CEAS$, 计算必选消息散列值 $h_{CEAS} = H(CEAS, T, n, \langle i \parallel M'[i] \rangle_{i \in CEAS})$; 对非必选的截取子消息 $i \in X' \setminus CEAS$, 计算 $h[i] = H(CEAS, T, n, i \parallel M'[i])$ 。

④验证 $\sigma^e = h_{CEAS} \prod_{i \in X' \setminus CEAS} h[i] \pmod{N}$ 是否成立, 若不成立, 返回验证失败; 否则, 返回验证成功。

4.2 方案正确性分析

1) 验证时首先计算截取消息 $M' = \{M[i] | i \in CI(M')\}$ 中子消息的散列值。

①必选消息的散列值为

$$h_{CEAS} = H(CEAS, T, n, \langle i \parallel M'[i] \rangle_{i \in CEAS}) \pmod{N}$$

②非必选截取消息的散列值为

$$\prod_{i \in CI(M') \setminus CEAS} h[i] \pmod{N} = \prod_{i \in CI(M') \setminus CEAS} H(CEAS, T, n, \langle i \parallel M'[i] \rangle_{i \in CEAS}) \pmod{N}$$

2) 验证收到的截取消息的签名, 步骤如下。

$$\begin{aligned} \sigma^e &= (\sigma_{CEAS} \prod_{i \in CI(M') \setminus CEAS} \sigma[i])^e \pmod{N} \\ &= \sigma_{CEAS}^e \left(\prod_{i \in CI(M') \setminus CEAS} \sigma[i]^e \pmod{N} \right) \\ &= \{ [H(CEAS, T, n, \langle i \parallel M'[i] \rangle_{i \in CEAS})]^d \}^e \\ &\quad \{ [\prod_{i \in CI(M') \setminus CEAS} H(CEAS, T, n, M'[i])^d]^e \pmod{N} \} \\ &= H(CEAS, T, n, \langle i \parallel M'[i] \rangle_{i \in CEAS}) \\ &\quad \prod_{i \in CI(M') \setminus CEAS} H(CEAS, T, n, M'[i]) \pmod{N} \end{aligned}$$

$$\begin{aligned}
&= H(CEAS, T, n, \langle i \parallel M'[i] \rangle_{i \in CEAS}) \\
&\quad \prod_{i \in CI(M') \setminus CEAS} H(CEAS, T, n, M'[i])(\text{mod } N) \\
&= h_{CEAS} \prod_{i \in CI(M') \setminus CEAS} h[i](\text{mod } N)
\end{aligned}$$

因此有 $\sigma^e \equiv h_{CEAS} \prod_{i \in CI(M') \setminus CEAS} h[i](\text{mod } N)$ 。

4.3 方案安全性分析

在随机预言机模型下，本文所提方案能够抵抗适应性选择消息攻击和身份伪造攻击，可以更深入地得到如下结果。

1) 如果 RSA 签名的全域 Hash 函数在适应性选择消息攻击下具有不可伪造性，并且 $CES - Tags$ 在签名算法中没有二次使用，那么本文提出的基于 RSA 可截取签名的改进方案具有 CES 不可伪造性。

2) 在本文提出的改进方案中，截取部分和未截取部分的签名相互独立，因此给出的改进方案具有 CES 隐私性。

3) 在可截取签名方案中，截取者的截取方式主要有以下 4 种情况。

① 截取者进行消息 M 的截取没有遵循 $CEAS$ 截取规则，即截取者可能故意截掉 $CEAS$ 中某个（或多个）标记为必选的子消息后得到 M'_1 ，验证者在验证签名前首先验证截取子集不满足截取规则，即 $CEAS \not\subset CI(M'_1)$ ，因此不能通过验证。

② 截取者按 $CEAS$ 截取规则对消息 M 进行截取得到 M'_2 ，并且截取后的消息不做任何修改，则 $CEAS \subset CI(M'_2)$ 且验证签名时有

$$\begin{aligned}
\sigma^e &= (\sigma_{CEAS} \prod_{i \in CI(M'_2) \setminus CEAS} \sigma[i])^e (\text{mod } N) \\
&= H(CEAS, T, n, \langle i \parallel M[i] \rangle_{i \in CEAS}) \\
&\quad \prod_{i \in CI(M'_2) \setminus CEAS} H(CEAS, T, n, M[i])(\text{mod } N) \\
&= H(CEAS, T, n, \langle i \parallel M'[i] \rangle_{i \in CEAS}) \\
&\quad \prod_{i \in CI(M'_2) \setminus CEAS} H(CEAS, T, n, M'[i])(\text{mod } N) \\
&= h_{CEAS} \prod_{i \in CI(M'_2) \setminus CEAS} h[i](\text{mod } N)(\text{mod } N)
\end{aligned}$$

即 $\sigma^e \equiv h_{CEAS} \prod_{i \in CI(M') \setminus CEAS} h[i](\text{mod } N)$ ，因此可以通过验证。

③ 截取者按 $CEAS$ 截取规则对消息 M 进行截取得到 M'_3 ，并把 M'_3 中的某些子消息 $M[i]$ 替换成 $M''[i]$ ，得到 M''_3 ，虽然满足 $CEAS \subset CI(M'_1)$ ，但是验证签名时有

$$\begin{aligned}
\sigma^e &= (\sigma_{CEAS} \prod_{i \in CI(M'_3) \setminus CEAS} \sigma[i])^e (\text{mod } N) \\
&= H(CEAS, T, n, \langle i \parallel M[i] \rangle_{i \in CEAS}) \\
&\quad \prod_{i \in CI(M'_3) \setminus CEAS} H(CEAS, T, n, M[i])(\text{mod } N) \\
&\neq H(CEAS, T, n, \langle i \parallel M''[i] \rangle_{i \in CEAS}) \\
&\quad \prod_{i \in CI(M'_3) \setminus CEAS} H(CEAS, T, n, M''[i])(\text{mod } N) \\
&= h_{CEAS} \prod_{i \in CI(M'_3) \setminus CEAS} h[i](\text{mod } N)
\end{aligned}$$

即 $\sigma^e \neq h_{CEAS} \prod_{i \in CI(M'_3) \setminus CEAS} h[i](\text{mod } N)$ ，因此不能通过验证。

④ 截取者按 $CEAS$ 截取规则对消息 M 进行截取得到 M'_4 ，并在 M'_4 后面添加 j 条消息得到 M''_4 ，虽然满足 $CEAS \subset CI(M'_1)$ ，但是验证签名时有

$$\begin{aligned}
\sigma^e &= (\sigma_{CEAS} \prod_{i \in CI(M'_4) \setminus CEAS} \sigma[i])^e (\text{mod } N) \\
&= H(CEAS, T, n, \langle i \parallel M[i] \rangle_{i \in CEAS}) \\
&\quad \prod_{i \in CI(M'_4) \setminus CEAS} H(CEAS, T, n, M[i])(\text{mod } N) \\
&\neq H(CEAS, T, n, \langle i \parallel M'[i] \rangle_{i \in CEAS}) \\
&\quad \prod_{i \in [n] \setminus CEAS} H(CEAS, T, n, M'[i]) \\
&\quad \prod_{i=n+1}^{n+j} H(CEAS, T, n, M''[i])(\text{mod } N) \\
&= h_{CEAS} \prod_{i \in [n] \setminus CEAS} h[i] \prod_{i=n+1}^{n+j} h[i](\text{mod } N)
\end{aligned}$$

即 $\sigma^e \neq h_{CEAS} \prod_{i \in [n] \setminus CEAS} h[i] \prod_{i=n+1}^{n+j} h[i](\text{mod } N)$ ，因此不能通过验证。

综上所述，本文方案在上述 4 种情况下都是安全的。

4.4 效率分析

本节对 2 种方案的复杂度进行比较，其中用 RSAP 表示 Steinfeld 等^[2]提出的基于 RSA 可截取签名方案，用 ARSAP 表示本文提出的改进方案，符号说明如表 3 所示。

表3 符号说明

符号	符号说明
n	原消息中子消息的数目
m	截取消息中子消息的数目
m_{CEAS}	必选子消息的数目
T_S^{RSA}	执行一次签名所需时间
T_V^{RSA}	执行一次验证所需时间
T_{HA}	计算一次散列函数所需时间
N	RSA 中模数因子
T_{MULT}^{RSA}	一次模 N 求积所需时间
l_S^{RSA}	签名长度
l_T	$CES-Tags$ 长度
l_H	散列函数长度
l_{CEAS}	$CEAS$ 编码长度
l_m	子消息长度, 假设每个子消息等长
l_{seq}	子消息编码 i 长度
l_R	散列消息长度 $l_R = l_m + l_{CEAS} + l_T + l_{seq}$

从表4可以看出, 由于结合批签名中统一签名的思想, 改进方案把消息 M 分成必选子消息 $\{M[i] | i \in CEAS\}$ 和非必选子消息 $\{M[i] | i \in \Gamma \setminus CEAS\}$ 这2部分, 允许对 m_{CEAS} 个必选子消息进行统一签名和验证, 减少了 $m_{CEAS} - 1$ 次签名和验证, 因而降低了计算量, 并且提高了方案效率。

5 结束语

不同于传统的数字签名方案, 在不与原始签名人交互的情况下, 可截取签名允许签名持有人根据需要, 针对原消息的一部分, 计算可公开验证的签名, 解决了信息传递时遇到的多次交互等问题, 在电子政务和电子商务中有极为广泛的应用。本文结合批签名^[12]中对签名文档统一签名的思想, 对文献[2]中的两类可截取签名方案进行了改进。改进后的方案实现了对部分子消息的统一签名和验证, 在不改变原方案安全性的基础上,

减少了计算量和通信开销, 提高了方案的效率。

参考文献:

- [1] 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.
- [2] STEINFELD R, BULL L, ZHENG Y. Content extraction signatures[C]//The International Conference on Information Security and Cryptology (ICISC 2001). 2001: 285-304.
- [3] 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.
- [4] SCHNORR C P. Efficient identification and signatures for smart cards[C]//Workshop on the Theory and Application of Cryptographic Techniques (Eurocrypt 1989). 1989: 239-252.
- [5] BONEH D. Digital signature standard[M]//Encyclopedia of Cryptography and Security. Berlin: Springer. 2011: 347-347.
- [6] LI J, ZHANG F, CHEN X, et al. Generic security-amplifying methods of ordinary digital signatures[J]. Information Sciences, 2012, 2011(9): 128-139.
- [7] BULL L, STANSKI P, SQUIRE D M G. Content extraction signatures using XML digital signatures and custom transforms on-demand[C]//The 12th International Conference on World Wide Web (WWW 2003). 2003: 170-177.
- [8] BARTEL M, BOYER J, FOX B, et al. XML-signature syntax and processing[J]. W3C Recommendation, 2002, (12).
- [9] 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.
- [10] 刘军龙, 王彩芬. 基于身份的可截取门限签名方案[J]. 计算机应用, 2006, 26(8): 1817-1820.
- [11] LIU J, WANG C F. ID-based CES threshold signature[J]. Computer Engineering and Applications, 2006, 26(8): 1817-1820.
- [12] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Workshop on the Theory and Application of Cryptographic Techniques (Eurocrypt 1984). 1984: 47-53.
- [13] FIAT A. Batch rsa[J]. Journal of Cryptology, 1997, 10(2): 75-88.
- [13] PAVLOVSKI C, BOYD C. Efficient batch signature generation using tree structures[C]//The International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC 1999). 1999: 70-77.

表4 2种方案复杂度比较

方案	时间复杂度			空间复杂度	
	签名时间	截取时间	验证时间	签名长度	截取长度
RSAP	$n(T_{HA}(l_R) + T_S^{RSA})$	mT_{MULT}^{RSA}	$m(T_{HA}(l_R) + T_{MULT}^{RSA}) + T_V^{RSA}$	$l_{CEAS} + l_T + nl_S^{RSA}$	$l_{CEAS} + l_T + l_S^{RSA}$
ARSAP	$(n - m_{CEAS} + 1) \cdot (T_{HA}(l_R) + T_S^{RSA})$	$(m - m_{CEAS} + 1)T_{MULT}^{RSA}$	$(m - m_{CEAS} + 1)(T_{HA}(l_R) + T_{MULT}^{RSA}) + T_V^{RSA}$	$l_{CEAS} + l_T + (n - m_{CEAS} + 1)l_S^{RSA}$	$l_{CEAS} + l_T + l_S^{RSA}$

- [14] 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, XU T, ZHANG Y L, et al. An access control scheme in cloud storage based on content extraction signature and attribute encryption[J]. Computer Engineering and Science, 2015, 37(2): 238-244.

- [15] 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.

LI X, DU X N, WANG C F, et al. Improved scheme of content extraction signatures based on RSA[J]. Computer Engineering and Applications, 2014, 50 (24): 96-99.

- [16] WANG C, LI Y, HUANG S Y, et al. A new forward secure content extraction signature scheme[C]//The International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2015). 2015: 1698-1702.



马金花 (1990-), 女, 江苏徐州人, 福建师范大学博士生, 主要研究方向为密码学和信息安全。



刘江华 (1988-), 男, 山西朔州人, 福建师范大学博士生, 主要研究方向为密码学和信息安全。

作者简介:



王敏 (1991-), 女, 福建漳州人, 福建师范大学硕士生, 主要研究方向为密码学和信息安全。



伍玮 (1981-), 女, 江苏南京人, 博士, 福建师范大学副教授、硕士生导师, 主要研究方向为公钥密码。