Garbage-man-in-The-middle (type 2) attack on the lucas based el-gamal cryptosystem in the elliptic curve group over finite Field  
CRYPTOLOGY 2018, pp. 35-41.

2) Kamarulhaili, H.  
Welcoming notes  
CRYPTOLOGY 2018, pp. v-vi.

3) Antony, S.N.F.M.A., Kamarulhaili, H.  
Construction of endomorphisms with j-invariant 1728 for ISD method  
CRYPTOLOGY 2018, pp. 26-34.

4) Abu, N.A., Latip, S.F.A., Sahib, S.  
Evaluation criteria on random ambience for cryptographic keys  
CRYPTOLOGY 2018, pp. 160-175.
5) Ir, T., Bin, S.N.

Opening remarks

5) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054544661&partnerID=40&md5=e2e0a09d04aa378a9de884eaf61359f

Document Type: Editorial
Publication Stage: Final
Source: Scopus


Extending pollard class of factorable RSA modulus

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

7) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054542882&partnerID=40&md5=9997d789161e14d1749dedb7b26d6c

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 encryption with GPU

8) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054540705&partnerID=40&md5=89375e76b022934504ec353f0aeaae7

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
CRYPTOLOGY 2018, pp. 64-75.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054540519&partnerID=40&md5=114d00588ab141265cc23a7ebc58ad7

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
CRYPTOLOGY 2018, pp. 176-188.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054529092&partnerID=40&md5=c70d96d62988828665f89f214cc0856d

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

Editorial preface

CRYPTOLOGY 2018, pp. vii-viii.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054528055&partnerID=40&md5=ba2b7d58dc828137d75bc5dfc621de8b

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

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054525635&partnerID=40&md5=35c1dfaf2e2ed373e65f8d7fc21b197

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

13) Ramchen, K.
Detecting general algebraic manipulation attacks
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) 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


*A new simultaneous diophantine attack upon RSA moduli N = pq*


15) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054510729&partnerID=40&md5=ef802665b23e80a1b0cc1e9461b45ee

**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*


16) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054509633&partnerID=40&md5=87e69a0216027c3791e381d282343

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


*New vulnerability on system of Ni = p2qi using good approximation of \( \Phi(N) \)*


18) Balfaqih, A., Kamarulhaili, H.

*On the unsolvability of the diophantine equation* $x_{a1}^1 + x_{a2}^2 + \ldots + x_{am}^m = ny^b$ *and Its cryptographic consequences*


https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054509165&partnerID=40&md5=14c32601d2b47824df1fcb7472ddcfc

19) Muslim, N., Said, M.R.M.

*Elliptic net scalar multiplication using generalized equivalent elliptic divisibility sequence*


https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054508929&partnerID=40&md5=c32a246768c2042dc5c77179a2d0f7d

20) Asbullah, M.A., Ariffin, M.R.K., Mahad, Z.

*Enhanced AAβ cryptosystem: The design*


https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054508827&partnerID=40&md5=24fb6b1cb3105a54da3bec106a04a6

21) Yassein, H.R., Al-Saidi, N.M.G.

*BCTRU: A new secure NTRUCrypt public key system based on a newly multidimensional algebra*


https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054473710&partnerID=40&md5=4644f5a2fa21faaf3eeef380d7df72e
Publication Stage: Final
Source: Scopus