Citation Evidence Report

EB-2 NIW Petition — National Interest Waiver

Matter of Dhanasar · Prong 2 (well-positioned)

Bo-Yin Yang

Academia Sinica

Google Scholar profile

Generated 2026-06-01 by CiteMap. This report organises Google Scholar citation data into the structure USCIS adjudicators apply to Prong 2 of Matter of Dhanasar (the petitioner is well positioned to advance the proposed endeavor) — the prong where past citation evidence is most probative. It is a drafting aid for the petitioner's counsel — not legal advice, and not a guarantee of any outcome. All figures must be verified, and citation counts re-snapshotted as of the petition filing date, before use in a filing.

A. Overview & Filtering Statement

2,180	2,610	30	46
Citing papers mapped	Citation edges	Home papers mapped	h-index (GS)

Filtering statement — methodology & limits

Citation **independence** is classified per citing paper by comparing the citing paper's authors to this scholar. *Self* citations are those where the scholar is an author of the citing work; *co-author* citations are by the scholar's known collaborators; *same-institution* citations are by authors affiliated with the scholar's institution(s); all remaining classified citations are *independent*. Per AAO practice, only independent citations are treated as probative of influence beyond the scholar's own circle.

Known limitations — counsel must verify. (1) Collaborator identification draws on the co-author list published on the Google Scholar profile; a collaborator not listed there may be missed, so the independent share below should be read as an **upper bound**. (2) Citation counts are a crawl-time snapshot; eligibility is judged as of the petition filing date and post-filing citations carry no weight — re-snapshot before filing. (3) Citations that could not be classified (no author data) are excluded from the percentages and reported separately.

B. Citation Independence

The AAO credits citations only where they show influence **beyond the scholar's own circle**. Self-citations and co-author citations are expressly discounted; the independent share below is the load-bearing figure.

90.7% independent of 1,417 classified citing papers

Citation type	Count
Independent	1,285
Self-citation	34
Co-author	98
Same-institution	0

763 citing papers could not be classified (no author data) and are excluded from the percentages above.

C. Significant Contributions & Their Citation Evidence

Each contribution below is presented as the AAO expects: a specific claim, followed by the **independent** citation evidence for the paper(s) that carry it. Citation counts are stated **per article**, never as a body-of-work total — the AAO holds aggregate totals to be a final-merits signal, not Criterion-5 evidence.

Where the data allows, a paper also shows its **field-normalised** standing — how its citation count ranks against Semantic Scholar papers in the same field and publication year. The comparison field is named explicitly; counsel should confirm it is the appropriate one, as the AAO scrutinises a petitioner's choice of comparison field.

Contribution 1

Claim — Contribution 1

The researcher advanced high-speed, high-security digital signatures through a seminal 2012 paper and subsequent work optimizing computational efficiency and multivariate scheme design.

The researcher established a foundational contribution to cryptographic signature schemes with the 2012 paper 'High-speed high-security signatures,' which serves as the core of this research line. This work is supported by follow-up publications that extend the initial framework, including studies on fast constant-time computations and design principles for HFEv-based multivariate schemes.

This line of work appears to address the critical challenge of balancing computational speed with robust security in digital signatures. The progression from the 2012 core paper to later works on modular inversion and multivariate design suggests a sustained effort to refine algorithmic efficiency and structural integrity in cryptographic protocols.

The significance of this contribution is evidenced by the core paper's 1,253 citations, indicating substantial uptake in the field. Furthermore, analysis shows that 90.7% of citing papers originate from independent researchers, demonstrating that this work has had a broad, independent impact beyond the researcher's immediate circle.

INDEPENDENT CITATIONS FOR THIS CONTRIBUTION: 766

CORE PAPER

High-speed high-security signatures

2012 · 1,253 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	zkbridge: Trustless cross-chain bridges made practical	Stanford University, Texas A&M University, Tsinghua University	China, United States	—
2	AEGIS: No Tool Call Left Unchecked--A Pre-Execution Firewall and Audit Layer for AI Agents	Carnegie Mellon University, University of California, Irvine Medical Center, University of Southern California	United States	—
3	Assessment and optimization of post-quantum cryptographic protocols for civil UAV communications	École Nationale de l'Aviation Civile	France	—
4	Post-quantum security: Opportunities and challenges	Hunan University of Science and Technology	China	—
5	A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions	Vellore Institute of Technology, Vellore Institute of Technology University	India	—
6	Internet of Things: A survey on the security of IoT frameworks	KU Leuven, University of Auckland	Belgium, New Zealand	—
7	Enhancing bitcoin security and performance with strong consistency via collective signing	EPFL	Switzerland	—
8	Succinct {Non-Interactive} zero knowledge for a von neumann architecture	Massachusetts Institute of Technology, Technion—Israel Institute of Technology, Tel Aviv University	Israel, United States	—
9	Ring confidential transactions	—	—	—

No.	Citing paper	Citing institution(s)	Country	S2
10	A Formal Security Analysis of the Signal Messaging Protocol: K. Cohn-Gordon et al.	Cisco Systems, ETH Zürich, Helmholtz Center for Information Security	Canada, Germany, Switzerland	—
11	Simple schnorr multi-signatures with applications to bitcoin	Agence Nationale de Sécurité du Médicament et des Produits de Santé, Carestream (United States), University of San Francisco	France, United States	—
12	Identity inference of genomic data using long-range familial searches	Columbia University, MyHeritage, The Hebrew University of Jerusalem	Israel, United States	—
13	Port contention for fun and profit	Polytechnic José Antonio Echeverría, Tampere University	Cuba, Finland	—
14	Telling your secrets without page faults: Stealthy page {Table-Based} attacks on enclaved execution	KU Leuven, Technische Universität Braunschweig	Belgium, Germany	—
15	HACL*: A verified modern cryptographic library	Inria, Microsoft Research	France, United States	—
16	Efficient and side-channel resistant Ed25519 on ARM Cortex-M4	Florida Atlantic University, Microsoft, University of South Florida	United States	—
17	A systematic look at ciphertext side channels on AMD SEV-SNP	Southern University of Science and Technology, The Ohio State University, University of Lübeck	China, Germany, United States	—
18	Maximal extractable value (mev) protection on a dag	Chainlink Labs	—	—
19	Keeping authorities" honest or bust" with decentralized witness cosigning	École Polytechnique Fédérale de Lausanne, Yale University	Switzerland, United States	—
20	How to issue a central bank digital currency	Bern University of Applied Sciences, Swiss National Bank	Switzerland	—
21	Cryptographic accelerators for digital signature based on Ed25519	Florida Atlantic University, Microsoft, University of South Florida	United States	—
22	Pact: Privacy sensitive protocols and mechanisms for mobile contact tracing	Amazon, Microsoft Research, University of Washington	United States	—
23	{CONIKS}: Bringing key transparency to end users	Princeton University, Stanford University	United States	—
24	ROAST: Robust asynchronous Schnorr threshold signatures	Blockstream, Friedrich-Alexander-Universität Erlangen-Nürnberg, Helmholtz Center for Information Security	Canada, Germany	—
25	DualRing: Generic Construction of Ring Signatures with Efficient Instantiations	The University of Hong Kong	Hong Kong	—
26	Vulnerability of blockchain technologies to quantum attacks	University of Kent	United Kingdom	—

No.	Citing paper	Citing institution(s)	Country	S2
27	hints: Threshold signatures with silent setup	Johns Hopkins University, Supra Research, University of California, Irvine Medical Center	United States	—
28	Preventing page faults from telling your secrets	ETH Zurich, National University of Singapore	Singapore, Switzerland	—
29	A survey on security challenges and solutions in the IOTA	Inria, IOTA Foundation, Lovely Professional University	France, India, Switzerland	—
30	Marlin: Two-phase BFT with linearity	Shandong University, Tsinghua University, Yangtze Delta Region Institute of Tsinghua University	China	—

Showing the 30 most-cited of 672 independent citing papers.

Independent citing papers only; self- and co-author citations excluded. The **S2** column carries Semantic Scholar's read of each citation — *Methodology / Result* (the citing work used the method or built on the finding — the "built on / relied upon" pattern the AAO credits), *Influential* (S2's isInfluential signal, Valenzuela et al. 2015), or *Background* (a passing mention).

FOLLOW-UP WORK

Fast constant-time gcd computation and modular inversion

2019 · 169 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	Efficient arithmetic in (pseudo-) mersenne prime order fields	—	—	—
2	Size, speed, and security: An Ed25519 case study	Huawei Technologies Oy, Tampere University	Finland	—
3	A prime-order group with complete formulas from even-order elliptic curves	NCC (Sweden)	Sweden	—
4	Batch point compression in the context of advanced pairing-based protocols	École Normale Supérieure de Lyon	France	—
5	Secure and efficient design of lattice-based cryptography	Ruhr University Bochum	Germany	—
6	High-speed and High-assurance Cryptographic Software	INESC TEC, Universidade do Porto	Portugal	—
7	Efficiently masking polynomial inversion at arbitrary order	Ruhr University Bochum	Germany	—
8	Systematic Use of Random Self-Reducibility against Physical Attacks	Virginia Tech, Yale University	United States	—
9	Lattice-based key-sharing schemes: A survey	Nanyang Technological University, PQShield, Ltd.	Singapore, United Kingdom	—
10	Improved quantum circuits for elliptic curve discrete logarithms	Microsoft, Microsoft Research, University of Oxford	United Kingdom, United States	—
11	dCTIDH: fast & deterministic CTIDH	Radboud University, RheinMain University of Applied Sciences, University of Applied Sciences	Germany, Netherlands	—

No.	Citing paper	Citing institution(s)	Country	S2
12	{CopyCat}: Controlled {Instruction-Level} attacks on enclaves	KU Leuven, University of California, Irvine Medical Center, Worcester Polytechnic Institute	Belgium, United States	—
13	Verifiable quantum advantage via optimized DQI circuits	Google Quantum AI	United States	—
14	All your pc are belong to us: Exploiting non-control-transfer instruction btb updates for dynamic pc extraction	Penn State University, University of Illinois at Urbana-Champaign	United States	—
15	Faster Montgomery multiplication and multi-scalar-multiplication for SNARKs	Aarhus University, Linea	Denmark, United States	—
16	Faster constant-time evaluation of the Kronecker symbol with application to elliptic curve hashing	Aarhus University, NTT (Japan)	Denmark, Japan	—
17	SwiftEC: Shallue–van de Woestijne Indifferentiable Function To Elliptic Curves: Faster Indifferentiable Hashing to Elliptic Curves	NTT, Technology Innovation Institute	Japan, United Arab Emirates	—
18	Fast polynomial inversion for post quantum QC-MDPC cryptography	University of Haifa	Israel	—
19	Constant time lattice reduction in dimension 4 with application to SQIsign	Eötvös Loránd University, ETH Zürich; IBM Research Europe, Technology Innovation Institute	Hungary, Switzerland, United Arab Emirates	—
20	Fully projective radical isogenies in constant-time	Radboud University, Technology Innovation Institute	Netherlands, United Arab Emirates	—
21	New space-efficient quantum algorithm for binary elliptic curves using the optimized division algorithm: H. Kim, S. Hong	Korea University	South Korea	—
22	When one vulnerable primitive turns viral: Novel single-trace attacks on ECDSA and RSA	Polytechnic José Antonio Echeverría, Tampere University	Cuba, Finland	—
23	Concrete quantum cryptanalysis of binary elliptic curves via addition chain	The University of Tokyo	Japan	—
24	RLHMBC: A novel lightweight symmetric cipher supporting multiplicative homomorphism	Saint Joseph University, Saint-Joseph University	Lebanon	—
25	Subgroup membership testing on elliptic curves via the Tate pairing	École Normale Supérieure de Lyon	France	—
26	Empirical analysis of software vulnerabilities causing timing side channels	Sabanci University, The University of Adelaide	Australia, Turkey	—
27	Déjà vu: Side-channel analysis of mozilla's NSS	Tampere University	Finland	—
28	High-assurance field inversion for curve-based cryptography	Aarhus University	Denmark	—
29	FPTRU: Optimization of NTRU-Prime and TLS Performance Assessment	Kingston and St George's University, Sheffield Emergency Care Forum, University of Bath	United Kingdom	—
30	Fast polynomial inversion algorithms for the post-quantum cryptography	DGIST, Seoul National University	South Korea	—

Showing the 30 most-cited of 45 independent citing papers.

Independent citing papers only; self- and co-author citations excluded. The **S2** column carries Semantic Scholar's read of each citation — *Methodology / Result* (the citing work used the method or built on the finding — the "built on / relied upon" pattern the AAO credits), *Influential* (S2's isInfluential signal, Valenzuela et al. 2015), or *Background* (a passing mention).

FOLLOW-UP WORK

Design principles for HFEv-based multivariate signature schemes

2015 · 174 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	Multivariate encryption schemes based on polynomial equations over real numbers	Okayama University of Science, University of Tokyo	Japan	—
2	Subliminal channels in high-speed signatures	TU Wien	Austria	—
3	GeMSS: a great multivariate short signature	CS Communication & Systèmes (France), Laboratoire de Mathématiques Blaise Pascal, Orange (France)	France	—
4	The rise and resilience of multivariate cryptography: Advances, pitfalls, and promising pathways	Maulana Azad National Institute of Technology	India	—
5	HFERP-a new multivariate encryption scheme	Kyushu University	Japan	—
6	Circulant UOV: a new UOV variant with shorter private key and faster signature generation.	—	—	—
7	Revisiting the Minrank problem on multivariate cryptography	Kyushu University, Nihon University, University of Tokyo	Japan	—
8	Software toolkit for hfe-based multivariate schemes	Institut national de recherche en sciences et technologies du numérique, LIP6	France	—
9	Geometric approach to the cryptanalysis of post-quantum multivariate signature schemes	Sorbonne Université	France	—
10	Security Analysis via Algebraic Attack Against "A New Encryption Scheme for Multivariate Quadratic System"	Kyushu University, Nihon University	Japan	—
11	Practical post-quantum cryptography	—	—	—
12	A novel homomorphic polynomial public key encapsulation algorithm	Quantropi (Canada)	Canada	—
13	A new symmetric homomorphic functional encryption over a hidden ring for polynomial public key encapsulations	Quantropi (Canada)	Canada	—
14	Progress in multivariate cryptography: systematic review, challenges, and research directions	Indian Institute of Technology Kharagpur	India	—
15	Field lifting for smaller UOV public keys	KU Leuven, University of Leuven	Belgium	—
16	Post-quantum cryptography techniques for secure communication in resource-constrained Internet of Things devices: A comprehensive survey	Thapar Institute of Engineering & Technology, Trinity College Dublin, University of the West of Scotland	India, Ireland, United Kingdom	—
17	Post-quantum zero-knowledge and signatures from symmetric-key primitives	Aarhus University, Austrian Institute of Technology, Graz University of Technology	Austria, Denmark, United States	—

No.	Citing paper	Citing institution(s)	Country	S2
18	Improvements of algebraic attacks for solving the rank decoding and MinRank problems	Centre Inria de Paris, Inria, National Institute of Standards and Technology	Colombia, France, United States	—
19	A comprehensive review of the security flaws of hashing algorithms	Arak University	Iran	—
20	Revisiting algebraic attacks on MinRank and on the rank decoding problem	Centre Inria de Paris, Centre Inria de Sorbonne Université, Université de Limoges	France	—
21	Improvement of algebraic attacks for solving superdetermined MinRank instances	Université de Rouen Normandie	France	—
22	On the complexity of "superdetermined" Minrank instances	Technology Innovation Institute, Universidad Nacional de Colombia, Universidad Nacional de Colombia, Sede Medellín	Colombia, United Arab Emirates	—
23	"Oops, I did it again"–Security of one-time signatures under two-message attacks	Eindhoven University of Technology, National Taiwan University	Netherlands, Taiwan	—
24	Post quantum proxy signature scheme based on the multivariate public key cryptographic signature	Guangdong University of Technology, National University of Singapore, South China University of Technology	China, Singapore, United Kingdom	—
25	Key recovery attack on the cubic ABC simple matrix multivariate encryption scheme	National Institute of Standards and Technology	United States	—
26	Revisiting the security of salted UOV signature	Indian Institute of Science, Society for Electronic Transactions and Security	India	—
27	Algebraic Cryptanalysis and Countermeasures of Lightweight Signature Scheme Based on Multivariate Quadratic Polynomials	Maulana Azad National Institute of Technology	India	—
28	Multivariate public key cryptosystems	University of the Ryukyus	Japan	—
29	On the differential security of the HFEv- signature primitive	Kingston and St George's University, Sheffield Emergency Care Forum, University of Bath	United Kingdom	—
30	An existential unforgeable signature scheme based on multivariate quadratic equations	National Institute for Mathematical Sciences	South Africa	—

Showing the 30 most-cited of 49 independent citing papers.

Independent citing papers only; self- and co-author citations excluded. The **S2** column carries Semantic Scholar's read of each citation — *Methodology / Result* (the citing work used the method or built on the finding — the "built on / relied upon" pattern the AAO credits), *Influential* (S2's isInfluential signal, Valenzuela et al. 2015), or *Background* (a passing mention).

Contribution 2

Claim — Contribution 2

The researcher established foundational asymptotic analyses of semi-regular polynomial systems, subsequently pioneering critical security evaluations and attacks on multivariate public key cryptography schemes.

The researcher's contribution centers on the theoretical analysis of polynomial systems and their application to cryptographic security. This line of work is anchored by the 2005 paper on the asymptotic behaviour of the degree of regularity of semi-regular polynomial systems, which serves as the theoretical foundation for subsequent research.

INDEPENDENT CITATIONS FOR THIS CONTRIBUTION: 387

CORE PAPER

Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems

2005 · 313 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	Recent progress in the security evaluation of multivariate public-key cryptography	Kyushu University, Nihon University, The University of Tokyo	Japan	—
2	A survey of public-key cryptographic primitives in wireless sensor networks	National Institute for Mathematical Sciences	South Africa	—
3	Efficient pseudorandom correlation generators: Silent OT extension and more	Aarhus University, Ben-Gurion University of the Negev, Karlsruhe Institute of Technology	Denmark, Germany, Israel	—
4	Improved cryptanalysis of UOV and rainbow	KU Leuven	Belgium	—
5	Pasta: A case for hybrid homomorphic encryption	Graz University of Technology, Know Center Research GmbH (Austria), Ruhr University Bochum	Austria, Germany	—
6	Horst Meets Fluid-SPN: Griffin for Zero-Knowledge Applications	Ruhr University Bochum	Germany	—
7	Feistel structures for MPC, and more	AIT Austrian Institute of Technology, King's College London, Royal Holloway, University of London	Austria, Germany, United Kingdom	—
8	Reinforced concrete: A fast hash function for verifiable computation	Graz University of Technology, Know Center Research GmbH (Austria), Ruhr University Bochum	Austria, Germany, Luxembourg	—
9	GeMSS: a great multivariate short signature	CS Communication & Systèmes (France), Laboratoire de Mathématiques Blaise Pascal, Orange (France)	France	—
10	Practical post-quantum signature schemes from isomorphism problems of trilinear forms	CISPA Helmholtz Center for Information Security, Nokia (France), University of Technology Sydney	Australia, France, Germany	—
11	Algebraic Cryptanalysis of STARK-Friendly Designs: Application to MARVELlous and MiMC	King's College London, Ruhr University Bochum, University of London	Germany, Luxembourg, United Kingdom	—
12	An algebraic attack on rank metric code-based cryptosystems	Centre Inria de Paris, Université de Limoges, Université de Rouen Normandie	France	—
13	On the complexity of the rank syndrome decoding problem	Université de Limoges	France	—

No.	Citing paper	Citing institution(s)	Country	S2
14	An algebraic attack on ciphers with low-degree round functions: application to full MiMC	Graz University of Technology, Ruhr University Bochum	Austria, Germany	—
15	A new algebraic approach to the regular syndrome decoding problem and implications for PCG constructions	Sorbonne Universités, UPMC Univ Paris 06	France	—
16	Cryptanalysis of minrank	ENSTA, LIP6	France	—
17	On the complexity of solving quadratic boolean systems	Inria, LIP6, Université de Rouen	France	—
18	From Farfalle to Megafono via Ciminion: The PRF Hydra for MPC Applications	Radboud University Nijmegen, Ruhr University Bochum, Sorbonne Universités, UPMC Univ Paris 06	France, Germany, Netherlands	—
19	Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic	LIP6	France	—
20	A new variant of unbalanced oil and vinegar using quotient ring: QR-UOV	Kyushu University, NTT, The University of Tokyo	Japan	—
21	Solving underdetermined systems of multivariate quadratic equations revisited	Ruhr University Bochum	Germany	—
22	A crossbred algorithm for solving Boolean polynomial systems	CISPA Helmholtz Center for Information Security, Université Grenoble-Alpes	France, Germany	—
23	Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology	Inria	France	—
24	Algebraic algorithms for LWE problems	King's College London, LIP6, Sorbonne Université	France, United Kingdom	—
25	Generalized Feistel ciphers for efficient prime field masking	Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier, Ruhr University Bochum, UCLouvain	Belgium, France, Germany	—
26	Qr-uov	Kyushu University, NTT, The University of Tokyo	Japan	—
27	Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree (1, 1): Algorithms and complexity	Inria, Institut national de recherche en sciences et technologies du numérique	France	—
28	Polynomial equivalence problems: Algorithmic and theoretical aspects	LIP6	France	—
29	Open problems related to algebraic attacks on stream ciphers	Inria	France	—
30	Sub-cubic change of ordering for Gröbner basis: a probabilistic approach	Centre Inria de l'Université de Lorraine, Centre Inria de Sorbonne Université, Sorbonne Universités UPMC Univ.	France	—

Showing the 30 most-cited of 187 independent citing papers.

Independent citing papers only; self- and co-author citations excluded. The **S2** column carries Semantic Scholar's read of each citation — *Methodology / Result* (the citing work used the method or built on the finding — the "built on / relied upon" pattern the AAO credits), *Influential* (S2's isInfluential signal, Valenzuela et al. 2015), or *Background* (a passing mention).

FOLLOW-UP WORK

Multivariate public key cryptography

2009 · 279 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	Quantum computing: A taxonomy, systematic review and future directions	Queen Mary University of London, Seneca International Academy, The University of Melbourne	Australia, Canada, India	—
2	Post-quantum cryptography acceleration for next generation computers	—	—	—
3	GeMSS: a great multivariate short signature	CS Communication & Systèmes (France), Laboratoire de Mathématiques Blaise Pascal, Orange (France)	France	—
4	The rise and resilience of multivariate cryptography: Advances, pitfalls, and promising pathways	Maulana Azad National Institute of Technology	India	—
5	On the Complexity and Admissible Parameters of the Crossbred Algorithm in	Ibaraki University	Japan	—
6	A Simple Noncommutative UOV Scheme	National Dong Hwa University	Taiwan	—
7	Cryptanalysis of the quaternion rainbow	University of the Ryukyus	Japan	—
8	Bases de Gröbner en Cryptographie Post-Quantique	LIP6	France	—
9	Cybersecurity threats and their mitigation approaches using Machine Learning—A Review	East Stroudsburg University, North Dakota State University, University of Wisconsin–Eau Claire	United States	—
10	A survey and comparison of post-quantum and quantum blockchains	Hamad Bin Khalifa University, King Abdullah University of Science and Technology, Washington University in St. Louis	Qatar, Saudi Arabia, United States	—
11	Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges	Cleveland State University, International Institute of Information Technology, Hyderabad, University of Illinois at Springfield	India, United States	—
12	Quantum computing challenges in the software industry. A fuzzy AHP-based approach	Lappeenranta-Lahti University of Technology, LUT University, Thapar Institute of Engineering & Technology	Finland, India, Norway	—
13	Handbook of finite fields	Carleton University	Canada	—
14	Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms	University of Strathclyde	United Kingdom	—
15	SoK of used cryptography in blockchain	Norwegian University of Science and Technology, University of Oslo	Norway	—

No.	Citing paper	Citing institution(s)	Country	S2
16	Building resilient web 3.0 infrastructure with quantum information technologies and blockchain: an ambilateral view	Beijing University of Posts and Telecommunications, Guangdong University of Technology, Nanyang Technological University	China, Singapore	—
17	Cybersecurity challenges associated with the internet of things in a post-quantum world	King's College London	United Kingdom	—
18	A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks	Kurukshetra University	India	—
19	Quantum money from hidden subspaces	MIT	United States	—
20	Future Digital Identity Management with Quantum Secure Blockchain	La Trobe University, RMIT University	Australia	—
21	Hardware security in the connected world	IIT Kharagpur, Radboud University Nijmegen	India, Netherlands	—
22	Indistinguishability obfuscation without multilinear maps: new methods for bootstrapping and instantiation	IIT Madras	India	—
23	A new approach based on quadratic forms to attack the McEliece cryptosystem	Helmholtz Center for Information Security, Inria, Laboratoire d'Informatique de l'École Polytechnique	France, Germany	—
24	High-performance and configurable SW/HW co-design of post-quantum signature CRYSTALS-Dilithium	BNU-HKBU United International College, City University of Hong Kong, University of California, Irvine Medical Center	China, Hong Kong, United States	—
25	Multivariable quantum signal processing (M-QSP): prophecies of the two-headed oracle	Massachusetts Institute of Technology	United States	—
26	A new post-quantum multivariate polynomial public key encapsulation algorithm: R. Kuang et al.	Carleton University, Quantropi (Canada)	Canada	—
27	Post-quantum verifiable random function from symmetric primitives in pos blockchain	Monash University, The University of Hong Kong, Tokyo Institute of Technology	Australia, Hong Kong, Japan	—
28	Quantum cryptography for secured communication networks	SRM Institute of Science and Technology	India	—
29	Homomorphic polynomial public key encapsulation over two hidden rings for quantum-safe key encapsulation: R. Kuang, M. Perepechaenko	Quantropi (Canada)	Canada	—
30	Building resilient Web 3.0 with quantum information technologies and blockchain: An ambilateral view	Beijing University of Posts and Telecommunications, Guangdong University of Technology, Nanyang Technological University	China, Singapore	—

Showing the 30 most-cited of 121 independent citing papers.

Independent citing papers only; self- and co-author citations excluded. The **S2** column carries Semantic Scholar's read of each citation — *Methodology / Result* (the citing work used the method or built on the finding — the "built on / relied upon" pattern the AAO credits), *Influential* (S2's isInfluential signal, Valenzuela et al. 2015), or *Background* (a passing mention).

FOLLOW-UP WORK

New differential-algebraic attacks and reparametrization of rainbow

2008 · 263 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	Recent progress in the security evaluation of multivariate public-key cryptography	Kyushu University, Nihon University, The University of Tokyo	Japan	—
2	A new variant of unbalanced oil and vinegar using quotient ring: QR-UOV	Kyushu University, NTT, The University of Tokyo	Japan	—
3	Qr-uov	Kyushu University, NTT, The University of Tokyo	Japan	—
4	A simple noncommutative UOV scheme	National Dong Hwa University	Taiwan	—
5	The rise and resilience of multivariate cryptography: Advances, pitfalls, and promising pathways	Maulana Azad National Institute of Technology	India	—
6	MQQ-SIG: An ultra-fast and provably CMA resistant digital signature scheme	LIP6, Norwegian University of Science and Technology	France, Norway	—
7	Cryptanalysis of enhanced TTS, STS and all its variants, or: Why cross-terms are important	Ruhr University Bochum	Germany	—
8	Circulant UOV: a new UOV variant with shorter private key and faster signature generation.	—	—	—
9	Geometric approach to the cryptanalysis of post-quantum multivariate signature schemes	Sorbonne Université	France	—
10	Cryptanalysis of the quaternion rainbow	University of the Ryukyus	Japan	—
11	A Study on Randomness Used in Signature Generation of UOV	Kyushu University	Japan	—
12	A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV	Kyushu University, NTT, The University of Tokyo	Japan	—
13	MQQ-SIG	Institut national de recherche en sciences et technologies du numérique, Norwegian University of Science and Technology, NTNU Samfunnsforskning	France, North Macedonia, Norway	—
14	Miller–Rabin Probabilistic Primality Test	The College of William and Mary	United States	—
15	Moore's Law	EMC Corporation	United States	—
16	Mix-Zones in Wireless Mobile Networks	KTH Royal Institute of Technology	Sweden	—
17	Multiple independent levels of security	University of Idaho	United States	—
18	Multiplicative Knapsack Cryptosystem	École Normale Supérieure	France	—
19	Monotone signatures	École Normale Supérieure	France	—
20	Machine Learning for Network Intrusion Detection	Institut Mines-Télécom	France	—
21	Miss-in-the-middle attack	University of Luxembourg	Luxembourg	—
22	McEliece Public Key Cryptosystem	Centre Inria de Paris	France	—

No.	Citing paper	Citing institution(s)	Country	S2
23	Meet-in-the-middle attack	University of Luxembourg	Luxembourg	—
24	Maxims	—	—	—
25	MASH Hash Functions (Modular Arithmetic Secure Hash)	University of Leuven	Belgium	—
26	Multiprecision Multiplication	Worcester Polytechnic Institute	United States	—
27	Modular Arithmetic	Royal Holloway University of London, Silverbrook Research, University of California, Irvine Medical Center	United Kingdom, United States	—
28	Modes of operation of a block cipher	University of Leuven	Belgium	—
29	Multiprecision Squaring	Worcester Polytechnic Institute	United States	—
30	Merkle Trees	University of Salerno	Italy	—

Showing the 30 most-cited of 79 independent citing papers.

Independent citing papers only; self- and co-author citations excluded. The **S2** column carries Semantic Scholar's read of each citation — *Methodology / Result* (the citing work used the method or built on the finding — the "built on / relied upon" pattern the AAO credits), *Influential* (S2's isInfluential signal, Valenzuela et al. 2015), or *Background* (a passing mention).

Contribution 3

Claim — Contribution 3

The researcher advanced efficient cryptographic primitives for constrained environments, establishing foundational work on high-speed smart card signatures and extending it to multivariate public-key encryption schemes.

The researcher's contribution centers on developing efficient cryptographic solutions for resource-constrained devices, anchored by the seminal 2004 paper on high-speed signatures for low-cost smart cards. This core work was subsequently expanded in 2006 with a follow-up study proposing a medium-field multivariate public-key encryption scheme, indicating a sustained focus on optimizing public-key cryptography for practical deployment.

This line of work appears to address the critical challenge of implementing robust security protocols on hardware with limited processing power and memory. By transitioning from signature schemes to encryption mechanisms within the multivariate framework, the researcher likely sought to broaden the applicability of these lightweight cryptographic methods, suggesting a novel approach to balancing security strength with computational efficiency in embedded systems.

The significance of this research is evidenced by substantial independent uptake, with the core paper accumulating 122 citations and the follow-up work garnering 86 citations. Notably, 90.7% of the 1,417 classified citations for this scholar originate from independent researchers, demonstrating that this body of work has been widely recognized and utilized by the broader academic community beyond the researcher's immediate circle.

INDEPENDENT CITATIONS FOR THIS CONTRIBUTION: 7

CORE PAPER

TTS: High-speed signatures on a low-cost smart card

2004 · 122 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	Miss-in-the-middle attack	University of Luxembourg	Luxembourg	—
2	Mdc-2 and mdc-4	University of Leuven	Belgium	—

No.	Citing paper	Citing institution(s)	Country	S2
3	A polynomial-time key-recovery attack on MQQ cryptosystems	Inria, LIP6, Norwegian University of Science and Technology	France, Norway	—
4	Malware detection	Technische Universität Darmstadt, TU Wien	Austria, Germany	—
5	Efficient implementations of MQPKS on constrained devices	Ruhr University Bochum	Germany	—
6	A Multivariate Convertible Group Signature Scheme	Indian Institute of Information Technology, Motilal Nehru National Institute of Technology Allahabad	India	—
7	Anonymous Proxy signature scheme based on multivariate polynomials over finite field	Indian Institute of Information Technology, Motilal Nehru National Institute of Technology Allahabad	India	—

Independent citing papers only; self- and co-author citations excluded. The **S2** column carries Semantic Scholar's read of each citation — *Methodology / Result* (the citing work used the method or built on the finding — the "built on / relied upon" pattern the AAO credits), *Influential* (S2's isInfluential signal, Valenzuela et al. 2015), or *Background* (a passing mention).

FOLLOW-UP WORK

A "medium-field" multivariate public-key encryption scheme

2006 · 86 citations (GS)

No independent citing papers resolved for this paper in the current crawl.

D. Citing-Institution Prestige & Geography

Top citing institutions

Institution	Country	World ranking	Citing papers
Tsinghua University	China	SCImago #8 · THE 12 · QS =17	42
LIP6	France	SCImago #3884	39
Ruhr University Bochum	Germany	SCImago #1358 · THE 251–300 · QS =395	39
Technische Universität Darmstadt	Germany	SCImago #1457	32
Aarhus University	Denmark	SCImago #293 · THE 101 · QS 131	32
Kyushu University	Japan	SCImago #873 · THE 301–350 · QS =170	23
Technology Innovation Institute	United Arab Emirates	SCImago #3413	22
KU Leuven	Belgium	SCImago #180 · THE 46 · QS 60	22
University of South Florida	United States	SCImago #806 · THE 351–400 · QS =654	22
University of Luxembourg	Luxembourg	SCImago #1629 · THE 251–300 · QS =381	21
University of Illinois at Chicago	United States	—	21

Institution	Country	World ranking	Citing papers
University of Campinas	Brazil	THE 351–400	21
ETH Zurich	Switzerland	THE 11 · QS 7	20
Radboud University Nijmegen	Netherlands	SCImago #1176 · THE =154	19
Eindhoven University of Technology	Netherlands	SCImago #890 · THE =192 · QS =140	19

Geographic distribution of citing authors

Country	Citing papers
United States	297
China	169
Germany	168
France	156
Japan	103
United Kingdom	96
India	68
Switzerland	68
Netherlands	66
Belgium	46
Canada	42
Taiwan	39

Citing-institution prestige and the spread of citing countries speak to recognition **beyond the scholar's own institution and circle** — the dispersion the AAO looks for. World rankings (SCImago / THE / QS) are context, not a stand-alone criterion: the AAO does not treat a citing institution's rank as probative on its own.

F. AAO Precedent Considerations

Pre-filing self-check (AAO denial patterns)

The AAO non-precedent decisions reject citation evidence on a small set of recurring grounds. Confirm the petition addresses each before filing:

- ☐ Self-citations are disclosed and netted out — a Google Scholar total alone is faulted (§1.1).
- ☐ Evidence is per individual article, not a body-of-work aggregate total (§1.2).
- ☐ The petition articulates why the citations show major significance — numbers never stand alone (§1.5).
- ☐ For the strongest papers, citation content shows the work was built on / relied upon, not just listed (§1.6, §2.2).
- ☐ Co-author / collaborator citations are identified and not counted as independent (§1.7).
- ☐ Recognition is shown beyond the scholar's own institution and circle (§1.8).
- ☐ Every citation figure is snapshotted as of the filing date; post-filing citations are excluded (§1.9).
- ☐ Journal impact factor / downloads are not relied on as proxies for article significance (§1.10, §1.12).
- ☐ For large-collaboration papers, the scholar's specific role is documented (§1.13).
- ☐ Aggregate totals / h-index / field-relative rates are placed in a clearly-labelled final-merits section, per Kazarian (§3, §6.1.7).

Disclaimer

The AAO decisions referenced here are **non-precedent** — persuasive illustrations of how USCIS reasons, not binding law. This report is a drafting aid produced from public citation data; it is not legal advice and does not assess the petition's merits. All analysis must be reviewed by qualified immigration counsel.

G. Citation Evidence Index

Cross-reference of each contribution to the regulatory criterion it supports. Counsel should map these to the petition's exhibit numbers.

Contribution	Core paper	Indep. cites	Supports
Contribution 1	High-speed high-security signatures	766	Dhanasar — Prong 2 (well-positioned)
Contribution 2	Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems	387	Dhanasar — Prong 2 (well-positioned)
Contribution 3	TTS: High-speed signatures on a low-cost smart card	7	Dhanasar — Prong 2 (well-positioned)