（t，n）门限 ECDSA 签密的安全混淆方法

严莹子[1]
YAN Ying-zi

摘 要 为保护恶意模型下门限签密算法中参与方的私钥安全，本文对混淆在 MPC（安全多方计算）上的应用进行了研究，结合（t，n）门限 ECDSA（椭圆曲线数字签名算法）和 ElGamal 加密体制构造了一种特殊签密算法的混淆方案，运用加法同态加密、茫然传输、承诺机制、零知识证明、秘密共享等密码学原语达成了方案在恶意模型下的安全性，在 DDH（判定 Diffie-Hellman）假设下证明了当恶意参与方人数不超过 t-1 时，混淆后的签密具有不可伪造性，混淆达到虚拟黑盒安全。

关键词 虚拟黑盒混淆；签密；ECDSA；门限签名；安全多方计算

doi：10.3969/j.issn.1672-9528.2021.01.008

0 引言

混淆算法可以看为一种在不改变程序功能情况下掩盖其内部逻辑的转换机制。Barak[1] 等人于 2001 年已经证实，不存在通用的黑盒混淆方法。如今，研究某类具体功能函数的混淆方法成为混淆领域的一大热点。Hohenberger 等人[2] 于 2007 年提出了首个对复杂密码函数的混淆，构造了一类特殊函数线性加密算法的重加密函数并对此进行了混淆。Hada 等人[3] 于 2010 年提出了一种对签密 (Encrypted Signature, ES) 函数的混淆，方案中的签密是用 waters 签名[4] 与 linear 加密[5] 组合而成。在 DBDH（Decisional Bilinear Diffie-Hellman）假设[6-7] 和 DL（Decisional Linear）假设下，Hada 证明了混淆满足虚拟黑盒特性。使用类似的技巧，Shi 等人[8] 于 2015 年提出了一个对加密群签名的虚拟黑盒混淆，能够抵抗群成员的勾结。除虚拟黑盒混淆之外，在有些研究中提出了一些另外的安全模型，比如虚拟灰盒混淆[9]、最可能混淆[10]、不可区分混淆[11] 等，从不同安全侧面研究了混淆的可能性和安全性，但这些模型都弱化了对理想混淆的安全性要求。

本文研究了对门限签密函数（Threshold Encrypted Signature）的虚拟黑盒混淆。门限签密算法是门限数字签名算法[12] 与加密算法的结合。签密将这两种算法融合在了一个逻辑步骤之内，可以同时保证传输数据的机密性与认证功能。在（t，n）门限签密协议中，有发起者和决策群组，决策群组由 n 个人组成。发起者向决策群组发送一个文件，如果决策群组中同意签名的成员达到 t 人，那么这 t 个人就可以代表决策群组生成一个对该文件的签密。该签密是由决策群组的签名私钥以及发起者的加密公钥生成的，因此只有发起者可以对其进行解密和验证。

对于（t，n）门限签密协议，最直观的实现方法就是将（t，n）门限签名算法与加密算法线性组合起来，但这样的实现使得该算法的输入必须包含发起者的加密公钥以及决策群组中某些参与方的签名私钥。在恶意模型下，一旦运行程序的主机被恶意攻击者入侵，签名者的私钥就会被泄露，这会对签名的不可伪造性造成威胁。因此本文构造了一个特殊的（t，n）门限签密程序，并且对其进行虚拟黑盒混淆，达到了保护签名者私钥的目的。

1 预备知识

1.1 ElGamal 密码体制

ElGamal[13] 是一个基于$(\mathbb{Z}_p^*, \cdot)$上的离散对数问题的公钥密码体制，p 是一个素数，g 是$\mathbb{Z}_p^*$的一个本原元。可以将 ElGamal 加密体制分为三个部分：密钥生成、加密和解密。

ElGamal 密码体制：

EKG(1^n)：

（1）随机选择一个整数 x，使得$1 \le x \le q-2$；

（2）计算$h := g^x$；

（3）输出加密公钥$pk_e = h$以及加密私钥$sk_e = x$。

Enc(pk_e, m)：

（1）将消息 m 映射为$\mathbb{Z}_q^*$上的元素（也就是将 m 表示为范围$\{0,1,\ldots,q-1\}$的数）；

（2）随机选择 Z，$1 \le Z \le q-2$（每次加密一条信息 m 都随机选择一个新的 Z）；

1. 同济大学电子与信息工程学院 上海 201804

（3）计算$s:=pk_e{}^{z}$ ；

（4）计算输出密文 $c=(c_1,c_2)=(g^z,\ s\cdot m)$ 。

Dec(sk_e,c)：

计算输出明文$m=c_2/c_1^{1/sk_e}$ 。

引理 1 在 DDH 假设下，ElGamal 密码体制具有不可区分性。

1.2 ECDSA

椭圆曲线数字签名算法[14-15]（Elliptic Curve Digital Signature Algorithm, ECDSA）是 DSA 算法[16]的一种演变，其安全性依赖于有限域上的椭圆曲线离散对数问题（ECDLP）的难解性。ECDSA 于 1999 年成为 ANSI 标准，并于 2000 年成为 IEEE 和 NIST 标准[17]，是目前应用最广泛的签名体制之一。

椭圆曲线的参数表示为$(\mathbb{G},G,q)$，其中$\mathbb{G}$是椭圆曲线上 q 个点组成的群，G 是这个群的生成元。消息 m 在私钥 sk 下的 ECDSA 签名可以表示为$\sigma=(\mathrm{sig},r_x)$，其中：

$$\mathrm{sig}=\frac{H(m)+\mathrm{sk}\cdot r_x}{k}$$

k 是$\mathbb{Z}_q$上的随机数，r_x是椭圆曲线点 R=kG 的 x 坐标。在验证时，计算：

$$(r_x^{'},r_y^{'})=R^{'}:=\frac{H(m)\cdot G+r_x\cdot pk}{sig}$$

如果$(r_x^{'}\ mod\ q)=(r_x\ mod\ q)$则通过验证。

Doerner 等人[18]提出了一个（t，n）门限 ECDSA 方案，将签名 sig 拆分为了 t 个相加份额的子签名sig_i，每个sig_i由对应参与方P_i在各自的私钥sk_i下生成，表示如下：

$$\mathrm{sig}_i=v_i\cdot H(m)+w_i\cdot r_x$$
$$\sum v_i=k^{-1}$$
$$\sum w_i=k^{-1}\cdot sk$$
$$\sum_{i\in\mathbf{P}}\mathrm{sig}_i=k^{-1}\cdot H(m)+k^{-1}\cdot sk\cdot r_x=\mathrm{sig}$$

引理 2 在 CDH 假设下，Doerner 提出的（t，n）门限 ECDSA 方案在恶意参与方人数不超过 t-1 的情况下具有不可伪造性。

1.3 其他功能函数

Doerner 在构建（t，n）门限 ECDSA 的过程中提出并使用了如下功能函数：

（1）承诺函数$\mathcal{F}_{\mathrm{Com}}^{n}$：允许一个参与方对一条消息作出承诺并发送给其他参与方，稍后再揭示这条消息以证明承诺的真实性。承诺可以用基于哈希函数的方法来构建[19]。

（2）零知识证明$\mathcal{F}_{\mathrm{Com-ZK}}^{R_{\mathrm{DL}},n}$：允许一个参与方对椭圆曲线上一个点作出承诺并且向其他参与方保证自己知道这个点的离散对数， 稍后再揭示这个承诺的真实性[19][20]。零知识证明可以用 Schnorr 协议[21]来实现。

（3）两方乘法函数$\mathcal{F}_{2PMul}^{l}$：将两个求积向量转化为两个求和向量，可以用 COTe[22-23]来实现。

（4）多方乘法$\mathcal{F}_{nPMul}^{l}$：将 n 个求积向量转化为 n 个求和向量，可用$\mathcal{F}_{2PMul}^{l}$来实现。

（5）求逆函数$\mathcal{F}_{Inv}^{n,t,P}$：生成 t 个随机数$\{u_i\}_{i\in\mathbf{P}}\leftarrow\mathbb{Z}_q$、一个椭圆曲线点$\mathrm{R}=\sum_{i\in\mathbf{P}}u_i\cdot G$以及另外 t 个随机数$\{v_i\}_{i\in\mathbf{P}}\leftarrow\mathbb{Z}_q$，使得它们满足关系式$\sum_{i\in\mathbf{P}}v_i=\frac{1}{\sum_{i\in\mathbf{P}}u_i}$。这些功能函数使得 Doerner 构建的（t，n）门限 ECDSA 能达到恶意模型（被控制的参与方人数小于等于 t）下的安全性。

2 提出的方案

本文基于 Doerner 等人提出的（t，n）门限 ECDSA 算法和 ElGamal 加密算法，构造了一个特殊的 ES 程序，使得“先在消息 m 上生成门限签名，然后对签名进行加密”在功能上等同于“先对签名私钥进行加密，再用私钥的密文在消息 m 上生成门限签名”。前者是一个 ES 程序，后者是一个混淆后的 ES 程序。

给出公共参数：素数 q，有限域$\mathbb{F}_q$上的椭圆曲线$\mathbb{G}$，$\mathbb{G}$的生成元G，$\mathbb{Z}_q^*$的生成元g，参与总人数 n，签名人数阈值 t，哈希函数 H，加法同态加密函数 E。

在运行 ES 程序之前首先需要运行 Setup 程序如下：

Setup(1^n)：

（1）每个参与方$\mathcal{P}_i$采样一个 t-1 次随机多项式p_i ；

（2）每个参与方$\mathcal{P}_i$计算

$$p(i):=\sum_{j\in[1,n]}p_j(i);$$

（3）计算：

$$T_i:=p(i)\cdot G;$$

并将$(p(i),T_i,\mathcal{P}_i)$输入$\mathcal{F}_{\mathrm{Com-ZK}}^{R_{\mathrm{DL}},n}$，当所有参与方都提交证明之后，再揭示证明；

（4）如果 $\sum_{j\in\mathbf{J}^x}\lambda_j^{\mathbf{J}^x}(0)\cdot T_j=\sum_{j\in\mathbf{J}^{x+1}}\lambda_j^{\mathbf{J}^{x+1}}(0)\cdot T_j,x\in[1,n-1]$,

那么$\mathrm{pk}:=\sum_{j\in\mathbf{J}}\lambda_j^{\mathbf{J}}(0)\cdot T_j$， 否则终止程序；

（5）运行$(pk_e,sk_e)\leftarrow ElGamal.EKG(1^n)$，其中$sk_e=x$，$pk_e=\mathrm{h}=g^x$ ；

（6）输出pk，$p(i)$，pk_e，sk_e 。

Setup 程序仅需运行一次，其输出的密钥可用于多次运行 ES 程序。Setup 输出中的$p(i)$可以看为签名私钥sk_i的一种形式，$p(i)$泄露就相当于sk_i泄露。

除了上述公共参数$(\mathbb{G},G,q,g,n,t,H,E)$以及 Setup 的输出之外，再给出 t 人组成的签名群组 P，就可以运行 ES 程序。为了书写方便，在后续协议中省略公共参数。

我们定义一类实现 ES 功能的电路$\mathcal{C}_{ES}=\{\mathcal{C}_n\}_{n\in\mathbb{N}}$，$\mathcal{C}_n$是电路$\mathcal{C}_{p(i),pk_e}$的集合，而每个$\mathcal{C}_{p(i),pk_e}$都是$F^{P}_{p(i),pk_e}$的 naïve 实现，使得我们可以从$\mathcal{C}_{p(i),pk_e}$中提取出$(p(i),pk_e)$。因此我们需要为$\mathcal{C}_{ES}$构造一个混淆器$Obf_{ES}$。

ES 函数$\mathrm{F}^{\mathrm{P}}_{\mathrm{p(i),pk,pk_e}}$可提供以下功能：

$ES^{P}_{p(i),pk_e}(m)$:

（1）$sk_i \coloneqq \lambda_i^{\mathrm{P}}(0)\cdot p(i)$ ；

（2）运行

$\acute{o}=(\mathrm{sig},r_x)=((H(m)+sk\cdot r_x)\cdot k^{-1},r_x)\leftarrow \mathrm{Sign}\ (sk_i,m)$ ；

（3）运行 $C=(g^{z},\ pk_e{}^{z}\cdot \mathrm{sig},r_x)\leftarrow \mathrm{Enc}\ (pk_e,\acute{o})$ ；

（4）输出C 。

注意，原本在 ElGamal 加密中需要先把消息 m 映射为$\mathbb{Z}_q^*$上的元素。在这里，由于 sig 原本就是$\mathbb{Z}_q^*$上的元素，因此不必再做映射。

$ES^{P}_{p(i),pk_e}(m)$的输出可以表示为：

$$\frac{H(m)\cdot pk_e{}^{z}+sk\cdot pk_e{}^{z}\cdot r_x}{k}$$

其中$sk\cdot pk_e{}^{z}$正好包含于$\mathrm{Enc}\ (pk_e,sk)$的输出，这样就达到了用混淆技术保护私钥的目的。接下来，我们需要构造（t，n）门限 ECDSA 的相加份额子签名sig_i，使得：

$$\mathrm{sig}_i=y_i\cdot H(m)+w_i\cdot r_x$$
$$\sum y_i=k^{-1}\cdot pk_e{}^{z}$$
$$\sum w_i=k^{-1}\cdot sk\cdot pk_e{}^{z}$$

在构建过程中会使用$\mathcal{F}^{n}_{\mathrm{Com}}$，$\mathcal{F}^{R_{\mathrm{DL}},n}_{\mathrm{Com-ZK}}$，$\mathcal{F}^{l}_{2PMul}$和$\mathcal{F}^{n,t,P}_{Inv}$，可参考 1.3 的内容。

本文基于 ElGamal 加密方案构造了一个新的 n 方 ElGamal 加密，如下：

$\mathrm{EncN}(pk\ ,m_i)$:$\mathrm{ES}^{\mathrm{P}}_{\mathrm{pk,p(i),pk}}\ (\mathrm{m})$

（1）t 人组成的群组中，每人生成一个随机数$z_i\in\mathbb{Z}_q^*$。

（2）设有加法同态密码体制（比如 Paillier 算法[24]），存在有效算法$\oplus$使得加密系统的加密函数 E 与解密函数 D 满足关系式：

$$x+y=D(E(x)\oplus E(y))$$

P 中每个人计算且公布$E(z_i)$。

（3）参与者P_i取回所有$E(z_i)$，计算：

$$Z\coloneqq D(E(z\ )\oplus\cdots\oplus(z_i)\oplus\cdots\oplus E(z\ ))$$

注意，此处满足$Z=\sum_{i\in P}z_i$，且$Z\in\mathbb{Z}_q^*$。

（4）计算$s\coloneqq pk_e{}^{z}$ 。

（5）参与者P_i计算输出密文：

$$(c_1,c_{2i})=(g^{z},\quad s\cdot m_i)=(g^{z},\quad pk_e{}^{z}\cdot m_i)$$

（6）由于$s=pk_e{}^{z}=pk_e{}^{\sum z_i}=\prod pk_e{}^{z_i}$，我们用$\mathcal{F}^{l}_{nPMul}$构造$\hat{z_i}$，满足$\sum\hat{z_i}=\prod pk_e{}^{z_i}$ 。

（7） 输出$(\hat{z_i},c_1,c_{2i})$ 。

给定一个电路$C_{p(i)\,pk_e}$，构建其混淆器Obf_{ES}如下：

（1） 提取参数$p(i),pk_e$。

（2）t 人组成的群组P中，每人计算：

$$\mathrm{sk}_i\coloneqq\lambda_i^{\mathrm{P}}(0)\cdot p(i)$$

（3）每个参与方P_i运行：

$$(\hat{z_i},c_1,c_{2i})\leftarrow EncN(pk_e,\mathrm{sk}_i)$$

（4）构造并且输出一个混淆电路Obf_{ES}，它包含公共参数以及$(\{\hat{z_i}\}_{i\in P},c_1,\{c_{2i}\}_{i\in P})$。注意，这里虽然$Obf_{ES}$包含了参数$(\{\hat{z_i}\}_{i\in P},c_1,\{c_{2i}\}_{i\in P})$，但每个参与方的视角下只能访问参数$(\hat{z_i},c_1,c_{2i})$。我们用$Obf^{i}_{ES}$来表示参与方$P_i$视角下的混淆电路。

当输入消息 m 时：

（a） 调用$\mathcal{F}^{n,t}_{Inv}$，每个参与方得到(u_i,v_i,R)，满足$\sum u_i=k$，$\sum v_i=1/k$，$R=(r_x,r_y)=kG$。

（b）参与方两两之间调用$\mathcal{F}^{\ell}_{\mathrm{2PMul}}$，其中$l=4$，我们用 Pi 和 Pj 来表示两个参与方，$P_i$的输入为$\{\hat{z_i},v_i,c_{2i},v_i\}$，$P_j$的输入为$\{v_j,\hat{z_j},v_j,c_{2j}\}$；他们得到的输出分别为$\{y_i^{j,1},y_i^{j,2},w_i^{j,1},w_i^{j,2}\}$和$\{y_j^{i,1},y_j^{i,2},w_j^{i,1},w_j^{i,2}\}$。过程如图 1 所示。

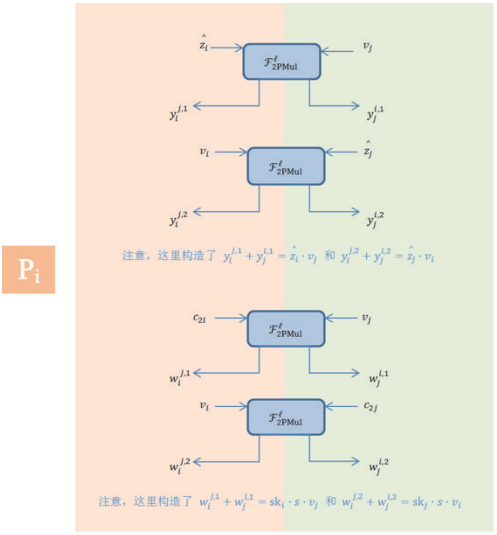

图 1 两个参与方调用两方乘法函数的过程

（c）计算：

$$y_i\coloneqq\hat{z_i}\cdot v_i+\sum_{j\in\mathbf{P}\backslash\{i\}}(y_i^{j,1}+y_i^{j,2})$$

注意，此处构造了$\sum y_i=\frac{s}{k}$ 。

计算：

$$w_i\coloneqq c_{2i}\cdot v_i+\sum_{j\in\mathbf{P}\backslash\{i\}}(w_i^{j,1}+w_i^{j,2})$$

注意，此处构造了$\sum w_i=\frac{sk\cdot s}{k}$ 。

（d）每个参与者P_i计算且输出：

$$\mathrm{sig}_i := H(m)\cdot y_i + r_x \cdot w_i$$

（e）计算：

$$sig := \sum_{i\in \mathbf{P}} \mathrm{sig}_i$$

$$\sigma := (\mathrm{sig}, r_x)$$

（f）Obf_{ES}输出$(\mathrm{c}_1, \mathrm{sig}, \mathrm{r}_\mathrm{x}\ (c_1, sig, r_x)$。

3 方案的分析

3.1 正确性分析

签密的接收者可以用pk和$sk_e = x$对(c_1, sig, r_x)进行解密以及验证：

（1）计算：

$$sig' = sig/c_1^x$$

$$= \sum_{i\in \mathbf{P}} (H(m)\cdot y_i + r_x \cdot w_i)/(g^x)^Z$$

$$= (H(m)\cdot \sum_{i\in \mathbf{P}} y_i + r_x \cdot \sum_{i\in \mathbf{P}} w_i)/h^Z$$

$$= (H(m)\cdot \frac{s}{k} + r_x \cdot \frac{sk\cdot s}{k})/\mathrm{s}$$

$$= H(m)\cdot \frac{1}{k} + r_x \cdot \frac{sk}{k}$$

（2）计算：

$$(r_x', r_y') = R' := \frac{H(m)\cdot G + r_x \cdot pk}{sig'}$$

（3）如果$(r_x' \ mod\ q) = (r_x\ mod\ q)$则输出1，否则输出0。

3.2 安全性分析

定义 1 平均情况安全混淆（Average Case Virtual Black-box Poverty, ACVBP[2]）：电路$\mathcal{C}$的一个混淆器Obf如果达到以下条件，那么这个Obf满足ACVBP：存在PPT（probabilistic polynomial-time）预言机作为模拟器S，使得：

$$\left|\Pr\begin{bmatrix} C\leftarrow \mathcal{C}_n; \\ C'\leftarrow \mathrm{Obf}(C); \quad :b=1 \\ b\leftarrow D^{\ll C\gg}(C'\ z)\end{bmatrix} - \Pr\begin{bmatrix} C\leftarrow \mathcal{C}_n; \\ C''\leftarrow \mathrm{S}^{\ll C\gg}(1^n, z); \quad :b=1 \\ b\leftarrow D^{\ll C\gg}(C''\ z)\end{bmatrix}\right| < \frac{1}{p(n)} \quad (1)$$

式中，D为任意PPT预言机区分器，$p(\cdot)$为任意多项式$n\in \mathbb{N}$，$z\in \{0,1\}^{poly(n)}$。

定义 2 基于依赖预言机的平均情况安全混淆（ACVBP w.r.t. Dependent Oracles[3]）：$T(\mathcal{C})$是一个在电路$\mathcal{C}$上的依赖预言机的集合。电路$\mathcal{C}$的混淆器Obf如果达到以下条件，那么该Obf满足ACVBP w.r.t. Dependent Oracles：存在一个PPT预言机S（模拟器），使得：

$$\left|\Pr\begin{bmatrix} C\leftarrow \mathcal{C}_n; \\ C'\leftarrow \mathrm{Obf}(C); \quad :b=1 \\ b\leftarrow D^{\ll C,T(C)\gg}(C', z)\end{bmatrix} - \Pr\begin{bmatrix} C\leftarrow \mathcal{C}_n; \\ C''\leftarrow \mathrm{S}^{\ll C\gg}(1^n, z); \quad :b=1 \\ b\leftarrow D^{\ll C,T(C)\gg}(C'', z)\end{bmatrix}\right| < \frac{1}{p(n)} \quad (2)$$

式中，D为任意PPT预言机区分器，$p(\cdot)$为任意多项式，$n\in \mathbb{N}$，$z\in \{0,1\}^{poly(n)}$。$D^{\ll C,T(C)\gg}$表示D可以访问所有包含$\mathcal{C}$和$T(\mathcal{C})$的取样预言机。

定理 1 令$T(C_{p(i),pk_e})$为签名预示机$S_{p(i)}$，如果一个签密电路$\mathcal{C}_{ES}$的混淆器Obf_{ES}满足基于依赖预言机T的ACVBP，那么ES程序具有不可伪造性可推出Obf_{ES}也具有不可伪造性。

证 明 假设存在敌手A能攻破Obf_{ES}的不可伪造性。构造一个可以取样访问$T(C_{p(i),pk_e})$的区分器D，D能区分敌手A是否成功攻破了Obf_{ES}的不可伪造性，如下：

（1）输入一个电路C和附加参数z（C可能是混淆电路也可能是模拟电路）。

（2）取样访问$C_{p(i),pk_e}$的$Setup(1^n)$，得到(pk, pk_e)。

（3）取样访问$S_{p(i)}$来模拟：

$$(m, \sigma, Q) \leftarrow A^{\ll S_{p(i)}\gg}(pk, pk_e, C, z)$$

（4）如果(m, σ)能通过签名验证并且$m\notin Q$，则输出1。

如果C是混淆电路，那么D输出1的概率等同于A攻破Obf_{ES}的不可伪造性的概率，在前面的假设下这个概率是不可忽略的。但如果C是模拟电路，那么这个概率应该是可忽略的。因此如果A能攻破Obf_{ES}的不可伪造性，则可以利用A来攻破ES程序的不可伪造性。

定理 2 令$T(C_{p(i)\ pk_e})$为签名预示机$S_{p(i)}$，在DDH假设下，签密电路$\mathcal{C}_{ES}$的混淆器Obf_{ES}满足基于依赖预言机T的ACVBP。

证 明 可以通过参数$(\{\hat{z_i}\}_{i\in P}, c_1, \{c_{2i}\}_{i\in P})$来确定一个混淆电路$Obf_{ES}$，它在每个参与方$P_i$的视角下包含的参数为$(\hat{z_i}, c_1, c_{2i})$。因此可以构造一个模拟器S来模拟$Obf_{ES}^i$的参数。

假设参与方P_i的模拟器S_i可以采样访问原始电路$C_{p(i),pk,pk_e}$：

（1）从原始电路中提取参数pk_e。

（2）随机选择$Junk\leftarrow \mathbb{Z}_q^*$。

（3）运行$(\hat{z_i}, c_1, c_{2i}) \leftarrow \mathrm{EncN}\ (pk_e, Junk)$。

（4）输出$(\hat{z_i}, c_1, c_{2i})$。

为了通过反证法证明模拟器S的输出分布与真实电路输出分布相同，这里给出两个概率如下：前者是给出真实电路的输出分布时D输出1的概率，后者是给出模拟电路的输出分布时D输出1的概率。$D^{\ll CS\gg}$代表D能采样访问电路$C_{p(i),pk,pk_e}$与模拟器S。为了产生矛盾，我们先假设区分器D能分辨以下这两个分布的概率是不可忽略的。

$$\Pr\begin{bmatrix} (pk_e, p(i)) \leftarrow \mathrm{Setup}(1^n) \\ \mathrm{sk}_i \leftarrow \lambda_i^{\mathrm{P}}(0)\cdot p(i) \\ \left(\hat{z_i}, c_1, c_{2i}\right) \leftarrow \mathrm{Enc}(pk_e, \mathrm{sk}_i) \\ b\leftarrow D^{\ll CS\gg}\left(\hat{z_i}, c_1, c_{2i}\right) \\ b=1\end{bmatrix}$$

$$\Pr\left[\begin{array}{c} pk_e \leftarrow \mathrm{Setup}(1^n) \\ Junk \leftarrow \mathbb{G} \\ \left(\hat{z_i}, c_1, c_{2i}\right) \leftarrow \mathrm{Enc}(pk_e, Junk) \\ b \leftarrow D^{\ll CS \gg}\left(\hat{z_i}, c_1, c_{2i}\right) \\ b = 1 \end{array}\right]$$

构造两个敌手(A_1, A_2)，他们可以通过如下步骤利用区分器 D 来打破门限 ECDSA 的不可区分性。

A_1产生两条消息(m_1, m_2)以及一个附加参数h：

（1）运行$\left(pk \quad p(i)\right) \leftarrow \mathrm{Setup}(1^n)$；

（2）$\mathrm{sk}_i \leftarrow \lambda_i^{\mathrm{P}}(0) \cdot p(i)$；

（3）$Junk \leftarrow \mathbb{G}$；

（4）令$m_1 = \mathrm{sk}_i$，$m_2 = Junk$，$h = pk$。

给出一个密文 c（可能是 m_1 的密文也可能是 m_2 的），加密公钥pk_e，敌手A_2可以利用区分器 D 来区分 c 对应的明文是 m_1 和 m_2：

（1）解析$c = (\hat{z_i}, c_1, c_{2i})$；

（2）模拟$D^{\ll CS \gg}\left(\hat{z_i}, c_1, c_{2i}\right)$；

（3）输出 D 的输出。

对应上面给出的两个概率，如果 c 对应的明文是 m_1，则 A_2 输出 1 的概率等同于前面的概率；如果 c 对应的明文是 m_2，则 A_2 输出 1 的概率等同于后面的概率。由于两个概率的差距不可忽略，所以 A_2 攻破了加密的不可区分性。这和前面的引理 1 矛盾。

推论 1 签密电路C_{ES}的混淆器Obf_{ES}具有不可伪造性。

4 结论

本文提出了一种对（t，n）门限签密协议的混淆方案，该方案在恶意参与方人数不超过 t-1 的情况下具有不可伪造性，能有效保护参与方的签名私钥。当恶意参与方不超过 t-1 个时，未混淆的（t，n）门限 ECDSA 签密协议具有暴露私钥sk_i的风险。在未混淆的协议中，多次签名只会运行一次 Set-up，也就是说，虽然少于 t 个sk_i无法恢复出联合私钥sk，但如果相同的群组 P 多次进行签名，并且恶意参与方群组和之前并不完全重复，那么就有可能使所有私钥sk_i暴露，从而攻破（t，n）门限 ECDSA 签密的不可伪造性。本文提出的混淆方案本质上是将sk_i的隐私性转移到了$\hat{z_i}$上，虽然即使有 t-1 个恶意参与方，即他们视角下的参数$(\hat{z_i}, c_1, c_{2i})$被泄露，也不会影响协议的安全性，因为每一次签名都会生成不同的$\hat{z_i}$。本方案还存在以下不足：本方案多次调用乘法函数，即将乘积分量转化为加法分量的函数，因此在效率上还有待提升。

参考文献：

[1] Barak B, Goldreich O, Impagliazzo R, et al· On the (im) possibility of obfuscating programs[J]· Journal of the ACM (JACM), 2012, 59(2): 1-48·

[2] Hohenberger S, Rothblum G N, Vaikuntanathan V· Securely obfuscating re-encryption[C]//Theory of Cryptography Conference· Springer, Berlin, Heidelberg, 2007: 233-252·

[3] Hada S· Secure obfuscation for encrypted signatures[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques· Springer, Berlin, Heidelberg, 2010: 92-112·

[4] Waters B· Efficient identity-based encryption without random oracles[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques· Springer, Berlin, Heidelberg, 2005: 114-127·

[5] Boneh D, Boyen X, Shacham H· Short group signatures[C]// Annual International Cryptology Conference· Springer, Berlin, Heidelberg, 2004: 41-55·

[6] Joux A· A one round protocol for tripartite Diffie–Hellman[C]//International algorithmic number theory symposium· Springer, Berlin, Heidelberg, 2000: 385-393·

[7] Diffie W, Hellman M· New directions in cryptography[J]· IEEE transactions on Information Theory, 1976, 22(6): 644-654·

[8] Shi Y, Zhao Q, Fan H, et al· Secure obfuscation for encrypted group signatures[J]· PLoS One, 2015, 10(7): e0131550·

[9] Bitansky N, Canetti R, Kalai Y T, et al· On virtual grey box obfuscation for general circuits[J]· Algorithmica, 2017, 79(4): 1014-1051·

[10] Goldwasser S, Rothblum G N· On best-possible obfuscation[C]//Theory of Cryptography Conference· Springer, Berlin, Heidelberg, 2007: 194-213·

[11] Brzuska C, Mittelbach A· Indistinguishability obfuscation versus multi-bit point obfuscation with auxiliary input[C]// International Conference on the Theory and Application of Cryptology and Information Security· Springer, Berlin, Heidelberg, 2014: 142-161·

[12] Desmedt Y· Society and group oriented cryptography: A new concept[C]//Conference on the Theory and Application of Cryptographic Techniques· Springer, Berlin, Heidelberg, 1987: 120-127·

[13] ElGamal T· A public key cryptosystem and a signature scheme based on discrete logarithms[J]· IEEE transactions on information theory, 1985, 31(4): 469-472·

（下转第 39 页）

表 1 系统测试结果

操作名称	具体操作	预期结果	实际结果	是否通过
主页面访问	输入网站主页面地址，并点击各个链接。	能正确显示主页并能从主页链接顺利转到相应详情页	与预期结果一致	通过
注册	在注册页面进行注册，注册时输入违法字符一次	正常注册能够成功，输入违法字符注册失败	与预期结果一致	通过
登录	输入注册的账号密码进行登录	登录成功返回主页	与预期结果一致	通过
旅游攻略分享	在旅游攻略页面点击分享，然后写一篇攻略点击上传	上传成功，返回旅游攻略详情页能看见自己的帖子	与预期结果一致	通过

5 结语

该系统采用了最先进的 SpringBoot 框架，在简化开发的同时让后期的维护升级变得更加简单。本文设计并实现的旅游资源管理网站，不仅方便了人们的出行游玩，也极大地推动了旅游业的发展。本系统是在“互联网 + 旅游”上的初步尝试，之后的工作是加入一些如“组团行”之类的功能。

参考文献：

[1] 范凌云 · 基于 MVVM 框架的旅游网站的设计与实现 [D]· 北京 : 北京交通大学 ,2016·

[2] 熊永平 · 基于 SpringBoot 框架应用开发技术的分析与研究 [J]· 电脑知识与技术 ,2019,15(36):76-77·

[3] 胡涛 , 兰全祥 · 基于 Spring Cloud 的西安旅游网站的设计与实现 [J]· 信息技术与信息化 ,2020(9):65-67·

[4] 王丹 , 孙晓宇 , 杨路斌 , 等 · 基于 SpringBoot 的软件统计分析系统设计与实现 [J]· 软件工程 ,2019,22(3):40-42·

[5] 张雷 , 王悦 · 基于 SpringBoot 微服务架构下的 MVC 模型研究 [J]· 安徽电子信息职业技术学院学报 ,2018,17(4):1-9·

【作者简介】

孙岩（1997—），男，黑龙江哈尔滨人，硕士研究生，研究方向：自然语言处理；

李晶（1968—），通讯作者，女，黑龙江桦南人，研究方向：数据与数据挖掘。

（收稿日期：2020-10-10 修回日期：2020-11-03）

（上接第 36 页）

[14] Johnson D, Menezes A, Vanstone S· The elliptic curve digital signature algorithm (ECDSA)[J]· International journal of information security, 2001, 1(1): 36-63·

[15] Brown D R L· Sec 2: Recommended elliptic curve domain parameters[J]· Standars for Efficient Cryptography, 2010·

[16] Kravitz D W· Digital signature algorithm: U·S· Patent 5,231,668[P]· 1993-7-27·

[17] Gallagher P· Digital signature standard (DSS)[J]· Federal Information Processing Standards Publications, volume FIPS, 2013, 186·

[18] Doerner J, Kondi Y, Lee E, et al· Threshold ECDSA from ECDSA assumptions: the multiparty case[C]//2019 IEEE Symposium on Security and Privacy (SP)· IEEE, 2019: 1051-1066·

[19] Brassard G, Chaum D, Cré peau C· Minimum disclosure proofs of knowledge[J]· Journal of computer and system sciences, 1988, 37(2): 156-189·

[20] Goldreich O, Micali S, Wigderson A· Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems[J]· Journal of the ACM (JACM), 1991, 38(3): 690-728·

[21] Schnorr C P· Efficient identification and signatures for smart cards[C]//Conference on the Theory and Application of Cryptology· Springer, New York, NY, 1989: 239-252·

[22] Beaver D· Correlated pseudorandomness and the complexity of private computations[C]//Proceedings of the twenty-eighth annual ACM symposium on Theory of computing· 1996: 479-488·

[23] Doerner J, Kondi Y, Lee E, et al· Secure two-party threshold ECDSA from ECDSA assumptions[C]//2018 IEEE Symposium on Security and Privacy (SP)· IEEE, 2018: 980-997·

[24] Paillier P· Public-key cryptosystems based on composite degree residuosity classes[C]//International conference on the theory and applications of cryptographic techniques· Springer, Berlin, Heidelberg, 1999: 223-238·

【作者简介】

严莹子（1995—），女，重庆人，同济大学硕士研究生，研究方向：密码学、机器学习、代码混淆。

（收稿日期：2020-11-03 修回日期：2020-11-25）