
Nelson H. F. Beebe  
University of Utah  
Department of Mathematics, 110 LCB  
155 S 1400 E RM 233  
Salt Lake City, UT 84112-0090  
USA  
Tel: +1 801 581 5254  
FAX: +1 801 581 4148  
E-mail: beebe@math.utah.edu, beebe@acm.org, beebe@computer.org (Internet)  
WWW URL: http://www.math.utah.edu/~beebe/  
14 October 2017  
Version 1.02

**Title word cross-reference**

2 [15]. $F_q$ [35].  

-Party [15].  

5th [41].  

Achieve [22]. against [36]. Algorithm [29]. Algorithms [23].  
Anonymous [33]. Application [6, 35]. Arguments [18]. Attack [28].  
Attacks [36]. Attribute [8]. Attribute-Based [8]. Authenticated [30].  


Code-Based [35, 36]. Codes [22, 28]. Coding [33]. Coin [14, 5].
[31]. Cryptographic [16, 15]. Cryptography [35, 41]. Cryptomania [7].

DML [40].

Extended [29].

Fischlin [12]. Forms [38]. Framework [30]. France [41]. Free [10]. Front


Hybrid [33].

Imply [14]. Improved [24, 34]. Intelligent [40]. interactive [18, 19].
International [41]. Invariants [32]. Inversion [36].

July [40]. June [41].

Key [30]. Knowledge [5, 4, 17].


Multivariate [29, 32, 38].

NIZK [19]. NIZKs [6]. Non [18, 19]. Non-interactive [18, 19].
Non-malleable [19].

Overcoming [1].
REFERENCES


Quadratic [29, 38]. Quantum [23, 16, 27, 30, 32, 41].


Scheme [24, 31, 37, 38]. Schemes [34]. Search [27]. Secure [20, 33].
Subset-Sum [23]. Succinct [18, 6]. Sum [23]. Syndrome [36]. Syndromes
[22]. Systems [40]. SZK [17].

Tossing [14]. Transformation [31].

UK [40]. Underdefined [29]. Unprovable [19]. UOV [34]. Using
[22, 27, 38].

Variant [28]. Vector [27]. Verification [34]. Versions [34]. via [3, 18].

Weak [1]. Workshop [41]. World [16].

XOR [10].


References

in Computer Science, 7785:1–22, 2013. CODEN LNCSD9. ISSN 0302-
9743 (print), 1611-3349 (electronic). URL http://link.springer.com/
chapter/10.1007/978-3-642-36594-2_1/; http://link.springer.
com/content/pdf/bfm:978-3-642-36594-2/1.pdf.

to the chain rule for conditional HILL entropy. Lecture Notes in Computer
REFERENCES


REFERENCES


REFERENCES


[27] Thijs Laarhoven, Michele Mosca, and Joop van de Pol. Solving the shortest vector problem in lattices faster using quantum search. Lecture Notes in


REFERENCES


