Practical Attack on All Parameters of the HPPC Signature Scheme

Pierre Briaud[1], Maxime Bros[2], Ray Perlner[2] and **Daniel Smith-Tone**[2,3]

[1]Simula UiB
[2]National Institute of Standards and Technology
[3]University of Louisville

14 August, 2025

NIST Additional Signatures

Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process

Updated October 2022 to reflect that IP statements can be accepted digitally.

Table of Contents

Authority: This work is bein
Federal Information Security I

NIST
Search CSRC
CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PROJECTS

Post-Quantum Cryptography: Additional Digital Signature Schemes

Overview

The Round 2 candidates were announced October 24, 2024. NIST IR 8528, *Status Report on the First Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process* is now available.

NIST announced that the PQC standardization process is continuing with a fourth round, with the following KEMs still under consideration: BIKE, Classic McEliece, HQC, and SIKE. However, there are no remaining digital signature candidates under consideration. As such, NIST posted a call for additional digital signature proposals to be considered in the PQC standardization process. The call for submissions closed June 1, 2023, with forty algorithms being evaluated in the first rounnd.

Background

PROJECT LINKS

Overview
News & Updates
Publications

ADDITIONAL PAGES

Standardization of Additional Digital Signature Schemes
Call for Proposals

Candidate: HPPC

Cryptology ePrint Archive

Papers Submissions About

Paper 2023/830

HPPC: Hidden Product of Polynomial Composition

Borja Gomez Rodriguez

Abstract

The article introduces HPPC a new Digital Signature scheme that intends to resist known previous attacks applied to HFE-based schemes like QUARTZ and GeMSS. The idea is to use maximal degree for the central HFE polynomial whereas the trapdoor polynomial has low degree in order to sign messages by finding polynomial roots in an extension field via Berlekamp's algorithm. This work has been submitted to NIST's Post-Quantum Cryptography challenge (PQC) and code is available at https://github.com/kub0x/MPKC-HPPC

Metadata

Available format(s)

PDF

Category

Attacks and cryptanalysis

Publication info

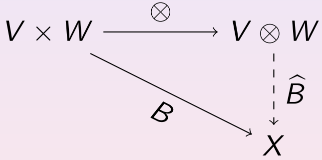
Preprint.

Keywords

multivariate public key cryptography, mpkc, digital signature, public key, quadratic equations, HFE

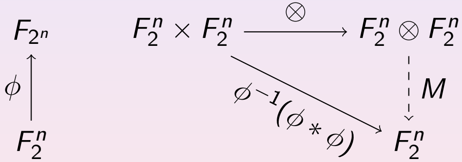
Foundational Idea

Exploit the universal property of the tensor product.



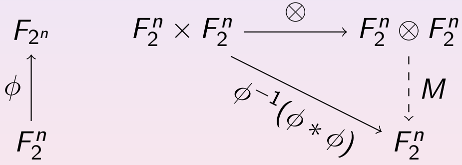
Foundational Idea

Exploit the universal property of the tensor product to model the product in F_{2^n}.



Foundational Idea

Exploit the universal property of the tensor product to model the product in F_{2^n}.



Given $F_{2^n} = F_2[x]/\langle f(x) \rangle$, we have $\mathbf{M} = \begin{bmatrix} \mathbf{I}_n & \mathbf{C}_f & \cdots & \mathbf{C}_f^{n-1} \end{bmatrix}$.

Utility

The mixed product property allows for some tricks.

Mixed Product Property

$$(\mathbf{A} \otimes \mathbf{B})(\mathbf{C} \otimes \mathbf{D}) = (\mathbf{AC}) \otimes (\mathbf{BD}).$$

$$\phi^{-1}\left(\phi\left(\mathbf{Ax}\right)\phi\left(\mathbf{Bx}\right)\right) = \mathbf{M}(\mathbf{A} \otimes \mathbf{B})(\mathbf{x} \otimes \mathbf{x}).$$

SQUARE in this Framework

Consider SQUARE. Choose invertible $S, T : F_q^n \to F_q^n$ and define $F(X) = X^2$.
The SQUARE public key is given by $P(\mathbf{x}) = T \circ \phi^{-1} \circ F \circ \phi \circ S(\mathbf{x})$.
With the above framework, we may express this map as

$$P(\mathbf{x}) = T(\mathbf{M}(S \otimes S)(\mathbf{x} \otimes \mathbf{x})),$$

or, using matrix forms $\mathbf{S}, \mathbf{T}$ of the linear maps S, T,

$$P(\mathbf{x}) = \mathbf{TM}(\mathbf{S} \otimes \mathbf{S})(\mathbf{x} \otimes \mathbf{x}).$$

HPPC

Hidden **P**roduct of **P**olynomials **C**omposition

Choose $n \in \mathbb{Z}^+$ and construct $F_{2^n} = F[x]/\langle f(x) \rangle$ using the irreducible f. Fix matrices $\mathbf{S}, \mathbf{T}, \mathbf{M}$ as above. Choose two linearized polynomials

$$\ell_1(X) = \sum_{i=0}^{n-1} \alpha_i X^{2^i}, \text{ and } \ell_2(X) = \sum_{i=0}^{d} \beta_i X^{2^i}.$$

Let $\mathbf{L}_1, \mathbf{L}_2$ be the matrix forms of ℓ_1, ℓ_2.

$$P(\mathbf{x}) = \mathbf{TM}(\mathbf{L}_1 \otimes \mathbf{L}_2\mathbf{L}_1)(\mathbf{S} \otimes \mathbf{S})(\mathbf{x} \otimes \mathbf{x}).$$

Inversion

Note that if $\mathbf{x}' = \mathbf{L}_1\mathbf{S}\mathbf{x}$, we have

$$Q(\mathbf{x}') = \mathbf{TM}(\mathbf{I}_n \otimes \mathbf{L}_2)(\mathbf{x}' \otimes \mathbf{x}') = \mathbf{TM}(\mathbf{L}_1 \otimes \mathbf{L}_2\mathbf{L}_1)(\mathbf{S} \otimes \mathbf{S})(\mathbf{x} \otimes \mathbf{x}) = P(\mathbf{x}).$$

Since $\mathbf{M}(\mathbf{I}_n \otimes \mathbf{L}_2)(\mathbf{x}' \otimes \mathbf{x}') = \phi^{-1}(\phi(\mathbf{x}')\phi(\mathbf{L}_2\mathbf{x}'))$, allowing $X' = \phi(\mathbf{x}')$,

$$Q(\mathbf{x}') = \mathbf{T}\phi^{-1}(X'\ell_2(X')).$$

We may invert $G(X') = X'\ell_2(X')$ (of degree $2^d + 1$) by Berlekamp.

On Semi-Regularity

The specification of HPPC claims (Section 7.2) that experiments support the semi-regularity of $P(\mathbf{x}) - \mathbf{y}$. However...

- Evidence suggests that experiments used the SageMath command `degree_of_semi_regularity`.
- The SageMath command `degree_of_semi_regularity` assumes a semi-regular input.

Thus, no actual experiment testing the semi-regular claim was performed.

Degree Falls

Our work toward a direct attack on HPPC

- Experiments targeting degree 3 show nontrivial degree falls.
- Specifically, two steps of F4 at degree 3 exhibit degree falls.
- We prove the existence and describe the structure of these degree falls in Propositions 1 and 2.

These results significantly undermine the claims of security. (The specification uses the direct attack (Table 9) as the limiting attack.)

HPPC is Specially Structured HFE

Recall that the inversion method with the private key uses the equivalent form

$$P(\mathbf{x}) = T \circ \phi^{-1} \circ G \circ \ell_1 \circ \phi \circ S(\mathbf{x}).$$

Setting $F = G$ and $S' = \phi^{-1} \circ \ell_1 \circ \phi \circ S$, we have

$$P(\mathbf{x}) = T \circ \phi^{-1} \circ F \circ \phi \circ S'(\mathbf{x}).$$

(The HPPC specification only considers $F' = G \circ \ell_1$ and assumes that this map is of large Q-rank.)

Attacking HPPC as HFE

The observation that the central map (the map G above in our formulation) has degree bound $2^d + 1$ is sufficient to break HPPC.

- Generic HFE with degree bound $D = 2^d + 1$ has Q-rank $d + 1$.
- Using the big field support minors approach of BBCPS-TV22 results in a reduction of security to 74 bits.

But this observation is not the end of the story.

More on the Q-rank of HPPC

Recall that we can express the central map as

$$G(X) = \phi(\mathbf{M}(\mathbf{I}_n \otimes \mathbf{L}_2)(\phi^{-1}(X) \otimes \phi^{-1}(X))) = X\ell_2(X)$$

Using the definition of ℓ_2 and the convenient F_{2^n}-algebra $\mathbb{A} = \{(\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}) : \alpha \in F_{2^n}\}$,

$$[G(X)] = \begin{bmatrix} X & X^2 & \cdots & X^{2^{n-1}} \end{bmatrix} \begin{bmatrix} \beta_0 & \beta_1 & \cdots & \beta_d & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} X \\ X^2 \\ \vdots \\ X^{2^{n-1}} \end{bmatrix}.$$

For char(2) HFE attacks, we consider the sum of this matrix and its transpose. Thus, we have a target rank of 2, not $d+1$ ($= 11$ NIST Security Level-II case).

Special as Q-rank 2 HFE

In general, the MinRank attack for even rank HFE in char(2) is complicated:

- Model rank condition and
- solve for input transformation simultaneously.

Complication arises due to spurious solutions related to the Frobenius:

$$\lambda F^{q^i} + \mu F^{q^{i+1}} \text{ has same Q-rank.}$$

For G above, $\lambda G^{q^i} + \mu G^{q^{i+1}}$ has Q-rank 4 in general.

MinRank Step Easier

The MinRank proceeds similar to the odd characteristic case for HFE.

1. Solve MinRank on public quadratic forms (solutions in F_{2^n}),
2. Interpret solution as linearized polynomial form of output transformation,
3. Impose linear constraints on recovered low rank matrix for known 0 locations,
4. Solve for linearized polynomial form of inverse of input transformation.

Effective in recovering a private key practically.

The Attack is Practical

Attack running times for each HPPC security level (in seconds).

NIST Level	n	κ	Build SM	Total Time
2	128	17	11.320	$464.819 \approx 00:07:45$
4	192	21	49.570	$5552.319 \approx 01:32:32$
5	256	12*	27.970*	$25290.409 \approx 07:01:30$*

* Due to memory limitations, we included a suboptimal number of columns and solved at a higher degree than 2.

Directions

Could HPPC be repaired?

- As a quadratic scheme...
  - e.g Replace $G(X) = X\ell_2(X)$ with a sum of similar maps

$$F(X) = \sum_{i=0}^{k-1} X^{2^i} \ell_{2,k}(X) \ldots$$

  - Still has HFE structure with a degree bound $2^d + 1$.
- Using higher rank tensors, e.g. 3-tensors...
  - It's been done before, for example 3-WISE, cubic HFE.
  - Much less efficient with scaling of parameters.
  - These schemes are also essentially broken.

Thank you for your attention.

References:

https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures

[R23] B. G. Rodriguez. HPPC: Hidden Polynomial Product Composition. Cryptol. ePrint Arch. https://eprint.iacr.org/2023/830 (2023).

[BBVPS-TV22] J Baena, P Briaud,D. Cabarcas, R. Perlner, D. Smith-Tone and J. Verbel. Improving Support-Minors Rank Attacks: Applications to GeMSS and Rainbow. Crypto 2022, Springer, LNCS 13509, pp.376-405 (2022).