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/  
16 April 2022  
Version 1.20

**Title word cross-reference**

256 [108], 384 [77], 64 [130], 8 [154],  
$N = p^2q$ [141], $t$ [272], $\tau$ [187], $GF(2^8)$ [199],  
x [246], $Z$ [48, 13].  


128 [85]. 128-bit [277].


512-bit [276].

academic [121]. accelerate [49]. accelerators [273]. account [135].  
Applications

cache [261, 251, 253]. cache-timing [251].

frequency [117, 91]. frequency-based [117]. fresh [88]. friendly [270].
FrodoKEM [266]. function [10].
functions [49, 162, 133, 54].

half [159]. half-size [159]. hands [105].
hard [4]. Harder [138]. Hardware [266, 140, 157, 48, 76, 10, 70, 154, 169, 55, 71, 147, 158, 135, 44, 106]. hardware-level [158]. hardware-software [147]. hardware/software [147]. Harvesting [7].
HC-128 [85]. HCCA [209].
HCCA-resistant [209]. Hellman [277].


history [119]. homomorphic [204, 25].

IC [265]. ICs [117]. identification [205].

instruction [29, 87, 16]. instructions [276]. integrated [189]. intensity [263].
Interdiction [157]. interference [221]. Internal [196, 101]. Internet [211].
Intersection [244]. Introduction [102, 74, 174, 150, 124, 163, 1, 2, 52, 229].

isogeny-based [226]. isomorphisms [131]. issue [102, 74, 257, 174, 150, 124, 52, 179].


key-extraction [105]. keying [88]. keys [255, 224]. Kite [217]. Koblitz [187].
ladder [5, 184]. ladder-based [5]. lambda [75]. laptop [105]. large [78, 260, 206].
leakage-resilient [88, 134]. leakages [167].

leaks [77, 43, 79]. learning [229, 136, 228, 26, 254, 107, 188, 251, 225].
length [171]. less [249, 130, 16]. level [208, 76, 5, 158, 149, 104]. levels [277].
library [202]. licensing [106]. lighter [271].
linear [148, 56, 37]. listening [121]. local
multiplication [269]. localized [177]. locations [69].
locking [259]. logarithm [255, 138].
low-energy [273]. low-latency [273].
LUCIFER [198]. LWE [128]. Lyra [81].

management [146]. map [263]. mask [221].
masked [107, 207]. Masking [78, 128, 154, 212, 250, 176, 203, 252, 275].
Melting [274]. memory [81, 62, 201].
MEMS [224]. Message [25, 49].
MICKEY [99]. micro [268].
micro-architectural [268].
microarchitectural [169].
microcontroller [30]. Minimizing [62].
Multi-level [149]. multidimensional [193].
multiparty [78]. multiple [167, 145].
multiplication [276, 118, 182, 209, 192, 100, 57, 13, 112, 269, 82, 231, 200, 16, 219].
multiplications [48, 130]. multiplicative [159, 200]. multiplier [209, 37, 214].
multipliers [216]. Multiprecision [112].

Naccache [210]. nano [7, 236].
nano-CMOS [7]. nano-scale [236].
Neumann [173]. neural [263].
on-profiled [56]. nonce [77]. nonlinear [148]. normalization [60]. novel [259].
NTRUEncrypt [71]. number [180, 122, 77, 227].

operands [209]. operations [148, 227].
Optimal [167, 22, 9]. optimization [238, 215].
optimizations [221]. Optimized [273, 56, 115, 82]. order [142, 83, 203, 252, 275, 39]. organized [121].
overflow [145]. overhead [62]. overview [158].

PAC [136]. pace [173]. pairing [204, 220].
pairing-based [204, 220]. Parallel [276, 202, 221]. Parallelism [266].
parallelizable [196]. Parallelizing [49].
password-based [81]. pay [106].
pay-per-use [106]. PC [218]. PC-based [218]. PCs [105]. pentanomials [216].
Performance [266, 247, 4, 55, 62, 17, 202, 44]. Peter [179].


Xilinx [70, 260, 106]. XOR [206].

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

References

REFERENCES


REFERENCES


Anon:2011:HCc


Anonymous:2011:HCc


Brier:2011:MFA


Brier:2011:MFA

Strenzke:2011:MAS


Hospodar:2011:MLS


Lux:2011:TSD


Anonymous:2011:HCd


Grabher:2012:EMD


Gouvea:2012:ESI


Gueron:2012:ESI


Carlet:2012:AAS


REFERENCES

13


Gerard:2013:UOL Benoît Gérard and François-Xavier Standaert. Unified and optimized linear collision attacks and their apli-

**Fouque:2013:ARC**


**Anonymous:2013:HCa**


**Ali:2013:DFA**


**Montminy:2013:ICD**


**Akinyele:2013:CFR**


**Kurdziel:2013:MPO**


**Anonymous:2013:HCb**


**Mohamed:2013:IAS**

[64] Mohamed Saied Emam Mohamed, Stanislav Bulygin, Michael Zohner, Annelie Heuser, Michael Welter, and Johannes Buchmann. Improved algebraic side-channel attack on AES.
REFERENCES


[Briais:2013:FST]


[Brown:2013:TTC]


[Anonymous:2013:HCc]


[Christofi:2013:FVC]


[Bhasin:2013:CHA]


[Kamal:2013:SHI]


REFERENCES

Anonymous:2014:HCa


Almeida:2014:LPB


Negre:2014:EBP


Carlet:2014:ASC


Biasi:2014:SEC


Paul:2014:DSC


Anonymous:2014:HCb


Moro:2014:FVS

Belaid:2014:TFR

Rauzy:2014:FPC

Kamel:2014:ULI

Tiran:2014:MLF

Anonymous:2014:HCc

Schindler:2014:PAP

Karati:2014:NAB

Clavier:2014:PIS
[95] Christophe Clavier, Jean-Luc Danger, Guillaume Duc, M. Abdelaziz Elaabid, Benoît Gérard, Sylvain Guilley, Annelie Heuser, Michael Kasper, Yang Li, Victor Lommé, Daisuke Nakatsu,

Bos:2014:CTM


Anonymous:2014:HC


Templin:2015:NPA


Banik:2015:IDF


Faz-Hernandez:2015:ESA

Templin:2015:NP

Anon

Anonymous:2014:HC


Anonymous:2014:HC


Faz-Hernández:2015:ESA


OFlynn:2015:SSC


Batina:2015:ICS


Coron:2015:FEP

Jean-Sébastien Coron, Arnab Roy, and Srinivas Vivek. Fast evaluation of

[Sugawara:2015:RSD]


[Genkin:2015:GYH]


[Vliegen:2015:PFE]


[Lerman:2015:MLA]


[Gueron:2015:FPF]


[Guo:2015:SAC]


[Perin:2015:VHC]


REFERENCES


REFERENCES


[139] Ayesha Khalid, Muhammad Hassan,

Moein:2016:HAA


Ghafar:2016:SRV


Carbone:2017:MIA


Guilley:2017:EAP


Idrissi:2017:TCM


Nashimoto:2017:BOA

REFERENCES


Robisson:2017:SSM


Lugou:2017:STU


Azzi:2017:ULC


Sauvage:2017:MLF


Gierlichs:2017:ICS


Yarom:2017:CTA


Ganji:2017:HNM

[152] Fatemeh Ganji, Shahin Tajik, Fabian Fäßler, and Jean-Pierre Seifert. Hav-

**Durvaux:2017:TEL**


**Boss:2017:SBS**


**Bottinelli:2017:CAC**


**Ordas:2017:EFI**


**Swierczynski:2017:IPH**


**Mayhew:2017:OHL**


**Negre:2017:ERM**


[167] Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, Damien Marion, and Olivier Rioul. Optimal side-channel attacks for multivariate leakages and multiple models. *Journal of Cryptographic
REFERENCES


Picek:2017:TAV


Ge:2018:SMT


Chakraborti:2018:TUT


Chakraborty:2018:DED


Chou:2018:MRT


Ferradi:2018:RPN


Fischer:2018:ICS


Chou:2018:MR

[175] Tung Chou. McBits revisited: toward a fast constant-time code-based
REFERENCES


Gross:2018:UMA


Immler:2018:YRC


Hatzivasilis:2018:RLB


Bajard:2018:MRW


Savas:2018:MI


Dai:2018:SAM

REFERENCES

Costello:2018:MCT


Oliveira:2018:MLB


Cenk:2018:KLF


Farias:2018:CSE


Jarvinen:2018:ATA


Lerman:2018:TA


DeVale:2018:ADI


Karmakar:2018:SBS

Skoric:2018:TDS


Dosso:2018:EAC


Hutchinson:2019:CMD


Batina:2019:OTA


Diop:2019:TPH


Saha:2019:IDF


Banik:2019:CCC

Konheim:2019:HFI


Ueno:2019:HEG


Robert:2019:EFB


Unterluggauer:2019:MME


Peccherillo:2019:PBA


Hutter:2019:CTH


Herbert:2019:DIL


Saha:2019:AFE


[212] Claude Carlet, Abderrahman Daif, Sylvain Guilley, and Cédric Tavernier. Polynomial direct sum masking to protect against both SCA and FIA.
REFERENCES

Kawamura:2019:RMR


Saldamli:2019:UMM


Drucker:2019:TSO


Banegas:2019:NCI


Cianfriglia:2019:KAR


Levina:2019:PMS


Wu:2019:FUE

[219] Tao Wu and Ruomei Wang. Fast unified elliptic curve point multiplication for NIST prime curves on FP-


REFERENCES


Heydemann:2021:EAP


Ganji:2021:RPC


Cheng:2021:DFI


Perianin:2021:EEA


Keren:2021:IRC


Ueno:2021:MCS


Kamel:2021:SCA

REFERENCES


REFERENCES


[268] Thomas Trouchkine, Sébanjila Kevin Bukasa, Mathieu Escoufleou, Ronan Lashermes, and Guillaume Boffard. Electromagnetic fault injec-

**Mittmann:2021:TAL**


**Bajard:2021:MFP**


**Lombardia:2021:SSL**


**Caforio:2022:MSV**


**Ouladj:2022:SAP**

to process the (multivariate) high-
order template attack against any
masking scheme. *Journal of Crypto-
graphic Engineering*, 12(1):75–93, April
2022. CODEN ????. ISSN 2190-
8508 (print), 2190-8516 (electronic).
URL https://link.springer.com/
article/10.1007/s13389-020-00253-
4.

[Buhrow:2022:PMM]

[276] Benjamin Buhrow, Barry Gilbert, and
Clifton Haider. Parallel modular mul-
tiplication using 512-bit advanced vec-
tor instructions. *Journal of Crypto-
graphic Engineering*, 12(1):95–105, April
2022. CODEN ????. ISSN 2190-
8508 (print), 2190-8516 (electronic).
URL https://link.springer.com/
article/10.1007/s13389-021-00256-
9.

[Nath:2022:SET]

[277] Kaushik Nath and Palash Sarkar. Secu-
rity and efficiency trade-offs for elliptic
curve Diffie–Hellman at the 128-bit and
224-bit security levels. *Journal of Cryp-
tographic Engineering*, 12(1):107–121,
April 2022. CODEN ????. ISSN 2190-
8508 (print), 2190-8516 (electronic).
URL https://link.springer.com/
article/10.1007/s13389-021-00261-
y.