A Complete Bibliography of Publications in the *Journal of Cryptographic Engineering*

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/  

30 November 2019  
Version 1.15

Title word cross-reference

256 [108], 384 [77], 64 [130], 8 [154], \(N = p^2q\) [141], \(\tau\) [188], \(GF(2^8)\) [200], \(Z\) [48, 13].

-adic [188], -bit [154, 77, 108, 130].

128 [85].

2.0 [99], 2012 [52], 2013 [74], 2014 [102], 2015 [143, 124], 2016 [150, 164], 2017 [175].

2nd [95].

academic [121], accelerate [49], account [135], Achieving [83], addition [193, 194],
adic [188], AES [120, 59, 148, 198, 10, 40, 95, 78, 7, 107, 64, 203, 39, 53, 18], against [66, 20, 40, 213, 65, 167, 109, 71, 107, 19, 87, 89, 132, 25, 157, 202], aimed [25], algebraic [32, 140, 64], Algorithm [5, 161, 210, 22, 162, 199, 38], Algorithm-level [5], algorithms [100, 94, 214], Analysis [32, 45, 44, 59, 88, 165, 137, 155, 40, 142, 22, 121, 109, 26, 71, 2, 189, 158, 3, 135, 101, 208, 132, 197, 53, 18, 207], analyzing [70, 166], any [126], application [148, 103, 56, 91, 38], applications [70, 194, 43, 44], applies [121], approach [177, 107, 140, 208], arbiter [136, 207], arbitrarily [207], architecture [10], area [10], Arithmetic [188, 173, 181, 184, 183, 13, 131, 204], ASICs [79], \(ASICs\) [111], aspects [155], assembly [208, 132], assessment [125], associated [186], asymmetric [165], attack [120, 99, 32, 218, 77, 191, 158, 64, 3, 145, 169, 47, 126, 151], attackers [207], Attacking...


Constructing [194]. Contacts [8, 14, 21, 28, 35, 41, 46, 51, 58, 63, 68, 73, 97, 80, 86, 92]. contemporary [170].


cross-device [60]. CRT [20, 65, 57, 89, 160]. cryptanalysis [129, 18]. cryptanalytic [123].

Cryptographic [1, 10, 70, 29, 199, 219, 163]. cryptography [70, 113, 137, 72, 30, 108, 4, 55, 7, 188].
cryptology [199]. cryptoprocessor [3].
cryptosystems [61, 24, 34, 84, 216, 25].

Data [192, 219, 85]. data-widths [85].
debiasing [192]. decomposition [116].

distinguishing [12]. do [172]. domain [91].
dopant [76, 104]. dopant-level [76, 104].
DPA [95, 114, 91]. drive [157]. dual [178].
dual-rail [178]. dynamic [29].
easy [153]. ECC [48]. ECDSA [77, 94].
ECHO [10]. ECSR [5]. Editorial [143].
Edwards [167, 187]. efficacy [142].
efficiency [137, 142]. Efficient [100, 30, 31, 82, 159, 163, 201, 84, 154, 193, 187, 200].
embedded [48, 70, 84]. emission [53].
encapsulation [134]. encoding [166].
encryption [198, 171, 172, 211, 205, 55, 62, 202].
encryption/decryption [198].
endomorphism [193]. Engineering [1].
enhancement [69]. enhancing [111].
ent [126]. Erratum [34]. error [5, 109].
Euclidean [161, 193, 162]. evaluation [103, 45, 106, 12, 111]. evaluations [90].
Exclusive [126]. execution [209, 9].
explanations [188]. experimental [45].
exploitable [206]. exploration [29].
exponent [201, 93, 126, 160].
exponentiation [31, 9, 159, 201, 38].
Extractors [19].
faults [57]. feasibility [106]. feedback [95].
Feistel [139, 199]. FIA [213]. field [210, 108]. fields [217, 103]. finite [103].
first [26]. Fixed [201]. Fixed-base [201].
flash [157]. flexible [218]. flip [156].
flip-flops [156]. flops [156]. flow [209].
FPGAs [178, 106, 138, 220]. framework [61, 139, 123, 206, 12]. free [131, 39].
frequency [117, 91]. frequency-based [117]. fresh [88]. function [10]. functions [49, 163, 133, 54].
 glitches [23]. glitchy-clock [23]. GLS [100].
GLV [100]. GLV-based [100]. GPU [218].
GPU-based [218]. GPUs [203].
hardware-software [48].
hardware/software [147]. Harvesting [7].
hash [10, 49]. hashing [130]. Having [152].
HC [85]. HC-128 [85]. HCCA [210].
HCCA-resistant [210]. Help [8, 14, 21, 28, 35, 41, 46, 51, 58, 63, 68, 73, 97, 80, 86, 92].
Helper [192]. hidden [77]. hide [178].
High [36, 17, 83, 4, 203, 157]. high-order [83].
high-performance [4, 203].
high-security [36, 157]. High-speed [36].
Higher [39, 142, 204]. Higher-order [39, 142, 204].
Highly [200]. history [119].
homomorphic [205, 25]. honor [180].
horizontal [196, 110]. Horse [135]. Horst [199]. hybrid [200].
ICs [117]. identification [206]. image [45].
image-based [45]. immunity [83].
impacts [17]. Implementation [134, 113, 65, 100, 30, 205, 163, 39].
implementations [196, 31, 115, 71, 47].
instruction [29, 87, 16]. integrated [190]. Interdiction [157]. Internal [197, 101]. Internet [212].
Methodology

[102, 74, 175, 150, 124, 164, 1, 2, 52].

inventor [199].

Inversion

[131, 96, 182, 200]. Inversion-free [131]. IP
[106]. irreducible [217]. isomorphisms
[131]. issue [102, 74, 175, 150, 124, 52, 180].

Java [27]. Journal [1].

Karatsuba [186, 82]. Karatsuba-like [186].

KEM [176]. key [81, 24, 34, 165, 22, 134, 105, 141, 30, 127, 47, 25]. key-extraction
[105]. keying [88]. Kite [218]. Koblitz
[188].

ladder [5, 185]. ladder-based [5]. lambda
[75]. laptop [105]. large [78, 207]. latches
[69]. lattice [173]. Lawrence [180].

Leakage [125, 88, 83, 11, 153, 134, 219, 91].

leakage-resilient [88, 134]. leakages [168].

leaks [77, 43, 79]. learning
[136, 26, 107, 189]. length [172]. less
[130, 16]. level [209, 76, 5, 158, 149, 104].

library [203]. licensing [106]. lightweight
[212, 179, 7, 188, 44]. like [186]. limitations
[90]. limits [59]. linear [148, 56, 37].

listening [121]. localized [178]. locations
[69]. logarithm [138]. logic [178]. logically
[15]. lose [207]. low [10, 205, 7]. low-area
[10]. low-depth [205]. LUCIFER [199].

LWE [128]. Lyra [81].

Machine [26, 107, 189]. machines [119].

maintaining [111]. Maiorana [163].

management [146]. masked [107, 208].

Masking [78, 128, 154, 213, 177, 204].

mathematical [152]. maxterm [218]. may
[152]. McBits [176]. McEliece [24, 34, 3].

McFarland [163]. MDPC [216]. mean
[60]. MEAS [202]. measurable [79].

mechanism [134]. mechanisms [29].

memory [81, 62, 202]. Message [25, 49].

Message-aimed [25]. Method
[135, 22, 6, 111]. methodology [125].

metric [117, 98]. MICKEY [99].

microarchitectural [170].

microcontroller [30]. Minimizing [62].

misplaced [144]. Mixed [211].

Mixed-radix [211]. mode [197]. model

models [67, 168]. modern [4]. modular

moments [142]. Montgomery
[181, 184, 183, 5, 57, 214, 185, 180, 215, 182].

MSP430X [30]. Multi [39, 149, 38, 203].

multi-cores [203]. Multi-exponentiation
[38]. Multi-level [149]. multidimensional
[194]. multiparty [78]. multiple [168, 145].

multiplication [118, 183, 210, 193, 100, 57, 13, 112, 82, 201, 16, 220]. multiplications
[48, 130]. multiplicative [159, 201].

multiplier [210, 37, 215]. multipliers [217].

Multiprecision [112]. multivariate [168].

Mutual [142]. my [105].

Naccache [211]. nano [7]. nano-CMOS
[7]. nanometer [117]. need [172].

networks [30]. Neumann [174].

Niederreiter [24, 34, 55]. NIST [220]. nm
[7]. no [152]. non [56]. non-profiled [56].

nonce [77]. nonlinear [148].

normalization [60]. NTRUEncrypt [71].

number [181, 122, 77].

oblivious [54]. off [105]. on-chip [23].

Online [195]. OpenSSL [151]. operands
[210]. operations [148]. Optimal
[168, 22, 9]. optimization [216]. optimized
[56, 115, 82]. order [142, 83, 204, 39].

organized [121]. oscillator [122].

oscillator-based [122]. oscillators [101].

outputting [69]. overflow [145]. overhead
[62]. overview [158].

PAC [136]. pace [174]. pairing [205].

pairing-based [205]. Parallel [203].

parallelizable [197]. Parallelizing [49].

Party [39]. passive [7]. password [81].
REFERENCES


T [120]. T-Box [120]. tags [7]. taking [135]. tampering [120]. tap [40]. targeting [122]. taxonomy [67]. techniques [186].


Two [75, 66, 171]. ultra [7]. ultra-low-voltage [7]. unclonable [54]. unconventional [17].


validation [117]. variance [116, 60]. variant [141]. Variety [69, 111].

verification [148, 209, 65, 94, 147, 87, 149].

version [76, 154, 77, 153, 100, 56, 178, 189, 127].

versus [189, 169, 44]. Vertical [110].

virtualized [209]. voltage [7]. vs [78].

vulnerabilities [161, 162].

weak [19]. web [43]. Weierstraß [13].

widths [85]. wire [40]. wire-tap [40].

within [181].

Xilinx [70, 106]. XOR [207].

zero [60]. zero-mean [60].

References


REFERENCES


REFERENCES


REFERENCES

??, May 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Bernstein:2012:HSH

Hasan:2012:SMS

Yen:2012:MEA

Roche:2012:HOG

Bringer:2012:PA

Anonymous:2012:HCB

Kasper:2012:SCB

Mather:2012:PSC
REFERENCES


Trujillo-Olaya:2012:APV


Shariati:2012:AEE


Anonymous:2012:HCC


Rolt:2012:SAS


Gueron:2012:PMS


Koeberl:2012:PD

REFERENCES


REFERENCES


NEGRE:2014:EBP


CARLET:2014:ASC


BIASSI:2014:SEC


PAUL:2014:DSC


ANONYMOUS:2014:HCb


MORO:2014:FVS


BELAÏD:2014:TFR


RAUZY:2014:FPC

REFERENCES


Anonymous:2014:HC

Anonymous:2014:HCc

Anonymous:2014:HC
REFERENCES

ISSN 2190-8508 (print), 2190-8516 (electronic).


[105] Daniel Genkin, Itamar Pipman, and Eran Tromer. Get your hands off

Vliegen:2015:PFE


Lerman:2015:MLA


Gueron:2015:FPF


Guo:2015:SAC


Perin:2015:VHC


Yamamoto:2015:NME


Hutter:2015:MMA

REFERENCES


[120] Alejandro Cabrera Aldaya, Alejandro J. Cabrera Sarmiento, and Santiago Sánchez-Solano. AES T-Box tam-

**Ferradi:2016:WOC**


**Bayon:2016:FME**


**Saarinen:2016:BAC**


**Guneysu:2016:ICS**


**Schneider:2016:LAM**


**Schindler:2016:EEB**


**Maes:2016:SKG**

Reparaz:2016:MRL


Coisel:2016:ICD


Lemire:2016:FBU


Goundar:2016:IFA


Rauzy:2016:FPS


Robisson:2016:PFC


Galindo:2016:ILR

Ngo:2016:MT


Ganji:2016:PLA


Bos:2016:SEC


Wenger:2016:HBF


Khalid:2016:RRP


Moein:2016:HAA


Lugou:2017:STU


Azzi:2017:ULC


Sauvage:2017:MLF


Yarom:2017:CTA


Ganji:2017:HNM


Durvaux:2017:TEL


Boss:2017:SBS

[154] Erik Boss, Vincent Grosso, Tim Güneysu, Gregor Leander, Amir Moradi, and Tobias Schneider. Strong...
REFERENCES


Picek:2017:TAV


Ge:2018:SMT


Chakraborti:2018:TUT


Chakraborty:2018:DED


Saarinen:2018:ACB


Ferradi:2018:RPN


Fischer:2018:ICS


Chou:2018:MR


[199] Alan G. Konheim. Horst Feistel: the inventor of LUCIFER, the crypto-


REFERENCES


Kawamura:2019:RMR


Saldamli:2019:UMM


Drucker:2019:TSO


Banegas:2019:NCI


Wu:2019:FUE