

一种基于环签名和短签名的可净化签名方案

张君何 周清雷 韩英杰

郑州大学信息工程学院 郑州 450000

(iezhangjunhe@163.com)

摘要 在现有的能够达到完全保密性要求的可净化数字签名方案中,基于群签名的方案因为效率较低而不够实用,而基于零知识证明的方案虽然效率较高但安全性较低。因此,文中提出了一种基于环签名和短签名的可净化数字签名方案,可满足可净化数字签名的不可伪造性、不可变形、透明性、完全保密性及可审计性 5 项基本安全需求,同时具有相对于基于零知识证明方案更强的可审计性和较高运算效率,具有较强的实用性。

关键词: 可净化数字签名;可审计性;数字签名;可转换环签名;短签名

中图法分类号 TP309;TP311.13

Sanitizable Signature Scheme Based on Ring Signature and Short Signature

ZHANG Jun-he, ZHOU Qing-lei and HAN Ying-jie

School of Information Engineering, Zhengzhou University, Zhengzhou 450000, China

Abstract Among the existing sanitizable signature schemes that achieve full security requirements, schemes based on group signatures are not practical due to their low efficiency, while those based on zero-knowledge proof are more efficient, but the security is poor. Therefore, this paper proposes a new sanitizable signature scheme based on ring signature and short signature. It can meet the five fundamental security requirements of sanitizable signatures, i. e., unforgeability, immutability, transparency, full privacy and auditability. Meanwhile, it has stronger auditability and higher computational efficiency than the zero-knowledge proof based scheme, and is more practical.

Keywords Sanitizable signature, Auditability, Digital signature, Verifiable ring signature, Short signature

随着区块链技术的成熟与发展,以太坊、超级账本等项目在更多领域的应用对数字签名提出了更加多样化的要求,仅仅满足不可伪造条件的数字签名方案在某些环境下已经无法满足应用要求。针对以太坊和超级账本在政府、法律、商业、物流、医疗数据等方向应用时的监管和可审计性要求,本文尝试提出了一种在保证消息匿名性和正确性的前提下,能够提供可更改和强可审计性的数字签名方案。

可净化签名的概念首先于 2005 年由 Ateniese 等^[1]提出,可净化方案可以使签名者为一个选定的代理人(被称为净化者(Sanitizer))更改已签名的消息中的一部分。例如在交易订单中,业务员签发订单:“购买某公司的 A 产品,运送至地址 B”,并将净化者密钥交给其主管经理。在签名时,“A”和“B”是可净化部分,其他的部分是固定部分。那么在必要情况下,主管经理可以通过持有的净化者密钥将消息更改为:“购买某公司的 C 产品,运送至地址 D”。

Ateniese 等^[1]指出了可净化数字签名在医疗数据、流媒体认证和安全路由等方向的应用价值,并且提出了一种基于变色龙散列函数(chameleon hash)的通用方案,但其在文中并没有对可净化签名进行完善的定义,且未对其安全需求进行形式化定义。

Brzuska 等^[2]对可净化签名进行了完善的形式化定义,并对基本安全需求进行了形式化定义,给出了 5 个形式化安全

属性:不可伪造性(Unforgeability)、不可变形(Immutability)、保密性(Privacy)、透明性(Transparency)和可审计性(Accountability),并且给出了这些安全需求之间的蕴涵关系。之后,Canard 等^[3]对 Klonowski 等^[4]提出的部分扩展思路进行了形式化处理。以上的通用方案都是对 Ateniese 等^[1]提出的基于变色龙安全散列方案的改进或扩展。

Brzuska 等^[5]对安全属性进行了进一步的完善,指出了一个未被研究但相关的属性:不可连接性(Unlinkable),当已净化的签名不存在可以与原始签名产生联系的特征时,该方案具有不可链接性,但由于其基于的群签名方案相对复杂且效率低,该方案较为复杂低效。2016 年,Lai 等^[6]提出了无随机预言模型的可净化签名,同年,Fleischhacker 等^[7]提出了一个基于可重新随机化的密钥的方案,该方案比文献^[6]的方案更加高效,但由于其在密钥对生成阶段使用零知识证明方案生成随机密钥,导致计算效率较低,同时也会带来可审计性上的风险。本文提出了一种基于可转换环签名和短签名的可净化签名,在保证效率的同时,具有不可连接性和强可审计性。

1 预备知识

1.1 传统数字签名方案

一个传统数字签名方案 D 由 3 个概率多项式时间算法构成:1) 密钥生成算法 $D.Gen$, 以安全参数 1^n 为输入参数,输

出公私钥对 (pk,sk) ;2)签名算法 $D. Sig$,以消息 m 和私钥 sk 作为输入参数,输出消息 m 的签名 σ ;3)验证算法 $D. Ver$,输入消息签名对 (m,σ) 和私钥 sk ,输出一个验证值 $v\in\{0,1\}$,当 $v=1$ 时,表示签名 σ 为私钥 sk 对消息 m 的有效签名,其他情况则 $v=0$ 。

本文采用一个满足在适应性选择消息攻击下存在不可伪造性(Existentially Unforgeability under Chosen Message Attack, EU-CMA)的传统数字签名方案^[8],为简化描述,称其为不可伪造性。

1.2 可验证环签名数字签名方案

可验证环签名(Verifiable Ring Signature, VRS)是由 Lv 等^[9]于 2003 年提出的,可转换环签名的主要优点是即保证了匿名性,又在必要的情况下可以通过真实签名者给出的相关数据证明签名者的真实身份。VRS 签名方案由定义的 5 个概率多项式时间算法构成:1)密钥生成算法 $V. Gen$,以安全参数 1^n 为输入参数,输出公私钥对 (pk,sk) ;2)签名算法 $V. Sig$,以公钥集 L 、私钥 sk 和消息 m 为输入参数,生成签名 σ ;3)验证算法 $V. Ver$,以公钥集 L 、消息 m 和签名 σ 为输入参数,对签名 σ 进行验证,输出验证值 $v\in\{0,1\}$,当 $v=1$ 时,表示签名 σ 为私钥 sk 和公钥集 L 对消息 m 的有效签名,其他情况则 $v=0$;4)证明算法 $V. Proof$,以公钥集 L 、消息 m 、签名 σ 、公钥 pk 和私钥 sk 为输入参数,输出证明值 π ;5)仲裁算法 $V. Judge$,以公钥集 L 、消息 m 、签名 σ 、公钥 pk 和证明值 π 为输入参数,输出一个值 $b\in\{0,1\}$,当 $b=1$ 时,表示证明值 π 证明签名 σ 来自签名者,当 $b=0$ 时,表示证明值 π 证明签名 σ 不来自签名者,其他情况输出错误符 $*$ 。

可验证环签名自提出后,经过王化群等^[10]和李晓琳等^[11]的多次改进后,依旧在不可伪造性方面存在安全缺陷。因此,本文采用文献[14]中一个效率较高的改进方案,该方案的不可伪造性由短签名在新构造签名中进行弥补。

1.3 短签名数字签名方案

短签名(Short Signature)是由 Boneh 等^[12]于 2001 年提出的,其长度为 DSA 签名标准长度的一半,但具有同等等级,其构成如下:令 (G_1,G_2) 为阶均为素数 p 的双线性群组, G_2 的生成元为 g_2 ,再令 $H:\{0,1\}^*\rightarrow G_1$ 是一个全域散列函数。此短签名方案由定义的 3 个概率多项式时间算法构成:1)密钥生成算法 $S. Gen$,随机选取 $x\in Z_p$ 作为私钥 sk ,并计算相应的公钥 $pk=g_2^x$;2)签名算法 $S. Sig$,以消息 m 和私钥 sk 为输入参数,输出签名 $\sigma=H(m)^x$;3)验证算法 $S. Ver$,以公钥 pk 、消息 m 和签名 σ 为输入参数,验证等式 $e(H(m),v)=e(\sigma,g_2)$ 是否成立,输出验证值 $v\in\{0,1\}$,当等式成立时,输出 $v=1$,表示签名 σ 为私钥 sk 对消息 m 的有效签名,等式不成立则输出 $v=0$ 。

本文采用文献[12]中提出的短签名方案,此方案在随机预言模型下满足不可伪造性。

2 一个基于可转换环签名的可净化数字签名方案

2.1 可净化数字签名的形式化定义

本文沿用 Brzuska 等^[5]完善后的形式化定义,其中涉及 3 个角色:签名者(Signer)、净化者(Sanitizer)以及仲裁者(Judge)。签名者生成两个无关的公私钥对,其中一对用来对某一消息进行签名,另一对交于选定的净化者,净化者的修改权限由签名者指定。当需要对消息净化时,净化者使用净化

算法对签名者生成的消息签名进行净化操作,并对净化后的消息重新签名。第三方可以通过验证算法对给出的消息签名对进行验证。当需要证明被公布的消息签名对的确切来源时,签名者或净化者可以通过证明算法生成一个证据,仲裁者在得到通过证明算法生成的证据后,可以通过仲裁算法对消息签名对进行仲裁,以判断该消息签名对是直接来自签名者还是来自净化者。

首先,在可净化签名中有两个定义的描述符,分别是 ADM 和 MOD。描述符 ADM 是描述处理被签名消息中允许被净化者净化部分的函数,它给定了净化者的权限。描述符 MOD 是描述净化者对消息进行净化的函数。

定义 1(可净化数字签名) 一个可净化数字签名方案由如下定义的 7 个概率多项式时间算法构成。

(1)签名者公私钥生成算法 SiGen。以安全参数 1^n 作为输入参数,输出签名者的公钥 pk 和私钥 sk 。

(2)净化者公私钥生成算法 SaGen。以安全参数 1^n 作为输入参数,输出净化者的公钥 spk 和私钥 ssk 。

(3)签名者签名算法 Sig。使用签名者私钥 sk 为消息 m 、净化者公钥 spk 和消息可净化部分 $ADM(m)$ 签名,生成签名 σ ,并对消息 m 的哈希值签名,生成签名 σ_1 。

(4)净化者净化签名算法 San。首先验证 ADM 和签名 σ ,如果 $ADM(MOD)=1$,则以净化者私钥 ssk 、签名者公钥 pk 和签名 σ 对经过 MOD 修改过后的消息 m' 进行签名,生成签名 σ' 。

(5)验证算法 Ver。以消息 m 、签名 σ 、签名 σ_1 、签名者公钥 pk 和净化者公钥 spk 为输入参数,输出验证值 $v\in\{0,1\}$ 。本文以 $v=0$ 表示该签名不正确,未通过验证;以 $v=1$ 表示签名通过验证。

(6)证明算法 Proof。以签名者私钥 sk 、消息 m 、签名者公钥 pk 、签名 σ 和签名 σ_1 为输入参数,输出一个证明值 $\pi\in\{0,1\}^*$ 。

(7)仲裁算法 Judge。以消息 m 、签名 σ 、签名 σ_1 、签名者公钥 pk 、净化者公钥 spk 和证明算法输出的证明值 π 作为输入参数,输出仲裁值 $j\in\{0,1\}$ 。本文以 $j=0$ 表示消息签名对是由净化者产生的; $j=1$ 表示消息签名对由签名者产生。

一个有意义的可净化数字签名需要满足以下 3 个要求:1)由签名者签名算法输出的可净化签名必须能够通过验证算法的检验;2)由净化者净化签名算法输出的可净化签名必须能够通过验证算法的检验;3)对于一个由净化算法产生的消息签名对,证明算法可以输出一个合法证据,有助于仲裁算法对消息的来源做出正确的判断。

2.2 方案描述

本文提出一种基于短签名和环签名的可净化数字签名(SSRS),它的 9 个概率多项式时间算法定义如下。

(1)签名者密钥生成算法 SSRS. SiGen。接收安全参数 1^n ,并进行如下操作:

- 1) $(pk_s,sk_s)\leftarrow S.Gen(1^n)$;
- 2) $(pk_d,sk_d)\leftarrow D.Gen(1^n)$;
- 3) $(pk_v,sk_v)\leftarrow V.Gen(1^n)$ 。

输出公钥 $pk=(pk_s,pk_d,pk_v)$ 和私钥 $sk=(sk_s,sk_d,sk_v)$ 。

(2)净化者密钥生成算法 SSRS. SaGen。接收安全参数 1^n ,并进行如下操作:

$(spk,ssk)\leftarrow V.Gen(1^n)$;输出公钥 spk 和私钥 ssk 。

(3)签名者签名算法 SSRS. Sig。接收消息 $m\in\{0,1\}^*$ 、

签名者私钥 $sk = (sk_s, sk_d, sk_v)$ 、净化者公钥 spk 以及描述符 AMD , 并进行如下操作:

- 1) 用描述符 ADM 计算消息固定部分 M ;
- 2) 对消息 m 的非固定部分进行哈希运算生成哈希值 $h \leftarrow H(m - M)$;

3) 计算 $\sigma_d \leftarrow D.Sig(sk_d, (M \parallel ADM \parallel pk \parallel spk \parallel h))$;

4) 计算 $\sigma_s \leftarrow S.Sig(sk_s, (M \parallel h))$;

5) 计算 $\sigma_v \leftarrow V.Sig(\{pk_v, spk\}, sk_v, (\sigma_d \parallel m))$;

输出消息 m 的可净化签名 $\sigma = (\sigma_d, \sigma_s, \sigma_v, ADM)$ 。

(4) 净化者净化签名算法 SSRS. San。接收消息签名对 $(m, \sigma) = (m, (\sigma_d, \sigma_s, \sigma_v, ADM))$ 、净化者私钥 ssk 、签名者公钥 $pk = (pk_s, pk_d, pk_v)$ 和描述符 MOD , 并执行如下操作:

1) 计算 $v \leftarrow S.Ver(m, \sigma, pk, spk, h)$, 如果 $v = 0$, 终止并退出;

2) 用描述符 MOD 对消息 m 进行净化, 生成净化消息 m' ;

3) 计算 $\sigma'_v \leftarrow V.Sig(\{pk_v, spk\}, ssk, (\sigma_d \parallel m'))$ 。

输出净化后的消息 m' 及其签名 $\sigma' = (\sigma_d, \sigma_s, \sigma'_v, ADM)$ 。

(5) 验证算法 SSRS. Ver。接收消息签名对 $(m, \sigma) = (m, (\sigma_d, \sigma_s, \sigma_v, ADM))$ 、消息 m 的哈希值 h 、签名者公钥 $pk = (pk_s, pk_d, pk_v)$ 和净化者公钥 spk , 并执行如下操作:

1) 用描述符 ADM 计算消息固定部分 M ;

2) 计算 $v_1 \leftarrow D.Ver(pk_d, (M \parallel ADM \parallel pk \parallel spk \parallel h), \sigma_d)$;

3) 计算 $v_2 \leftarrow S.Ver(pk_s, (M \parallel h), \sigma_s)$;

4) 计算 $v_3 \leftarrow V.Ver(\{pk_v, spk\}, (\sigma_d \parallel m), \sigma_v)$ 。

输出验证结果 $v = (v_1 \& \& v_2 \& \& v_3)$, 只有当 3 个结果都为 1 时验证值才为 1。

(6) 签名者证明生成算法 SSRS. SiProof。接收签名消息对 $(m, \sigma) = (m, (\sigma_d, \sigma_s, \sigma_v, ADM))$ 、签名者的密钥对 (pk, sk) , 并执行如下操作:

1) 计算 $v \leftarrow SSRS.Ver(pk, skp, m, \sigma)$, 如果 $v = 0$, 终止并退出;

2) 计算 $\pi_{si} \leftarrow V.Proof(\{pk_v, spk\}, (\sigma_d \parallel m), \sigma_v, pk_v, sk_v)$ 。

输出证明 π_{si} 。

(7) 净化者证明生成算法 SSRS. SaProof。接收签名消息对 $(m, \sigma) = (m, (\sigma_d, \sigma_s, \sigma_v, ADM))$ 、签名者公钥 pk 、净化者的私钥 ssk , 并执行如下操作:

1) 计算 $v \leftarrow SSRS.Ver(pk, skp, m, \sigma)$, 如果 $v = 0$, 终止并退出;

2) 计算 $\pi_{sd} \leftarrow V.Proof(\{pk_v, spk\}, (\sigma_d \parallel m), \sigma_v, pk_v, ssk)$ 。

输出证明 π_{sd} 。

(8) 签名者仲裁算法 SSRS. SiJudge。接收签名消息对 $(m, \sigma) = (m, (\sigma_d, \sigma_s, \sigma_v, ADM))$ 、签名者公钥 pk 、净化者公钥 spk 、原始消息的哈希值 h 和签名者证明 π_{si} , 并执行如下操作:

1) 计算 $v \leftarrow SSRS.Ver(pk, skp, m, \sigma)$, 如果 $v = 0$, 终止并退出;

2) 计算 $j_1 \leftarrow V.Judge(\{pk_v, spk\}, (\sigma_d \parallel m), \sigma_v, pk_v, \pi_{si})$;

3) 计算接收签名消息对中的消息的哈希值 h' , 计算 $j_2 = h \oplus h'$;

4) 计算 $J = j_1 \& \& (1 - j_2)$ 。

输出仲裁结果 J 。

(9) 净化者仲裁算法 SSRS. SaJudge。接收签名消息对 $(m, \sigma) = (m, (\sigma_d, \sigma_s, \sigma_v, ADM))$ 、签名者公钥 pk 、净化者公钥 spk 、原始消息的哈希值 h 、签名者证明 π_{si} , 并执行如下操作:

1) 计算 $v \leftarrow SSRS.Ver(pk, skp, m, \sigma)$, 如果 $v = 0$, 终止并退出;

2) 计算 $j_1 \leftarrow V.Judge(\{pk_v, spk\}, (\sigma_d \parallel m), \sigma_v, pk_v, \pi_{si})$;

3) 计算接收签名消息对中的消息的哈希值 h' , 计算 $j_2 = h \oplus h'$;

4) 计算 $J = (1 - j_1) \& \& j_2$ 。

输出仲裁结果 J 。

容易证得, 上述新构造的可净化签名方案满足 2.1 节的正确性要求。

3 安全性分析

本文采用文献[5, 13]中给出的相关形式化模型对提出的可净化签名方案进行安全性分析。下文依次证明可净化数字签名 SSRS 满足不可变形性、透明性、不可连接性和可审计性。因为 Brzuska 等^[2]指出可审计性涵盖不可伪造性, 所以该方案还满足不可伪造性。因此可以证明本文提出的方案 SSRS 满足可净化签名的所有 5 项安全性要求。

3.1 不可变形性

引理 1 如果数字签名方案 D 满足不可伪造性(unf), 那么可净化签名方案 SSRS 满足不可变形性(immu)。

证明: 假设存在一个敌手 A , 意图针对可净化签名方案 SSRS 的不可变形性进行攻击, 且 $\lambda(n) = \Pr[Exp_{SSRS, A}^{immu}(n) = 1]$ 是不可忽略的。那么我们构造一个算法 B , 且 $\Pr[Exp_{D, B}^{unf}(n) = 1]$ 是不可忽略的, 对数字签名方案 D 的不可伪造性进行攻击。挑战游戏如下:

算法 B 调用签名者密钥生成算法 S , $SiGen$ 生成一对挑战密钥 (pk^*, sk^*) , 并将其中的公钥发送给敌手 A 生成 (spk^*, m^*, σ^*) 。在挑战过程中, B 对 $S.Sig$ 和 $S.SiProof$ 的模拟如下:

SSRS. Sig: 对第 i 次签名询问 (m_i, ADM_i, spk_i) , B 首先计算消息固定部分 M 并且将 $(M_i \parallel ADM_i \parallel pk_i \parallel spk_i \parallel h_i)$ 发送至签名过程 $D.Sig$, 收到消息签名 σ_{i1} , 并通过 $V.Sig$ 生成 σ_{i2} , 输出 $\sigma_i = (\sigma_{di}, \sigma_{si}, \sigma_{vi}, ADM_i)$ 。

SSRS. SiProof: 对第 i 次输入 $(m_i', \sigma_i', spk_i')$, 首先解析 $\sigma_i' = (\sigma_{di}', \sigma_{si}', \sigma_{vi}', ADM_i')$, 通过 $V.Proof$ 生成 π_{si}' 。

最后 B 解析 σ^* , 计算消息固定部分 M^* , 并返回消息对 $((M^* \parallel ADM^* \parallel pk \parallel spk^* \parallel h^*), \sigma_1^*)$ 。

分析: 上述过程已表明, 如果敌手 A 赢得挑战游戏, 那么算法 B 同样赢得挑战游戏。假设敌手 A 赢得挑战游戏, 那么以下等式成立:

$$D.Ver(m^*, \sigma^*, pk, spk^*, h^*) = 1 \quad (1)$$

$$(spk^* \neq spk_i) \text{ 或 } ADM^*(m^*) \neq ADM_i(m_i), i \in [1, q_{sig}] \quad (2)$$

由式(1)可得以下等式:

$$D.Ver(pk_d, (M^* \parallel ADM^* \parallel pk \parallel spk^* \parallel h^*), \sigma_1^*) = 1$$

由式(2)可得:

$$(M^* \parallel ADM^* \parallel pk \parallel spk^* \parallel h^*) \neq (M_i \parallel ADM_i \parallel pk \parallel spk_i \parallel h_i), i \in [1, q_{sig}]$$

由此我们可以推定, B 不能发送消息 $(M^* \parallel ADM^* \parallel pk \parallel$

$spk * \parallel h_*$) 给 D . Sig, 并且可推定, 如果 A 赢得挑战游戏, B 也赢得挑战游戏, 则有 $\Pr[Exp_{D,B}^{mf}(n)=1] \geq \lambda(n)$ 。因此, 如果底层的签名方案 D 是不可伪造的, 则可净化签名方案 SSRS 具有不可变形性。证毕。

3.2 透明性

引理 2 如果环签名方案 V 满足匿名性(ano), 那么可净化签名方案 SSRS 满足透明性(trans)。

证明: 假设存在一个敌手 A , 意图针对可净化签名方案 SSRS 的透明性进行攻击, 且 $\lambda(n) = \Pr[Exp_{SSRS,A}^{trans}(n)=1]$ 是不可忽略的。那么我们构造一个算法 B , 且 $\Pr[Exp_{D,B}^{ano}(n)=1]$ 是不可忽略的, 对数字签名方案 D 的不可伪造性进行攻击。挑战游戏如下:

算法 B_1 接收 (spk, pk_v) , 并返回 $(1, 2)$ 。算法 B_2 调用 SSRS. SiGen 生成公钥 $pk = (pk_s, pk_d, pk_v)$, 由敌手 A 通过 (pk, spk) 输出 b' , 在挑战过程中, B_2 模拟如下:

SSRS. Sig: 对第 i 次签名询问 (m_i, ADM_i, spk_i) , B_2 首先计算固定部分消息 M_i , 并计算 $\sigma_{di} \leftarrow D. Sig(sk_d, (M_i \parallel ADM_i \parallel pk \parallel spk_i \parallel h_i))$, 传输 $(\{pk_v, spk\}, 1, (\sigma_{di} \parallel m_i))$ 给 $V. Sig$ 生成 σ_{vi} , B_2 输出 $\sigma_i = (\sigma_{di}, \sigma_{si}, \sigma_{vi}, ADM_i)$ 至 A 。

SSRS. San: 对第 i 次输入 $(m_i', MOD_i', \sigma_d', pk_i')$, 解析 $\sigma_i' = (\sigma_{di}', \sigma_{si}', \sigma_{vi}', ADM_i')$ 和 $pk_i' = (pk_{si}', pk_{di}', pk_{vi}')$ 。首先计算净化消息 m_{i1}' , 并传输 $(\{pk_v', spk\}, 2, (\sigma_{di}' \parallel m_{i1}'))$ 至 $V. Sig$ 生成 σ_{vi}' , 构成签名 $\sigma_i' = (\sigma_{di}', \sigma_{si}', \sigma_{vi}', ADM_i')$ 。

SSRS. SiProof: 对第 i 次输入 $(m_i'', \sigma_d'', pk_i'')$, B 解析 $\sigma_i'' = (\sigma_{di}'', \sigma_{si}'', \sigma_{vi}'', ADM_i'')$, 传输 $(\{pk_v, spk_i''\}, (\sigma_{di}'' \parallel m_{i1}''), \sigma_{vi2}'', pk_v, 1)$ 至 $V. Proof$ 生成证明 π_{si}'' 。

SSRS. SaProof: 对第 i 次输入 $(m_i'', \sigma_d'', pk_i'')$, B 解析 $\sigma_i'' = (\sigma_{di}'', \sigma_{si}'', \sigma_{vi}'', ADM_i'')$ 和 $pk_i'' = (pk_{si}'', pk_{di}'', pk_{vi}'')$, 传输 $(\{pk_v, spk_i''\}, (\sigma_{di}'' \parallel m_{i1}''), \sigma_{vi2}'', pk_v, 2)$ 至 $V. Proof$ 生成证明 π_{sai}'' 。

SSRS. Sa/SSRS. Si: 对第 i 次输入 (m_i, MOD_i, ADM_i) , 如果 $ADM_i(MOD_i) = 0$, 则 B_2 返回错误。其他情况下 B_2 计算固定消息部分 M_i , B_2 生成 $\sigma_i^* = (\sigma_{di}^*, \sigma_{si}^*, \sigma_{vi}^*, ADM_i^*)$ 给 A 。

分析: 假设敌手 A 赢得挑战, 则有 $b = b'$, 且 $S_{Sa/Si} \cap (SSRS. SiProof \cup SSRS. SaProof) = \emptyset$, 当 $S_{Sa/Si} (SSRS. SiProof$ 和 $SSRS. SaProof)$ 符合 SSRS. SiProof 和 SSRS. SaProof 的输出集合, 则说明发送给 $V. Proof$ 的消息并未正确签名。则有算法 B 赢得挑战的可能和敌手 A 赢得挑战的可能性 $\Pr[Exp_{D,B}^{mf}(n)=1] \geq \lambda(n)$ 。证毕。

3.3 不可连接性

引理 3 如果数字签名方案 D 满足不可伪造性(unf), 那么可净化签名方案 SSRS 满足不可连接性(unlink)。

证明: 假设存在一个敌手 A , 其优势 $\lambda(n) = \Pr[Exp_{SSRS,A}^{unlink}(n)=1] - 1/2$ 是不可忽略的, 我们构造如下算法 B , 有 $\Pr[Exp_{D,B}^{mf}(n)=1]$ 是不可忽略的。挑战游戏如下:

算法 B_1 接收 pk_d 作为输入, B 通过 SSRS. SiGen 生成 (pk_v, sk_v) 和 (spk, ssk) , 并生成 $pk = (pk_s, pk_d, pk_v)$ 。首先选择 $b \leftarrow \{0, 1\}$ 并计算 $b' \leftarrow A(pk, spk)$ 。在挑战过程中, B_2 模拟如下:

SSRS. Sig: 对第 i 次签名询问 (m_i, ADM_i, spk_i) , B 首先计算固定部分消息 M_i , 并计算 $\sigma_{di} \leftarrow D. Sig(sk_d, (M_i \parallel ADM_i \parallel pk \parallel spk_i \parallel h_i))$, 通过 $V. Sig$ 生成 σ_{vi} , 输出 $\sigma_i = (\sigma_{di}, \sigma_{si},$

$\sigma_{vi}, ADM_i)$ 。

SSRS. SiProof: 对第 i 次输入 (m_i', σ_i', pk_i') , 首先解析 $\sigma_i = (\sigma_{di}, \sigma_{si}, \sigma_{vi}, ADM_i)$, 通过 $V. Proof$ 生成 π_{si}' 并输出。

SSRS. San: 对第 i 次输入 $(m_i'', \sigma_d'', pk_i'')$, B 生成 σ_i'' 并输出给 A 。

SSRS. SaProof: 对第 i 次输入 $(m_i''', \sigma_d''', pk_i''')$, B 生成 π_{sai}''' 并输出给 A 。

LRSSRS. San: 对第 i 次输入 $((m_{0i}, MOD_{0i}, \sigma_{0i})(m_{1i}, MOD_{1i}, \sigma_{1i}))$, 如果有 $j \in \{0, 1\}$, $S. Ver(m_{ji}, \sigma_{ji}, pk, spk) = 1$, 且有 $ADM_{0i} = ADM_{1i}$, $ADM_{ji}(MOD_{ji}) = 1$, $MOD_{0i}(m_{0i}) = MOD_{1i}(m_{1i})$, 则输出 σ_i' 给 A 。

分析: 如果对于任意 $i \in \{1, \dots, q\}$, q 是多项式 LRSSRS. San 的查询数, 有 $j \in \{0, 1\}$, $S. Ver(m_{ji}, \sigma_{ji}, pk, spk) = 1$, 且有 $ADM_{0i} = ADM_{1i}$, $ADM_{ji}(MOD_{ji}) = 1$, $MOD_{0i}(m_{0i}) = MOD_{1i}(m_{1i})$, 且 $D. Sig$ 已经输出 σ_{ji}' , 可知:

$$(m_{0i} - ADM_{0i}(m_{0i})) \parallel ADM_{0i} \parallel pk \parallel spk \parallel h = (m_{1i} - ADM_{1i}(m_{1i})) \parallel ADM_{1i} \parallel pk \parallel spk \parallel h$$

因为数字签名 D 是确定的, 则可推论 $\sigma_{1bi}' = \sigma_{0i} = \sigma_{1i}$, 并且输出的第二部分签名 σ_{2bi}' 并不取决于 b , 最后有 $ADM_{bi}' = ADM_{0i} = ADM_{1i}$, 则 ADM_{bi}' 的值不取决于 b 。则可以推论签名 σ_{bi}' 与 b 无关。因此, A 只能通过随机预言 b' 赢得挑战。

如果存在任意 $i \in \{1, \dots, q\}$, q 是多项式 LRSSRS. San 的阶, 有 $j \in \{0, 1\}$, $S. Ver(m_{ji}, \sigma_{ji}, pk, spk) = 1$, 且有 $ADM_{0i} = ADM_{1i}$, $ADM_{ji}(MOD_{ji}) = 1$, $MOD_{0i}(m_{0i}) = MOD_{1i}(m_{1i})$, 如果存在 x 使多项式 $D. Sig$ 未输出 σ_{xi} , 则 B 输出 $((m_{xi} - ADM_{xi}(m_{xi})) \parallel ADM_{xi} \parallel pk \parallel spk \parallel h), \sigma_{xi})$ 给敌手并赢得挑战, 对此我们用 E 表示, 则有:

$$\Pr[Exp_{D,B}^{mf}(n)=1] \geq \Pr[E]$$

且有:

$$\begin{aligned} \Pr[Exp_{SSRS,A}^{unlink}(n)=1] &= \Pr[E] \cdot \Pr[Exp_{SSRS,A}^{unlink}(n)=1|E] + (1 - \Pr[E]) \cdot \Pr[Exp_{SSRS,A}^{unlink}(n)=1|\neg E] \\ &= \Pr[E] \cdot \Pr[Exp_{SSRS,A}^{unlink}(n)=1|E] + \frac{1}{2} - \frac{1}{2} \cdot \Pr[E] \end{aligned}$$

则有:

$$\begin{aligned} \Pr[E] &= \frac{\Pr[Exp_{SSRS,A}^{unlink}(n)=1] - \frac{1}{2}}{\Pr[Exp_{SSRS,A}^{unlink}(n)=1|E] - \frac{1}{2}} \\ &= \frac{\pm \lambda(n)}{\Pr[Exp_{SSRS,A}^{unlink}(n)=1|E] - \frac{1}{2}} \geq \lambda(n) \end{aligned}$$

则可得:

$$\Pr[Exp_{D,B}^{mf}(n)=1] \geq \lambda(n)$$

证毕。

3.4 可审计性

3.4.1 签名者可审计性

引理 4 如果短签名方案 S 满足不可伪造性(unf), 那么可净化签名方案 SSRS 满足签名者可审计性(SiAcc)。

证明: 假设存在一个敌手 A , 其 $\lambda(n) = \Pr[Exp_{SSRS,A}^{SiAcc}(n)=1]$ 是不可忽略的, 我们构造如下算法 B , 有 $\Pr[Exp_{S,B}^{mf}(n)=1]$ 是不可忽略的。挑战游戏如下:

B 接收 (spk) 作为输入, 并输出 $(pk_s, m_s, \sigma_s, \pi_{si_s})$ 。在挑战过程中, B 模拟如下:

SSRS. San: 对第 i 次输入 $(m_i, MOD_i, \sigma_i, pk_i)$, 解析 $\sigma = (\sigma_{di}, \sigma_{vi}, \sigma_{si}, ADM_i)$ 和 $pk_i = (pk_{si}, pk_{di}, pk_{vi})$ 。首先计算净化消息 $\bar{m}_i$ 并传输 $(\{pk, spk\}, 1, (\bar{m}_i \parallel \sigma_{di}))$ 给 $V. Sig$, 返回 σ_{vi} , σ_{si} 。B2 输出 $\sigma_i = (\sigma_{di}, \bar{\sigma}_{vi}, \bar{\sigma}_{si}, ADM_i)$ 至 A 。

SSRS. SaProof: 对第 i 次输入 (m_i', σ_i', pk_i') , B 解析 $\sigma_i' = (\sigma_{i1}', \sigma_{i2}', \sigma_{i3}', ADM_i')$ 以及 $pk_i' = (pk_{si}', pk_{di}', pk_{vi}')$, 并传输 $(\{pk_v', spk'\}, (\sigma_{i1}' \parallel m_i'), \sigma_{i2}', pk_v, 1)$ 给 $V. Proof$, 输出 π_{si}' 给 A 。

最后, B 输出 $(\{pk_{v*}, spk\}, (\sigma_{1*} \parallel m_*), \sigma_{2*}, pk_{v*}, \pi_{si*})$ 。
分析: 假设 A 赢得挑战, 则有:
对任意 $i \in \{1, \dots, q_{San}\}$, $\sigma_* \neq \sigma_i'$ (3)
SSRS. $Ver(m_*, \sigma_*, pk_*, spk) = 1$ (4)
SSRS. $SiJudge(m_*, \sigma_*, pk_*, spk, \pi_{si*}) = 0$ (5)
因为 $\{spk, pk_{v*}\} \subset \{spk\} \cup \{pk_{v*}\}$, 由式(3)可知对任意 $i \in \{1, \dots, q_S\}$, $\sigma_{*2} \neq \bar{\sigma}_{i2}$ 。所以有: 如果 $\sigma_* \neq \sigma_i'$, 则有 $\sigma_{d*} \neq \sigma_{di}$ 或 $\sigma_{v*} \neq \sigma_{vi}$ 或 $ADM_* \neq ADM_i$, 如果 $ADM_* \neq ADM_i$, 则有 $\sigma_{d*} \neq \sigma_{di}$, 如果 $\sigma_{d*} \neq \sigma_{di}$, 则有 $\sigma_{v*} \neq \sigma_{vi}$ 。

由式(4)可知: $V. Ver(\{pk_{v*}, spk\}, \sigma_{v*}, (\sigma_{d*} \parallel m_*)) = 1$, 则有 $V. Judge(\{pk_{v*}, spk\}, (\sigma_{d*} \parallel m_*), \sigma_{v*}, pk_{v*}, \pi_{si*}) = 0$ 。
另一方面有:
 $S. Ver(m_*, \sigma_*, pk, spk_*, h_*) = 1$ (6)
 $(spk_* \neq spk_i)$ 或 $ADM_*(m_*) \neq ADM_i(m_i), i \in [1, q_{sig}]$ (7)

由式(6)可得以下等式:
 $S. Ver(pk_i, (M_* \parallel ADM_* \parallel pk \parallel spk_* \parallel h_*), \sigma_{3*}) = 1$
由式(7)可得:
 $(M_* \parallel ADM_* \parallel pk \parallel spk_* \parallel h_*) \neq (M_i \parallel ADM_i \parallel pk \parallel spk_i \parallel h_i), i \in [1, q_{sig}]$

由此我们可以推定 B 不能发送消息 $(M_* \parallel ADM_* \parallel pk \parallel spk_* \parallel h_*)$ 给 $S. Sig$, 并且可推定, 如果 A 赢得挑战游戏, B 也赢得挑战游戏, 则有 $\Pr[Exp_{SSRS,B}^{smf}(n) = 1] \geq \lambda(n)$ 。因此, 即使在环签名 V 无法保证安全性的情况下, 如果短签名 S 满足不可伪造性, 可净化签名 SSRS 满足签名者可审计性。证毕。

3.4.2 净化者可审计性

引理 5 如果短签名方案 S 满足不可伪造性(unf), 那么可净化签名方案 SSRS 满足净化者可审计性(SaAcc)。
证明: 假设存在一个敌手 A , 其 $\lambda(n) = \Pr[Exp_{SSRS,A}^{SaAcc}(n) = 1]$ 是不可忽略的, 我们构造如下算法 B , 有 $\Pr[Exp_{SSRS,B}^{smf}(n) = 1]$ 是不可忽略的。挑战游戏如下:

B 接收 (pk_v) 作为输入, 生成 (pk_d, sk_d) , 令 $pk = (pk_s, pk_d, pk_v)$, 并输出 (spk_*, m_*, σ_*) 。在挑战过程中, B 模拟如下:
SSRS. Sig: 对第 i 次输入 (m_i, ADM_i, spk_i) , 首先计算固定消息部分 M_i 并生成 σ_{di} , 传输 $(\{pk_v, spk_i\}, 1, (m_i \parallel \sigma_{di}))$ 给 $V. Sig$, 返回 σ_{vi}, σ_{si} 。 B 输出 $\sigma_i = (\sigma_{di}, \sigma_{vi}, \sigma_{si}, ADM_i)$ 至 A 。
SSRS. SiProof: 对第 i 次输入 (m_i', σ_i', pk_i') , B 解析 $\sigma_i' = (\sigma_{di}', \sigma_{vi}', \sigma_{si}', ADM_i')$, 并传输 $(\{pk_v, spk_i'\}, (\sigma_{di}' \parallel m_i'), \sigma_{vi}', pk_v, 1)$ 给 $V. Proof$, 输出 π_{si}' 给 A 。
最后, B 输出 $(\{pk_v, spk_*\}, (\sigma_{d*} \parallel m_*), \sigma_{v*})$ 。
分析: 假设 A 赢得挑战, 对任意 π_{si*} , 有:
对任意 $i \in \{1, \dots, q_{Sig}\}$, $\sigma_* \neq \sigma_i'$ (8)
SSRS. $Ver(m_*, \sigma_*, pk, spk_*) = 1$ (9)
SSRS. $SaJudge(m_*, \sigma_*, pk, spk_*, \pi_{si*}) \neq 1$ (10)

由式(8)知, 对任意 $i \in \{1, \dots, q_S\}$, $\sigma_{v*} \neq \bar{\sigma}_{vi}$ 。所以有: 如果 $\sigma_* \neq \sigma_i'$, 则有 $\sigma_{d*} \neq \sigma_{di}$ 或 $\sigma_{v*} \neq \sigma_{vi}$ 或 $ADM_* \neq ADM_i$, 如果 $ADM_* \neq ADM_i$, 则有 $\sigma_{d*} \neq \sigma_{di}$, 如果 $\sigma_{d*} \neq \sigma_{di}$, 则有 $\sigma_{v*} \neq \sigma_{vi}$ 。
由式(9)可知: $V. Ver(\{pk_v, spk_*\}, \sigma_{v*}, (\sigma_{d*} \parallel m_*)) = 1$, 则可知: $V. Judge(\{pk_v, spk_*\}, (\sigma_{d*} \parallel m_*), \sigma_{v*}, pk_v, \pi_{si*}) = 0$, 因为 $\pi_{si*} \leftarrow SiProof(sk, m_*, \sigma_*, spk_*)$, 则有 $\pi_{si*} \leftarrow V. Proof(\{pk_v, spk_*\}, (\sigma_{d*} \parallel m_*), \sigma_{v*}, pk_v, sk_v)$ 。

另一方面有:
 $S. Ver(m_*, \sigma_*, pk, spk_*, h_*) = 1$ (11)
 $(spk_* \neq spk_i)$ 或 $ADM_*(m_*) \neq ADM_i(m_i), i \in [1, q_{sig}]$ (12)

由式(11)可得以下等式:
 $S. Ver(pk_i, (M_* \parallel ADM_* \parallel pk \parallel spk_* \parallel h_*), \sigma_{3*}) = 1$
由式(12)可得:
 $(M_* \parallel ADM_* \parallel pk \parallel spk_* \parallel h_*) \neq (M_i \parallel ADM_i \parallel pk \parallel spk_i \parallel h_i), i \in [1, q_{sig}]$

由此我们可以推定 B 不能发送消息 $(M_* \parallel ADM_* \parallel pk \parallel spk_* \parallel h_*)$ 给 $S. Sig$, 并且可推定, 如果 A 赢得挑战游戏, B 也赢得挑战游戏, 则有 $\Pr[Exp_{SSRS,B}^{smf}(n) = 1] \geq \lambda(n)$ 。因此, 即使在环签名 V 无法保证安全性的情况下, 如果短签名 S 满足不可伪造性, 可净化签名 SSRS 满足签名者可审计性。证毕。

4 比较与分析

现有的可净化数字签名方案中, 效率最高的是 Fleischhacker 等^[7]提出的方案(EUSS), 在此通过每一步算法幂运算次数对本文提出的可净化签名方案 SSRS 和方案 EUSS 进行对比, 结果如表 1 所列。

表 1 方案 SSRS 与方案 EUSS 幂运算次数对比
Table 1 Comparison of power operation times between scheme SSRS and scheme EUSS

	SiGen	SaGen	Sig	San	Ver	SiProof	SaProof
EUSS	7	1	14	15	17	23	6
SSRS	3	1	8	7	11	3	4

从表 1 可以看出签名方案 EUSS 应用零知识证明的方案需要较多的幂运算, 执行效率较低。而从第 3 节的安全性分析可以看出, 本文提出的可净化签名方案 SSRS 满足所有基本安全性需求, 同时加强了可审计性上的安全性, 并且在增加安全性的同时一定程度上增加了执行效率。

结束语 本文提出了一种新的可净化签名方案。本方案基于传统数字签名、短签名和可转换环签名构造而成, 在满足所有 5 个安全需求的同时, 在可审计性上有更好的鲁棒性, 即在可转换环签名被攻破的条件下依旧可以保持其可审计性, 并且算法执行效率较前人的方案有了一定的提高, 因此在对可审计性有较高要求的应用场景中更具有实用价值。

参 考 文 献

[1] ATENIESR G, CHOU D H, DE MEDEIROS B, et al. Sanitizable Signatures [C] // Proc. of Computer Security-ESORICS. Springer Berlin Heidelberg, 2005: 159-177.
[2] BRZUSKA C, FISCHLIN M, FREUDENREICH T, et al. Security of sanitizable signatures revisited[C] // PKC 2009. Springer, 2009: 317-336.

ty:privacy beyondk-anonymity[C] // Proceedings of the 22nd International Conference on Data Engineering. Atlanta, GA, USA;IEEE Press,2006:24-36.

[6] TRUTA T M,VINAY B. Privacy protection:p-sensitive k-anonymityproperty[C] // Proceedings of the 22nd International Conference on Data Engineering Workshops (ICDEW). Washington,DC,USA;IEEE Computer Society,2006:94.

[7] WONG C R,LI J,FU A,et al. (α,k) -anonymity:an enhancedk-anonymity model for privacy preserving data publishing[C] // Proceedings of the 12th ACM SIGKDD Conference. Philadelphia,PA;ACM Press,2006:754-759.

[8] LI N H,LI T C,VENKATASUBRAMANIAN S. t-Closeness: privacy beyond k-anonymity and l-diversity[C] // Proceedings of the 23rd International Conference on Data Engineering(ICDE). Istanbul,Turkey;IEEE Press,2007:106-115.

[9] XIAO X K,TAO Y F. Personalized privacy preservation[C] // Proceedings of the 2006 ACM SIGMOD International Conference on Management of Data. Chicago,USA;ACM Press,2006: 229-240.

[10] YANG X C,LIU X Y,WANG B,et al. K-Anonymization approaches for supporting multiple constraints[J]. Journal of Software,2006,17(5):1222-1231.

[11] LEFEVRE K,DEWITT D J,RAMAKRISHNAN R. Incognito: Efficient full-domain K-anonymity[C] // Proc. of the ACM SIGMOD Int'l Conf. on Management of Data (SIGMOD). ACM Press,2005:49-60.

[12] XU J,WANG W,PEI J,et al. Utility-Based anonymization using local recoding[C] // Proc. of the 12th ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining (SIGKDD). ACM Press,2006:785-790.

[13] LEFEVRE K,DEWITT D J,RAMAKRISHNAN R. Mondrian multidimensional K-anonymity[C] // Proc. of the 22nd Int'l

Conf. on Data Engineering (ICDE). IEEE,2006:25.

[14] XIAO X K,TAO Y. Anatomy:Simple and effective privacy preservation[C] // Proc. of the 32nd Int'l Conf. on Very Large Data Bases (VLDB). VLDB Endowment,2006:139-150.

[15] TAO Y F,CHEN H K,XIAO X,et al. ANGEL: Enhancing the utility of generalization for privacy preserving publication[J]. IEEE Trans. on Knowledge and Data Engineering (TKDE), 2009,21(7):1073-1087.

[16] WONG R C W,LI J Y,FU A W C,et al. (α,k) -Anonymity: An enhanced k-anonymity model for privacy preserving data publishing[C] // Proc. of the 12th ACM SIGKDD Int'l Conf. on Knowledge discovery and Data Mining (SIGKDD). ACM Press, 2006:754-759.

[17] MACHANAVAJJHALA A,KIFER D,GEHRKE J,et al. l-Diversity: Privacy beyond k-anonymity [J]. ACM Trans. on Knowledge Discovery Data (TKDD),2007,1:3.

[18] 任向民. 基于 K-匿名的隐私保护方法研究[D]. 哈尔滨:哈尔滨工程大学,2012.



ZHANG Wang-ce, born in 1994, master, is a student member of CCF. His main interests include network security and machine learning.



FAN Jing, postgraduate, professor, is a member of China Computer Federation. Her main research interests include network security,intelligent sensor net and intelligent control.

(上接第 390 页)

[3] CANARD S,JAMBERT A. On extended sanitizable signature schemes[C] // Cryptographers' Track at the RSA Conference. Berlin;Springer,2010:179-194.

[4] KLONOWSKI M,LAUKS A. Extended sanitizable signatures [C] // Proc of Information Security and Cryptology-ICISC. Berlin;Springer,2006:343-355.

[5] BRZUSKA C,FISCHLIN M,LEHMANN A,et al. Unlinkability of sanitizable signatures[C] // Proc. of Public-Key Cryptography-PKC. Berlin;Springer,2010:444-461.

[6] LAI W F,ZHANG T,CHOW S M,et al. Efficient Sanitizable Signature Without Random Oracles[C] // Proc. of ESORICS. Springer,2016:363-380.

[7] FLEISCHHACKER N,KRUPP J,MALAVOLTA G,et al. Efficient unlinkablesanitizable signatures from signatures with re-randomizable keys[C] // Proc. of Public-Key Cryptography-PKC. Berlin;Springe,2016:301-330.

[8] POINTCHEVAL D,SANDERS O. Short randomizable signatures[C] // Cryptographers' Track at the RSA Conference. Springer,Cham,2016:111-126.

[9] LV J Q,WANG X M. Verifiable ring signature[C] // Proc. of 9th International Conference on Distributed Multimedia System. Miami,USA,2003:663-665.

[10] 王化群,郭显久,于红,等. 几种可转换环签名方案的安全性分析和改进[J]. 电子与信息学报,2009,35(15):135-137.

[11] 李晓琳,梁向前,刘奎,等. 可验证环签名方案的分析与改进[J]. 计算机应用,2012,32(12):3466-3469.

[12] BONEH D,LYNN B,SHACHAM H. Short signatures from weil pairing[C] // Proc of Advances in Cryptology-ASIACRYPTY. Berlin;Springer,2001:512-532.

[13] BRZUSKA C,FISCHLIN M,LEHMANN A,et al. Sanitizable Signatures:How to partially delegate control for authenticated data. [C] // Proc. of Special Interest Group on Biometrics and Electronic Signatures. Bonn;GI,2009:117-128.

[14] LV X,XU F,PING P,et al. Schnorr ring signature scheme with designated verifiability[C] // 2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES). IEEE,2015:163-166.



ZHANG Jun-he, born in 1991, postgraduate. His main research interests include mimic defense, and digital signature.