

YuS：基于新型二次置换的FHE友好流密码技术文档

摘要

本文提出了一种有限域 \mathbb{F}_p^n 上新型二次置换的构造方法，刻画了其差分均匀性、沃尔什谱等密码学性质，并基于该置换设计了FHE（全同态加密）友好流密码YuS。YuS采用SPN结构，以 \mathbb{F}_p^3 上的二次置换为S盒，搭配固定线性映射，在BGV和BFV方案下，80位和128位安全级别下的评估速度与吞吐量均优于Masta、PASTA、PASTA_v2和HERA等现有方案。核心贡献包括：证明了 \mathbb{F}_p^2 上二次置换的差分均匀性恒为 p^2 ；给出 \mathbb{F}_p^n （ $n \geq 3$ ）上二次置换的构造条件，其差分均匀性可达 p^{n-1} ，沃尔什系数2-范数有界；YuS在HElib和SEAL库中的实现验证了其性能优势。

1 引言

1.1 研究背景

- FHE允许对加密数据直接计算，但存在密文体积大、通信开销高的问题。
- HHE（混合同态加密）框架通过对称密码加密原始数据（密文与明文等长），服务器对对称解密电路进行同态评估，降低通信开销。
- 现有FHE友好对称密码分为两类：优化现有对称密码（如AES）的FHE实现；设计专用密码（基于 \mathbb{F}_2 操作：LowMC、Kreyvium等；基于大有限域 \mathbb{F}_q 操作：MiMC、Masta等）。
- 流密码因支持密钥流离线预生成，可提升在线解密效率，成为HHE框架的研究热点；FHE友好密码设计的核心是最小化乘法深度（乘法操作会快速累积密文噪声）。

1.2 核心目标

设计低乘法深度、高安全性、FHE评估高效的流密码，解决现有方案在乘法深度、评估速度或吞吐量上的不足。

2 预备知识

2.1 FHE相关方案

2.1.1 BGV方案

- 基于RLWE问题，明文空间 $P = \mathbb{Z}_t/(X^n + 1)$ ，密文空间 $C = \mathbb{Z}_{q_\ell}/(X^n + 1) \times \mathbb{Z}_{q_\ell}/(X^n + 1)$ (q_ℓ 为层级 ℓ 的密文模数)。
- 密钥生成：私钥 sk 采样自汉明重量为 w 的多项式，公钥 $pk = ([-(a \cdot sk + t \cdot e)]_{q_\ell}, a)$ 。
- 加密： $c = ([pk_1 \cdot u + t \cdot e_1 + m]_{q_\ell}, [pk_2 \cdot u + t \cdot e_2]_{q_\ell})$ 。
- 解密： $m = [[c_1 + c_2 \cdot sk]_{q_\ell}]_t$ 。

2.1.2 BFV方案

- 基于RLWE问题，明文空间 $P = \mathbb{Z}_t/(X^n + 1)$ ，密文空间 $C = \mathbb{Z}_q/(X^n + 1) \times \mathbb{Z}_q/(X^n + 1)$ 。
- 密钥生成：私钥 sk 采样自汉明重量为 w 的多项式，公钥 $pk = ([-(a \cdot sk + e)]_q, a)$ 。
- 加密： $c = ([pk_1 \cdot u + e_1 + \Delta \cdot m]_q, [pk_2 \cdot u + e_2]_q)$ ($\Delta = \lfloor q/t \rfloor$)。
- 解密： $m = [\lfloor t \cdot [c_1 + c_2 \cdot sk]_q / q \rfloor]_t$ 。

2.2 S盒的密码学性质

- 差分均匀性 $\Delta(F)$: $\max_{\bar{a} \neq 0, \bar{b}} |\{\bar{x} | F(\bar{x}) - F(\bar{x} - \bar{a}) = \bar{b}\}|$ ，衡量抵抗差分攻击的能力。
- 沃尔什变换 $\lambda_f(\bar{u}) = \sum_{\bar{x}} \chi(f(\bar{x}) - \bar{u} \cdot \bar{x})$ ($\chi(x) = e^{2\pi i x/p}$)，线性度 $L(F)$ 为沃尔什系数的最大2-范数，衡量抵抗线性攻击的能力。
- 置换： $n = m$ 时的平衡函数（每个输出值对应 p^{n-m} 个输入值）。

3 有限域上的二次置换

3.1 关键定理与构造方法

3.1.1 \mathbb{F}_p^2 上的二次置换

- 定理1: \mathbb{F}_p^2 (p 为奇素数) 上的二次置换，其差分均匀性恒为 p^2 。

3.1.2 \mathbb{F}_p^n ($n \geq 3$) 上的二次置换构造

- 构造方法：设 M_0, M_1 为 $(n-1) \times (n-1)$ 矩阵，定义 $M_{x_0} = x_0 \cdot M_0 + M_1$ ，置换 $F(\bar{x}) = (x_0, M_{x_0} \cdot (x_1, \dots, x_{n-1})^T)$ 。

- 置换条件：若 M_{x_0} 的行列式多项式 $d(x_0)$ 在 \mathbb{F}_p 中无零点，则 F 是 \mathbb{F}_p^n 上的置换。
- 差分均匀性：若 $\text{rank}(M_0) = n - 1$ ，则 $\Delta(F) = p^{n-1}$ 。
- 沃尔什谱：若输入掩码或输出掩码的最后 $n - 1$ 项非零，则沃尔什系数的最大2-范数 $\leq p^{n-1}$ 。

3.1.3 \mathbb{F}_p^3 上的具体二次置换（YuS的S盒）

- 条件： $p \equiv 2 \pmod{3}$ （确保行列式多项式 $x^2 + x + 1$ 在 \mathbb{F}_p 中无零点）。
- 置换表达式： $S(x_0, x_1, x_2) = (x_0, x_0x_2 + x_1, -x_0x_1 + x_0x_2 + x_2)$ 。
- 密码学性质：
 - 差分均匀性 $\Delta(S) = p^2$ ；
 - 沃尔什系数：当 $(b_1, b_2) \neq (0, 0)$ 且特定矩阵秩 $\neq 2$ 时， $|\lambda_S(\bar{a}, \bar{b})| = p^2$ ；否则为 p^3 或0。

4 YuS流密码详细设计

4.1 基本参数

- 密钥空间： \mathbb{F}_p^{36} ；
- 密钥流输出： \mathbb{F}_p^{24} （经截断后）；
- 基域要求： $p > 2^{16}$ 且 $p \equiv 2 \pmod{3}$ （推荐 $p = 65537$ （17位）或 $p = 4298506241$ （33位））；
- 推荐轮数：80位安全 \rightarrow 5轮；128位安全 \rightarrow 6轮；
- 截断数： $m = 12$ （截断前12个元素）。

4.2 整体结构

$$YuS_{Key,nc}^r(\bar{x}) = TF_{12} \circ LP \circ RF_r \circ \dots \circ RF_1 \circ AK_{rk}^{-0}(\bar{x})$$

- 输入：常量向量 $CV = (1, 2, \dots, 36) \in \mathbb{F}_p^{36}$ ；
- 流程：密钥白化 $\rightarrow r$ 轮变换 \rightarrow 线性层 \rightarrow 截断 \rightarrow 输出密钥流。

4.3 核心组件实现

4.3.1 轮变换 $RF_i(\bar{x})$

$$RF_i(\bar{x}) = AK_{rk}^{-i} \circ SL \circ LP(\bar{x})$$

- 线性层（LP）： $LP(\bar{v}) = M \cdot (v_0, \dots, v_{35})^T$ ， M 为36阶0-1矩阵（附录A），采用“四俄罗斯方法”优化，加法次数从876降至412。
- S盒层（SL）：将36维输入按3维分组，每组应用 \mathbb{F}_p^3 上的二次置换 S ：

$$SL(v_0, \dots, v_{35}) = (S(v_0, v_1, v_2), \dots, S(v_{33}, v_{34}, v_{35}))$$

- 轮密钥加法 (AK): $AK_{\overline{rk}}(\overline{v}) = (v_0 + rk_0, \dots, v_{35} + rk_{35})$ 。

4.3.2 截断函数 TF_{12}

$$TF_{12}(v_0, \dots, v_{35}) = (v_{12}, \dots, v_{35})$$

- 功能：将36维向量映射为24维，隐藏低次方程，增强安全性。

4.3.3 轮密钥生成

- 轮常量: $\overline{rc}^i = XOF(nc \parallel j, i)$ ($i = 0, \dots, r$), 采用SHAKE128生成;
- 轮密钥: $\overline{rk}^i = (rc_0^i \cdot k_0, \dots, rc_{35}^i \cdot k_{35})$, k_0, \dots, k_{35} 为原始密钥。

4.3.4 密钥流生成

$$YuS_{KG} = YuS_{Key, nc \parallel j}^r(CV), j = 0, \dots, t - 1$$

- 计数器模式生成 t 块密钥流，支持批量数据加密。

5 设计原理

5.1 S盒选择

- 选择3维二次置换：乘法深度=1（最低），乘法复杂度低（每轮12个S盒，仅需24次乘法），差分均匀性 p^2 （优于2维二次置换）。

5.2 状态长度选择

- 36维状态：可被3整除（适配3维S盒），4轮即可抵抗平凡线性化攻击（80位安全），满足 $\log_2 \binom{36+2^4}{2^4} = 43.24 \geq 40$ （安全参数的一半）。

5.3 线性映射选择

- 采用12阶循环矩阵（每个元素为3×3二进制矩阵），最大差分分支数=10，最大线性分支数=6，避免常量乘法开销。

5.4 截断数选择

- 截断12个元素：抵消最后一轮12个低次（ 2^{r-1} 次）输出项，防止攻击者通过逆线性映射推导低次方程。

6 安全性分析

6.1 攻击类型与抵抗能力

| 攻击类型 | 80位安全 (轮数， \log_2 时间) | 128位安全 (轮数， \log_2 时间) | 核心依据 |
|-----------|----------------------------------|--------------------------------|---|
| 线性/差分攻击 | (2, -) | (2, -) | 线性分支数=6（每2轮≥6个活性S盒）， 差分分支数=10（每2轮差分概率 $\geq p^{-10}$ ） |
| 平凡线性化攻击 | (4, ≥ 86.5) | (5, ≥ 128.9) | 4轮单项式数量 $\binom{36+16}{16}$ ，高斯消元复杂度 $\geq 2^{86.5}$ |
| 格罗奔尼乌斯基攻击 | (4, 86.5) | (5, 128.9) | 正则度= 2^r ，复杂度不优于平凡线性化攻击 |
| XL攻击 | (2, 211.3) | (3, 211.3) | 强假设下2轮即可满足方程数 \geq 单项式数， 复杂度 $\geq 2^{211.3}$ |
| GCD攻击 | (1, 479.0) | (1, 479.0) | 单轮攻击复杂度 $O(p^{35}r^22^r)$ ， $p > 2^{16}$ 时 $\geq 2^{479}$ |
| 多碰撞攻击 | 免疫 | 免疫 | 截断操作破坏最后一轮非线性层剥离条件 |

6.2 安全声明

- 同一密钥加密的数据量限制为 $2^{\lambda/2}$ （ λ 为安全级别）；
- 仅保证“秘密密钥模型”下的安全性。

7 实现与性能对比

7.1 实验环境

- 硬件：12代Intel Core i5-12500H（2.50GHz），13GiB内存，18GiB交换空间；Linux服务器（Intel Xeon Gold 6230R，2.10GHz，252GiB内存）；
- 软件：WSL2 Ubuntu 22.04 LTS，C++17，GNU C++11.4.0，HElib-2.3.0（BGV），SEAL-4.1.2（BFV）；
- 打包策略：行-wise打包（并行处理多块数据，吞吐量最优）；
- 评估指标：总评估时间（s）、吞吐量（KiB/s）、每字节周期数（CPB）、噪声预算（bit）。

7.2 客户端性能对比 ($p = 65537$)

| 安全级别 | 算法 | 参数 (r, ks, ps) | 块大小 | 总周期数 | CPB (周期/字节) |
|------|----------|----------------|-------|------------|-------------|
| 80位 | Masta | (4,32,32) | 16384 | 1705935666 | 1531 |
| | Masta | (5,16,16) | 16384 | 654336658 | 1174 |
| | HERA | (4,16,16) | 16384 | 247775198 | 444 |
| | YuS | (5,36,24) | 16384 | 367442978 | 439 |
| 128位 | Masta | (6,32,32) | 16384 | 2233567571 | 2004 |
| | HERA | (5,16,16) | 16384 | 279224559 | 501 |
| | PASTA | (4,64,32) | 16384 | 6053424632 | 5433 |
| | PASTA_v2 | (4,64,32) | 16384 | 3537588770 | 3175 |
| | YuS | (6,36,24) | 16384 | 400495603 | 479 |

7.3 服务器端性能对比 (HElib-BGV)

7.3.1 $p = 65537$

| 安全级别 | 算法 | 参数 (r, ks, ps) | N | 总时间 (s) | 吞吐量 (KiB/s) |
|------|----------|----------------|-------|---------|-------------|
| 80位 | Masta | (4,32,32) | 16384 | 18.338 | 59.331 |
| | Masta | (5,16,16) | 32768 | 22.327 | 48.730 |
| | HERA | (4,16,16) | 32768 | 13.094 | 83.094 |
| | YuS | (5,36,24) | 16384 | 7.474 | 109.179 |
| 128位 | Masta | (6,32,32) | 32768 | 89.936 | 24.195 |
| | HERA | (5,16,16) | 32768 | 19.774 | 55.022 |
| | PASTA | (4,64,32) | 32768 | 100.343 | 21.686 |
| | PASTA_v2 | (4,64,32) | 32768 | 57.173 | 38.060 |
| | YuS | (6,36,24) | 32768 | 19.233 | 84.856 |

7.3.2 $p = 4298506241$

| 安全级别 | 算法 | 参数 (r, ks, ps) | N | 总时间 (s) | 吞吐量 (KiB/s) |
|------|----------|----------------|-------|---------|-------------|
| 80位 | Masta | (4,32,32) | 32768 | 76.891 | 54.935 |
| | Masta | (5,16,16) | 32768 | 38.731 | 54.529 |
| | HERA | (4,16,16) | 32768 | 21.209 | 99.580 |
| | YuS | (5,36,24) | 16384 | 8.441 | 187.660 |
| 128位 | Masta | (6,32,32) | 65536 | 331.497 | 25.484 |
| | HERA | (5,16,16) | 32768 | 30.693 | 68.809 |
| | PASTA | (4,64,32) | 32768 | 151.785 | 27.829 |
| | PASTA_v2 | (4,64,32) | 32768 | 92.894 | 45.471 |
| | YuS | (6,36,24) | 32768 | 28.522 | 111.072 |

7.4 服务器端性能对比（SEAL-BFV，128位安全）

7.4.1 $p = 65537$

| 算法 | 参数 (r, ks, ps) | N | 总时间 (s) | 吞吐量 (KiB/s) | 噪声预算 (bit) |
|--------------------------------------|----------------|-------|---------|-------------|------------|
| Masta | (6,32,32) | 16384 | 52.796 | 20.608 | 4 |
| HERA | (5,16,16) | 16384 | 8.325 | 65.349 | 4 |
| PASTA | (4,64,32) | 16384 | 74.709 | 14.563 | 74 |
| PASTA_v2 | (4,64,32) | 16384 | 32.747 | 33.224 | 98 |
| YuS ($\lceil \log q \rceil = 301$) | (6,36,24) | 16384 | 7.610 | 107.229 | 20 |
| YuS ($\lceil \log q \rceil = 424$) | (6,36,24) | 16384 | 8.832 | 92.392 | 133 |

7.4.2 $p = 4298506241$

| 算法 | 参数 (r, ks, ps) | N | 总时间 (s) | 吞吐量 (KiB/s) | 噪声预算 (bit) |
|--------------------------------------|----------------|-------|---------|-------------|------------|
| Masta | (6,32,32) | 32768 | 375.803 | 11.240 | 224 |
| HERA | (5,16,16) | 32768 | 74.777 | 28.244 | 254 |
| PASTA | (4,64,32) | 32768 | 563.248 | 7.499 | 343 |
| PASTA_v2 | (4,64,32) | 32768 | 259.467 | 16.280 | 369 |
| YuS ($\lceil \log q \rceil = 424$) | (6,36,24) | 16384 | 13.338 | 118.761 | 4 |
| YuS ($\lceil \log q \rceil = 881$) | (6,36,24) | 32768 | 77.420 | 40.920 | 451 |

7.5 关键性能结论

- YuS在客户端CPB指标上优于所有对比方案（80位安全439，128位安全479）；
- 服务器端BGV方案下，80位安全（ $p = 65537$ ）YuS比HERA快1.752倍，吞吐量高1.314倍；
- 33位基域（ $p = 4298506241$ ）下，YuS吞吐量可达187.66 KiB/s（80位安全），远超其他方案；
- SEAL-BFV方案中，YuS噪声预算显著高于HERA（128位安全下133 vs 4），功能稳定性更优。

8 结论与未来工作

8.1 核心贡献

1. 提出有限域上新型二次置换构造方法，刻画其密码学性质，为FHE友好密码设计提供基础组件；
2. 设计YuS流密码，乘法深度低、FHE评估高效，性能全面优于现有方案；
3. 完整的安全性分析与实验验证，覆盖80/128位安全级别，支持不同基域配置。

8.2 未来工作

- 优化嵌入式和GPU平台的实现，拓展实际应用场景；
- 评估YuS抵抗侧信道攻击的能力，增强真实环境安全性；
- 研究更优的二次置换构造，进一步降低乘法复杂度。