Cryptanalysis of the Binary Permuted Kernel Problem

Thales Bandiera Paiva   Routo Terada

Institute of Mathematics and Statistics
University of Sao Paulo, Brazil

tpaiva@ime.usp.br
rt@ime.usp.br

2021-06-18

Motivation

Recently, NIST expressed concerns about lack of diversity in signatures

Permuted Kernel Problem is an interesting candidate for signatures

1. Combinatorial NP-hard problem
2. Easy to understand and implement
3. Relatively efficient signatures

However

- Quantum security is not sufficiently studied
- **Security of the PKP for small fields is not well understood**

Permuted Kernel Problem

(Generalized) Permuted Kernel Problem - PKP

- Fix a prime field order p
- Let $\mathbf{A}$ be a matrix from $\mathbb{F}_p^{m \times n}$ with $n > m$
- Let $\mathbf{V}$ be a matrix from $\mathbb{F}_p^{n \times \ell}$
- Find row permutation π such that $\mathbf{AV}_\pi = \mathbf{0}$

Shamir [Sha89] showed an IDS based on a proof of knowledge of π

PKP-DSS [BFK$^+$19] applies Fiat-Shamir transform over Shamir's IDS

Today we focus only on the problem, not in the DSS

Attacks and parameters of Binary PKP

Attacks are usually based on a time-memory tradeoff

Best attack is by Koussa et al. [KMRP19]

Parameter set	Targeted security level	After [KMRP19]	p	n	m	ℓ
Binary PKP–76 [LP12]	79	76	2	38	15	10
Binary PKP–89 [LP12]	98	89	2	42	15	11

Two opportunities for improvement:

1. Previous approaches assume hashtables of size 2^{50} bytes ≥ 1 petabyte
2. None of the previous works consider the Binary PKP variant [LP12]

Contribution

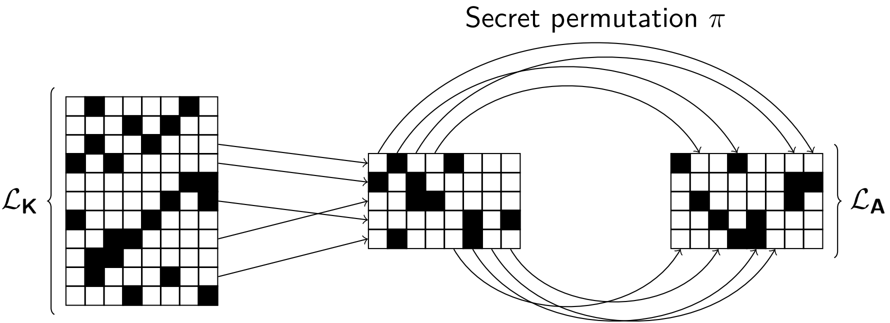
We present the first attack targeting binary PKP

- Does not need a huge amount of memory, unlike previous work
- We implemented the attack and tested its practical performance
- We provide both concrete and asymptotic analyses of the algorithms

Parameter set	Targeted security level	After [KMRP19]	Our attack
Binary PKP–76 [LP12]	79	76	63
Binary PKP–89 [LP12]	98	89	77

Our attack: outline

- Let w be a small integer
- Build set $\mathcal{L}_{\mathbf{A}}$ of vectors of weight w in the rowspace of $\mathbf{A}$
- Build set $\mathcal{L}_{\mathbf{K}}$ of vectors of weight w in $\mathbf{K} = \ker \mathbf{V}$
  $\mathbf{A}\mathbf{V}_\pi = \mathbf{0} \implies$ Every element in $\mathcal{L}_{\mathbf{A}}$ must appear permuted in $\mathcal{L}_{\mathbf{K}}$
- Find subset of $\mathcal{L}_{\mathbf{K}}$ that is equal to $\tau(\mathcal{L}_{\mathbf{A}})$ for some permutation τ
- Get lucky so that $\tau = \pi$



Building sets of low weight vectors

In general, this is a very hard task

However, the parameters of binary PKP are very small ($m = 15, n = 38$)

- Stern's algorithm runs efficiently
- One can even use brute-force in some cases

For Binary PKP-76, a few minutes in SageMath are enough

Matching step

We use a simple depth-first search based algorithm with the invariant

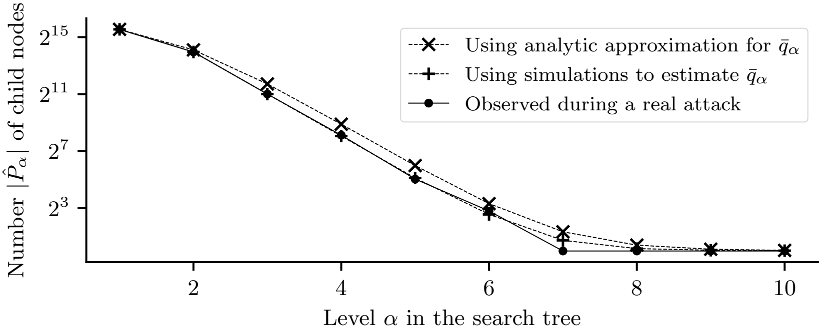
- At each level α, the algorithm holds a matrix $\mathbf{M}$ that is equal to the first α rows of $\mathcal{L}_{\mathbf{A}}$ up to some permutation τ

We provide a concrete analysis of the expected number of child nodes

Let $\overline{q}_\alpha$ be the fraction of vectors in $\mathcal{L}_{\mathbf{K}}$ that can be added in each level

We show how to estimate $\overline{q}_\alpha$ analytically or with simulations

Matching step: analysis



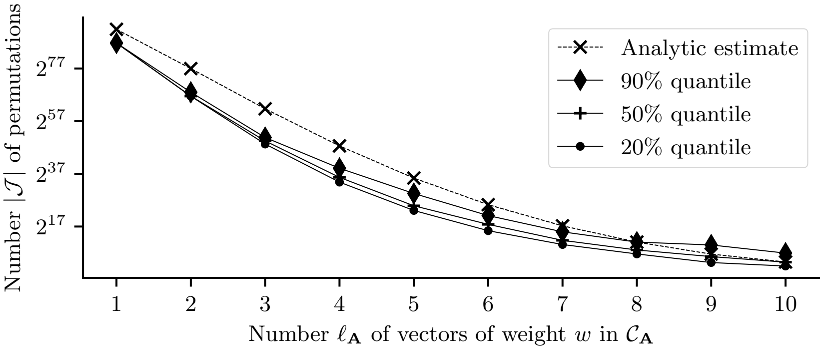
Binary PKP–76 parameter set with attack parameter $w = 8$

Finding permutation π

After a matching is found, we want to use it to find π

- If $\mathcal{L}_{\mathbf{A}}$ has a large number of repeated columns $\Rightarrow$ more permutations
- But the linear relation $\mathbf{AV}_{\pi} = \mathbf{0}$ may be used to speed up the search

Let $\ell_{\mathbf{A}}$ be the size of $\mathcal{L}_{\mathbf{A}}$



Binary PKP–76 parameter set with attack parameter $w = 8$

Choosing attack parameters $\ell_{\mathbf{A}}$ and w

The attack will only be effective if

- The rowspace of $\mathbf{A}$ has at least $\ell_{\mathbf{A}}$ vectors of weight w

The maximum possible value for $\ell_{\mathbf{A}}$ be modeled as a Binomial r.v.

- $N = \binom{n}{w}$ (Number of vectors of weight w)
- $p = 2^{m-n}$ (Probability that a vector is in the rowspace $\mathcal{C}_{\mathbf{A}}$ of $\mathbf{A}$)

With respect to w

- Parameter w must be the smallest possible so that $\mathcal{L}_{\mathbf{K}}$ **is small**
- Parameter w must be the large enough so that $\mathcal{L}_{\mathbf{A}}$ is **not too small**

Complexity of the attack

The work factor of the attack using parameters $(w, \ell_{\mathbf{A}})$ is

$$\mathbf{WF}_{\textsc{Attack}} = \mathbf{WF}_{\textsc{LowWeightSets}} + \left(\mathbf{WF}_{\textsc{Search}}\right)\left(\mathbf{WF}_{\textsc{Perms}}\right)$$

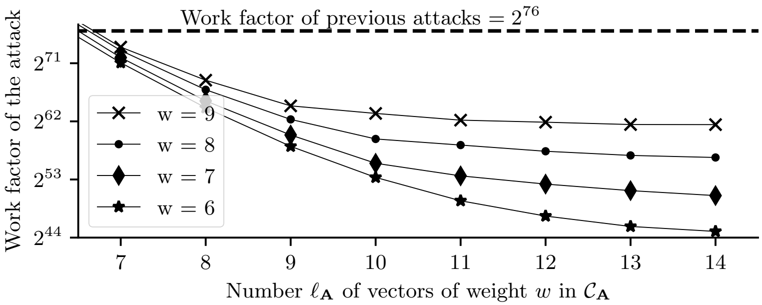
In which each term is

$$\mathbf{WF}_{\textsc{LowWeightSets}} \leq 2\binom{n}{w}$$ ☺

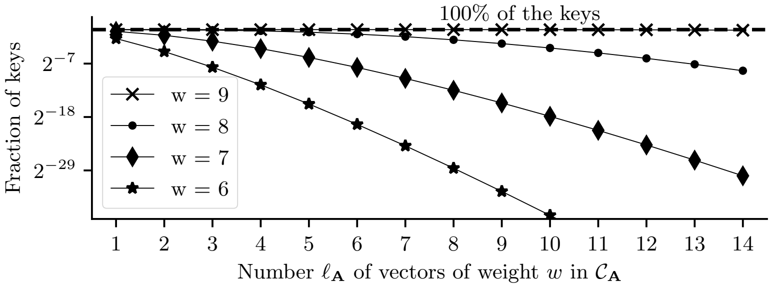
$$\mathbf{WF}_{\textsc{Search}} = |\mathcal{L}_{\mathbf{K}}|^{\ell_{\mathbf{A}}} \prod_{\alpha=0}^{\ell_{\mathbf{A}}-1} \left(\frac{1}{\binom{n}{w}} \prod_{k=0}^{\alpha} \binom{np(k,\alpha)}{wp(k,\alpha)}^{\binom{\alpha}{k}} \right)$$ ☹

$$\mathbf{WF}_{\textsc{Perms}} = \prod_{k=0}^{\ell_{\mathbf{A}}} \left(\frac{(np(k,\ell_{\mathbf{A}}))!}{(mp(k,\ell_{\mathbf{A}}))!} \right)^{\binom{\ell_{\mathbf{A}}}{k}}$$ ☹

$$\text{where } p(k,\alpha) = \left(\frac{w}{n}\right)^{k} \left(1 - \frac{w}{n}\right)^{\alpha-k}$$ 😐



Work factor of previous attacks = 2^{76}
Work factor of the attack
2^{71}
2^{62}
2^{53}
2^{44}
w = 9
w = 8
w = 7
w = 6
7
8
9
10
11
12
13
14
Number $\ell_{\mathbf{A}}$ of vectors of weight w in $\mathcal{C}_{\mathbf{A}}$



100% of the keys
Fraction of keys
2^{-7}
2^{-18}
2^{-29}
w = 9
w = 8
w = 7
w = 6
1
2
3
4
5
6
7
8
9
10
11
12
13
14
Number $\ell_{\mathbf{A}}$ of vectors of weight w in $\mathcal{C}_{\mathbf{A}}$

Asymptotic complexity

Let $n \to \infty$

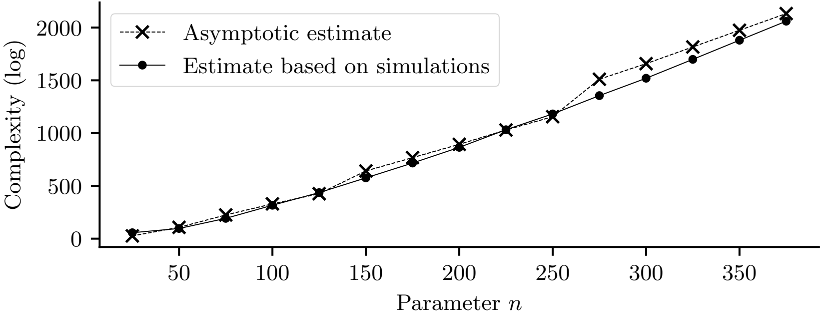
- $w \approx n/2 \implies$ Allows some simplifications $p(k, \alpha) = 2^{-\alpha}$
- $\ell_{\mathbf{A}} \approx \lceil \log n \rceil \implies \mathbf{WF}_{\text{PERMS}} = 1$

We show that the asymptotic work factor of the attack is given as

$$\begin{aligned}\mathbf{WF}_{\text{ATTACK}} &= \mathbf{WF}_{\text{LOWWEIGHTSETS}} + (\mathbf{WF}_{\text{SEARCH}})(\mathbf{WF}_{\text{PERMS}}) \\ &= O\left(2^{\left(n-l-mn^{-1/5}\right)(\lceil \log n \rceil - 1) - 0.91n + \frac{1}{2}\log n}\right)\end{aligned}$$

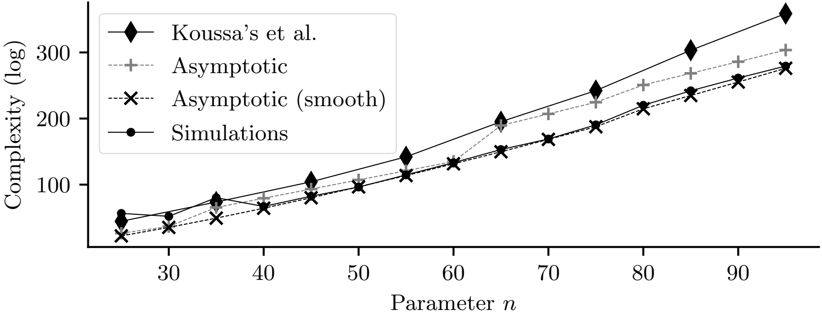
Asymptotic estimates

$$\mathbf{WF}_{\text{ATTACK}} = O\left(2^{\left(n-l-mn^{-1/5}\right)(\lceil \log n \rceil - 1) - 0.91n + \frac{1}{2}\log n}\right)$$



Asymptotic comparison with Koussa's et al.

$$\mathbf{WF}^{\text{Smooth}}_{\text{Attack}} = O\left(2^{\left(n-l-mn^{-1/5}\right)(\log n - 1) - 0.91n + \frac{1}{2}\log n}\right)$$



Conclusion and Future Work

We presented the first attack against binary PKP

Binary PKP should be avoided

- Use larger fields for better security

We are working on extending the analysis for small fields ($p = 3, 5$)

- Faster to search for matchings and valid permutations
- Low weight codewords are more rare

The attack does not apply directly for PKP-DSS

- However it may be interesting to consider backdoors in matrix $\mathbf{A}$

Source code is available at `www.ime.usp.br/~tpaiva`

References I

[BCCG92] Thierry Baritaud, Mireille Campana, Pascal Chauvaud, and Henri Gilbert, *On the security of the permuted kernel identification scheme*, Annual International Cryptology Conference, Springer, 1992, pp. 305–311.

[BFK+19] Ward Beullens, Jean-Charles Faugère, Eliane Koussa, Gilles Macario-Rat, Jacques Patarin, and Ludovic Perret, *PKP-based signature scheme*, International Conference on Cryptology in India, Springer, 2019, pp. 3–22.

[KMRP19] Eliane Koussa, Gilles Macario-Rat, and Jacques Patarin, *On the complexity of the Permuted Kernel Problem*, IACR Cryptology ePrint Archive **2019** (2019), 412.

[LP12] Rodolphe Lampe. and Jacques Patarin., *Analysis of some natural variants of the PKP algorithm*, Proceedings of the International Conference on Security and Cryptography - Volume 1: SECRYPT, (ICETE 2012), INSTICC, SciTePress, 2012, pp. 209–214.

[PC93] Jaques Patarin and Pascal Chauvaud, *Improved algorithms for the permuted kernel problem*, Annual International Cryptology Conference, Springer, 1993, pp. 391–402.

[Pou97] Guillaume Poupard, *A realistic security analysis of identification schemes based on combinatorial problems*, European transactions on telecommunications **8** (1997), no. 5, 471–480.

[Sha89] Adi Shamir, *An efficient identification scheme based on permuted kernels*, Conference on the Theory and Application of Cryptology, Springer, 1989, pp. 606–609.