Highly Cited Research Papers

These citations counts are from http://scholar.google.com, on Thursday, August 31st, 2017. Full bibliographical listings are available from my 19-page CV (available at the URL below). The 86 invited research talks that I have given are listed there also. http://www.gregorybard.com/papers/CV_long_form.pdf

- Nicolas Courtois and G. Bard, "Algebraic Cryptanalysis of the Data Encryption Standard," 190 citations.
- Nicolas Courtois, G. Bard, and David Wagner, "Algebraic and Slide Attacks on KeeLoq," 141 citations.
- G. Bard, *Algebraic Cryptanalysis.* 137 citations.
- G. Bard, "Spelling-Error and Reordering Tolerant Pass-phrases via the Damerau-Levenshtein String-Edit Distance Metric," 61 citations.
- G. Bard, "A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL," 55 citations.
- G. Bard, Nicolas Courtois, Jorge Nakahara Jr., Pouyan Sepehrdad, and Bingsheng Zhang. "Algebraic, AIDA/Cube and Side Channel Analysis of the KATAN Family of Block Ciphers," 47 citations.
- G. Bard, PhD Dissertation: "Algorithms for solving linear and polynomial systems of equations over finite fields, with applications to cryptanalysis," 42 citations.
- G. Bard, "Vulnerability of SSL to Chosen-Plaintext Attack," 42 citations.
- Martin Albrecht, G. Bard, and Bill Hart. "Algorithm 898: Efficient Multiplication of Dense Matrices over $GF(2)$," 30 citations.
- G. Bard, "Accelerating Cryptanalysis with the Method of Four Russians," 22 citations.
- Nicolas Courtois, G. Bard, and Andrey Bogdanov. "Periodic Ciphers with Small Blocks and Cryptanalysis of KeeLoq," 20 citations.
- G. Bard, Shaun van Ault, and Nicolas Courtois. "Statistics of Random Permutations and the Cryptanalysis Of Periodic Block Ciphers," 16 citations.
- G. Bard, *Sage for Undergraduates*, 16 citations.
- Nicolas Courtois, G. Bard, and Daniel Hulme. "A New General-Purpose Method to Multiply 3×3 Matrices Using Only 23 Multiplications," 14 citations.
- Michael Black and G. Bard. "SAT Over BOINC: An Application-Independent Volunteer Grid Project," 10 citations.
- G. Bard, "Achieving a log(n) Speed Up for Boolean Matrix Operations and Calculating the Complexity of the Dense Linear Algebra step of Algebraic Stream Cipher Attacks and of Integer Factorization Methods," 10 citations.
- Nicolas Courtois, and G. Bard. "Random Permutation Statistics and An Improved Slide-Determine Attack on KeeLoq," 8 citations.
- G. Bard, "Modes of Encryption Secure Against Blockwise-Adaptive Chosen-Plaintext Attack," 7 citations.
- Martin Albrecht, G. Bard, and Clement Pernet. "Efficient Dense Gaussian Elimination over the Finite Field with Two Elements," 7 citations.

- Kenneth Wong, and G. Bard. "Improved Algebraic Cryptanalysis of QUAD, Bivium, and Trivium via Graph Partitioning on Equation Systems," 5 citations.

- G. Bard, Nicolas Courtois, and Chris Jefferson. "Solution of Sparse Polynomial Systems over GF(2) via SAT-Solvers," 5 citations.

- G. Bard. "Algorithms for Fast Matrix Operations," 4 citations.

- K. Wong, G. Bard, and R. Lewis. "Partitioning Multivariate Polynomial Equations via Vertex Separators for Algebraic Cryptanalysis and Mathematical Applications," 3 citations.

- G. Bard. "Matrix Inversion, LUP-Factorization, and System Solving, via the Method of Four Russians, in $\Theta(n^3/\log n)$ Time," 2 citations.

- G. Bard, "Numerically Estimating Derivatives during Simulations," 1 citation.

- G. Bard. "DEMOCRACY: A Heuristic for Polynomial Systems of Equations over Finite Fields," 1 citation.

- G. Bard, C. Gressel, and A. Hecht. "Security Analysis of the ZK Crypt Data Authenticator and Stream Cipher against Algebraic Cryptanalysis, Differential and Correlation Attacks," 1 citation.

- G. Bard. "The Application of Polynomials over the Field of Two Elements to a problem in Intellectual Property," 1 citation.

- G. Bard, "FLOWHUNT— An Attempt at Specification-Based Intrusion Detection using Neural Networks," 1 citation.

Abstract Only: G. Bard. "DEMOCRACY: A Heuristic for Polynomial Systems of Equations over Finite Fields," 1 citation.

- G. Bard, "An inequality for detecting financial fraud, derived from the Markowitz Optimal Portfolio Theory," 0 citations.