IPRainbow

PQCrypto 2022

Ryann Cartor*[1], Max Cartor[2], Mark Lewis[2], Daniel Smith-Tone[2],[3]

(1) Clemson University, (2) University of Louisville, (3) NIST

September 28, 2022

UOV and Rainbow

UOV [Pat97, KS98]

$$P : \mathbb{F}_q^n \to \mathbb{F}_q^{(v+1)}, \quad P = U \circ F \circ T, \quad F = (f^{(1)}, \dots, f^{(v+1)})$$

$$f^{(k)}(\mathbf{x}) = \sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{ij} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{ij} x_i x_j + \sum_{i=1}^{n} \gamma_i x_i + \delta$$

Rainbow [DS05]

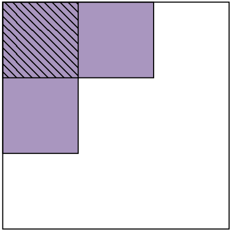
$$P : \mathbb{F}_q^n \to \mathbb{F}_q^{(v+1)(n-v_\ell)}, \quad P = U \circ F \circ T, \quad F = \left(F^{(1)}, F^{(2)}, \dots, F^{(v+1)}\right)$$

$$f_\ell^{(k)}(\mathbf{x}) = \sum_{i=1}^{v_\ell} \sum_{j=1}^{v_\ell} \alpha_{ij\ell} x_i x_j + \sum_{i=1}^{v_\ell} \sum_{j=v_\ell+1}^{n} \beta_{ij\ell} x_i x_j + \sum_{i=1}^{n} \gamma_{i\ell} x_i + \delta_\ell$$

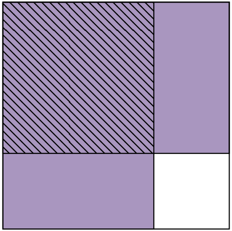
$$0 < v_1 < v_2 < \dots < v_L < n$$

Rainbow

Let $\mathbf{x} \in \mathbb{F}_q^n$. Consider the matrices $\mathbf{F}$ such that $f(x) = \mathbf{x}^\top \mathbf{F} \mathbf{x}$.



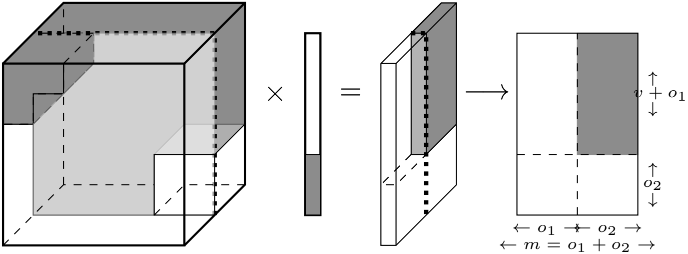
Layer 1 Rainbow Map



Layer 2 Rainbow Map

Rectangular MinRank Attack, [Beu21]

Goal: find $\mathbf{y}$ such that $\operatorname{rank}\left(\sum_{i=1}^{n-o_2+1} y_i \mathbf{P}_i\right) \leq o_2$.



This instance of the MinRank problem requires $n - o_2 + 1$ different $n \times m$ matrices with a target rank of o_2.

Simple Attack, [Beu22]

Discrete differential of the public key:

$$P'(\mathbf{x}, \mathbf{y}) = P(\mathbf{x} + \mathbf{y}) - P(\mathbf{x}) - P(\mathbf{y}).$$

Structure of nested subspaces:

$$\begin{array}{ccccc}
O_2 & \subset & O_1 & \subset & \mathbb{F}_q^n \\
\Big| & \searrow & \Big| & & \Big| \\
P & P'(x,\cdot) & P & & P \\
\downarrow & \searrow & \downarrow & & \downarrow \\
\{0\} & \subset & W & \subset & \mathbb{F}_q^m
\end{array}$$

Simple Attack, [Beu22]

Finding an oil vector

- Fix a random nonzero $\mathbf{x} \in \mathbb{F}_q^n$, define

$$D_{\mathbf{x}}(\mathbf{y}) = P(\mathbf{x}+\mathbf{y}) - P(\mathbf{x}) - P(\mathbf{y}).$$

- Try to find a solution to

$$\begin{cases} D_{\mathbf{x}}(\mathbf{y}) = 0 \\ P(\mathbf{y}) = 0. \end{cases}$$

- For a fixed $\mathbf{x}$, the probability there exists a nontrivial kernel vector $\mathbf{y} \in O_2$ such that $D_{\mathbf{x}}(\mathbf{y}) = 0$ is

$$1 - \prod_{i=0}^{o_2-1} (1 - q^{i-o_2}) \approx q^{-1}.$$

Internal Perturbation Modifier, [Din04]

Given public key $\mathcal{P} = \mathcal{U} \circ \mathcal{F} \circ \mathcal{T}$, where $\mathcal{F} = (f_1, \ldots, f_m)$, choose random quadratic maps $\mathcal{Q} = (q_1, \ldots, q_m)$ with support s.

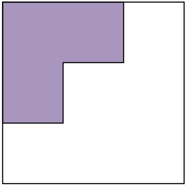
Compute:

$$\text{IP-}\mathcal{P} = \mathcal{U} \circ (\mathcal{F} + \mathcal{Q}) \circ \mathcal{T}$$

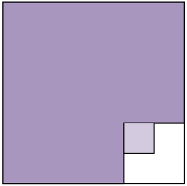
2nd layer central maps:

$$f(\mathbf{x}) = \sum_{i=1}^{v_2} \sum_{j=1}^{v_2} \alpha_{ij} x_i x_j + \sum_{i=1}^{v_2} \sum_{j=v_2+1}^{n} \beta_{ij} x_i x_j + \sum_{i=v_2+1}^{v_2+s} \sum_{j=v_2+1}^{v_2+s} \mu_{ij} x_i x_j,$$

IPRainbow



Layer 1 Rainbow Map.



Layer 2 Rainbow Map.

Figure: The first layer maps remain the same as the unmodified Rainbow first layer maps. Now we consider a $s \times s$ submatrix of the oil times oil section of the second layer map.

Signing Algorithm

Input: IPRainbow central map $\mathcal{F} + \mathcal{Q} = (f_{v_1+1}, \ldots, f_m)$, vector $\mathbf{x} \in \mathbb{F}^m$.
Output: $\mathbf{y} \in \mathbb{F}^n$ such that $\mathcal{F} + \mathcal{Q}(\mathbf{y}) = \mathbf{x}$

1. $y_1, \ldots, y_{v_1} \xleftarrow{\$} \mathbb{F}_q$
2. $\tilde{f}_i := f_i(y_1, \ldots, y_{v_1})$ for $i \in \{v_1 + 1, \ldots, m\}$.
3. $y_{v_1+1}, \ldots, y_{v_2} :=$ GaussElim$(\tilde{f}_{v_1+1}, \ldots, \tilde{f}_m)$.
4. $\hat{f}_j := \tilde{f}_j(y_{v_1+1}, \ldots, y_{v_2})$ for $j \in \{v_2 + 1, \ldots, m\}$.
5. $g_1, \ldots, g_s :=$ GaussElim$(\hat{f}_{v_2+1}, \ldots, \hat{f}_m)$.
6. $y_{v_2+1}, \ldots, y_n :=$ PolySolve$(g_1, \ldots, g_s)$.
7. $\mathbf{y} := y_1, \ldots, y_{v_1}, y_{v_1+1}, \ldots, y_{v_2}, y_{v_2+1}, \ldots, y_n$.

IPRainbow: Security Estimates

Simple Attack

Lemma

For sufficiently small s, *the linear map* $D_{\mathbf{x}}$ *has an* O_2 *vector* $\mathbf{y}$ *in its left kernel that satisfies* $P(\mathbf{y}) = \mathbf{0}$ *with probability approximately* q^{-s-1}.

IPRainbow: Security Estimates

Rectangular MinRank Attack

- The Simple attack can be combined with the Rectangular MinRank attack.
- The attack still involves the finding a second layer oil variable and uses the property that such a vector satisfies the public equations

$$3q^{s+1}(n-m-1)(o_2+1)\binom{m'}{r}^2\binom{n-m+b-3}{b}^2$$

field multiplications, where $m' \leq m$ and b are chosen to optimize the attack.

Parameters: NIST Level I

Scheme-(q, o_1, o_2, v, s)	Signing time	Verif. time	Key size	Sign. size	Security
UOV-$(257, 47, 0, 71, 0)$	0.75ms	0.37ms	330.2KB	118	144.5
IPR-$(257, 32, 32, 32, 9)$	13700ms	0.37ms	298.2KB	96	145
IPR-$(257, 32, 32, 36, 8)$	1976.5ms	0.38ms	323.4KB	100	144.3
IPR-$(257, 32, 32, 38, 7)$	491ms	0.44ms	336.4KB	102	142.4
IPR-$(257, 32, 36, 44, 6)$	127ms	0.51ms	430.6KB	112	143.1

Parameters: NIST Level III

Scheme-(q, o_1, o_2, v, s)	Signing time	Verif. time	Key size	Sign. size	Security
UOV-$(257, 71, 0, 107, 0)$	138ms	1.19ms	1131.9KB	178	205.5
IPR-$(257, 32, 42, 68, 9)$	16552ms	0.85ms	751.9KB	142	207.1
IPR-$(257, 32, 48, 70, 8)$	4579ms	1.10ms	906.6KB	150	206.8
IPR-$(257, 32, 48, 76, 7)$	987ms	1.02ms	980.4KB	156	206.9
IPR-$(257, 32, 50, 84, 6)$	269ms	1.44ms	1137.4KB	166	206.9

Parameters: NIST Level V

Scheme-(q, o_1, o_2, v, s)	Signing time	Verif. time	Key size	Sign. size	Security
UOV-$(257, 97, 0, 146, 0)$	5.240ms	4.63ms	2854.1KB	243	271
UOV-$(257, 98, 0, 147, 0)$	5.320ms	4.67ms	2931.3KB	245	275
IPR-$(257, 36, 64, 112, 9)$	22026ms	2.39ms	2259.4KB	212	272
IPR-$(257, 36, 64, 122, 8)$	29597ms	2.46ms	2477KB	222	271
IPR-$(257, 36, 64, 135, 7)$	1123ms	5.30ms	2774.9KB	235	271.5
IPR-$(257, 36, 66, 148, 6)$	298ms	5.28ms	3202.5KB	250	272.4

References I

Ward Beullens.
Improved cryptanalysis of UOV and rainbow.
In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I*, volume 12696 of *Lecture Notes in Computer Science*, pages 348–373. Springer, 2021.

Ward Beullens.
Breaking rainbow takes a weekend on a laptop.
IACR Cryptol. ePrint Arch., page 214, 2022.

Jintai Ding.
A new variant of the matsumoto-imai cryptosystem through perturbation.
In Feng Bao, Robert H. Deng, and Jianying Zhou, editors, *Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004*, volume 2947 of *Lecture Notes in Computer Science*, pages 305–318. Springer, 2004.

References II

Jintai Ding and Dieter Schmidt.
Rainbow, a new multivariable polynomial signature scheme.
In John Ioannidis, Angelos D. Keromytis, and Moti Yung, editors, *Applied Cryptography and Network Security, Third International Conference, ACNS 2005, New York, NY, USA, June 7-10, 2005, Proceedings*, volume 3531 of *Lecture Notes in Computer Science*, pages 164–175, 2005.

Aviad Kipnis and Adi Shamir.
Cryptanalysis of the oil & vinegar signature scheme.
In Hugo Krawczyk, editor, *Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings*, volume 1462 of *Lecture Notes in Computer Science*, pages 257–266. Springer, 1998.

Jacques Patarin.
The oil and vinegar signature scheme.
Presented at the Dagstuhl Workshop on Cryptography, September 1997.

Thank you for your attention!