arxiv:2504.15202v1 中译本

将 ElGamal 密码系统扩展到单位的第三组中 $\mathbb{Z}_n$

Jana Hamza [*1], Mohammad EL Hindi [†2], Seifeddine Kadri [‡3], Therrar Kadri [§4], and Yahya Awad [¶5]

[1,5] *Department of Mathematics and Physics, Faculty of Arts and Sciences, Lebanese International University, Bekaa, Lebanon*

[2] *Department of Mathematics and Computer Science, Faculty of Science, Beirut Arab University, Beirut, Lebanon*

[3] *Faculty of Applied Computing and Technology, Norof University College, Kristiansand, Norway*

[4] *Department of Science, Nourthwestern Polytechnic, Grande Prairie, Canada*

摘要

在本文中，我们将 ElGamal 密码系统扩展到环 $\mathbb{Z}_n$ 的第三个单位群，并证明这种扩展比之前的扩展更安全。我们描述了新设置下所需的算术运算。我们还提供了一些数值模拟，显示了所提出的密码系统的安全性和效率。

关键词： ElGammal 密码系统，单位群，群的阶，循环群，环

1 介绍

ElGamal 密码系统最初由 T. ElGamal 在 [7] 中提出。经典情况下，该系统是在乘法群 $\mathbb{Z}_p^*$ 上定义的，即模素数 p 的整数群，这是一个由其元素之一生成的循环群，但这个密码系统可以在任何循环群 G 中工作。在群 G 中离散

[*] jana.hamza115@gmail.com

[†] mohammadyhindi98@gmail.com

[‡] Seifedine.kadry@norof.no

[§] TKadri@nwpolytech.ca

[¶] yehya.awad@liu.edu.lb

对数问题的难解性是广义 ElGamal 密码系统的安全基础。此外，这个群组 G 应该仔细选择，以便于操作 G 的效率较高。该密码系统已经在不同的群组中进行了多次泛化。有关这些推广的更多信息，我们指引读者参考以下内容（[9],[10],[11],[13],[14],[16]）。

在 2006 年，El-Kassar 和 Chehade 在 [1] 中介绍了环 $\mathbb{Z}_n$ 的单位群的一个推广，表示为 $\mathbb{Z}_n$ 的 k^{th} 单位群，即 $U^k(\mathbb{Z}_n)$。有关 k^{th} 单位群的更多信息，请参见 ([1],[6],[9])。作者在 [1] 中确定了所有具有循环单位群 2^{nd} 的环 $R = \mathbb{Z}_n$。这些群组被用作 Haraty 等人在 [9] 中给出的 ElGamal 密码系统的扩展。他们研究了 $U^2(Z_n)$ 的两种情况：

1. $U(\mathbb{Z}_n)$ 和 $U^2(\mathbb{Z}_n)$ 都是循环的。

2. $U^2(\mathbb{Z}_n)$ 是循环的，而 $U(\mathbb{Z}_n)$ 不是循环的。

卡德里和埃尔-卡萨尔在 [9] 中考察了单位的第三组 $\mathbb{Z}_n$，并确定所有使得 $\mathbb{Z}_n$ 具有 $U^3(\mathbb{Z}_n)$ 循环的环，并建议将 ElGamal 密码系统扩展到这些在循环情况下的群。

在这篇论文中，我们将 ElGamal 密码系统扩展到 $\mathbb{Z}_n$ 的第三个单位群，在它们是循环群的情况下。换句话说，我们通过扩展在这个领域所需的算术运算来修改 ElGamal 公钥加密方案，使其从其经典域自然地扩展到 $U^3(\mathbb{Z}_n)$ 的域。

在第 2 节中，我们描述了 $U^3(\mathbb{Z}_n)$ 的构造以及与该群相关的某些定理。第 3 节提供了我们提出的密码系统的描述。最后，第 4 节展示了我们的工作与其他先前结果之间的比较。

2 预备知识

在本节中，我们将简要介绍经典的 ElGamal 公钥密码系统以及在模 n 整数环的第二单位群设置下的修改版 ElGamal 密码系统。

该密码系统的基本算法如下三个算法所述：

算法 1 密钥生成

1. 找到生成元 α 的 $\mathbb{Z}_p^*$。

2. 选择一个随机整数 a，$1 \leq a \leq p-2$，并计算 $a^{\alpha} \bmod p$。

3. A 的公钥是 (p, α, α^a)；A 的私钥是 a。

以下算法展示了 B 如何将消息 m 加密为 A。

算法 2 加密

1. 获取 A 的真实公钥 (p, α, α^a)。

2. 将消息表示为范围内的整数 $m(0, 1, ..., p-1)$。

3. 选择一个随机整数 k，$1 \leq k \leq p-2$。

4. 计算 $\gamma = \alpha^k \bmod p$ 和 $\delta = m \cdot (\alpha^a)^k \bmod p$。

5. 将密文 $c = (\gamma, \delta)$ 发送给 A。

这是算法使用 A 恢复消息 m 的方法。

算法 3 解密

1. 使用私钥 a 进行计算 $\gamma^{p-1-a} \bmod p = \gamma^{-a}$

2. 恢复 m 通过计算 $(\gamma^{-a}) \cdot \delta \bmod p$。

现在对于 $U^2(\mathbb{Z}_n)$ 上的修改后的 ElGamal 加密系统，如我们之前提到的，考虑了两种情况。
情况 1：$U(\mathbb{Z}_n)$ 和 $U^2(\mathbb{Z}_n)$ 是循环的：在这种情况下，$U^2(\mathbb{Z}_n)$ 的元素具有形式 $U^2(\mathbb{Z}_n) = \{r^i \bmod n : \gcd(i, \varphi(n)) = 1\}$，其中 r 是 $U(\mathbb{Z}_n)$ 的生成元。

扩展的 ElGamal 公钥密码系统在 $U^2(\mathbb{Z}_n)$ 上遵循以下四个算法：

算法 4 生成器 $ca\ U^2(\mathbb{Z}_n)$

1. 找到生成元 θ_1 的 $U(\mathbb{Z}_n)$。

2. 将 $U^2(\mathbb{Z}_n)$ 的顺序写为 $p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$。

3. 选择一个随机整数 s,$0 \leq s \leq \varphi(n) - 1$,$(s, \varphi(n)) = 1$。

4. 对于 $j = 1$ 到 i，执行：

4.1. 计算 $\theta_1^{N/p_j} \bmod n$。

4.2. 如果 $\theta_1^{s(N/p_j)} \bmod n \equiv \theta_1$，则转至步骤 3。

5. 返回 s。

对于密钥生成，使用此算法：

算法 5 密钥生成

1. 找到生成元 θ_1 的生成器 $U(\mathbb{Z}_n)$。
2. 使用之前的算法找到 s。
3. 计算 $U^2(\mathbb{Z}_n)$ 的阶使用 $\varphi^2(n)$。
4. 选择一个随机整数 a，$2 \leq a \leq \varphi^2(n) - 1$，并计算 $f = s^a (\mathrm{mod} \varphi(n))$。
5. A 的公钥是 (n, θ_1, s, f) 且 A 的私钥是 a。

对于消息 m 的加密，使用以下算法：

算法 6 加密

1. B 获得 A 的真实公钥 (n, θ_1, s, f)。
2. 将消息表示为 $U^2(\mathbb{Z}_n)$ 中的整数。
3. 选择一个随机整数 k，$2 \leq k \leq \varphi^2(n) - 1$。
4. 计算 $q = s^k (\mathrm{mod} \varphi(n)), r = f^k (\mathrm{mod} \varphi(n))$, $\gamma = \theta^k = \theta_1^q (\mathrm{mod} n)$ 和 $\delta = m^r (\mathrm{mod} n)$。
5. 将密文 $c = (q, \delta)$ 发送给 A。

最后，要解密消息，请使用以下算法：

算法 7 解密

1. 使用私钥 a 计算 $b = \varphi^2(n) - a$。
2. 通过计算 $t = q^b (\mathrm{mod} \varphi(n))$ 和 $\delta^t (\mathrm{mod} n)$ 来恢复消息。

情况 2：$U^2(\mathbb{Z}_n)$ 是循环的，当 $U(\mathbb{Z}_n)$ 不是循环时：扩展的 ElGamal 公钥密码系统在 $U^2(\mathbb{Z}_n)$ 上遵循以下四个算法：

算法 8 生成器 $U^2(\mathbb{Z}_n)$

1. 找到生成元 θ_1 的生成器 $U(\mathbb{Z}_n)$。
2. 将 $U^2(\mathbb{Z}_n)$ 的阶写为 $p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$。
3. 选择一个随机整数 s，$0 \leq s \leq \varphi(p)-1$，$(s,\varphi(p))=1$。
4. 对于 $j=1$ 到 i，执行：
   4.1. 计算 $\theta_1^{N/p_j} \bmod p$。
   4.2. 如果 $\theta_1^{s(N/p_j)} \bmod p \equiv \theta_1$，则转到步骤 3。
5. 使用中国剩余定理通过求解同余方程组：$x \equiv 2(\mathrm{mod}3)$ 和 $x \equiv \theta_1^s(\mathrm{mod}\ p)$ 来找到 θ 和 s。
6. 返回 s。

现在，对于密钥生成，A 使用以下算法：

算法 9 密钥生成

1. 找到生成元 θ_1 的生成器 $U(\mathbb{Z}_p)$。
2. 使用之前的算法找到 s。
3. 计算使用 $\varphi^2(p)$ 的 $U^2(\mathbb{Z}_p)$ 的阶。
4. 选择一个随机整数 a，$2 \leq a \leq \varphi^2(p)-1$，并计算 $f = s^a(\mathrm{mod}\varphi(p))$。
5. A 的公钥是 (p,θ_1,s,f) 且 A 的私钥是 a。

为了加密 m 给 A 的消息 B，他使用以下算法：

算法 10 加密

1. B 获得 A 的真实公钥 (n,θ_1,s,f)。
2. 将消息表示为 $U^2(\mathbb{Z}_p)$ 中的整数。

3. 选择一个随机整数 k，$2 \leq k \leq \varphi^2(p) - 1$。

4. 计算 $q = s^k(\mathrm{mod}\varphi(p)), r = f^k(\mathrm{mod}\varphi(p))$, $\gamma = \theta^k = \theta_1^q(\mathrm{mod}p)$ 和 $\delta = m^r(\mathrm{mod}p)$。

5. 将密文 $c = (q, \delta)$ 发送到 A。

最后对消息 m 进行解密，应用下一个算法 A:

算法 11 解密

1. 使用私钥 a 计算 $b = \varphi^2(p) - a$。

2. 通过计算 $t = q^b(\mathrm{mod}\varphi(p))$ 和 $\delta^t(\mathrm{mod}p)$ 来恢复消息。

3 构造 $U^3(\mathbb{Z}_n)$

在这篇论文中，为了将 ElGamal 密码系统应用于 $U^3(\mathbb{Z}_n)$ 上，它必须是一个循环群，所以我们关心的是使得 $U^3(\mathbb{Z}_n)$ 成为循环群的 n 的值。

引理 12 $U(\mathbb{Z}_{3^\alpha})U(\mathbb{Z}_{\varphi(3^\alpha)})$ 和 $U(\mathbb{Z}_{\varphi(\varphi(3^\alpha))})$ 对所有情况都是循环的 $\alpha > 0$.

引理 13 $U(\mathbb{Z}_{2.3^\alpha})U(\mathbb{Z}_{\varphi(2.3^\alpha)})$ 和 $U(\mathbb{Z}_{\varphi(\varphi(2.3^\alpha))})$ 对所有情况都是循环的 $\alpha > 0$.

现在，我们定义将群同构到 $U^3(\mathbb{Z}_n)$ 的操作如下:

定理 3.1 设 $U(\mathbb{Z}_n)$, $U(\mathbb{Z}_{\varphi(n)})$ 和 $U(\mathbb{Z}_{\varphi(\varphi(n))})$ 是循环群。然后 $f : U^3(\mathbb{Z}_n) \longrightarrow \mathbb{Z}_{\varphi(\varphi(\varphi(n)))}$ 由

$$f(a) = \log_{g_3} \log_{g_2} \log_{g_1} a \bmod n$$

给出的是一个同构，其中 g_1、g_2 和 g_3 分别是 $U(\mathbb{Z}_n)$、$U(\mathbb{Z}_{\varphi(n)})$ 和 $U(\mathbb{Z}_{\varphi(\varphi(n))})$ 的生成元。

Proof. 设 $U(\mathbb{Z}_n)$，$U(\mathbb{Z}_{\varphi(n)})$ 和 $U(\mathbb{Z}_{\varphi(\varphi(n))})$ 是循环群。设 g_1 是 $U(\mathbb{Z}_n)$ 的一个生成元。由于 $U(\mathbb{Z}_n)$ 是有限的循环群，阶为 $\varphi(n)$，则 $U(\mathbb{Z}_n) \approx \mathbb{Z}_{\varphi(n)}$ 由函数 $h_1 : U(\mathbb{Z}_n) \longrightarrow \mathbb{Z}_{\varphi(n)}$ 定义为 $h_1(a) = log_{g_1} a \bmod n$。现在由于 $U^2(\mathbb{Z}_n)$ 是 $U(\mathbb{Z}_n)$ 的子集，且 $U(\mathbb{Z}_{\varphi(n)})$ 是 $\mathbb{Z}_{\varphi(n)}$ 的子集，则 $h_1 : U^2(\mathbb{Z}_n) \longrightarrow U(\mathbb{Z}_{\varphi(n)})$ 是一个同构。令 g_2 为 $U(\mathbb{Z}_{\varphi(n)})$ 的一个生成元。由于 $U(\mathbb{Z}_{\varphi(n)})$ 是循环的且

阶为 $\varphi(\varphi(n))$ 的有限群，则 $U(\mathbb{Z}_{\varphi(n)}) \approx \mathbb{Z}_{\varphi(\varphi(n))}$ 由函数 $h_2 : U(\mathbb{Z}_{\varphi(n)}) \longrightarrow \mathbb{Z}_{\varphi(\varphi(n))}$ 定义，该函数定义为 $h_2(b) = \log_{g_2} b \bmod \varphi(n)$ 或由 $h_2 \circ h_1(a) = \log_{g_2} \log_{g_1} a \bmod n$ 定义的 $h_2 \circ h_1 : U^2(\mathbb{Z}_n) \longrightarrow \mathbb{Z}_{\varphi(\varphi(n))}$。现在由于 $U^3(\mathbb{Z}_n)$ 是 $U^2(\mathbb{Z}_n)$ 的一个子群，且 $U(\mathbb{Z}_{\varphi(\varphi(n))})$ 是 $\mathbb{Z}_{\varphi(\varphi(n))}$ 的一个子群，则 $h_2 \circ h_1 : U^3(\mathbb{Z}_n) \longrightarrow U(\mathbb{Z}_{\varphi(\varphi(n))})$ 是一个同构。现在令 g_3 为 $U(\mathbb{Z}_{\varphi(\varphi(n))})$ 的一个生成元。由于 $U(\mathbb{Z}_{\varphi(\varphi(n))})$ 是有限循环群，阶数为 $\varphi(\varphi(\varphi(n)))$，则由 $h_3(c) = \log_{g_3} c \bmod \varphi(\varphi(n))$ 定义的函数 $h_3 : U(\mathbb{Z}_{\varphi(\varphi(n))}) \longrightarrow \mathbb{Z}_{\varphi(\varphi(\varphi(n)))}$ 是一个同构。这意味着由 $h_3 \circ h_2 \circ h_1(a) = \log_{g_3} \log_{g_2} \log_{g_1} a \bmod n$ 定义的 $h_3 \circ h_2 \circ h_1(a) : U^3(\mathbb{Z}_n) \longrightarrow \mathbb{Z}_{\varphi(\varphi(\varphi(n)))}$ 也是一个同构。■

现在对于构建 $U^3(\mathbb{Z}_n)$，我们使用以下算法：

1. 找到群 $U(\mathbb{Z}_n)$ 的一个生成元 g_1。
2. 将 $U(\mathbb{Z}_n)$ 中的每个元素写成 g_1 的幂。$U(\mathbb{Z}_n) = \{g_1^i \bmod n, 0 \leq i \leq \varphi(n)\}$。
3. 找到群 $U(\mathbb{Z}_{\varphi(n)})$ 的一个生成元 g_2。
4. 将 $U(\mathbb{Z}_{\varphi(n)})$ 中的每个元素写成 g_2 的幂。$U(\mathbb{Z}_{\varphi(n)}) = \{g_2^i \bmod \varphi(n), 0 \leq i \leq \varphi(\varphi(n))\}$。
5. 找到 $U^3(\mathbb{Z}_n) = \{g_1^{g_2^i \bmod \varphi(n)} \bmod n, \gcd(i, \varphi(\varphi(n))) = 1\}$。

下列示例展示了如何找到 $U^3(\mathbb{Z}_{11})$，以及与其每个元素对应的同构元素在 $\mathbb{Z}_2$

示例 14 一个生成元 g_1 是 $U(\mathbb{Z}_{11})$ 的 2。我们有 $U(\mathbb{Z}_{11}) = \{1 = 2^0, 2 = 2^1, 3 = 2^8, 4 = 2^2, 5 = 2^4, 6 = 2^9; 7 = 2^7, 8 = 2^3, 9 = 2^6, 10 = 2^5\}$ 所有的 mod11，以及 $U(\mathbb{Z}_{\varphi(11)}) = U(\mathbb{Z}_{10})$。生成器 g_2 是 $U(\mathbb{Z}_{10})$ 的 3。$U(\mathbb{Z}_{10}) = \{1 = 3^0, 3 = 3^1, 7 = 3^3, 9 = 3^2\}$ 都是 mod10。

$$
\begin{aligned}
U^3(\mathbb{Z}_{11}) &= \{2^{3^i} \bmod 11, \gcd(i, 4) = 1\} \\
&= \{2^{3^1} \bmod 11, 2^{3^3} \bmod 11\} \\
&= \{2^3 \bmod 11, 2^7 \bmod 11\} \\
&= \{8, 7\}
\end{aligned}
$$

$U(\mathbb{Z}_{\varphi(\varphi(11))}) = U(\mathbb{Z}_{\varphi(10)}) = U(\mathbb{Z}_4) = \{1, 3\}$。现在要找 $U^3(\mathbb{Z}_{11})$ 的同构群，

我们找到 g_3，$U(\mathbb{Z}_4)$ 的生成元 $g_3 = 3$。

$$\begin{aligned} f(7) &= \log_3 \log_3 \log_2 7 \bmod 11 \\ &= \log_3 \log_3 \log_2 2^7 \bmod 11 \\ &= \log_3 \log_3 7 \bmod 11 \\ &= \log_3 \log_3 3^3 \bmod 11 \\ &= \log_3 3 \bmod 11 \\ &= 1 \end{aligned}$$

$$\begin{aligned} f(8) &= \log_3 \log_3 \log_2 8 \bmod 11 \\ &= \log_3 \log_3 \log_2 2^3 \bmod 11 \\ &= \log_3 \log_3 3 \bmod 11 \\ &= \log_3 1 \bmod 11 \\ &= 0 \end{aligned}$$

因此，7 在 $U^3(\mathbb{Z}_{11})$ 中与 1 同构，并且 8 在 $U^3(\mathbb{Z}_{11})$ 中与 0 同构，从而得到 $U^3(\mathbb{Z}_{11}) = \{7, 8\} \approx \{0, 1\} = \mathbb{Z}_2$。

以下定理解释了如何找到生成元 $U^3(\mathbb{Z}_n)$。

定理 3.2 令 g 为 $U^3(\mathbb{Z}_n)$ 的一个生成元。然后 g 具有形式 $g_1^{g_2^{g_3 (\bmod \varphi(n))}} (\bmod n)$，其中 g_1、g_2 和 g_3 分别是 $U(\mathbb{Z}_n)$、$U(\mathbb{Z}_{\varphi(n)})$ 和 $U(\mathbb{Z}_{\varphi(\varphi(n))})$ 的生成元。

Proof. 我们从定理 3.1得知 $U^3(\mathbb{Z}_n) \approx \mathbb{Z}_{\varphi(\varphi(\varphi(n)))}$ 由函数 $f : U^3(\mathbb{Z}_n) \longrightarrow \mathbb{Z}_{\varphi(\varphi(\varphi(n)))}$ 定义为 $f(a) = \log_{g_3} \log_{g_2} \log_{g_1} a \mod n$, 其中 f 是在 $\mathbb{Z}_{\varphi(\varphi(\varphi(n)))}$. 上加法的群同构。此外, 如果 $U^3(\mathbb{Z}_n)$ 是生成元为 g, 的循环群, 则 $\mathbb{Z}_{\varphi(\varphi(\varphi(n)))}$ 是生成元为 $f(g)$. 的循环群

然而，如果 $(\mathbb{Z}_{\varphi(\varphi(\varphi(n)))}, +)$ 是生成元为 1, 的循环群，则 $f(g) = 1$. 因此

$$\begin{aligned} g &= f^{-1}(1) \\ &= (\log_{g_3} \log_{g_2} \log_{g_1})^{-1}(1) \\ &= \log_{g_1}^{-1} \log_{g_2}^{-1}(g_3^1) \\ &= \log_{g_1}^{-1}(g_2^{g_3}) \\ &= g_1^{g_2^{g_3 (\bmod \varphi(n))}} (\bmod n). \end{aligned}$$

■

定义 15 令 f 是定理 *3.1*中定义的函数。$(U^3(\mathbb{Z}_n), \oplus, \otimes)$ 中的操作定义如下：

1. $x \oplus y = x^{\log_r y} \bmod n$ 其中 r 是 $U(\mathbb{Z}_n)$ 的生成元。

2. $x \otimes y = f^{-1}(f(x) + f(y))$.

3. $x^n = f^{-1}(nf(x))$.

4 ElGamal 密码系统上的 $U^3(\mathbb{Z}_n)$

以下三种算法说明了在 $U^3(\mathbb{Z}_n)$ 上的 ElGamal 密码系统。

对于密钥生成，实体 A 必须执行以下操作：

算法 16 （密钥生成）

1. 找到生成元 g 的一个 $U^3(\mathbb{Z}_n)$.

2. 选择一个随机整数 b, $1 \leq b \leq \varphi^3(n)$.

3. 计算 $B = g^b$。

4. A 的公钥是 (g, B) 和 A 的私钥是 b.

要加密消息 m 给 A，实体 B 必须使用以下算法：

算法 17 （加密）

1. 获得 A 的公钥 (g, B).

2. 将消息表示为整数 m 在 $U^3(\mathbb{Z}_n)$.

3. 选择一个随机整数 a, $1 \leq a \leq \varphi^3(n)$.

4. 计算 $s = B^a$.

5. 计算 $A = g^a$.

6. 计算 $X = m \otimes s$.

7. 发送密文 $c = (A, X)$.

为了恢复消息 m，实体 A 使用此算法：

算法 18 （解密）

1. 使用私钥进行计算 $s = A^b$.

2. 计算 s^{-1}.

3. 通过计算恢复消息 $mm = X \otimes s^{-1}$.

定理 4.1 给定生成元 g 的 $U^3(\mathbb{Z}_n)$。定义 $B = g^b$，$A = g^a$，$s = B^a = A^b$ 和 $X = m \otimes s$。如果 $k \in U^3(\mathbb{Z}_n)$ 满足 $k = X \otimes s^{-1}$，则 $k = m$。

Proof. 我们有 $s = B^a = A^b = g^{ab}$，和 $X = m \otimes s = m \otimes g^{ab}$，然后 $k = X \otimes s^{-1} = m \otimes g^{ab} \otimes (g^{ab})^{-1} = m$。■

以下示例是我们的加密系统的一个应用。

示例 19 令 $n = 3^4 = 81$。
通过应用定理 *3.1*，我们得到 $U^3(\mathbb{Z}_{81}) \approx \mathbb{Z}_6$，其中

$$5 \approx 4, 23 \approx 3, 32 \approx 0, 50 \approx 1, 59 \approx 2, 77 \approx 5$$

密钥生成

1. $g = 50$ 是生成器的 $U^3(\mathbb{Z}_{81})$

2. 选择 $b = 4$

3. 计算

$$B = g^b = 50^4 = f^{-1}(4f(50)) = f^{-1}(4) = 5$$

4. 公钥是 $(50, 5)$，私钥是 4。

加密

1. 选择 $a = 2$

2. 计算

$$s = B^a = 5^2 = f^{-1}(2f(5)) = f^{-1}(2.4 \bmod 6) = f^{-1}(2) = 59$$

3. 计算

$$A = g^a = 50^2 = f^{-1}(2f(50)) = f^{-1}(2) = 59$$

4. 选择 $m = 77$。

5. 计算

$$X = m \otimes s = 77 \otimes 59 = f^{-1}(f(77) + f(59)) = f^{-1}(5 + 2 \bmod 6) = f^{-1}(1) = 50.$$

6. 密文是 $(59, 50)$。

解密

1. 计算

$$s = A^b = 59^4 = f^{-1}(4f(59)) = f^{-1}(4.2 \bmod 6) = f^{-1}(2) = 59$$

2. 计算

$$s^{-1} = f^{-1}([f(59)]^{-1}) = f^{-1}(2^{-1}) = f^{-1}(4) = 5$$

3. 计算

$$m = X \otimes s^{-1} = 50 \otimes 5 = f^{-1}(f(50) + f(5)) = f^{-1}(1 + 4 \bmod 6) = f^{-1}(5) = 77.$$

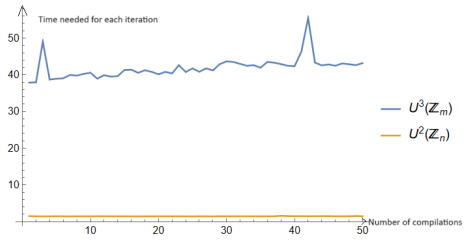
5 效率和密码系统的安全性

在本节中，我们展示了我们的密码系统与 [9] 中提出的系统的效率和安全性之间的比较研究。由于婴儿步-巨人步攻击算法主要依赖于操作 g^i，其中 g 是选定群的生成元，所以我们只需比较两个群中 g^i 的编译时间即可。我们在 Wolfram Mathematica 12 上生成了我们的算法。我们使用了两个近似等阶的群 $U^2(\mathbb{Z}_n)$ 和 $U^3(\mathbb{Z}_m)$（阶数之差为 2），并在随机选择的元素上运行这两个程序各 50 次，结果如图 1 所示。结果显示，$U^3(\mathbb{Z}_m)$ 中每次迭代的时间大约是 $U^2(\mathbb{Z}_n)$ 的 30 倍，这表明我们的新密码系统中的迭代复杂得多，并且使破解系统变得更加困难。请注意，蓝色曲线对应的是 $U^3(\mathbb{Z}_m)$ 的时间，而橙色曲线对应的是 $U^2(\mathbb{Z}_n)$ 的时间。

参考文献

[1] A.-N. El-Kassar, H. Y. Chehade. Generalized group of units. *Math. Balkanica.* 2006;20(3):275-286.

图 1: $U^2(\mathbb{Z}_n)$ 和算法迭代的时间比较 $U^3(\mathbb{Z}_m)$



[2] A.-N. El-Kassar, H. Y. Chehadi, D. Zentout. Quotient rings of polynomials over finite fields with cyclic group of units. *Proceedings of the International Conference on Research Trends in Science and Technology*. 2002; 257-266.

[3] A.-N. El-Kassar, R. A. Haraty. ElGamal public-key cryptosystem using reducible polynomials over a finite field. *IASSE* . 2004;189-194.

[4] A.-N. El-Kassar, R. A. Haraty. ElGamal Public-key cryptosystem in multiplicative groups of quotient rings of polynomials over finite fields. *Computer Science and Information Systems*. 2005;2(1):63-77.

[5] A.-N. El-Kassar, M. Rizk, N. M. Mirza, Y. A. Awad. ElGamal public key cryptosystem in the domain of Gaussian integers. *Int. J. Appl. Math*. 2001;7(4):405-412.

[6] M. El Hindi, T. Kadri. On the generalized multiplicative euler phi function. *arXiv: 2111.13474*. 2021.

[7] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *Advances in Cryptography*. Springer, Berlin, Heidelberg. 1985;10-18.

[8] J. A. Gallian. *Contemporary Abstract Algebra*, 7th ed., Cengage: Learning. 2012.

[9] R. Haraty, A. -N. Kassar, S. Fanous. Hardening the ElGamal cryptosystem in the setting of the second group of units, *International*

Arab Journal of Information Technology (IAJIT). 2014;11(5):514-520.

[10] Irawadi, S. Nonsingular matrix as private key on ElGamal cryptosystem. In Journal of Physics: Conference Series (Vol. 1821, No. 1, p. 012018). IOP Publishing. 2021.

[11] Irawadi, S. Discrete Logarithmic Improvement for ElGamal Cryptosystem Using Matrix Concepts. In 2020 8th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-5). IEEE. 2020.

[12] T. Kadri, A.-N. El-Kassar. The third group of units of the ring $\mathbb{Z}_n$. *JP Journal of Algebra, Number Theory and Applications.* 2016;38(4):385-413.

[13] Mahalanobis, A. A simple generalization of the ElGamal cryptosystem to non-abelian groups. Communications in Algebraő. 2008;36(10), 3878-3889.

[14] Mahalanobis, A. A simple generalization of the ElGamal cryptosystem to non-abelian groups II. Communications in Algebra. 2012;40(9), 3583-3596.

[15] R. Rivest, A. Shamir, L. Aldeman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM.* 1978;21(2):120-126,

[16] Ranasinghe, R., Athukorala, P. A generalization of the ElGamal public-key cryptosystem. Journal of Discrete Mathematical Sciences and Cryptography; 2022;25(8), 2395-2403.