NORDSEC 2026 · AARHUS UNIVERSITY

HOVER

Higher-Order Vanishing Endomorphism Recovery

Markku-Juhani O. Saarinen
Tampere University, Finland
markku-juhani.saarinen@tuni.fi

20261111-nordsec-hover.pdf

https://mjos.fi/doc/20261111-nordsec-hover.pdf

TLP:CLEAR

CONTENTS

001 1978-2026: Classic McEliece

002 July 2026: HOV and HOVER

003 August: GIJS and the Aftermath

SECTION

001

1978-2026: CLASSIC MCELIECE

MCELIECE TIMELINE

- **1978:** Robert McEliece (Caltech/JPL) publishes a 3-page technical report *"A Public-Key Cryptosystem Based On Algebraic Coding Theory"* [14].
- **1980s-2010s:** The McEliece cryptosystem is described in textbooks but rarely used due to much larger public keys (100s of kB) than RSA or Elliptic Curve Cryptography. Many "optimized" variants are proposed & broken.
- **2017** Daniel J. Bernstein, Tanja Lange & Coauthors submit a modern version **Classic McEliece** to the first round of the U.S. NIST PQC competition [9].
- **2020:** German Cyber agency BSI starts recommending Classic McEliece [7].
- **2025:** NIST says Classic McEliece won't be standardized by them [1].
- **2026:** In June Classic McEliece becomes an international ISO Standard [13].

★ **July-August 2026 – Structural Cryptanalysis of McEliece** ★

MCELIECE KEY GENERATION (n, m, t)

Let $q = 2^m$. Each irreducible g of degree t over $\mathbb{F}_q$ and support $\alpha_i \in \mathbb{F}_q$ give a binary Goppa code Γ_2 of length $n \leq q$, dimension $k = n - mt$, correcting t errors.

Goppa code is linear: can be expressed with generator matrix $\mathbf{G} \in \mathbb{F}_2^{k \times n}$.
With any linear code, the n-bit codeword $\mathbf{c}$ corresponding to k-bit vector $\mathbf{v}$ can be obtained from the vector-matrix product $\mathbf{c} = \mathbf{vG}$. Note that $\mathbf{v}$ is a row vector.

1. $\mathbf{G} \in \mathbb{F}_2^{k \times n}$	Generator matrix for the binary Goppa code Γ_2.
2. $\mathbf{P} \xleftarrow{\$} \mathbb{F}_2^{n \times n}$	Uniform random permutation matrix.
3. $\mathbf{S} \xleftarrow{\$} \mathbb{F}_2^{k \times k}$	Uniform random nonsingular (invertible) matrix.
4. $\mathcal{D}_{\Gamma_2}$	An efficient t-error correcting decoder for Γ_2.
5. $pk \leftarrow \mathbf{G}' = \mathbf{SGP}$	Scrambled generator matrix $\mathbf{G}' \in \mathbb{F}_2^{k \times n}$ is kn bits.
6. $sk \leftarrow (\mathbf{S}, \mathbf{P}, \mathcal{D}_{\Gamma_2})$	Secret descrambling and decoding information.

McEliece Encryption and Decryption

Encrypt($pk = \mathbf{G}'$, $\mathbf{v} \in \mathbb{F}_2^k$):

1. Sample a random error vector $\mathbf{e} \in \mathbb{F}_2^n$ with weight $\mathrm{Wt}(\mathbf{e}) = t$.
2. Encode with $\mathbf{G}'$ and add error to obtain n-bit ciphertext: $\mathbf{c} \leftarrow \mathbf{v}\mathbf{G}' + \mathbf{e}$.

Decrypt($sk = (\mathbf{S}, \mathbf{P}, \mathcal{D}_{\Gamma_2})$, $ct = \mathbf{c}$):

1. Compute $\mathbf{c}' = \mathbf{c}\mathbf{P}^{-1}$, applying the inverse permutation ($\mathbf{c}'$ also has t errors.)
2. Now apply the decoding algorithm to find $\mathbf{v}' = \mathcal{D}_{\Gamma_2}(\mathbf{c}') = \mathbf{v}\mathbf{S}$.
3. Apply inverse scrambling matrix to recover decrypted message: $\mathbf{v} = \mathbf{v}'\mathbf{S}^{-1}$.

Information Set Decoding (ISD) message recovery attacks: Guess k error-free positions of $\mathbf{c}$, solve for $\mathbf{v}$ by linear algebra, and retry until $\mathbf{c} + \mathbf{v}\mathbf{G}'$ has weight t.

BACK IN 2023-24: TII MCELIECE CHALLENGES

ISD / (Single) Message recovery: There are many versions (Prange 1962 [17], BJMM 2012 [3], Quantum variants) – all are exponential in the error weight t.

Structural/Algebraic attacks instead look for structure in the public matrix $\mathbf{G}'$.

Until 2025-26, to recover the **secret key** one would expect to do a brute force search on (n, m, t): Goppa-polynomial search $\times$ support-set search $\times$ trial cost:

$$\text{TII-n labels:} \quad \lambda_{\text{TII}} = \log_2 \left(I(t,q) \cdot \binom{q}{n} \cdot n^3 \right)$$

The Technology Innovation Institute (UAE) ran a McEliece challenge in 2023-24.

TII offered cash prizes – the reward for TII-70 and above was $ 10,000 each.
https://github.com/ElenaKirshanova/tii_decoding_challenge

THE NIEDERREITER CRYPTOSYSTEM

- A variant of McEliece developed in 1986 by Harald Niederreiter [15].
- Uses the $(n-k) \times n$ parity check matrix $\mathbf{H}$ instead of the $k \times n$ generator $\mathbf{G}$. (Parity check matrix satisfies $\mathbf{H}\mathbf{c}^T = 0$ if $\mathbf{c}$ is a codeword of Γ_2).
- With equivalent parameters has the same security as its “dual”, McEliece.
- Many McEliece-like cryptosystems (based on various codes) have been proposed over the last five decades, but constructions based on Goppa codes are among the very few that had “survived” cryptanalysis efforts.
- The “Classic McEliece” algorithm [9] is actually a Niederreiter cryptosystem. Was standardized as a part of ISO/IEC 18033-2:2006/Amd 2:2026 [13].
- Was considered “Quantum-Safe”: ISD only gets a “Grover”-like speedup [4].

SECTION

002

JULY 2026: HOV AND HOVER

HIGHER-ORDER VANISHING (HOV)

Over $\mathbb{F}_q$, the public dual code splits into m Frobenius-conjugate Generalized Reed–Solomon (GRS) blocks of dimension t:

$$\Gamma_2^{\perp} \otimes_{\mathbb{F}_2} \mathbb{F}_q = \bigoplus_{i=0}^{m-1} \mathcal{G}_i, \qquad \mathcal{G}_i = \mathrm{GRS}_t(\boldsymbol{\alpha}, g(\boldsymbol{\alpha})^{-1})^{[2^i]}.$$

Note: A random code of dimension k has no such hidden decomposition.

Shorten the dual on s_* public coordinates, leaving $\kappa = mt - s_*$ variables. Find binary square-free degree-p forms $f(x_1, \ldots, x_\kappa)$ whose derivatives vanish at every remaining public column. This is a large, sparse binary linear system.

Distinguisher: for a random code kernel $L = 0$; for a Goppa code $\dim L = m$.

HEMMERT'S HOV KEY RECOVERY

Over $\mathbb{F}_q$, L is spanned by m determinant forms $h_i = \det Q_i$ in one Frobenius orbit: squaring every coefficient of h_i gives h_{i+1} (up to scale).

Windows: any combination of a cyclically consecutive h_i omits one $\mathcal{G}_i$; its derivatives lift into $\bigoplus_{j \neq i} \mathcal{G}_j$.

MinRank: stack a window's partial derivatives $\partial f / \partial x_r$ as rows of a *derivative matrix*; its rank is unusually low, $\leq b$. Hemmert searches $L \otimes \mathbb{F}_q$ for such combinations, assuming $ap^2 > b$ so that only windows qualify.

Completion: align windows across shortenings, isolate one $\mathcal{G}_i$ by Frobenius intersections, expose a GRS code by a Schur product; Sidelnikov–Shestakov [21] gives $(g, \boldsymbol{\alpha})$. This is *equivalent* to the private key information $(\mathbf{S}, \mathbf{P}, \mathcal{D}_{\Gamma_2})$.

THE HOVER SHORTCUT

HOVER (Higher-Order Vanishing Endomorphism Recovery) was found in our AI experiments only weeks after Hemmert's HOV key recovery ePrint came out.

Observation: all derivative matrices *together* carry more than the rank of any single combination. With a basis $v_1, \ldots, v_m$ of L, their derivative matrices M_i form a public three-way tensor $\beta(z, \lambda) = \left(\sum_i \lambda_i M_i\right)^{\top} z$.

Shortcut: Ask which binary maps on L are compatible with it:

$$\mathcal{E}_\beta = \{B \in \mathrm{End}_{\mathbb{F}_2}(L) : \exists A_B \text{ with } A_B\, \beta(z, \lambda) = \beta(z, B\lambda)\}.$$

$\mathcal{E}_\beta$ is the nullspace of *one* binary linear system in m^2 unknowns. **TII-252:** $58{,}500$ equations in 100 unknowns replace the original exhaustive search in $\mathbb{P}^9(\mathbb{F}_{2^{10}})$.

HOVER EXPOSES THE "HIDDEN FIELD"

Little bit more intuition: The McEliece public key pk carries a fingerprint of the hidden field structure: an algebra we can compute from public data.

1. Public field check. If $\dim L = \dim \mathcal{E}_\beta = m$ and $B \in \mathcal{E}_\beta$ has an irreducible characteristic polynomial, then $\mathcal{E}_\beta = \mathbb{F}_2[B] \cong \mathbb{F}_{2^m}$.

2. Hidden directions. Over $\mathbb{F}_{2^m}$, every compatible map just rescales each hidden direction h_i, by $\mu, \mu^2, \mu^4, \ldots$. So B is diagonal in the hidden basis: its m eigenlines *are* the h_i, and squaring orders them into one cycle.

3. Why it matters. Their order gives all HOV windows without a MinRank search. If a check fails, HOVER stops. The recovered secret keys are verified against pk.

JULY 2026: NEW TII KEY RECOVERY RECORDS

In practice, the "HOVER" variant [this work] of Hemmert's HOV key recovery [11] turned out to be very effective against low-degree challenge parameters:

Challenge	(n, m, t)	Wall Time	Memory	System
TII-252	$(1008, 10, 11)$	6 min 15 s	2.7 GiB	12-core laptop
TII-246	$(1009, 10, 11)$	3 min 11 s	2.7 GiB	12-core laptop
TII-240	$(1010, 10, 11)$	3 min 06 s	2.7 GiB	12-core laptop
TII-213	$(496, 9, 10)$	6 h 45 min	144 GiB	28-vCPU server
TII-129	$(509, 9, 9)$	4 h 30 min	80 GiB	28-vCPU server

Evidence (secret keys): https://github.com/mjosaarinen/tii-solved

Note: TII-83 was the "highest" challenge broken by the May 2024 deadline.

SECTION

003

AUGUST: GIJS AND THE AFTERMATH

FAVOURABLE REGIMES FOR STRUCTURAL ATTACKS

OBSERVATIONS

- These attacks are all conditional on parameter ranges (or even keys!)
- There is no single “input size” security parameter for asymptotics.
- A distinguisher does not directly imply decryption or OW-CPA break.

Attack	**Type**	**Indicative Conditions** *(very rough)*	**Asymptotics**
Pfaffian [2]	key recovery	Very high rate; square defect visible	poly in (m, t)
HOV [12]	distinguisher	Random HOV kernel dies; Goppa not	–
HOV [11]	key recovery	Clean Frobenius-split HOV kernel	–
Rank-2 [6]	key recovery	Rank-2 relation at low solving degree	subexp $2^{o(t)}$
Holdout [10]	key recovery	Kernel survives past Hermite threshold	qpoly $n^{O(\log n)}$

HOLDOUT / GIJS: THE MISSING COLUMN IS FORCED

Over $\mathbb{F}_q$, the public columns are scaled points $y_i = \lambda_i p(\alpha_i)$ on a hidden polynomial curve, with $\deg p_j \le D = n - 2t - 1$.

Hold out y_τ. Find a nonzero homogeneous polynomial h of degree d whose Hasse derivatives of order $< s$ vanish at every other column. Then $\phi(Z) = h(p(Z))$ has degree at most dD and at least $s(n-1)$ zeros, counting multiplicity:

$$s(n-1) > dD \quad \Longrightarrow \quad \phi \equiv 0 \quad \Longrightarrow \quad h(y_\tau) = 0.$$

There are still enough coefficients to find such an h; a random held-out column has no reason to satisfy the last equality. For $d = s + 1 = \Theta(\log n)$ this gives a quasipolynomial distinguisher [10].

AUGUST 2026: HOLDOUT / GIJS: AI DISCLOSURE [10]

AI disclosure. Our main results emerged from the failed PIR attempt described above and were obtained through traditional human trial and error, without the use of AI. Still, AI was instrumental for many aspects of this work. OpenAI Codex (ChatGPT-5.6 Sol) was used to verify the results, analyze and improve concrete efficiency, draft some of the proofs, design and implement experiments, and help with literature review and other aspects of writing. Amazon Quick and Google AI harness were used for extra sanity checks.

AI played a more significant role in developing our key-recovery algorithm. The algorithm, inspired by the Sidelnikov–Shestakov algorithm, was proposed by the authors. ChatGPT-5.6 Sol then helped with the routine but tedious derivations of the structure of the interpolation coefficients. It also helped us quickly run the experiments measuring nullities, which were important for guiding the choice of parameters and gaining confidence in our conjectures.

Most importantly, an audit by ChatGPT identified a dimension gap that made our initial algorithm fail for binary Goppa codes and required changing the parameters. ChatGPT also helped run experiments to confirm the structure of the required interpolation coefficients for Goppa codes. We sent the resulting algorithm to Steve Weis from Anthropic, who was able (with the help of Claude) to successfully run our algorithm on small binary Goppa instances.

The authors verified the correctness and originality of all content.

HOLDOUT: COST AGAINST CLASSIC MCELIECE

Weis & Claude in August 2026: the interpolation relations also encode the hidden support. After removing local jet relations, their top-order blocks satisfy $V_{2,j} = \alpha_j^{s'-1} V_{1,j}$ (up to normalization and Frobenius conjugacy). Read off the α_j, recover the multipliers, and obtain an equivalent decoding key [22]. **Estimates:**

Parameter set	**NIST Req** [16]	**ISD** [5]	**GIJS** [10]	**Weis** [22]	**Saarinen** [18]
mceliece348864	143	151	114.2	94.3	126.8
mceliece460896	207	191	120.3	99.3	145.2
mceliece6688128	272	257	124.0	102.4	137.5
mceliece8192128	272	287	124.0	102.4	137.5

TII-253 $(n, m, t) = (214, 8, 9)$: two sparse kernels, ≈ 700 core-hours each [22].

SPECIAL HOLDOUT: TII-254 KEY RECOVERY

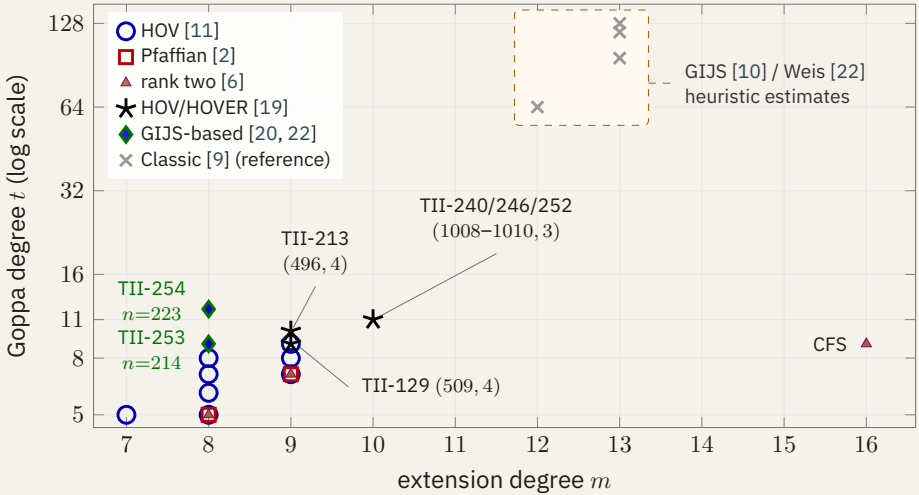
TII-254 $(n, m, t) = (223, 8, 12)$: hardest solved challenge so far [20].

I ran a human-directed, AI-operated algorithm improvement loop for 8 days.

TII-254-specific, 13-step process: Degree-6 holdout system; remove 4.8M provable "nuisance" directions (20.3M $\to$ 15.5M). Solve at two anchor columns: two 121-dim kernels. Their pair core splits as $80 = 64 + 16$; the common 64 is noise, and the $16 \cong \mathbb{F}_{2^8}^2$ has the support locators as its $\mathbb{F}_{2^8}$-lines.

Stage (per anchor)	Time	Hardware
Block Wiedemann sequence (width 512)	13.6 h	$1\times$ NVIDIA GH200
Polynomial-matrix basis	0.8–5.1 h	12–64 CPU threads
Kernel reconstruction	$\approx$2 h	$8\times$ GH200

CHARTING THE MCELIECE KEY RECOVERIES





Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Hinweise zu aktuellen Entwicklungen um Classic McEliece

Stand: 29.09.2026

SEP 29, 2026: CURTAINS ON CLASSIC MCELIECE

Since 2020, Germany's cyber authority BSI has recommended Classic McEliece in its Technical Guideline TR-02102-1.

The January 2026 version still stated: *"The underlying mechanism, which is instantiated with binary Goppa codes, is about as old as the RSA mechanism and is therefore considered conservative and very thoroughly analysed."* [7]

On September 29, 2026 BSI revised their guidance:

"Classic McEliece should currently no longer be used in new developments or when planning new cryptographic applications." [8]

The BSI Classic McEliece security advisory [8] cites the same 2026 works as we did here [2, 6, 10–12, 22], including my works [19, 20].

END OF TALK!

QUESTIONS



https://mjos.fi/doc/20261111-nordsec-hover.pdf

REFERENCES (1)

[1] Gorjan Alagic, Maxime Bros, Pierre Ciadoux, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Hamilton Silberg, Daniel Smith-Tone, and Noah Waller. “Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process”. Interagency or Internal Report NIST IR 8545. National Institute of Standards and Technology, Mar. 2025, p. 34. DOI 10.6028/NIST.IR.8545.

[2] Magali Bardet, Axel Lemoine, and Jean-Pierre Tillich. “An Attack on the CFS Scheme and on TII McEliece Challenges”. In: *Advances in Cryptology - CRYPTO 2026 - 46th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-20, 2026, Proceedings, Part IV*. Ed. by Nadia Heninger and Mike Rosulek. Vol. 16803. Lecture Notes in Computer Science. Springer, 2026, pp. 380–412. DOI 10.1007/978-3-032-35398-6_13. URL: https://eprint.iacr.org/2026/430.

REFERENCES (2)

[3] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. “Decoding Random Binary Linear Codes in $2^{n/20}$: How $1 + 1 = 0$ Improves Information Set Decoding”. In: *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*. Ed. by David Pointcheval and Thomas Johansson. Vol. 7237. Lecture Notes in Computer Science. Springer, 2012, pp. 520–536. DOI 10.1007/978-3-642-29011-4_31. URL: https://eprint.iacr.org/2012/026.

[4] Daniel J. Bernstein. “Grover vs. McEliece”. In: *Post-Quantum Cryptography, Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010. Proceedings*. Ed. by Nicolas Sendrier. Vol. 6061. Lecture Notes in Computer Science. Springer, 2010, pp. 73–80. DOI 10.1007/978-3-642-12929-2_6. URL: https://cr.yp.to/codes/grovercode-20091123.pdf.

[5] Daniel J. Bernstein and Tung Chou. “CryptAttackTester: high-assurance attack analysis”. In: *Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part VI*. Ed. by Leonid Reyzin and Douglas Stebila. Vol. 14925. Lecture Notes in Computer Science. Full version is available as IACR ePrint Report 2023/940. Springer, 2024, pp. 141–182. DOI 10.1007/978-3-031-68391-6_5. URL: https://eprint.iacr.org/2023/940.

REFERENCES (3)

[6] Pierre Briaud, Axel Lemoine, Hugues Randriambololona, and Jean-Pierre Tillich. “A Heuristic Subexponential Attack on the McEliece Cryptosystem”. Cryptology ePrint Archive, Paper 2026/1232. 2026. URL: https://eprint.iacr.org/2026/1232.

[7] BSI. “Cryptographic Mechanisms: Recommendations and Key Lengths”. Technical Guideline TR-02102-1. Bundesamt für Sicherheit in der Informationstechnik, Jan. 2026, p. 92. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf.

[8] BSI. “Notes on recent developments concerning Classic McEliece”. Security Advisory. Sept. 2026. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Notes_Classic_McEliece.pdf.

[9] Classic McEliece Team. “Classic McEliece: conservative code-based cryptography: guide for security reviewers”. Document of official Classic McEliece web site. Oct. 2022. URL: https://classic.mceliece.org/mceliece-security-20221023.pdf.

[10] Ashrujit Ghoshal, Yuval Ishai, Aayush Jain, and Nuozhou Sun. “Quasipolynomial Cryptanalysis of the McEliece Cryptosystem (or: PIR Meets McEliece)”. Cryptology ePrint Archive, Paper 2026/1630. Aug. 2026. URL: https://eprint.iacr.org/2026/1630.

REFERENCES (4)

[11] Tobias Hemmert. “Key Recovery for the McEliece Cryptosystem Using Higher-Order Vanishing”. Cryptology ePrint Archive, Paper 2026/1339. 2026. URL: https://eprint.iacr.org/2026/1339.

[12] Tobias Hemmert and Andreas Wiemers. “Distinguishing Goppa Codes Using Higher-Order Vanishing”. In: *Advances in Cryptology – CRYPTO 2026. 46th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17–20, 2026, Proceedings, Part IV*. Ed. by Nadia Heninger and Mike Rosulek. Vol. 16803. Lecture Notes in Computer Science. Springer, 2026, pp. 191–223. DOI 10.1007/978-3-032-35398-6_7. URL: https://eprint.iacr.org/2025/1661.

[13] ISO. “Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers – Amendment 2”. en. Standard ISO/IEC 18033-2:2006/Amd 2:2026. International Organization for Standardization, 2026. URL: https://www.iso.org/standard/86890.html.

[14] Robert J. McEliece. “A Public-Key Cryptosystem Based on Algebraic Coding Theory”. Progress Report DSN PR 42-44. Deep Space Network, 1978, pp. 114–116. URL: https://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF.

[15] Harald Niederreiter. “Knapsack-type Cryptosystems and Algebraic Coding Theory”. In: *Problems of Control and Information Theory* 15.2 (1986), pp. 159–166. URL: http://real-j.mtak.hu/7997/.

REFERENCES (5)

[16] NIST. “Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process”. NIST Call for PQC Standardization Candidates. Dec. 2016. URL: https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

[17] Eugene Prange. “The use of information sets in decoding cyclic codes”. In: *IRE Transactions on Information Theory* 8.5 (1962), pp. 5–9. DOI 10.1109/TIT.1962.1057777.

[18] Markku-Juhani O. Saarinen. “Bit Operation Cost of “Holdout” Key-Recovery Attacks Against Classic McEliece”. Cryptology ePrint Archive, Paper 2026/1786. Sept. 2026. URL: https://eprint.iacr.org/2026/1786.

[19] Markku-Juhani O. Saarinen. “HOVER: Higher-Order Vanishing Endomorphism Recovery”. In: *Secure IT Systems: 31st Nordic Conference, NordSec 2026, Aarhus, November 11-12, 2026 Proceedings*. Ed. by Aslan Askarov, Abhishek Vaish, and Christian Damsgaard Jensen. Vol. to appear. Lecture Notes in Computer Science. Springer, Nov. 2026, to appear. URL: https://eprint.iacr.org/2026/1778.

[20] Markku-Juhani O. Saarinen. “Two-Anchor Holdout/Hermite: Solving the TII-254 McEliece Key Recovery Challenge”. Cryptology ePrint Archive, Paper 2026/1986. Sept. 2026. URL: https://eprint.iacr.org/2026/1986.

REFERENCES (6)

[21] Vladimir M. Sidelnikov and Sergey O. Shestakov. “On the insecurity of cryptosystems based on generalized Reed-Solomon codes”. In: *Discrete Mathematics and Applications* 2.4 (1992), pp. 439–444. DOI 10.1515/dma.1992.2.4.439.

[22] Stephen A. Weis. “Improving GIJS Key Recovery for Classic McEliece”. Cryptology ePrint Archive, Paper 2026/1984. Sept. 2026. URL: https://eprint.iacr.org/2026/1984.