A Cryptanalysis of LUOV using the Subfield Differential Attack (SDA)

PI: Jintai Ding Email: jintai.ding@gmail.com
Department of Mathematical Sciences, University of Cincinnati

University of CINCINNATI

Abstract

In 2017 Ward Beullens *et al* submitted the digital signature scheme Lifted Unbalanced Oil Vinegar as a potential candidate for NIST's post-quantum cryptography standardization. LUOV is a modified version of Patarin's Oil and Vinegar Scheme intended to increase efficiency. A new attack called SDA is introduced which exploits the "lifted" structure. The parameters originally set fail to meet NIST security requirements due to SDA. The Oil and Vinegar structure is never exploited making other such signature schemes secure from SDA.

LUOV

LUOV is a multivariate signature scheme, so the public key $\mathcal{P} : \mathbb{F}_{2^r}^n \rightarrow \mathbb{F}_{2^r}^m$ is composed of m quadratic polynomials in $n = m + v$ variables over a finite field (which in LUOV's case has characteristic two). $\mathcal{P}$ will have both Oil and Vinegar structure and be "lifted."

The Oil and Vinegar structure of $\mathcal{P}$ means that $\mathcal{P} = \mathcal{F} \circ \mathcal{T}$ where $\mathcal{T} : \mathbb{F}_{2^r}^n \rightarrow \mathbb{F}_{2^r}^n$ is an invertible linear map and $\mathcal{F} : \mathbb{F}_{2^r}^n \rightarrow \mathbb{F}_{2^r}^m$ is composed of Oil and Vinegar polynomials. By Oil and Vinegar polynomial it is meant quadratics of the form:

$$\sum_{i=1}^{v}\sum_{j=i}^{n} \alpha_{i,j} x_i x_j + \sum_{i=1}^{n} \beta_i x_i + \gamma.$$

This allows efficient preimages for $\mathcal{F}$ to be found by randomly assigning values for the first v variables, resulting in a linear system. As $\mathcal{T}$ is also easily inverted, knowing the decomposition of $\mathcal{P}$ provides an efficient way to find preimages for $\mathcal{P}$ which are used as signatures.

The new "lifted" structure of $\mathcal{P}$ is that all the coefficients of $\mathcal{F}$ and $\mathcal{T}$, and thus $\mathcal{P}$, are from the prime subfield $\mathbb{F}_2 = \{0, 1\}$. The authors of LUOV claimed that this does not adversly effect the scheme's security, but it allows one to exploit the structure of field extensions.

Finite Field Representation

It is elementary field theory that all finite fields can be represented as a quotient ring of a polynomial ring of a smaller finite field. That is

$$\mathbb{F}_{2^r} \cong \mathbb{F}_{2^d}[t] / < f(t) >$$

provided that $d | r$ and $f(t)$ is an irreducible polynomial of degree r/d in $\mathbb{F}_{2^d}[t]$.
This allows less intensive computation.

A Lemma on Random Maps

During SDA we will restrict the domain to a smaller subset. We will need to calculate the probability for a given message to have a signature, which we will do heuristically using random maps. Suppose there exists a random map $\mathcal{Q} : \mathbb{F}_{2^d}^n \rightarrow \mathbb{F}_{2^r}^m$. For a given $\mathbf{y} \in \mathbb{F}_{2^r}^m$, the probability that there is no preimage for $\mathbf{y}$ is given by the probability that all elements of the domain are not mapped to $\mathbf{y}$. That is

$$(1 - |\mathbb{F}_{2^r}^m|)^{\left|\mathbb{F}_{2^d}^n\right|} = \left(1 - \frac{1}{2^{mr}}\right)^{2^{dn}} = \left[\left(1 - \frac{1}{2^{mr}}\right)^{2^{mr}}\right]^{2^{dn-mr}} \approx \frac{1}{e^{2^{dn-mr}}}.$$

The Subfield Differential Attack

Let $\mathcal{P} : \mathbb{F}_{2^r}^n \rightarrow \mathbb{F}_{2^r}^m$ be a LUOV public key with $\mathcal{P} = \{\tilde{f}_1, \cdots, \tilde{f}_m\}$. We note that each $\tilde{f}_k$ will look like a random quadratic over $\mathbb{F}_2$. Let $\mathbf{y} = (y_1, \cdots, y_m) \in \mathbb{F}_{2^r}^m$ be the message we want to sign.
The differential is defined to be $\mathbf{x}' + \bar{\mathbf{x}}$ where $\mathbf{x}' = (x_1', \cdots, x_n') \in \mathbb{F}_{2^r}^n$ is fixed and $\bar{\mathbf{x}} = (\bar{x}_1, \cdots, \bar{x}_n) \in \mathbb{F}_{2^d}^n$ is indeterminate in some subfield $\mathbb{F}_{2^d} \leq \mathbb{F}_{2^r}$. Let $s = r/d$. We note that $P(\mathbf{x}' + \bar{\mathbf{x}})$ is a map from $\mathbb{F}_{2^d}^n$ to $\mathbb{F}_{2^r}^m$ which we hope to solve.
After expanding and separating the quadratic terms in $P(\mathbf{x}' + \bar{\mathbf{x}}) = \mathbf{y}$, the k^{th} component looks like:

$$\tilde{f}_k(\mathbf{x}' + \bar{\mathbf{x}}) = \sum_{i=1}^{n}\sum_{j=i}^{n} \alpha_{i,j,k}(x_i' x_j' + x_i' \bar{x}_i + x_j' \bar{x}_j) + \sum_{i=1}^{n} \beta_{i,k}(x_i' + \bar{x}_i) + \gamma_k \quad + \sum_{i=1}^{n}\sum_{j=i}^{n} \alpha_{i,j,k} \bar{x}_i \bar{x}_j = \quad y_k.$$

Using the quotient ring representation, the fact that $\alpha_{i,j,k}$'s, $\beta_{i,k}$'s $\in \mathbb{F}_2$, and x_i''s are known, this can be further expressed as:

$$\tilde{f}_k(\mathbf{x}' + \bar{\mathbf{x}}) = \sum_{i=1}^{s-1} L_{i,k}(\bar{x}_1, \cdots, \bar{x}_n) t^i + Q_k(\bar{x}_1, \cdots, \bar{x}_n) = y_k = \sum_{i=0}^{s-1} w_{i,k} t^i,$$

where $L_{i,k}(\bar{x}_1, \cdots, \bar{x}_n)$ is a linear and $Q_k(\bar{x}_1, \cdots, \bar{x}_n)$ is a quadratic polynomial in $\mathbb{F}_{2^d}[\bar{x}_1, \cdots, \bar{x}_n]$, and $w_{i,k} \in \mathbb{F}_{2^d}$.
If we treat $P(\mathbf{x}' + \bar{\mathbf{x}})$ as a random map, by the lemma above, if d is sufficiently large there should exist at least one solution. For efficiency, choose the smallest such d.
To find a solution, one first finds the solution space S to the system of linear equations

$$\{L_{i,k}(\bar{x}_1, \cdots, \bar{x}_n) = w_{i,k} | 1 \leq i \leq s - 1, 1 \leq k \leq m\}$$

which represents the coefficients of t^i where i is from 1 to $s - 1$. Using S as a change of variables for the Q_k's, one then uses the already known ways to brute force the new quadratic system: $\{Q_k(S) = w_{0,k} | 1 \leq k \leq m\}$. The solution to this is the desired $\bar{\mathbf{x}}$ and the signature is $\mathbf{x}' + \bar{\mathbf{x}}$.

SDA NIST Round 2 Parameters

In the following table we provide the submitted parameters for LUOV in the second round of the NIST competition as well as our choose of intermediate field, projected chance of failure, and the complexity of SDA for those parameters.

Security Level	r	m	v	n	d	Probability of Failure	$\log_2$ Complexity
II	8	58	237	295	2	$\exp(-2^{126})$	107
IV	8	82	323	405	2	$\exp(-2^{154})$	143
V	8	107	371	478	2	$\exp(-2^{100})$	184
II	48	43	222	265	8	$\exp(-2^{56})$	135
IV	64	61	302	363	16	$\exp(-2^{1904})$	202
V	80	76	363	439	16	$\exp(-2^{944})$	244

Conclusion

So the problem of brute forcing a signature for a LUOV scheme over the field $\mathbb{F}_{2^r}$ has been reduced to brute forcing a solution to a quadratic system over a suitable subfield $\mathbb{F}_{2^d}$, provided one exists. The following table shows the NIST security requirements for the levels submitted:

Level	$\log_2$ Complexity
II	146
IV	210
V	272

As the complexity of SDA is lower for each category, LUOV as it was presented in the second round is not viable.
We feel strongly that SDA has great potential to be expanded upon, and that there are more ways to exploit the structure of "lifted" quadratic maps.

Why this Matters

As our society relies more and more on the ability to digitally communicate openly but securely, effective cryptography must be developed and tested. Especially with the advent of algorithms with ability to exploit quantum computation, like Shor's Algorithm, and computers that can perform these algorithms becoming a reality, post-quantum schemes like LUOV need to be pursued and tested for any flaws in design.

Acknowledgement

We would like to thank the following for funding:

- NSF: "Multivariate Public Key Cryptosystems - Candidates for the Next Generation Post-Quantum Standards": #CNS-1814221
- NIST: "National Institute of Standards and Technology Benchmark the Security and Performance Parameters for Post-Quantum Cryptography - Multivariate Public Key Cryptosystems": #60NANB15D029.
- The Taft Research Center.

NSF NIST