How to Securely Delegate and Revoke Partial Authorization Credentials (TDSC 2025)

content

目录

引言与背景

01

身份管理中的隐私保护需求

用户中心身份管理

随着用户中心身份管理的兴起，对身份隐私的保护需求日益增加。

隐私友好的身份管理要求凭证系统支持用户选择性披露属性以及有效的撤销凭证。

基于属性的凭证

由签发者在一组属性（如姓名、年龄、地址等）和用户公钥上签名。用户是唯一可以通过零知识证明来证明其凭证所有权的人，也可以有选择地向服务提供商披露属性子集或证明属性关系（如年龄大于 18 岁）

证明关系

凭证系统需要支持用户证明未披露属性满足某些关系。

在日常生活中使用基于属性的凭证时，我们经常需要一些额外的要求，如授权和撤销。有时，我们需要将权限委托给他人，或与他人共享我们对服务的访问权限。

基于属性的凭证

01

Attributed-based credential

基于属性的凭证(ABC) 允许用户从发行者处获得基于一组属性(如姓名、年龄、地址等)的凭证。ABC支持用户通过零知识证明声明其对秘密信息的知识，从而证明对凭证的所有权，同时可以选择性地披露属性子集或证明属性之间的关系，而不泄露任何未披露属性的信息。

02

实际应用案例

Name：Bob
Age：30
Departments：Marketing
Positions：Manager

Departments：Marketing
Positions：Manager

可委托属性凭证系统的挑战

在可委托 ABC（DABC）系统中，用户可以将自己的证书委托给其他用户。

认证链的局限

大多数现有系统基于认证链（Certification chains），导致凭证大小随层级呈指数或线性增长，影响实际应用效率。

属性不可分割

无法支持仅部分属性的委托，缺乏灵活性不适用于许多场景的需求。

隐私泄露风险

一旦凭证被使用，原委托者可能识别接收者，严重侵犯隐私。

论文的贡献

02

可净化签名的引入

新密码原语

提出了一种名为 Purgeable Signatures的签名方案，其灵感源于Redactable Signatures和Malleable Signatures，允许在不破坏签名有效性的情况下，以不可追踪的方式编辑（更新/删除）已签名的消息。

安全定义

正式定义了可净化签名的安全属性，包括不可伪造性和不可链接性，确保签名的完整性和隐私保护。

应用潜力

可净化签名不仅适用于属性基础凭证系统，还可能具有独立的兴趣和广泛的应用潜力。

可委托与撤销属性的凭证设计

委托功能

设计了一种允许用户匿名委托凭证上部分属性给其他实体的机制，确保了用户可以在不暴露所有信息的情况下，选择性地分享权限。

撤销功能

实现了高效的凭证撤销机制，用户可以自主撤销自己的凭证或通过授权机构撤销被委托的凭证，增强了系统的安全性。

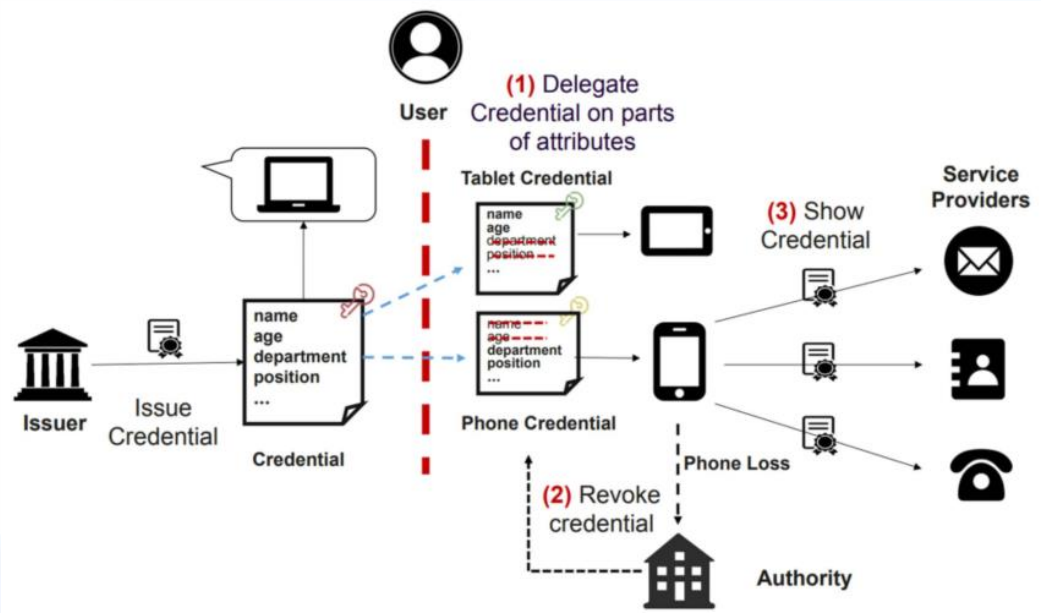
属性披露与证明

支持用户选择性披露凭证中的属性子集，保持了用户隐私的同时提供了必要的验证手段。

系统模型与定义

03

系统总体架构



申请凭证→委托部分属性→使用/撤销

委托与撤销属性基础凭证的定义

角色与功能

系统包含发行者、用户、服务提供者和撤销权威四个角色，支持凭证的发行、委托、出示和撤销，同时保证匿名性和不可链接性。

凭证委托机制

用户可以将凭证部分属性委托给其他实体，通过更新和移除操作保持凭证的有效性和隐私。

凭证撤销机制

撤销权威能够通过动态累加器撤销凭证，确保一旦凭证丢失或被滥用，用户申请撤销可以立即生效，防止进一步的安全风险。

正确性与安全性

系统设计需满足验证正确性、委托正确性和匿名性，确保所有操作在符合规则的情况下有效执行，同时保护用户隐私。

方案构造与分析

04

Purgeable Signature

Sign($sk, \overrightarrow{m}, T$):

$\tilde{\sigma}_1 \xleftarrow{\$} \tilde{g}^r$

$\tilde{\sigma}_2 \leftarrow \tilde{\sigma}_1{}^{(x+\sum_{i=1}^{n} y_i \cdot m_i)}$

$uk \leftarrow (\tilde{\sigma}_1{}^{y_i})_{i \in T}$

$\sigma = (1_{\mathbb{G}_1}, 1_{1_{\mathbb{G}_1}}, \tilde{\sigma}_1, \tilde{\sigma}_2)$

Edit($pk, \sigma, \overrightarrow{m}, \overrightarrow{m}', \mathrm{uk}, \mathrm{I}$):

Update:

$\tilde{\sigma}_1' \leftarrow \tilde{\sigma}_1{}^{r}$

$\tilde{\sigma}_2' \leftarrow (\tilde{\sigma}_2 \cdot \prod_{i \in T} (\tilde{\sigma}_1{}^{y_i})^{m_i' - m_i})^r$

Remove:

$\sigma_1'' \leftarrow g^t \prod_{j \in \bar{I}} Y_j^{m_j'}$

$\sigma_2'' \leftarrow (\prod_{i \in I} Y_i)^t \prod_{i \in I, j \in \bar{I}} Z_{i,j}^{m_j'}$

$\tilde{\sigma}_1'' \leftarrow (\tilde{\sigma}_1')^s$

$\tilde{\sigma}_2'' \leftarrow (\tilde{\sigma}_2')^s \cdot (\tilde{\sigma}_1')^t$

$\sigma = (\sigma_1'', \sigma_2'', \tilde{\sigma}_1'', \tilde{\sigma}_2'')$

Verfiy($pk, \sigma, \overrightarrow{m}$):

$Parse\ \sigma = (\sigma_1, \sigma_2, \tilde{\sigma}_1, \tilde{\sigma}_2)$

$e(\sigma_1, \prod_{i \in I} \tilde{Y}_i) = e(\sigma_2, \tilde{g})$

$e(X \cdot \sigma_1 \cdot \prod_{i \in I} Y_i^{m_i}, \tilde{\sigma}_1) = e(g, \tilde{\sigma}_2)$

Purgeable Signature

委托与撤销属性基础凭证的具体实现

01

用户申请Eid

用户向RA请求有效eid以及身份证明。

02

用户申请凭证

从发行者处获得含属性、实体标识的凭证。

03

凭证更新及委托

用户可利用更新密钥进行凭证部分属性的委托。

04

凭证出示

出示凭证并通过零知识证明出示eid。

05

凭证验证

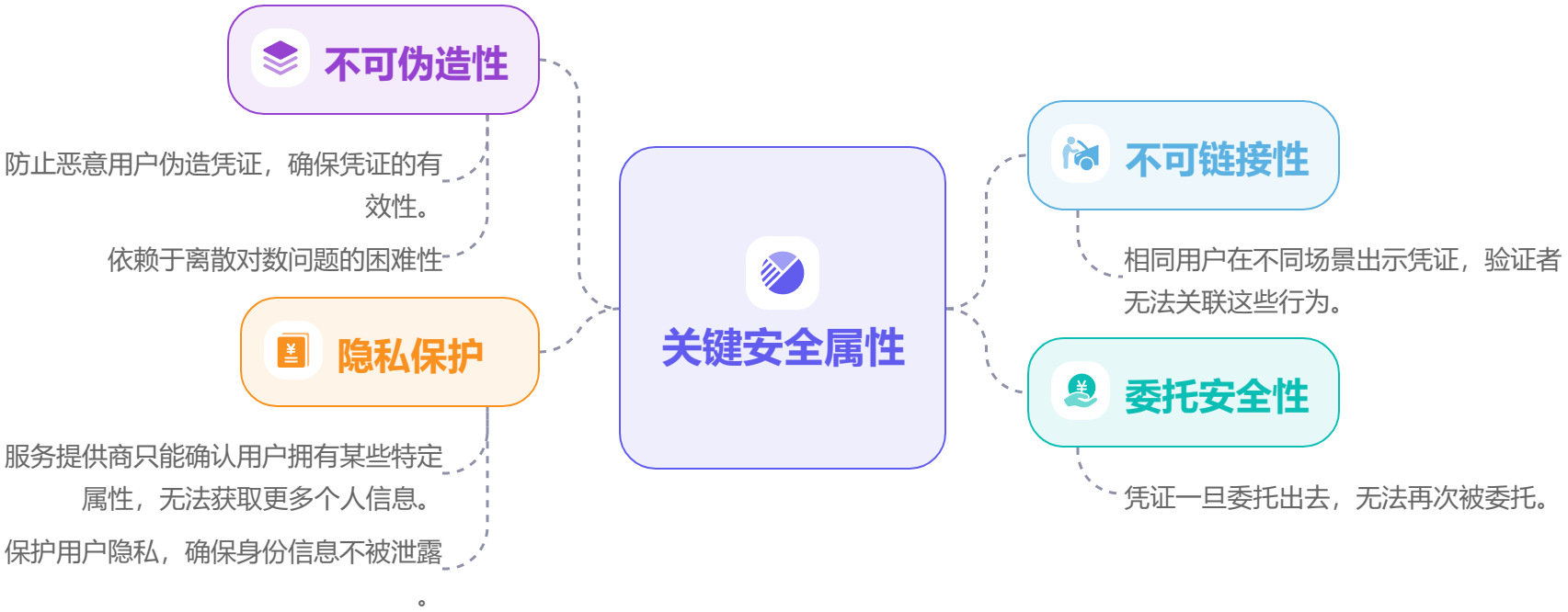
验证方对用户提交的零知识证明以及凭证进行验证，确认凭证的合法性、未撤销状态与所声明属性的真实性

06

撤销实体标识

撤销权威通过更新动态累加器和实体标识符集合，可撤销实体标识。

整体方案的安全性


关键安全属性
不可伪造性
防止恶意用户伪造凭证，确保凭证的有效性。
依赖于离散对数问题的困难性
隐私保护
服务提供商只能确认用户拥有某些特定属性，无法获取更多个人信息。
保护用户隐私，确保身份信息不被泄露。
不可链接性
相同用户在不同场景出示凭证，验证者无法关联这些行为。
委托安全性
凭证一旦委托出去，无法再次被委托。

实验结果与结论

05

性能评估

凭证发行效率

请求包含10个属性的凭证时，凭证发行部分约54.51毫秒，凭证获取则需要约105.46毫秒。

凭证撤销效率

撤销包含50个属性的凭证仅需65.17毫秒。

Systems	Protocol	$n = 10$	$n = 20$	$n = 30$
Our System	CredIssue	54.51	57.95	61.64
	CredObtain	105.46	109.16	114.12
[22]	CredIssue	15.87	17.26	18.60
	CredObtain	39.38	42.36	46.22

凭证发行效率(ms)

Algorithm	$N = 50$	$N = 100$	$N = 200$
CredRevoke	65.17	102.19	106.75

凭证撤销效率(ms)

性能评估

凭证委托速度

拥有10个属性凭证的用户可以在183.38毫秒内将新凭证委托给其他实体，即使属性数量增加到30个，整个委托过程也仅需不到193.49毫秒。

10 attributes in credential			
Protocol	I = 2	I = 5	I = 10
CredDelegate	173.05	177.53	183.38
CredReceive	156.73	160.25	164.29
20 attributes in credential			
Protocol	I = 2	I = 5	I = 10
CredDelegate	178.44	180.43	185.71
CredReceive	157.30	161.03	166.24
30 attributes in credential			
Protocol	I = 2	I = 5	I = 10
CredDelegate	184.67	186.41	193.49
CredReceive	157.98	161.87	167.19

性能评估

凭证出示与验证

用户可以高效地展示凭证上的属性子集，例如展示2、5或10个属性分别需要103.82毫秒、108.87毫秒或112.82毫秒，同时验证过程也相当迅速。

10 attributes in credential				
Systems	Protocol	$\mathcal{S} = 2$	$\mathcal{S} = 5$	$\mathcal{S} = 10$
Our System	CredShow	103.82	108.87	112.82
	CredVerify	245.77	247.69	251.24
	CredShow*	105.86	108.55	112.15
	CredVerify*	249.46	256.34	260.25
[22]	CredShow	23.30	24.62	26.13
	CredVerify	90.27	91.23	92.54
20 attributes in credential				
Systems	Protocol	$\mathcal{S} = 2$	$\mathcal{S} = 5$	$\mathcal{S} = 10$
Our System	CredShow	105.30	109.43	114.56
	CredVerify	246.51	248.55	251.69
	CredShow*	106.59	108.89	112.77
	CredVerify*	250.34	256.94	261.12
[22]	CredShow	24.90	25.75	27.22
	CredVerify	92.82	93.54	95.17
30 attributes in credential				
Systems	Protocol	$\mathcal{S} = 2$	$\mathcal{S} = 5$	$\mathcal{S} = 10$
Our System	CredShow	106.62	110.45	115.37
	CredVerify	247.10	249.21	252.48
	CredShow*	107.57	109.42	113.53
	CredVerify*	250.80	257.79	261.96
[22]	CredShow	25.34	26.27	27.87
	CredVerify	94.11	95.56	96.89

总结

01

提出 Purgeable Signature：一种结合可编辑性与不可链接性的签名方案。

02

在PS的基础上提出了一种可委托和可撤销的基于属性的凭证，允许用户将部分属性的证书委托给其他实体，以及有选择地披露其证书的属性子集

03

实现了原型系统，评估了方案在各方面的性能，证明了方案的效率以及可行性。