Documents

Export Date: 19 Nov 2019

Search: SRCTITLE(6th International Cryptology and Information Securi...

1) Sarbini, I.N.B., Jin, W.T., Feng, K.L., Othman, M., Said, M.R.M., Hung, Y.P.
Garbage-man-in-The-middle (type 2) attack on the lucas based el-gamal cryptosystem in the elliptic curve group over finite Field
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 35-41.

1) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054554349&partnerID=40&md5=ff9c470e262da8c5036935cb210dae4
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

2) Kamarulhaili, H.
Welcoming notes
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. v-vi.

2) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054553762&partnerID=40&md5=c0058823393574930 8fd67149e8212
Document Type: Editorial
Publication Stage: Final
Source: Scopus

3) Antony, S.N.F.M.A., Kamarulhaili, H.
Construction of endomorphisms with j-invariant 1728 for ISD method
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 26-34.

3) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054548185&partnerID=40&md5=27783d367af77132b57f1195b437fa7
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

4) Abu, N.A., Latip, S.F.A., Sahib, S.
Evaluation criteria on random ambience for cryptographic keys
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 160-175.

4) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054545251&partnerID=40&md5=a46cd071a33b8f5066c7578bd8a1a5
Document Type: Conference Paper

Publication Stage: Final
Source: Scopus

5) Ir, T., Bin, S.N.
Opening remarks
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. iii-iv.

5) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054544661&partnerID=40&md5=e2e0a09d04aa378a9de884eaf61359
Document Type: Editorial
Publication Stage: Final
Source: Scopus

6) Ghafar, A.H.A., Ariffin, M.R.K., Asbullah, M.A.
Extending pollard class of factorable RSA modulus
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 103-118. Cited 2 times.

6) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054544143&partnerID=40&md5=d1fba64f900e22e487283416d9913db
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

7) Loh, J.-C., Heng, S.-H., Tan, S.-Y.
Revisiting the invisibility of yuen et al.'s undeniable signature scheme
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 76-84.

7) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054542882&partnerID=40&md5=9997d789161e14d1749dedb7b26d60
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

8) Goey, J.-Z., Goi, B.-M., Lee, W.-K., Phan, R.C-W.
Accelerating DGHV's fully homomorphic encryptionwith GPU
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 151-159.

8) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054540705&partnerID=40&md5=89375e76b022934504ec353f0aeaae
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

9) Vangujar, A.K., Chin, J.-J., Tan, S.-Y., Ng, T.-S.
Hierarchical twin-schnorr identity-based identification scheme
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 64-75.

9) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054540519&partnerID=40&md5=114d00588ab141265cc23a7ebc58ad
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

10) Jamil, N., Qassim, Q., Daud, M., Abidin, I.Z., Jaaffar, N., Kamarulzaman, W.A.W.
A practical SCADA testbed in electrical power system environment for cyber-security exercises
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 176-188.

10) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054529092&partnerID=40&md5=c70d96d62988828665f89f214cc0856
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

Editorial preface
11) (2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. vii-viii.

11) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054528055&partnerID=40&md5=ba2b7d58dc828137d75bc5dfc621de
Document Type: Editorial
Publication Stage: Final
Source: Scopus

12) Mandangan, A., Kamarulhaili, H., Asbullah, M.A.
On the underlying hard lattice problems of GGH encryption scheme
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 42-50.

12) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054525635&partnerID=40&md5=35c1fdfaf2e2ed373e65f8d7fc21b197
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

13) Ramchen, K.
Detecting general algebraic manipulation attacks
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 51-63.

13) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054523835&partnerID=40&md5=deb69f9dbe232ccabef9a848a9a9c48

Document Type: Conference Paper

Publication Stage: Final

Source: Scopus

Proceedings of the 6th International Cryptology and Information Security Conference 2018, CRYPTOLOGY 2018

14) (2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, 201 p.

14) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054520595&partnerID=40&md5=1d51cf1bd7712793c8d1fca7580b975

Document Type: Conference Review

Publication Stage: Final

Source: Scopus

15) Abubakar, S.I., Ariffin, M.R.K., Asbullah, M.A.

A new simultaneous diophantine attack upon RSA moduli N = pq

(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 119-138. Cited 2 times.

15) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054510729&partnerID=40&md5=ef802665b23e80a1b0cc1e9461b45e

Document Type: Conference Paper

Publication Stage: Final

Source: Scopus

16) Mohamad, M.S., Tan, S.-Y., Chin, J.-J.

Searchable symmetric encryption: Defining strength against query recovery attacks

(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 85-93.

16) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054509633&partnerID=40&md5=87e69a0216027c3791e381d2d8234

Document Type: Conference Paper

Publication Stage: Final

Source: Scopus

17) Rahman, N.N.A., Ariffin, M.R.K., Asbullah, M.A., Yunos, F.

New vulnerability on system of Ni = p2iqi using good approximation of Φ(N)

(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 139-150. Cited 3 times.

17) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054509313&partnerID=40&md5=466ed0404e1cbfe3290ebe51d3f19c2

Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

18) Balfaqih, A., Kamarulhaili, H.
On the unsolvability of the diophantine equation xa11 + xa22 ++ xamm = nyb and Its cryptographic consequences
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 12-18.

18) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054509165&partnerID=40&md5=14c32601d2b47824df1fcb7472ddcfc
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

19) Muslim, N., Said, M.R.M.
Elliptic net scalar multiplication using generalized equivalent elliptic divisibility sequence
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 19-25.

19) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054508929&partnerID=40&md5=c32a246768c2042dc5c77179a2d0f7c
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

20) Asbullah, M.A., Ariffin, M.R.K., Mahad, Z.
Enhanced AAβ cryptosystem: The design
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 94-102.

20) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054508827&partnerID=40&md5=24fb6b1cb3105a54daf3bec106a04a6
Document Type: Conference Paper
Publication Stage: Final
Source: Scopus

21) Yassein, H.R., Al-Saidi, N.M.G.
BCTRU: A new secure NTRUCrypt public key system based on a newly multidimensional algebra
(2018) Proceedings of the 6th International Cryptology and Information Security Conference 2018,

CRYPTOLOGY 2018, pp. 1-11.

21) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054473710&partnerID=40&md5=4644f5a2fa21faafd3eef380d7d4f72e
Document Type: Conference Paper

Publication Stage: Final

Source: Scopus

Search: SRCTITLE(6th International Cryptology and Information Security Conference 2018)