C-L（Camenisch-Lysyanskaya）签名

Sammy Li

2021-01-12

目录

1 符号定义

表 1: 符号定义

符号	说明
$\mathbb{G} = \langle G \rangle$	椭圆曲线群，生成元/基点记为 G
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$	椭圆曲线群 $\mathbb{G}_1 = \langle G_1 \rangle$ 和 $\mathbb{G}_2 = \langle G_2 \rangle$ 到 $\mathbb{G}_T = \langle G_T \rangle$ 的双线性映射
$s \in_R S$	表示从集合 S 随机选取一个元素 s
p	群 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 的阶，即元素个数

本文涉及的群，均以椭圆曲线群为例。

2 理论概念

本节参考 C-L 签名介绍 一文。

C-L 签名即为 Camenisch-Lysyanskaya 签名 [1]，以作者名字命名，于 2001 年提出。

C-L 签名可用于群签名或聚合签名的场景，提高签名的匿名性，并降低签名的计算复杂度。C-L 签名也是一种适用于零知识证明的签名方案，能够对一组数据进行签名，并且能够体现这些被证明组件的关系。这样的性质恰好与零知识证明所需性质契合。

介绍 C-L 签名之前，首先需要介绍双线性群的概念。

设 $\mathbb{G}_1 = \langle G_1 \rangle$ 和 $\mathbb{G}_2 = \langle G_2 \rangle$ 是阶为 p 的加法循环群。双线性群是满足下列性质的一个映射 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$

1. 双线性性：对任意的 $x, y \in \mathbb{Z}_p$，有 $e(xG_1, yG_2) = (x + y) \cdot e(G_1, G_2)$
2. 非退化性：$e(G, G) \neq 1$
3. 可计算性：对所有的 $X \in \mathbb{G}_1, Y \in \mathbb{G}_2$，存在有效的算法计算 $e(X, Y)$

如果 $\mathbb{G}_1 = \mathbb{G}_2$，则可得一个对称群（$\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}_T$），以下交换律成立

$$e(xG_1, yG_2) = e(yG_1, xG_2) = xy \cdot e(G_1, G_2) = xy \cdot e(G_2, G_1)$$

C-L 签名也可使用这样的对称群。

3 单组消息版 C-L 签名

3.1 密钥生成

随机生成私钥 $sk = (x, y, z)$，并计算其对应公钥 $pk = (X_1, Y_1, Z_1)$ 如下

1. $x \in_R \mathbb{Z}_p$，$y \in_R \mathbb{Z}_p$，$z \in_R \mathbb{Z}_p$
2. $X_1 = xG_1$，$Y_1 = yG_1$，$Z_1 = zG_1$

3.2 签名

3.2.1 输入

- 消息 $M = (m, r)$
- 私钥 $sk = (x, y, z)$

3.2.2 输出

- 签名 σ

3.2.3 过程

1. 随机挑选 $r' \in_R \mathbb{Z}_p$，计算 $R'_2 = r'G_2$
2. 计算

$$\begin{aligned} Z_2 &= zR'_2 \\ Y_2 &= yR'_2 \\ Y'_2 &= yZ_2 \\ C &= (x + xym + xyrz) \cdot R'_2 \end{aligned}$$

3. 输出签名 $\sigma = (R'_2, Z_2, Y_2, Y'_2, C)$

3.3 验签

3.3.1 输入

- 消息 $M = (m, r)$
- 公钥 $pk = (X_1, Y_1, Z_1)$
- 签名 $\sigma = (R_2', Z_2, Y_2, Y_2', C)$

3.3.2 过程

验证以下等式是否成立

- $e(R_2', Z_1) = e(Z_2, G_1)$ 证明 Z_2 合法
- $e(R_2', Y_1) = e(Y_2, G_1)$ 证明 Y_2 合法
- $e(Z_2, Y_1) = e(Y_2', G_1)$ 证明 Y_2' 合法
- $e(X_1, R_2') + m \cdot e(X_1, Y_2) + r \cdot e(X_1, Y_2') = e(G_1, C)$ 证明 C 合法

成立即证明签名合法，否则签名非法。

3.3.3 证明

$$
\begin{aligned}
&e(R_2', Z_1) = e(R_2', zG_1) = e(zR_2', G_1) = e(Z_2, G_1) \\
&e(R_2', Y_1) = e(R_2', yG_1) = e(yR_2', G_1) = e(Y_2, G_1) \\
&e(Z_2, Y_1) = e(Z_2, yG_1) = e(yZ_2, G_1) = e(Y_2', G_1) \\
&e(X_1, R_2') + m \cdot e(X_1, Y_2) + r \cdot e(X_1, Y_2') \\
&= e(X_1, R_2') + m \cdot e(X_1, yR_2') + r \cdot e(X_1, yZ_2) \\
&= e(X_1, R_2') + ym \cdot e(X_1, R_2') + r \cdot e(X_1, yzR_2') \\
&= (1 + ym) \cdot e(X_1, R_2') + yzr \cdot e(X_1, R_2') \\
&= (1 + ym + yzr) \cdot e(xG_1, R_2') \\
&= x \cdot (1 + ym + yzr) \cdot e(G_1, R_2') \\
&= (x + xym + xyzr) \cdot e(G_1, R_2') \\
&= e(G_1, (x + xym + xyzr) \cdot R_2') \\
&= e(G_1, C)
\end{aligned}
$$

4 多组消息版 C-L 签名

本节参考论文 [1] 的第 3.3 节。

4.1 密钥生成

随机生成私钥 $sk = (x, y, \{z_i\}_{i=1}^{\ell})(\ell \geq 2)$，并计算其对应公钥 $pk = (X_1, Y_1, \{Z_i\}_{i=1}^{\ell})$ 如下

1. $x \in_R \mathbb{Z}_p$， $y \in_R \mathbb{Z}_p$， $z_i \in_R \mathbb{Z}_p$
2. $X_1 = xG_1$， $Y_1 = yG_1$， $Z_i = z_iG_1$

4.2 签名

4.2.1 输入

- 消息 $M = \{m_i\}_{i=1}^{\ell}$
- 私钥 $sk = (x, y, \{z_i\}_{i=1}^{\ell})$

4.2.2 输出

- 签名 σ

4.2.3 过程

1. 随机挑选 $r' \in_R \mathbb{Z}_p$，计算 $R_2' = r'G_2$
2. 计算

$$
\begin{aligned}
Z_{2,i} &= z_i R_2' \\
Y_2 &= y R_2' \\
Y_{2,i}' &= y Z_{2,i} \\
C &= x R_2' + xy m_1 R_2' + \sum_{i=2}^{\ell} xy m_i z_i R_2'
\end{aligned}
$$

3. 输出签名 $\sigma = (R_2', \{Z_{2,i}\}_{i=1}^{\ell}, Y_2, \{Y_{2,i}'\}_{i=1}^{\ell}, C)$

4.3 验签

4.3.1 输入

- 消息 $M = (m, r)$
- 公钥 $pk = (X_1, Y_1, \{Z_i\}_{i=1}^{\ell})$
- 签名 $\sigma = (R_2', \{Z_{2,i}\}_{i=1}^{\ell}, Y_2, \{Y_{2,i}'\}_{i=1}^{\ell}, C)$

4.3.2 过程

验证以下等式是否成立

- $e(R_2', Z_{1,i}) = e(G_1, Z_{2,i})$ 证明 $Z_{2,i}$ 合法
- $e(R_2', Y_1) = e(Y_2, G_1)$ 证明 Y_2 合法
- $e(Z_{2,i}, Y_1) = e(Y_{2,i}', G_1)$ 证明 $Y_{2,i}'$ 合法
- $e(X_1, R_2') + m_1 \cdot e(X_1, Y_2) + \sum_{i=2}^{\ell} m_i \cdot e(X_1, Y_{2,i}') = e(G_1, C)$ 证明 C 合法

成立即证明签名合法，否则签名非法。

4.3.3 证明

$$
\begin{aligned}
&e(R'_2, Z_{1,i}) = e(R'_2, z_i G_1) = e(z_i R'_2, G_1) = e(Z_{2,i}, G_1) \\
&e(R'_2, Y_1) = e(R'_2, yG_1) = e(yR'_2, G_1) = e(Y_2, G_1) \\
&e(Z_{2,i}, Y_1) = e(Z_{2,i}, yG_1) = e(yZ_{2,i}, G_1) = e(Y'_{2,i}, G_1) \\
&e(X_1, R'_2) + m_1 \cdot e(X_1, Y_2) + \sum_{i=2}^{\ell} m_i \cdot e(X_1, Y'_{2,i}) \\
&= e(X_1, R'_2) + m_1 \cdot e(X_1, yR'_2) + \sum_{i=2}^{\ell} m_i \cdot e(X_1, yZ_{2,i}) \\
&= e(X_1, R'_2) + ym_1 \cdot e(X_1, R'_2) + \sum_{i=2}^{\ell} ym_i \cdot e(X_1, Z_{2,i}) \\
&= (1 + ym_1) \cdot e(X_1, R'_2) + \sum_{i=2}^{\ell} ym_i \cdot e(X_1, z_i R'_2) \\
&= (1 + ym_1) \cdot e(X_1, R'_2) + \sum_{i=2}^{\ell} yz_i m_i \cdot e(X_1, R'_2) \\
&= (1 + ym_1 + \sum_{i=2}^{\ell} yz_i m_i) \cdot e(X_1, R'_2) \\
&= (1 + ym_1 + \sum_{i=2}^{\ell} yz_i m_i) \cdot e(xG_1, R'_2) \\
&= x \cdot (1 + ym_1 + \sum_{i=2}^{\ell} yz_i m_i) \cdot e(G_1, R'_2) \\
&= (x + xym_1 + \sum_{i=2}^{\ell} xyz_i m_i) \cdot e(G_1, R'_2) \\
&= e(G_1, (x + xym_1 + \sum_{i=2}^{\ell} xyz_i m_i) \cdot R'_2) \\
&= e(G_1, C)
\end{aligned}
$$

参考文献

[1] Camenisch J., Lysyanskaya A. (2003) A Signature Scheme with Efficient Protocols. In: Cimato S., Persiano G., Galdi C. (eds) Security in Communication Networks. SCN 2002. Lecture Notes in Computer Science, vol 2576. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-36413-7_20

[2] Aranha, Diego F. , et al. "Faster explicit formulas for computing pairings over ordinary curves." (2011).

[3] Camenisch-Lysyanskaya Signatures

[4] Camenisch-Lysyanskaya Signatures in Go