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/

07 May 2021  
Version 1.18

**Title word cross-reference**

256 [108]. 384 [77]. 64 [130]. 8 [154]. 
\( N = p^2q \) [141]. \( \tau \) [188]. \( GF(2^8) \) [200]. \( x \) [247]. \( Z \) [48, 13].


128 [85].

2.0 [99]. 2012 [52], 2013 [74], 2014 [102], 2015 [143, 124], 2016 [150, 164], 2017 [175], 2nd [95].

algebraic [32, 140, 64, 244]. Algorithm [5, 161, 210, 22, 162, 199, 38].
art [234]. ASCAD [230]. ASIC [79].

base [201]. based [239, 81, 217, 122, 84, 117, 227, 176, 218, 5, 216, 100, 114, 20, 55, 221, 191, 139, 219, 82, 110, 201, 45, 200, 38].
bitsliced [203]. black [22]. Bleichenbacher [77]. blinding [173, 93, 126, 160]. block [212, 179, 139, 206, 244]. blocks [42].
BRUTUS [123]. Buffer [145]. building [42].

CacheBleed [151]. can [144]. cannot [178]. card [121]. cards [72]. carry [130, 16].
cipher [88, 129]. ciphers [165, 212, 179, 191, 139, 231, 85, 206, 197, 244].
Constant-time [204, 176, 151].
Constructing [194]. Contacts [8, 14, 21, 28, 35, 41, 46, 51, 58, 63, 68, 73, 97, 80, 86, 92]. contemporary [170].
contest [95]. context [181, 242]. control [241]. coordinates [75]. coprocessor [7].
CPA [114, 91]. crime [121]. critical [243].
cross [60]. cross-device [60]. CRT [20, 65, 57, 89, 160]. cryptanalysis [129, 18].
cryptanalytic [123]. crypto [227].
Cryptographic [1, 10, 70, 241, 29, 199, 219, 163, 225].
cryptography [70, 113, 137, 72, 30, 108, 4, 55, 7, 188, 221, 235]. cryptology [199].

Data [192, 219, 85]. data-widths [85].
database [230]. debiasing [192].
decomposition [116]. decryption [198].
DCT [129]. Deep [230, 226]. depth [205].
derivation [81]. deriving [225]. descent [239]. Design
Designing [85]. designs [147]. detect [135].
detection [5, 109, 27]. device [121, 50, 60].
devices [227, 4, 237, 146]. Differential
[59, 99, 109, 194, 2, 231, 197, 18]. dimension
[190]. dimensionality [189]. direct [213].
discrete [138]. Disk [172]. dispersion
[135]. distinguishers [12]. do [172]. does
[226]. 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 [248, 48]. ECDSA
[77, 94]. ECHO [10]. ECSI [5]. Editorial
[238, 143]. Edwards [223, 167, 187].
efficacy [142]. efficiency [137, 142].
Efficient [233, 228, 100, 30, 31, 82, 159, 163, 201, 84, 154, 193, 187, 240, 200].
Electromagnetic [156, 122]. ElGamal
embedded [239, 48, 70, 84, 227]. emission
[53]. encapsulation [134]. encoding [166].
enetration [198, 171, 172, 211, 205, 55, 62, 202].
encryption/decryption [198].
endomorphism [193]. Engineering [1].
engineers [246]. enhancement [69].
enhancing [111]. enough [126]. Erratum
[34]. Error [241, 5, 109, 234]. Euclidean
[161, 193, 162]. evaluation
[103, 234, 45, 106, 12, 111]. evaluations
[90, 240]. Exclusive [126]. execution
[209, 9]. expansions [188]. experimental
[45]. exploitable [206]. exploration [29].
exponent [201, 93, 126, 60].
exponentiation [31, 9, 159, 201, 38].
exponentiations [196, 110]. extended
[161, 76, 154, 77, 153, 100, 56, 178, 162, 189, 127]. extension [167, 29]. extraction [105].
Extractors [19].
factor [133]. fails [178]. fair [12]. family
[231]. Fantomas [233]. Fast
[113, 103, 108, 220, 171, 176, 22]. Faster
[227, 130, 245, 247, 138]. fastest [75]. Fault
Feistel [139, 199]. FIA [213]. field
[210, 108]. fields [217, 103, 232]. finite
[103, 232]. first [26]. Fixed [201].
Fixed-base [201]. flash [157]. flexible
[218]. flip [156]. flip-flops [156]. flops [156].
flow [209]. forensic [121]. Formal
[165, 65, 87, 148, 66, 89, 149]. Formally
[132]. formula [247]. formulae [186].
FPGA [4, 98]. FPGAs
[234, 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].
gap [78]. gate [37]. GCD [38]. generalized
[163, 226]. generation [210, 127].
generator [23]. generators [122]. Generic
[160, 222]. Get [105]. GF [200]. GHASH
[17]. glitch [39]. glitchy [23]. glitchy-clock
[23]. GLS [100]. GLV [100]. GLV-based
[100]. GPU [218]. GPU-based [218].
GPUs [203]. gradient [239].
half [159]. half-size [159]. hands [105].
hard [4]. Harder [138]. Hardware
[140, 157, 48, 76, 10, 70, 154, 170, 55, 71, 147, 158, 135, 44, 106]. hardware-level [158].
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,

Java [27]. Journal [1].


Parallelizable

Pairing-based

Multiplication

Multi-level

Multidimensional

Multiparty

Multiple

Multiplications

Multiplicative

Multiplier

Multifiers

Multivariate

Mutual

Multivariate

Multi-exponentiation

Multi-exponentiation

Multi-cores

Multi-parallel

Multiplicity

Multi-party

Multilevel

Multipliers

Multi-core

Multi-parallel

Multiphotonic

Multiple

Multiplicative

Multi-Factor

Multi-redundant

Multiprecision

Multiplier

Multiplication

Multipliers

Multiplication

Multi-dimensional

Multi-core

Multi-core

Multi-dimensional

Multi-Oscillator

Multi-Layer

Multi-Layer

Multi-Interleaved

Multi-Layer

Multi-Interleaved

Multi-Interleaved

Multi-Oscillator

Multi-Oscillator

Multi-Interleaved

Multi-interleaved

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core

Multi-core

Multi-exponentiation

Multi-core
safe [187]. Same [223]. sampling [101].
Boxes [154]. SCA [213, 6]. scalable [85].
Scalar [13, 48, 210, 193, 100, 201, 16]. scale [237]. Scaling [84]. Scan [191, 47].
Scan-based [191]. schedules [49]. scheme [241, 205, 50, 192, 106]. schemes [166, 171].
search [218, 22]. secrets [224]. section [164]. Secure
[127, 171, 233, 100, 152, 146, 202, 39].
semi [245]. semi-honest [245]. sensitive
[219], sensor [30], sensors [225].
sequencing [210]. Sequential [37]. Set
[245, 29]. setting [56, 245]. Side
Side-channel [24, 34, 208, 248, 230, 117, 166, 40, 246, 168, 83, 95, 103, 72, 105, 229, 26, 221, 90, 189, 43, 19, 64, 135, 133, 47, 240, 79, 202, 12, 236, 38, 226].
signatures [36, 20, 57, 94, 173]. SIKE [247]. Simple
[53, 3]. simplicity [246]. simulations [90].
single [203]. single-source [203]. size [159].
skip [87]. small [44]. Smart [146, 72].
smart-cards [72]. SMASHUP [147].
software [48, 113, 233, 216, 30, 31, 147, 87].
solution [77]. solutions [222]. Some [118].
source [203]. SPA [161, 141, 162, 9].
SPA-resistant [9]. Special
[180, 102, 74, 175, 150, 124, 164, 52].
Spectral [183]. speed [36]. Speeding [16].
SPICE [90]. splitting [159, 201]. SPN
[139]. SPN-based [139]. squeezing [83].
SRAM [50]. standard [129, 94]. state
[234]. state-of-the-art [234]. static [27].
statistical [142, 158]. statistics [114].
statistics-based [114]. Stealthy [76, 104].
Stern [211]. stream [191, 231, 85].
Strengthening [71]. Strong [154, 19].
stronger [138]. study [166, 66, 26, 85]. sub
[37]. sub-linear [37]. success [114, 236].
sun [213]. Survey [248, 170, 229, 235].
symbolic [208]. Synchronization [6].
Synchronous [101]. synthesis [72]. system
[181, 209, 228]. system-level [209].
systems [48, 219, 235, 192].
T [120]. T-Box [120]. tags [7]. taking
[135]. tampering [120]. tap [40]. targeting
[122]. taxonomy [67]. techniques
[186, 229]. teller [119]. Template
[189, 169, 237, 195, 242]. templates [33].
testing [23]. their
[186, 184, 100, 56, 194, 119]. theory [196].
Things [212]. Throughput [115].
Throughput-optimized [115]. time
[96, 176, 204, 9, 240, 151]. timing
[170, 27, 126, 151]. tool [27]. toolbox [216].
toolchain [147]. traces [226]. transfer [54].
Triathlon [212]. TriviA [171]. trivial [192].
Trojan [135, 157]. Trojans [76]. true [122].
Trust [144, 190]. tunable [81]. tweaking
[55]. Two [75, 66, 171].
ultra [7]. ultra-low-voltage [7].
unbalanced [245]. unclonable [54].
unconventional [17]. Understanding [90].
Unified [56, 10, 177, 147, 220]. Uniform
[215]. unit [60]. unit-variance [60].
[232]. USB [157]. use [54, 106]. Using
uTriviA [171].
validation [117]. value [223]. 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].
Xilinx [70, 106]. XOR [207].
zero [60]. zero-mean [60].

References


REFERENCES


REFERENCES


REFERENCES


[38] Sung-Ming Yen, Chien-Ning Chen, and SangJae Moon. Multi-exponentiation algorithm based on binary GCD computation and its application to side-channel countermeasure. *Journal of
REFERENCES


REFERENCES


REFERENCES

Ruhrmair:2013:PUP


Heyse:2013:CBC


Gerard:2013:UOL


Fouque:2013:ARC


Anonymous:2013:HCa


Ali:2013:DFA


Montminy:2013:ICD


Akinyele:2013:CFR

REFERENCES


Kurdziel:2013:MPO


Anonymous:2013:HCb


Mohamed:2013:IAS


Christoﬁ:2013:FVC


Briais:2013:FST


Brown:2013:TTC


Yamamoto:2013:VEP


REFERENCES

16


REFERENCES

DeMulder:2014:UBS


Grosso:2014:MVM


Sugawara:2014:MSC


Anonymous:2014:HCa


Almeida:2014:LPB


Negre:2014:EBP


Carlet:2014:ASC


Biasi:2014:SEC


Schindler:2014:PAP


Karati:2014:NAB


Clavier:2014:PIS


Bos:2014:CTM


Anonymous:2014:HC


Templin:2015:NPA


Banik:2015:IDF


Faz-Hernandez:2015:ESA

Armando Faz-Hernández, Patrick Longa, and Ana H. Sánchez. Efficient and secure algorithms for GLV-based scalar multiplication and their implementation on GLV–GLS curves (extended

OFlynn:2015:SSC


Batina:2015:ICS


Genkin:2015:GYH


Vliegen:2015:PFE


Lerman:2015:MLA


Lerman:2015:MLA


Gueron:2015:FPF


Guo:2015:SAC


Perin:2015:VHC


Yamamoto:2015:NME


Hutter:2015:MMA


Bluhm:2015:FSI


Fei:2015:SBS


REFERENCES


[130] Daniel Lemire and Owen Kaser. Faster 64-bit universal hashing using carry-

**Goundar:2016:IFA**


**Rauzy:2016:FPS**


**Robisson:2016:PFC**


**Galindo:2016:ILR**


**Ngo:2016:MTA**


**Ganji:2016:PLA**

REFERENCES

Bos:2016:SEC


Wenger:2016:HBF


Khalid:2016:RRP


Moein:2016:HAA


Ghafar:2016:SRV


Carbone:2017:MIA


REFERENCES


George Hatzivasilis, Konstantinos Fysarakis, Ioannis Papafstathiou, and Charalampos Manifavas. A review of lightweight...


[194] Aaron Hutchinson and Koray Karabina. Constructing multidimensional differential addition chains and their


**Unterluggauer:2019:MME**


**Peccherillo:2019:PBA**


**Hutter:2019:CTH**


**Herbert:2019:DIL**


**Saha:2019:AFE**


**Wisiol:2019:WAL**


**Ouahma:2019:SCR**

 Baumann:2019:VSL

 Das:2019:AGH

 Géraud:2019:MRN

 Kawamura:2019:RMR

 Saldamli:2019:UMM


REFERENCES


REFERENCES


[244] Sze Ling Yeo, Duc-Phong Le, and Khoongming Khoo. Improved algebraic attacks on lightweight block ciphers. Journal of Cryptographic

