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

2021-06-23

The problem

Binary Permuted Kernel Problem [LP12]

- Let $\mathbf{A}$ be a binary $m \times n$ matrix
- Let $\mathbf{V}$ be a binary $n \times \ell$ matrix
- Find a row permutation π such that $\mathbf{AV}_\pi = \mathbf{0}$

PKP is believed to be secure against quantum computers

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

- But uses p-ary matrices and $\ell = 1$

Contribution

We present the first attack targeting binary PKP

- Low memory requirements, unlike previous work (petabytes)
- We implemented the attack and tested its practical performance
- We provide both concrete and asymptotic analyses of the algorithms

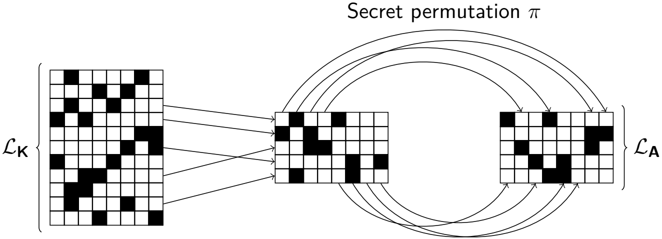
Parameter set	Targeted security level	After [KMRP19]	Our attack
Binary PKP–76 [LP12]	79	76	63
Binary PKP–89 [LP12]	98	89	77

Important limitation: The attack only works for Binary PKP

Outline of our attack

1. Let w and $\ell_{\mathbf{A}}$ be a small integers
2. Build sets
   - $\mathcal{L}_{\mathbf{A}}$ of $\ell_{\mathbf{A}}$ vectors of weight w in the rowspace $\mathcal{C}_{\mathbf{A}}$ of $\mathbf{A}$
   - $\mathcal{L}_{\mathbf{K}}$ of vectors of weight w in $\mathbf{K} = \ker \mathbf{V}$, that is $\mathbf{KV} = \mathbf{0}$

   Since $\mathbf{AV}_{\pi} = \mathbf{0}$ then each vector in $\mathcal{L}_{\mathbf{A}}$ must appear in $\mathcal{L}_{\mathbf{K}}$ permuted by π^{-1}
3. Find subset $\mathbf{M}$ of $\mathcal{L}_{\mathbf{K}}$ such that $\tau(\mathbf{M}) = \mathcal{L}_{\mathbf{A}}$ for some column permutation τ
4. Get lucky so that $\tau = \pi$



Example for $w = 2$ and $\ell_{\mathbf{A}} = |\mathcal{L}_{\mathbf{A}}| = 5$

Complexity of the attack

For the attack to work, rowspace $\mathcal{C}_{\mathbf{A}}$ must contain $\ell_{\mathbf{A}}$ vectors of weight w

- Small w means $\mathcal{L}_{\mathbf{K}}$ is smaller, which makes attack faster
- But if w is too small then $\mathcal{L}_{\mathbf{A}}$ may have lots of repeating columns
  $\implies$ Exponential number of permutations to test (unless $\ell_{\mathbf{A}}$ large)

Performance when attacking BPKP–76

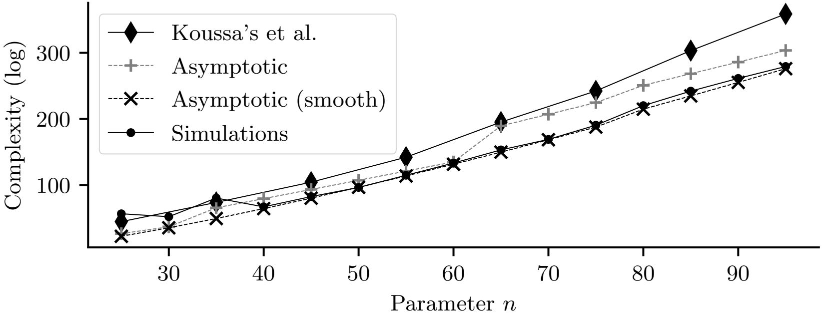
w	$\ell_{\mathbf{A}}$	Fraction of keys	Predicted work factor (matrix-vector products)	Empirical estimate (clock cycles)
5	14	0	$2^{39.46}$	$2^{34.39}$
6	11	$2^{-43.32}$	$2^{49.75}$	$2^{47.58}$
7	10	$2^{-17.86}$	$2^{55.84}$	$2^{48.62}$
8	9	$2^{-2.88}$	$2^{62.28}$	$2^{60.54}$
9	9	$2^{-0.00}$	$2^{64.16}$	$2^{62.31}$

Asymptotic complexity

The attack works when $w \approx n/2$ and $\ell_{\mathbf{A}} \approx \log n$ for 100% of keys with

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

Can be smoothed by considering $\log n$ instead of $\lceil \log n \rceil$



Conclusion and Future Work

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`
- `https://github.com/thalespaiva/attack-on-binary-pkp`

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.