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: https://www.math.utah.edu/~beebe/

08 August 2024  
Version 1.26

**Title word cross-reference**

256 [108]. 384 [77]. 64 [130]. 8 [154]. GF($2^m$) [305]. $F_2[X]$ [301]. $N = p^2q$ [141]. $P$ [313, 319]. $t$ [272]. $r$ [187]. $GF(2^8)$ [199]. $x$ [246]. $Z$ [48, 13].


3 [344]. 512-bit [276]. 64 [312]. 65nm [327].

algebraic [32, 283, 140, 64, 243].
Algorithm [5, 161, 333, 209, 22, 198, 357, 269, 315, 38].
awakener [329]. aware [98].
C [319]. cache [261, 251, 350, 253].
cache-timing [251]. CacheBleed [151].
caches [261]. calculus [272]. can [144].
cannot [177]. card [121, 343]. card-based [343].
cards [72]. carry [130, 16].
carry-less [130, 16]. case [317, 337, 85, 319].
chaos-based [349]. characteristic [289].
Charm [61]. CHES [102, 74, 174, 150, 124, 52]. chip [23].
cipher [88, 129]. ciphers [164, 211, 178, 190, 260].
information [130]. Having [152]. HC [85].


Horst [198]. HPC [238]. HPC-based [238]. hybrid [303, 199].


Internal [196, 101]. Internet [211, 279].


ladder [5, 184]. ladder-based [5]. lambda [75]. laptop [105]. large [78, 260, 206].


leak [258, 253]. Leakage [125, 342, 88, 83, 11, 153, 134, 218, 91].


learning [229, 278, 136, 228, 26, 254, 318, 325, 107, 188, 307, 251, 225].

learning-based [318]. length [353, 171].

less [249, 130, 16]. level [208, 76, 5, 158, 149, 104]. library [202]. licensing [106]. lighter
Machine [26, 278, 228, 357, 107, 188, 251]. machines [119]. maintaining [111].


mechanism [261, 134, 327, 332]. mechanisms [29]. Melting [274].


Modulus [20]. moments [142].

Montgomery [180, 270, 183, 182, 5, 57, 213, 354, 184, 179, 214, 181].


multi-fault [308]. Multi-level [149].

multi-task [307]. multidimensional [193].

multiparty [78]. multiple [167, 312, 145].

multiplication [276, 118, 182, 209, 192, 100, 57, 13, 112, 269, 305, 82, 231, 200, 301, 358, 16, 219, 289].

multiplications [48, 130, 330].

multiplicative [159, 200]. multiplier [209, 37, 214]. multipliers [216].

Multiprecision [112]. multivariate [167, 310, 241, 275]. Mutual [142]. my [105].

Naccache [210]. nano [7, 236].

nano-CMOS [7]. nano-scale [236].


network [263]. networks [30]. Neumann [173].


non [221, 56, 325]. non-interference [221].

non-profiled [56, 325]. nonce [77].

nonlinear [148]. nonparametric [349]. nor [357].

normalization [60]. NORX [295].

novel [286, 259]. NTRUEncrypt [71]. NTT [358].

NTT-based [358]. number [180, 122, 77, 286, 227, 348].


ones [249]. Online [194]. only [246].

OpenSSL [151]. operands [209].

operations [148, 227, 345]. Optimal


REFERENCES

Koc:2011:IBC


Kocher:2011:IDP

Paul Kocher, Joshua Jaffe, Benjamin

REFERENCES

10


Molter:2011:SPA


Guneysu:2011:UHC


Dominguez-Oviedo:2011:ALE


Skorobogatov:2011:SMS


Hocquet:2011:HPN


Anonymous:2011:HCa


Moreno:2011:SRB

REFERENCES


REFERENCES


Hospodar:2011:MLS


Lux:2011:TSD


Anonymous:2011:HCd


Grabher:2012:EMD


Gouvêa:2012:ESI


Gueron:2012:ESI


Carlet:2012:AAS


Elaabid:2012:PT
REFERENCES


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

Kasper:2012:SCB


Mather:2012:PSC


Trujillo-Olaya:2012:APV


Shariati:2012:AEE


Anonymous:2012:HCC


Rolt:2012:SAS


Baldwin:2012:CES


Gueron:2012:PMS

[49] Shay Gueron and Vlad Krasnov. Parallelizing message schedules to accel-
REFERENCES


[72] Jean-Luc Danger, Sylvain Guilley, Philippe Hoogvorst, Cédric Murdica,
REFERENCES

19


Anonymous:2013:HCd


Bertoni:2014:ICS


Oliveira:2014:TFP


Becker:2014:SDL


DeMulder:2014:UBS


Grosso:2014:MVM


Sugawara:2014:MSC


REFERENCES

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 Elaïbid, Benoît Gérard, Sylvain Guilley, Annelie Heuser, Michael Kasper, Yang Li, Victor Lonné, Daisuke Nakatsu,

Bos:2014:CTM


Anonymous:2014:HC


Templin:2015:NPA


Banik:2015:IDF


OFlynn:2015:SSC


Batina:2015:ICS


Coron:2015:FEP

[103] 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]


Robisson:2016:PFC


Galindo:2016:ILR


Ngo:2016:MTA


Ganji:2016:PLA


Ganji:2016:PLA


Bos:2016:SEC


Khalid:2016:RRP

[139] Ayesha Khalid, Muhammad Hassan,
REFERENCES


Moën: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-
no mathematical model may not secure PUFs. *Journal of Cryptographic Engineering*, 7(2):113--128, June 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).


REFERENCES


REFERENCES


Picek:2017:TAV


Ge:2018:SMT


Chakraborti:2018:TUT


Chakraborty:2018:DED


Ferradi:2018:RPN


Fischer:2018:ICS


Chou:2018:MR


Chou:2018:MRT

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

Gross:2018:UMA


Immler:2018:YRC


Hatzivasilis:2018:RLB


Rodriguez-Henriquez:2018:SIH


Bajard:2018:MRW


Savas:2018:MI


Dai:2018:SAM


Skoric:2018:TDS


Dosso:2018:EAC


Hutchinson:2019:CMD


Batina:2019:OTA


Diop:2019:TPH


Saha:2019:IDF


Banik:2019:CCC

REFERENCES


[Wisiol:2019:WAL](#)


[BenElOuahma:2019:SCR](#)


[Baumann:2019:VSL](#)


[Das:2019:AGH](#)


[Geraud:2019:MRN](#)


[Dinu:2019:TLB](#)


[Carlet:2019:PDS](#)

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


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


REFERENCES (print), 2190-8516 (electronic). URL

**Didier:2020:EMO**


**Hettwer:2020:AML**


**Benadjila:2020:DLS**


**Orumiehchiha:2020:DFA**


**Piccoli:2020:PMB**


**Cruz:2020:ESS**


**Hiller:2020:REC**

REFERENCES


REFERENCES


Ouladj:2020:PTA


Baksi:2020:IIC


Yeo:2021:IAA


Resende:2021:FUP


Bronchain:2021:RRT


Pereira:2021:OPA


Abarzua:2021:SPS

REFERENCES


REFERENCES


Heydemann:2021:CEA


Chang:2021:ASI


Shiozaki:2021:SEA


Zhang:2021:NTG


Gu:2021:LSC


Bandara:2021:ACD

REFERENCES


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

Mittmann:2021:TAL


Bajard:2021:MFP


Lombardia:2021:SSL


Molteni:2022:RCR


Bozilov:2022:OTI


Caforio:2022:MSV


Ouladj:2022:SAP

Maamar Ouladj, Sylvain Guilley, and Farid Mokrane. Spectral approach


REFERENCES


REFERENCES

Chavez-Saab:2022:SCS


Chang:2022:ASI


Saarinen:2022:DRV


Rührmair:2022:SFS


Jin:2022:PAC


Jana:2022:DFA


Fustos:2022:FLS


References

Adj:2023:KBS


Werner:2023:EEA


Masure:2023:SCA


Nadikuda:2023:LAT


Peng:2023:SNP


Koshelev:2023:SMT


Debnath:2023:MIM

Joshi:2023:SSP


Cui:2023:CEL


Luengo:2023:STS


Koseki:2023:HES


Salam:2023:DFA


LeGrow:2023:FMF


Alves:2023:PHT


[324] Aurélien Vasselle, Hugues Thiebeauld, and Philippe Maurine. Spatial dependency analysis to extract information
REFERENCES


Kuroda:2023:PAN


Kuroda:2023:SCA


Lhumba:2023:SAA


Komissarov:2023:SAA


Krachenfels:2023:TAD


Oberhansl:2024:UIS


[331]
Kumar:2024:RNC


Ribeiro:2024:SPQ


Cai:2024:ENA


Shao:2024:DSV


Marchiori:2024:PRF


Gurler:2024:CGL


Joshi:2024:DRK

[337] Priyanka Joshi and Bodhisatwa Mazumdar. Deep round key recovery attacks and countermeasure in persistent fault model: a case study on GIFT and KLEIN. *Journal of Cryptographic Engineering*, 14(1):103–125, April 2024. CODEN ???? ISSN 2190-


[352] Muayad J. Aljafar, Florence Azais, Marie-Lise Flottes, and Samuel Pagliarini. Utilizing layout effects for analog...

**Alshaer:2024:CLA**


**Kim:2024:MCA**


**Jana:2024:DFA**


**Hu:2024:UGE**


**Lashermes:2024:GSR**


**Salarifard:2024:EHA**