Title word cross-reference

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

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

128 [85].

2.0 [99]. 2012 [52]. 2013 [74]. 2014 [102].
2nd [95].

authenticated [170]. authentication [50, 119]. Automated [119]. automatic
based [81, 122, 84, 117, 175, 5, 100, 114, 55, 139, 82, 110, 45, 38]. bases [17]. batch [94].
binary [161, 113, 118, 103, 9, 82, 75, 16, 38].
bit [154, 77, 108, 130, 54]. black [22].

building [42].
CacheBleed [151]. can [144]. cannot [177]. card [121]. cards [72]. carry [130, 16].
constant-time [175, 151]. Contacts [8, 14, 21, 28, 35, 41, 46, 51, 58, 63, 68, 73, 97, 80, 86, 92]. contemporary [169].
contest [95]. coordinates [75].
cross-device [60]. CRT [20, 65, 57, 89, 160].
cryptanalysis [129, 18]. cryptanalytic [123]. Cryptographic [1, 10, 70, 29, 162].
cryptography [70, 113, 137, 72, 30, 108, 4, 55, 7].
data [85]. data-widths [85].
decomposition [116]. DECT [129].
Designing [85]. designs [147]. detect [135].
detection [5, 109, 27]. device [121, 50, 60].
do [171]. domain [91]. dopant [76, 104].
dopant-level [76, 104]. DPA [95, 114, 91].
drive [157]. dual [177]. dual-rail [177].
dynamic [29].
easy [153]. ECC [48]. ECDSA [77, 94].
ECHO [10]. ECEM [5]. Editorial [143].
Edwards [166]. efficacy [142]. efficiency [137, 142]. Efficient [100, 30, 31, 82, 159, 162, 84, 154].
Euclidean [161]. evaluation [103, 45, 106, 12, 111]. evaluations [90].
Exclusive [126]. execution [9].
experimental [45]. exploration [29].
exponent [93, 126, 160]. exponentiation [31, 9, 159, 38].
exponentiations [110]. extended

mechanisms [29]. memory [81, 62].
Method [135, 22, 6, 111]. methodology [125]. metric [117, 98]. MICKEY [99].
microcontroller [169].
microcontroller [30]. Minimizing [62].
miplaced [144]. model [122, 114, 152, 91].
MSP430X [30]. Multi [39, 149, 38].
Multi-exponentiation [38]. Multi-level [149]. multiparty [78]. multiple [167, 145].
multiplication [118, 100, 57, 13, 112, 82, 16].
my [105].
nano [7]. nano-CMOS [7]. nanometer [117]. need [171]. networks [30].
Neumann [173]. Niederreiter [24, 34, 55].
nm [7]. no [152]. non [56]. non-profiled [56]. nonce [77]. nonlinear [148].
normalization [60]. NTRUEncrypt [71].
number [122, 77].

oblivious [54]. off [105]. on-chip [23].
OpenSSL [151]. operations [148].
oscillators [101]. outputting [69].
overflow [145]. overhead [62]. overview [158].
PAC [136]. pace [173]. Parallelizing [49].
Party [39]. passive [7]. password [81].
password-based [81]. pay [106].
pay-per-use [106]. PCs [105].
performance [4, 55, 62, 17, 44]. photonic [53].
Physical [133, 66, 105, 54].
Pinpointing [43]. platforms [84]. polynomial [118, 82]. polynomials [103].
Portability [33]. potential [7]. Power [93, 155, 22, 2, 158, 3, 132, 160, 98].
power-aware [98]. Practical [95, 18, 106, 50, 54]. practice [157].
predictors [164]. presence [93]. preserve [171]. prevent [126]. PRFs [88].
prime [108, 75]. primes [108]. primitives [79].
proof [89]. PROOFS [143, 163].
properties [25]. protect [117, 166].
Protecting [40, 70]. protocols [119, 39, 54].
prototyping [61, 139]. provably [166].
proved [132]. proven [145]. public [24, 34, 141, 30, 47, 25].
public-key [24, 34, 30, 47]. PUF [69, 111]. PUFs [136, 152, 15, 50, 127, 45].

QUAD [115].

Rabin [141]. rail [177]. rails [177].
realizations [44]. reconfigurable [55, 15].
reconstruction [82]. recovery [101].
Recyclable [15]. regular [159].
Regulating [173]. relevance [90].
reliability [111]. resilient [88, 134].
resistant [165, 9, 47]. respect [165].
responses [69, 111]. results [118, 121, 160].
Reversing [104]. review [178]. revisited [175, 112]. RFID [7]. ring [122, 128].
ring-LWE [128]. RNS [110]. RNS-based [110].
RS [69]. RSA [20, 65, 57, 89, 126, 160, 151]. RunFein [139].
sampling [101]. Sboxes [154]. SCA [6].
scalable [85]. Scalar [13, 48, 100, 16].
Scaling [84]. Scan [47]. schedules [49].
scheme [50, 106]. schemes [165, 170].
search [22]. section [163]. Secure [127, 170, 100, 152, 146, 39]. Security
REFERENCES


Synchronization [6]. Synchronous [101]. synthesis [72]. systems [48].


tool [27]. toolchain [147]. transfer [54].


Tweaking [55]. Two [75, 66, 170].

ultra [7]. ultra-low-voltage [7].

unclonable [54]. unconventional [17].

Understanding [90]. Unified [56, 10, 176, 147]. unit [60]. unit-variance


Utilizing [4]. uTriviA [170].

validation [117]. variance [116, 60].

variant [141]. Variety [69, 111].

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

version [76, 154, 77, 153, 100, 56, 177, 127].

versus [168, 44]. Vertical [110]. voltage [7]. vs [78]. vulnerabilities [161].

weak [19]. web [43]. Weierstraß [13].

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

Xilinx [70, 106].

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

References


Molter:2011:SPA


Guneysu:2011:UHC


Dominguez-Oviedo:2011:ALE


Skorobogatov:2011:SMS


Hocquet:2011:HPN


Anonymous:2011:HCa


Moreno:2011:SRB


Beuchat:2011:LAU

REFERENCES


REFERENCES

Avanzi:2012:ESC


Anonymous:2012:HCa


Bernstein:2012:HSH


Hasan:2012:SMS


Yen:2012:MEA


Roche:2012:HOG


Bringer:2012:PAA


Anonymous:2012:HCb


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

Koeberl:2012:PDA


Anon:2012:HCd


Prouff:2013:ICS


Schlosser:2013:SPE


Ruhrmair:2013:PUP


Heyse:2013:CBC


Gerard:2013:UOL


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

**Anonymous:2013:HCd**


**Bertoni:2014:ICS**


**Oliveira:2014:TFP**


**Becker:2014:SDL**


**DeMulder:2014:UBS**


**Grosso:2014:MVM**


**Sugawara:2014:MSC**


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 Lonné, Daisuke Nakatsu,


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


REFERENCES

Yamamoto:2015:NME


Hamlet:2015:TOI


Lerman:2015:BVD


Bongiovanni:2015:DVT


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


[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**

Aldaya:2017:SVB


Pasalic:2017:EIG


Homma:2017:IPS


Bhattacharya:2017:FFA


Breier:2017:SAS


Dugardin:2017:UME


Bruneau:2017:OSC


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


