改进的不使用双线性对无证书签密方案

岳泽轮

武警后勤学院

2019 年 10 月

内容提要

研究背景

定义 (离散对数问题)

令 p 和 q 为满足条件 $q|p-1$ 的两个大素数，g 是 $\mathbb{Z}_p^*$ 中阶为 q 的生成元，给定 $g, g^a \in \mathbb{Z}_p^*$，求出 $a \in \mathbb{Z}_q^*$。

定义 (计算性 Diffie-Hellman(CDH) 问题)

令 p 和 q 为满足条件 $q|p-1$ 的两个大素数，g 是 $\mathbb{Z}_p^*$ 中阶为 q 的生成元，给定 $g, g^a, g^b \in \mathbb{Z}_p^*$，求出 $g^a b \in \mathbb{Z}_p^*$。

方案细节

系统建立阶段

输入安全参数 k，输出满足条件 $q|p-1$ 的两个大素数 p 和 q，取 g 为群 $\mathbb{Z}_p^*$ 中任意阶为 q 的生成元。

定义抗碰撞的安全哈希函数：

$H_1 : \{0,1\}^L \times \mathbb{Z}_p^* \times \mathbb{Z}_p^* \to \mathbb{Z}_q^*$,

$H_2 : \{0,1\}^L \times \mathbb{Z}_p^* \times \mathbb{Z}_p^* \times \mathbb{Z}_p^* \to \mathbb{Z}_q^*$，其中，$L$ 为用户身份标识 ID 的长度。

方案细节

系统建立阶段

随机选取系统主密钥 $s \in \mathbb{Z}_p^*$，计算 $P_{Pub} = g^s \ mod \ p$；公开 $Params =< p, q, \mathbb{Z}_p^*, g, P_{pub}, H_1, H_2 >$，秘密保存主密钥 s。

方案细节

用户密钥生成阶段

用户 ID_i 的密钥生成过程如下：
1）随机选取秘密值 $x_i \in \mathbb{Z}_q^*$，计算 $X_i = g^{x_i}$，发送身份标识 ID_i 和公开参数 X_i 给 KGC。
2）给定用户身份标识 ID_i 及公开参数 X_i，KGC 随机选取秘密数 $r_i \in \mathbb{Z}_q^*$，分别计算 $Y_i = g^{r_i}$ 和 $y_i = r_i + sH_1(ID_i, X_i, Y_i)$，通过安全信道将 y_i 和 Y_i 返回给用户 ID_i，其中 y_i 为用户的部分私钥，Y_i 为用户的部分公钥。因此，用户 ID_i 人公私钥对为 $< PK_i = (X_i, Y_i), SK_i = (x_i, y_i) >$。

方案细节

用户密钥生成阶段

设发送方为 Alice $(ID_a) < PK_a = (X_a, Y_a), SK_a = (x_a, y_a) >$，接收方为 Reciver$(ID_b) < PK_b = (X_b, Y_b), SK_b = (x_b, y_b) >$。通过等式 $g^{y_a} = Y_a P_{Pub}^{H_1(ID_a, X_a, Y_a)}$ 和 $g^{y_b} = Y_b P_{Pub}^{H_1(ID_b, X_b, Y_b)}$ 来验证 KGC 生成的部分私钥和部分公钥的正确性。

方案细节

签密阶段

要发送的明文消息为 m，进行如下操作：1）随机选取秘密数 $\omega \in c$，计算 $R = g^{\omega}$；

2）计算 $h_1^B = H_1(ID_b, X_b, Y_b)$，$T = (X_b Y_b P_{Pub}^{h_1^B})^{\omega}$ 和 $C = m \cdot T$；

3）计算 $h = H_2(ID_a, T, m, C)$ 和 $S = h \cdot \omega(x_a + y_a)^{-1}$；

4）发送 $\sigma = (R, C, S)$ 给接收者 Bob。

方案细节

解签密阶段

收到 $\sigma = (R, C, S)$ 后，进行如下操作：1）计算 $T' = R^{x_b + y_b}$，$m' = T'^{-1} \cdot C$。

2）计算 $h' = H_2(ID_a, T', m', C)$ 和 $h_1^A = H_1(ID_a, X_a, Y_a)$；

3）验证等式 $R^{h'} = (X_a Y_a P_{Pub}^{h_1^A})^S$，若成立，则接受 m'，否则输出 $\perp$。

方案正确性

解密正确性

$$T' = R^{x_b+y_b} = g^{(x_b+y_b)\omega}$$
$$= g^{(x_b+r_b+sh_1^B)\omega}$$
$$= (X_b Y_b P_{Pub}^{h_1^B})^{\omega} = T$$

签名正确性

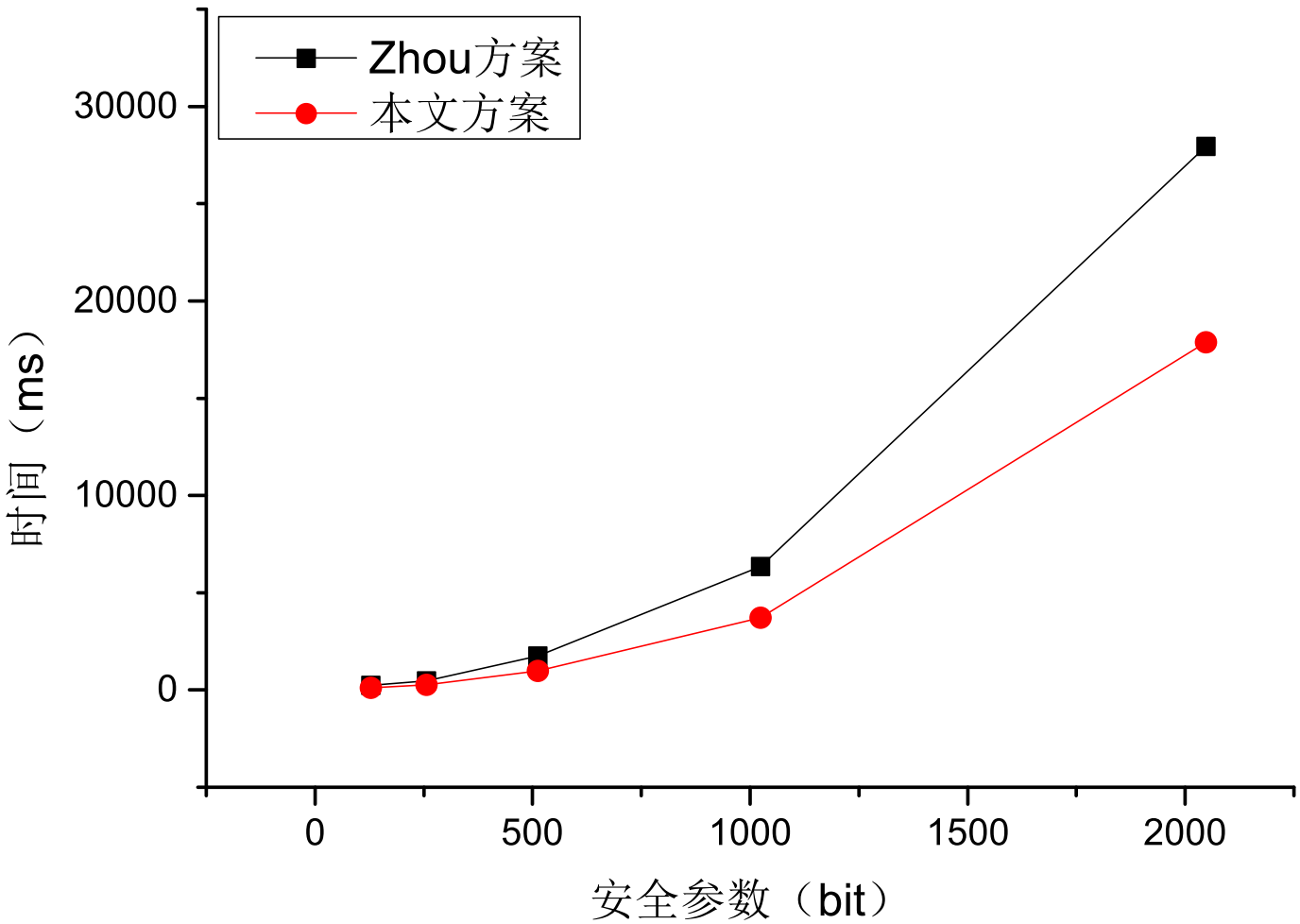
由 $T' = T$ 可得 $h' = H_2(ID_a, T', m', C) = h$,
$R^{h'} = g^{h'\omega} = g^{h\omega}$,
$(X_a Y_a P_{Pub}^{h_1^A})^S = g^{(x_a+y_a)\cdot h\cdot\omega\cdot(x_a+y_a)^{-1}} = g^{h\omega}$

实验分析

实验数据

方案	128bit	256bit	512bit	1024bit	2048bit
Zhou 方案	230.3	469.7	1760.3	6341.1	27950.2
本文方案	115.7	252.4	979.4	3711.1	17863.2

实验分析


Zhou方案
本文方案
30000
20000
10000
0
时间（ms）
0
500
1000
1500
2000
安全参数（bit）

方案改进

签密阶段

要发送的明文消息为 m，进行如下操作：1）随机选取秘密数 $\omega \in \mathbb{Z}_q^*$，计算 $R = g^{\omega}$；

2）计算 $h_1^B = H_1(ID_b, X_b, Y_b)$，$T = (X_b Y_b P_{Pub}^{h_1^B})^{\omega}$ 和 $C = m \cdot T$，

$m = [m_1, m_2, \ldots, m_\mu]$，$\mu = |m|/|\mathbb{Z}_p^*|$，

$C_1 = m_1 \cdot T$，$C_2 = m_2 \cdot T$，$\ldots$，$C_\mu = m_\mu \cdot T$，

$C = [C_1, C_2, \ldots, C_\mu]$；

3）计算 $h = H_2(ID_a, T, m, C)$ 和 $S = h \cdot \omega(x_a + y_a)^{-1}$；

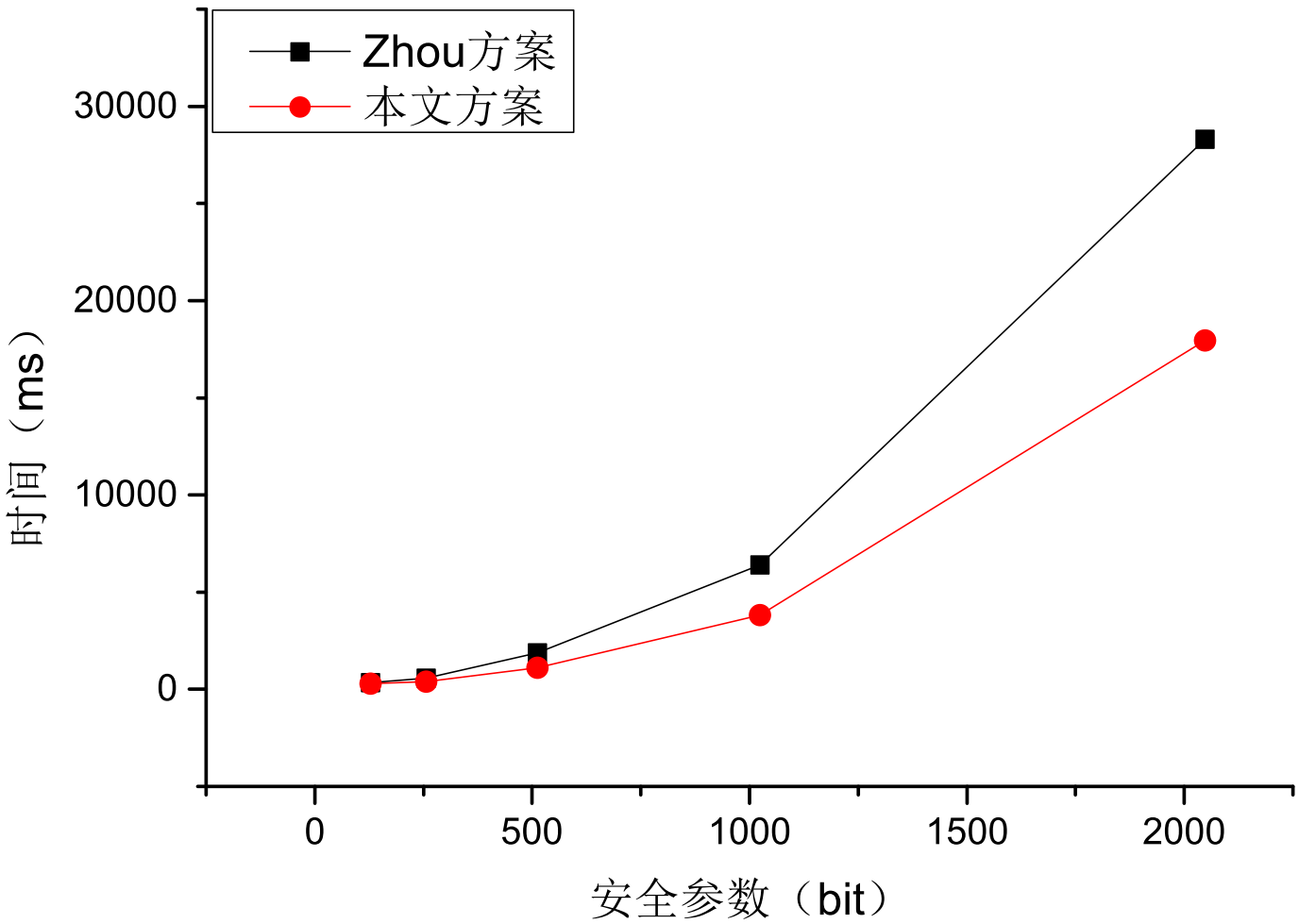
4）发送 $\sigma = (R, C, S)$ 给接收者 Bob。

改进后方案实验分析

实验数据

方案	128bit	256bit	512bit	1024bit	2048bit
Zhou 方案	330.1	559.4	1868.9	6398.9	28312.2
本文方案	301.2	397.9	1101.1	3815.8	17941.9

改进后方案实验分析


Zhou方案
本文方案
30000
20000
10000
0
时间（ms）
0
500
1000
1500
2000
安全参数（bit）

结论与展望

1 结论

与周彦伟方案相比，本文方案在效率上有较大提升。

2 不足之处

本文方案对明文的加密方式造成加密的效率并不是很高，改进后虽然可以加密任意长度的明文，但在一定程度上会造成安全性的降低。

3 下一步的研究方向

进一步提升无证书签密方案的加解密效率和安全性，探索无证书签密方案在前沿研究领域的应用。

谢　谢!

Thank you!