可共享驗證的特定驗證者方法設計

指導老師：林韓禹
專題組員：林弈呈、潘昱任

Abstract

- 本研究SV-SDVS只允許被授權的特定驗證者使用他/她的私鑰來進行驗證，因為匿名的關係，導致特定驗證者無法使用自己產生的副本去使第三方相信。
- 本研究SV-SDVS允許多個特定驗證者合作驗證一簽章，並且不會增加其簽章的大小。
- 本研究同時也證明此SV-SDVS方法之安全性，滿足了不可偽造性、不可轉移性及來源隱密性。

Introduction

- 數位簽章方法具有三個性質：不可否認性、來源驗證性及完整性。數位簽章的真實性可被所有擁有私鑰的簽署者驗證。
- 數位簽章方法在公開金鑰系統中是一個非常重要的技術。然而，在某些特殊應用上卻是不適用的，就像是電子發票。
- Saeednia等人發展出SDVS，也帶出私鑰在指定驗證者驗證的概念。
- 本研究SV-SDVS不單單只把驗證者限縮在少數人，而是使驗證者可以群體的方式驗證

Preliminaries

（一）雙線性配對(Bilinear Pairing)

令$(G_1,+)$和$(G_2,\times)$是兩個以大質數q為排序依據的加法和乘法群，e: $G_1 \times G_1 \to G_2$是一雙線型映射，滿足以下性質：

1.雙線性(Bilinearity)

$e(P_1+P_2,Q)=e(P_1,Q)e(P_2,Q)$;
$e(P,Q_1+Q_2)=e(P,Q_1)e(P,Q_2)$;
$e(aP,bQ)=e(P,Q)^{ab}$;

2.非退化性(Non-degeneracy)

如果P是G_1的生成元，則$e(P,P)$是G_2生成元。

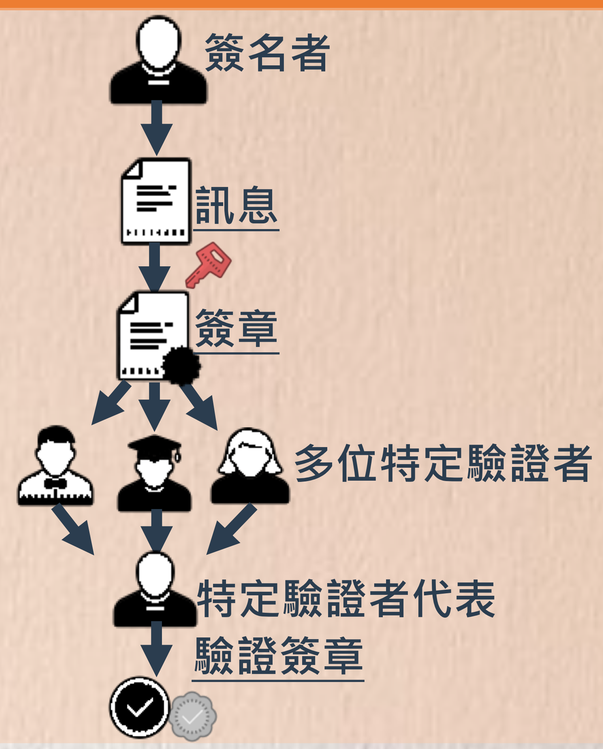
3.可計算性(Computability)

對於任意的$P,Q \in {G_1}^2$，存在一個有效率的多項式演算法能夠計算$e(P,Q)$。

（二）雙線性Diffie-Hellman問題(BDHP)

令$a,b,c \in {Z_q}^*$為未知數，給定$P,aP,bP,cP \in G_1$，計算abc且滿足$e(P,P)^{abc} \in G_2$為解BDH問題。

Architecture



SV-SDVS

〈Setup〉公開參數包含$\{G_1,G_2,q,P,e,h_1,h_2\}$。

〈SDVS-Gen〉首先令$VG=\{U_1,U_2,\cdots,U_n\}$為一組特定驗證者，$x_i \in Z_q$，$Y_i=x_iP$。為了簽署訊息$m$給所有$U_v$，$SG$隨機挑選了$t \in {Z_q}^*$來計算

$$R=tP$$
$$W_i=tY_{V_i}$$
$$Z=e\left(x_s\sum_{i=1}^{n}Y_{v_i},h_2\left(\sum_{i=1}^{n}W_i\right)\right)$$
$$\sigma=e(\left(x_s+h_1(m,Z,R)\right)R,P)$$

訊息m的SV-SDVS為$\delta=(R,\sigma)$，傳送給所有特定驗證者。

〈SDVS-Verify〉接收到訊息m以及SV-SDVS $\delta=(R,\sigma)$，U_{v_i}首先計算：

$$Z_i=e(x_{v_i}Y_i,h_2(x_{v_i}R))$$

將U_{v_i}算出的Z_i傳遞給U_v代表，U_v代表再將所有的Z_i相乘得到Z值：

$$Z=\prod_{U_j \in VG}Z_i$$
$$\sigma=e(\left(Y_s+h_1(m,Z,R)\right)P,R)$$

最後，我們將證明σ等式的正確性：

$$\sigma=(\left(x_s+h_1(m,Z,R)\right)R,P)$$
$$=(\left(x_s+h_1(m,Z,R)\right)P,R)$$
$$=(\left(Y_s+h_1(m,Z,R)\right)P,R)$$

推導完成後，等號右邊與σ等式相符合。

〈Transcript-Simulation〉為了產生另一個對訊息m有效的SV-SDVS副本，U_v代表首先選擇一$R' \in {}_RG_1$並傳遞給每位U_{v_i}計算：

$$Z_i'=e(x_{v_i}Y_s,h_2(x_{v_i}R'))$$

將U_{v_i}算出的Z_i'傳遞給U_v代表，U_v代表再將所有的Z_i'相乘得到Z'值：

$$Z'=\prod_{U_j \in VG}Z_i'$$
$$\sigma'=e(\left(Y_s+h_1(m,Z',R')\right)P,R')$$

至此，$\delta'=(R',\sigma')$是訊息m的另一個有效SV-SDVS。

Comparison

群體人數 / 項目	N=1	N=2	N=5	N=10
簽章大小	|G1|+|G2|	|G1|+|G2|	|G1|+|G2|	|G1|+|G2|
簽名者計算量	2B+4M+2H	2B+5M+2H	2B+8M+2H	2B+13M+2H
特定驗證者代表clerk計算量	無	B	B	B
每一特定驗證者計算量	1B+2M+1H	1B+2M+1H	1B+2M+1H	1B+2M+1H

B:雙線性配對計算量　M:乘法計算量　H:Hash函數計算量　N:特定驗證者群體之人數