Citation Evidence Report

EB-2 NIW Petition — National Interest Waiver

Matter of Dhanasar · Prong 2 (well-positioned)

Oded Goldreich

Professor of Computer Science, Weizmann Institute of Science

Google Scholar profile

Generated 2026-06-10 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

556	561	31	102
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.

89.1% independent of 550 classified citing papers

Citation type	Count
Independent	490
Self-citation	15
Co-author	45
Same-institution	0

8 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 established foundational frameworks for modern cryptography and computational complexity, creating seminal reference works that define core theoretical limits and concepts in the field.

CLAIM: The researcher's primary contribution lies in establishing the theoretical bedrock of cryptography and computational complexity, anchored by the highly cited monograph "Foundations of Cryptography" (2001). This work serves as the central pillar for a sustained line of inquiry into the fundamental limits of computation and security.

ORIGINALITY: This line of work appears to address the need for rigorous, unified theoretical frameworks in a rapidly evolving field. By publishing a comprehensive foundation in 2001, followed by targeted investigations into program obfuscation (2012) and conceptual complexity perspectives (2008), the researcher systematically expanded the theoretical boundaries. The titles suggest a progression from establishing general foundations to tackling specific, hard problems like obfuscation, indicating a deep and original engagement with the conceptual underpinnings of the discipline.

SIGNIFICANCE: The impact of this work is evidenced by substantial citation counts, with the core text accumulating over 8,000 citations and follow-up papers garnering thousands more. Crucially, analysis of 550 citing papers reveals that 89.1% originate from independent researchers, demonstrating that this work has been widely adopted and relied upon by the broader scientific community rather than just the researcher's immediate circle. This high degree of independent uptake confirms the work's status as a standard reference and a significant driver of progress in the field.

INDEPENDENT CITATIONS FOR THIS CONTRIBUTION: 57

CORE PAPER

Foundations of Cryptography

2001 · Cambridge University Press, 2001 · 8,271 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	An overview of implementing security and privacy in federated learning	Nanjing University of Information Science and Technology	China	—
2	A hybrid approach to privacy-preserving federated learning	Georgia Institute of Technology, IBM Research, IBM Research Almaden	Japan, United States	—
3	CryptGPU: Fast privacy-preserving machine learning on the GPU	Facebook AI Research, University of California, Irvine Medical Center, University of Virginia	United States	—
4	Cheetah: Lean and fast secure {Two-Party} deep neural network inference	Alibaba Group	China	—
5	More efficient oblivious transfer and extensions for faster secure computation	Bar-Ilan University, Climate Outreach, Technical University of Darmstadt	Germany, Israel, United Kingdom	—
6	Differentially private federated learning: A systematic review	East China Normal University, Institute of Science Tokyo, Northeastern University	China, Japan, United States	—
7	Why language models hallucinate	Georgia Tech, Google Research, Microsoft Research	United States	—
8	Privacy-preserving deep learning via additively homomorphic encryption	Kobe University, National Institute of Information and Communications Technology	Japan	—

No.	Citing paper	Citing institution(s)	Country	S2
9	Secure single-server aggregation with (poly) logarithmic overhead	Alberta Machine Intelligence Institute, Google, Google (United Kingdom)	Canada, United Kingdom, United States	—
10	Random oracles are practical: A paradigm for designing efficient protocols	IBM, University of California San Diego	United States	—
11	A survey on trust management for Internet of Things	Luleå University of Technology, Xi'an University of Posts and Telecommunications, Xidian University	China, Sweden	—
12	Bumblebee: Secure two-party inference framework for large transformers	Alibaba Group	China	—
13	Secure federated matrix factorization	Hong Kong University of Science and Technology, KAUST, Peking University	China, Hong Kong	—
14	Evaluating 2-DNF formulas on ciphertexts	Stanford University	United States	—
15	Entity authentication and key distribution	University College Cork	Ireland	—
16	Chameleon: A hybrid secure computation framework for machine learning applications	TU Darmstadt, UC San Diego	Germany, United States	—
17	The SPHINCS+ Signature Framework	Cybercrypt, Fraunhofer Institute for Secure Information Technology, National Taiwan University	Denmark, Germany, Netherlands	—
18	Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities	Beijing Institute of Technology, Qatar University, Stevens Institute of Technology	China, Qatar, United States	—
19	On the (im) possibility of obfuscating programs	Yamagata University Faculty of Medicine	Japan	—
20	On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption	Massachusetts Institute of Technology, New York University, Tel Aviv University	Israel, United States	—
21	Non-malleable cryptography	IBM (United States)	United States	—
22	How to simulate it–a tutorial on the simulation proof technique	Climate Outreach	United Kingdom	—
23	{ABY2. 0}: Improved {mixed-protocol} secure {two-party} computation	Indian Institute of Science, Technical University of Darmstadt, TU Darmstadt	Germany, India	—
24	Reasoning about uncertainty	—	—	—
25	Privacy preserving keyword searches on remote encrypted data	Harvard University	United States	—
26	Σ οφος: Forward secure searchable encryption	Direction Générale de l'Armement	France	—
27	Prio: Private, robust, and scalable computation of aggregate statistics	Stanford University	United States	—
28	Can llms separate instructions from data? and what do we even mean by that?	CISPA Helmholtz Center for Information Security, ISTA	Austria, Germany	—
29	Security and privacy aspects of low-cost radio frequency identification systems	Massachusetts Institute of Technology	United States	—

No.	Citing paper	Citing institution(s)	Country	S2
30	Scalable private set intersection based on OT extension	National Research Center for Applied Cybersecurity ATHENE, Technical University of Darmstadt	Germany	—

Showing the 30 most-cited of 56 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

On the (im) possibility of obfuscating programs

2012 · 2,559 citations (GS)

Field-normalised: 1,502 Semantic Scholar citations place it in the top 1% of Computer Science papers from 2012 indexed by Semantic Scholar, by citation count.

No.	Citing paper	Citing institution(s)	Country	S2
1	Development of protecting a software product mathematical model from unlicensed copying based on the GERT method	National Technical University "Kharkiv Polytechnic Institute", Neijiang Normal University	China, Ukraine	—

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

Computational Complexity: A Conceptual Perspective

2008 · 1,106 citations (GS)

Field-normalised: 588 Semantic Scholar citations place it in the top 1% of Computer Science papers from 2008 indexed by Semantic Scholar, by citation count.

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

Contribution 2

Claim — Contribution 2

The researcher established foundational methods for constructing random functions, a seminal contribution that underpins modern cryptographic protocols and probabilistic proof systems.

CLAIM: The researcher's core contribution is the development of methods for constructing random functions, as detailed in the 1986 paper 'How to construct random functions.' This work serves as the foundational pillar for a broader research line that extends into modern cryptography and pseudorandomness.

ORIGINALITY: The titles suggest this line of work addresses the fundamental challenge of generating reliable randomness in computational contexts. By moving from the basic construction of random functions in 1986 to exploring their applications in probabilistic proofs and pseudorandomness by 1999, the researcher appears to have bridged theoretical foundations with practical cryptographic needs, establishing a new framework for understanding these concepts.

SIGNIFICANCE: The impact of this work is evidenced by the core paper's 3,314 citations and the follow-up paper's 637 citations. Notably, 89.1% of the classified citations originate from independent researchers, indicating that this contribution has been widely adopted and validated by the broader scientific community rather than just the researcher's immediate circle.

INDEPENDENT CITATIONS FOR THIS CONTRIBUTION: 84

CORE PAPER

How to construct random functions

1986 · 3,314 citations (GS)

Field-normalised: 2,311 Semantic Scholar citations place it in the top 1% of Mathematics papers from 1986 indexed by Semantic Scholar, by citation count.

No.	Citing paper	Citing institution(s)	Country	S2
1	HHGS: Forward-secure Dynamic Group Signatures from Symmetric Primitives	—	—	—
2	Complete Primitives for Information-Theoretically Secure Two-Party Computation	Ruhr University Bochum, University of Bristol, University of Haifa	Germany, Israel, United Kingdom	—
3	A theory of the learnable	—	—	—
4	Analytic and simulation results of a Gaussian analog random constant based on resistance dispersion	—	—	—
5	Efficient Group Proof of Storage With Malicious-Member Distinction and Revocation	Beijing Institute of Technology, University of New Brunswick	Canada, China	—
6	Experimenting with Fast Private Set Intersection	UC Irvine Health, University College London	United Kingdom, United States	—
7	A MODERN APPROACH	—	—	—
8	Collaborative Wikipedia Hosting	—	—	—
9	On the Security of Generalized Selective Decryption	Institute of Science and Technology Austria, Northeastern University	Austria, United States	—
10	A low-time-consumption image encryption combining 2D parametric Pascal matrix chaotic system and elementary operation	Gansu Institute of Political Science and Law, Nanjing University of Aeronautics and Astronautics	China	—
11	A secure regenerating code-based cloud storage with efficient integrity verification	National Institute of Technology Calicut	India	—
12	An incrementally deployable anti-spoofing mechanism for software-defined networks	ETH Zurich, Korea University	South Korea, Switzerland	—
13	Bounds on the Efficiency of Black-Box Commitment Schemes	University of Maryland, College Park	United States	—
14	Separating Quantum and Classical Learning	—	—	—
15	Computational Hardness of Optimal FairComputation: Beyond Minicrypt	—	—	—
16	Random Image Matching CAPTCHA System	Abu Dhabi University	United Arab Emirates	—
17	Le chiffrement asymétrique et la sécurité prouvée	—	—	—

No.	Citing paper	Citing institution(s)	Country	S2
18	Key agreement from weak bit agreement	—	—	—
19	Reclaiming privacy for smartphone applications	University College London, University of California, Irvine Medical Center	United Kingdom, United States	—
20	Security for the Cloud	—	—	—
21	RFID Security and Privacy	Bedford Research Foundation	United States	—
22	A Uniform Min-Max Theorem and Characterizations of Computational Randomness	—	—	—
23	Lower bounds in communication complexity and learning theory via analytic methods	The University of Texas at Austin	United States	—
24	On the performance of certain Private Set Intersection protocols. (And some remarks on the recent paper by Huang et al. in NDSS'12)	University College London	United Kingdom	—
25	Leakage-Resilient RFID Authentication with Forward-Privacy	Google (United States), National Institute of Information and Communications Technology	Japan, United States	—
26	Towards a Separation of Semantic and CCA Security for Public Key Encryption	Columbia University, Indiana University, University of Illinois Urbana-Champaign	United States	—
27	Computational-Statistical Tradeoffs from NP-hardness	Stanford	United States	—
28	On Nonadaptive Security Reductions of Hitting Set Generators	Kyushu University, National Institute of Informatics	Japan	—
29	7 : 2 On the Average-Case Complexity of MCSP and Its Variants	The University of Tokyo, University of Oxford	Japan, United Kingdom	—
30	Round-Optimal Password-Based Group Key Exchange Protocols in the Standard Model	Chinese Academy of Sciences, PLA Information Engineering University	China	—

Showing the 30 most-cited of 84 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

Modern cryptography, probabilistic proofs and pseudorandomness

1999 · 637 citations (GS)

Field-normalised: 322 Semantic Scholar citations place it in the top 5% of Computer Science papers from 1999 indexed by Semantic Scholar, by citation count.

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

Contribution 3

Claim — Contribution 3

The researcher established foundational frameworks for modern cryptography, creating a seminal body of work that has become a standard reference in the field.

The researcher's primary contribution rests on the 2001 publication titled 'Foundations of Cryptography.' This work appears to serve as a cornerstone text, defining core principles that underpin subsequent developments in the discipline. The titles indicate a focus on establishing rigorous theoretical bases rather than incremental improvements.

This line of work addresses the need for a unified and rigorous theoretical framework in cryptography. By publishing a comprehensive foundational text, the researcher likely filled a critical gap in systematizing cryptographic concepts, moving the field from ad-hoc constructions to structured theoretical models. The absence of follow-up papers by the same researcher suggests this work stands as a complete, self-contained theoretical contribution.

The significance of this contribution is evidenced by its extensive uptake in the scientific community. With over 8,000 citations, the work is clearly highly influential. Furthermore, analysis of 550 citing papers reveals that 89.1% originate from independent researchers, indicating that the work has been widely adopted and utilized by the broader global research community beyond the author's immediate circle.

INDEPENDENT CITATIONS FOR THIS CONTRIBUTION: 0

CORE PAPER

Foundations of Cryptography

2001 · 8,271 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
University of California, Irvine Medical Center	United States	—	21
Massachusetts Institute of Technology	United States	SCImago #41 · THE 2 · QS 1	21
Weizmann Institute of Science	Israel	SCImago #739	18
Technion – Israel Institute of Technology	Israel	SCImago #1195 · THE 301–350 · QS =350	16
Weizmann Institute of Science	—	—	15
Aarhus University	Denmark	SCImago #293 · THE 101 · QS 131	13
Bar-Ilan University	Israel	SCImago #2119 · THE 601–800 · QS =660	13
Tel Aviv University	Israel	SCImago #507 · THE 201–250 · QS 223	10
Cornell University	United States	SCImago #61 · THE =18 · QS 16	10
Technical University of Darmstadt	Germany	SCImago #1457 · THE 251–300 · QS =253	10
Johns Hopkins University	United States	SCImago #33 · THE 16 · QS 24	8
Northeastern University	United States	QS 384	8

Institution	Country	World ranking	Citing papers
Georgia Institute of Technology	United States	SCImago #270 · THE =41 · QS =123	7
ETH Zurich	Switzerland	THE 11 · QS 7	7
UCLA Health	United States	—	6

Geographic distribution of citing authors

Country	Citing papers
United States	170
Israel	60
China	54
Germany	39
United Kingdom	34
France	25
Japan	22
Canada	20
Denmark	17
Switzerland	16
India	15
Taiwan	14

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	Foundations of Cryptography	57	Dhanasar — Prong 2 (well-positioned)
Contribution 2	How to construct random functions	84	Dhanasar — Prong 2 (well-positioned)
Contribution 3	Foundations of Cryptography	0	Dhanasar — Prong 2 (well-positioned)