Unvollständige Sammlung diverser Link im Kontext zu Verschlüsselung, Zufallsgeneratoren und kryptografische Verfahren

1. http://www.golem.de/news/elliptische-kurven-die-herkunft-der-nist-kurven-1309-101567.html
2. http://www.golem.de/news/zufallszahlen-taiwanische-buergerzertifikate-geknackt-1309-101631.html
3. http://www.golem.de/news/verschluesselung-was-noch-sicher-ist-1309-101457.html
4. http://www.golem.de/news/imho-keine-krypto-vom-staat-1309-101538.html
5. http://www.golem.de/news/linux-kernel-bessere-zufallszahlen-selbst-mit-nsa-backdoor-1309-101525.html
6. http://www.golem.de/news/verschluesselung-nist-raet-von-dual-ec-drbg-wegen-moeglicher-nsa-backdoor-ab-1309-101521.html
7. http://www.welt.de/wirtschaft/article119782731/Wie-die-NSA-Verschluesselungen-knackt.html
8. http://www.golem.de/print.php?a=101457
9. http://www.golem.de/news/cryptocat-verschluesseltes-chatsystem-gebrochen-1307-100204.html
10. http://www.heise.de/newsticker/meldung/NIST-laesst-Zufalls-Generatoren-neu-pruefen-1954677.html
11. http://www.golem.de/news/gstool-bsi-bedroht-sicherheitsforscher-1309-101531.html
12. http://www.golem.de/news/bitcoin-unsichere-virtuelle-geldboersen-unter-android-1308-100914.html
13. http://www.golem.de/news/openssl-fork-und-der-zufall-1308-101170.html
14. http://www.golem.de/news/fehler-im-zufallsgenerator-netbsd-erzeugt-schwache-schluessel-1303-98350.html
15. http://www.heise.de/newsticker/meldung/PHP-stuempert-bei-Zufallszahlen-967062.html
16. http://www.heise.de/security/meldung/RSA-Schluessel-zertifizierter-Smartcards-geknackt-1959704.html
17. http://www.heise.de/security/meldung/Schwache-Schluessel-bei-NetBSD-1829052.html
18. http://www.heise.de/security/meldung/Mathematiker-entlarvt-schwache-DKIM-Schluessel-1736107.html
19. http://www.heise.de/security/meldung/MIPS-Router-mit-Entropieproblemen-1953097.html
20. http://www.heise.de/security/meldung/OpenSSL-erzeugt-zu-oft-den-gleichen-Zufall-1942299.html
21. http://www.heise.de/security/meldung/Androids-Verschluesselung-angreifbar-1936181.html
22. http://www.heise.de/security/meldung/RSA-warnt-vor-Schwachstelle-in-eigenem-Tool-1962442.html
23. http://www.heise.de/security/meldung/Forscher-beschreiben-Chip-Sabotage-ab-Werk-1961412.html
24. http://www.amazon.de/Pseudozufallszahlen-Kryptographie-Christian-Schiestl/dp/3832441492
25. http://www.heise.de/newsticker/meldung/Schwaechen-im-Zufallszahlengenerator-von-Windows-2000-195089.html

26. http://www.heise.de/newsticker/meldung/Verschluesselungsstandard-unter-Backdoor-Verdacht-196659.html
27. http://www.heise.de/newsticker/meldung/Zu-wenig-Zufall-im-Zufallszahlengenerator-von-OpenBSD-178124.html
28. http://www.heise.de/newsticker/meldung/Apache-Tool-erzeugt-Passwort-Hashes-mit-vorhersagbaren-Salts-180864.html
29. http://www.heise.de/security/artikel/Gute-Zahlen-schlechte-Zahlen-270078.html
30. http://www.heise.de/security/artikel/Im-Zugzwang-270080.html
31. www.springerlink.com/index/73wv01812724286j.pdf
32. http://www.heise.de/security/artikel/Todesurteil-fuer-Verschluesselung-in-den-USA-1972561.html
33. http://www.golem.de/news/security-mehrere-sicherheitsluecken-in-drupal-entdeckt-1312-103108.html
34. http://www.heise.de/newsticker/meldung/Kryptographie-nach-Snowden-Die-Mathematik-ist-unser-Freund-2059964.html
35. http://www.heise.de/tr/artikel/Die-Krypto-Strategie-der-NSA-ist-keine-Ueberraschung-1955013.html
36. http://www.heise.de/security/meldung/NSA-Affaere-Generatoren-fuer-Zufallszahlen-unter-der-Lupe-1953716.html
37. http://www.golem.de/news/freebsd-misstrauen-bei-rngs-von-intel-und-via-1312-103305.html
38. http://www.golem.de/news/bsafe-rsa-security-warnt-vor-nsa-zufallsgenerator-1309-101727.html
39. http://www.heise.de/newsticker/meldung/NSA-zahlte-10-Millionen-US-Dollar-fuer-Krypto-Backdoor-2071567.html
40. http://www.heise.de/newsticker/meldung/OpenSSL-mit-kaputter-Hintertuer-2072370.html
41. http://www.heise.de/newsticker/meldung/OpenSSL-erzeugt-zu-oft-den-gleichen-Zufall-1942299.html
42. http://www.heise.de/newsticker/meldung/MIPS-Router-mit-Entropieproblemen-1953097.html
43. http://www.heise.de/newsticker/meldung/Androids-Verschluesselung-angreifbar-1936181.html
44. http://www.golem.de/news/verschluesselung-2013-das-jahr-der-kryptokalypse-1312-103617.html
45. http://www.heise.de/newsticker/meldung/Windows-Verschluesselung-offen-fuer-US-Geheimdienst-15925.html
46. http://www.heise.de/newsticker/meldung/Debatte-um-NSAKey-geht-weiter-16037.html
47. http://www.heise.de/newsticker/meldung/Penetrating-Hard-Targets-NSA-arbeitet-an-Quantencomputern-zur-Kryptoanlayse-2074540.html
48. http://www.heise.de/security/meldung/Mehr-Details-zur-Hintertuer-im-Zufallszahlengenerator-Dual-EC-DRBG-2159523.html
49. http://www.heise.de/security/meldung/OpenSSL-mit-kaputter-Hintertuer-2072370.html
50. http://www.spiegel.de/netzwelt/web/steelwinter-supercomputer-norwegens-geheimdienst-kooperiert-mit-nsa-a-966541.html
51. http://www.spiegel.de/netzwelt/web/warum-die-nsa-quantencomputer-will-a-941683.html
52. http://www.golem.de/news/ex-nsa-chef-alexander-unsere-aufgabe-ist-es-code-zu-knacken-1405-106375.html
53. http://www.golem.de/news/dual-ec-das-patent-auf-die-nsa-hintertuer-1406-107219.html
54. http://www.heise.de/newsticker/meldung/4-Bremer-IT-Sicherheitstag-Angriffserkennung-und-Angriffsbehandlung-2250020.html

55. http://www.golem.de/news/fork-libressl-hat-zufallsprobleme-unter-linux-1407-107911.html
56. http://www.golem.de/news/dan-kaminsky-sichere-zufallszahlen-zum-standard-machen-1408-108469.html
57. http://www.heise.de/newsticker/meldung/Linux-3-17-wird-Zufallszahlen-zuverlaessiger-liefern-2293032.html
58. http://deutsche-wirtschafts-nachrichten.de/2014/09/05/google-holt-sich-experten-fuer-quanten-computer/
59. http://www.heise.de/newsticker/meldung/BND-will-SSL-geschuetzte-Verbindungen-abhoeren-2444901.html
60. http://www.linux-magazin.de/NEWS/Gute-Crypto-schlechte-Crypto-in-srand
61. http://www.heise.de/newsticker/meldung/31C3-Die-Angriffe-auf-Verschluesselung-durch-NSA-und-GCHQ-2507004.html
62. http://www.golem.de/news/dual-ec-drbg-die-fehler-des-nist-1501-111534.html
63. http://www.heise.de/ix/artikel/Tohuwabohu-905336.html
64. http://www.linux-magazin.de/Blogs/Insecurity-Bulletin/Ruby-Identische-Seeds-fuer-den-Pseudo-Zufallszahlen-Generator
65. http://www.heise.de/tp/artikel/44/44820/1.html
66. http://www.heise.de/newsticker/meldung/Logjam-Attacke-Verschluesselung-von-zehntausenden-Servern-gefaehrdet-2657502.html
67. http://www.heise.de/newsticker/meldung/Cisco-Gateways-durch-Standard-SSH-Schluessel-angreifbar-2730383.html
68. http://www.heise.de/newsticker/meldung/NIST-beerdigt-umstrittenen-Zufallszahlengenerator-Dual-EC-DRBG-2731747.html
69. http://iso-blog.anracom.com/2013/10/it-sicherheit-und-zufallszahlengeneratoren-i/
70. http://www.google.de/imgres?imgurl=http%3A%2F%2Fwww.golem.de%2F1308%2F101170-63578-i_rc.jpg&imgrefurl=http%3A%2F%2Fwww.golem.de%2Fnews%2Fopenssl-fork-und-der-zufall-1308-101170.html&h=234&w=416&tbnid=BI_MtGF5sBwYXM%3A&zoom=1&docid=T2lF2Uw-8XW2-M&ei=zImeVbKYBYjvywOIsYXwCg&tbm=isch&iact=rc&uact=3&dur=4918&page=3&start=91&ndsp=55&ved=0CCkQrQMwDDhk
71. https://anonymous-proxy-servers.net/wiki/index.php/Ver%C3%B6ffentlichungen_zu_Kryptografie
72. http://www.zeit.de/2012/19/N-zufaellige-Zahlenreihen
73. http://www.golem.de/news/bsi-lagebericht-2015-bund-plant-kein-programm-gegen-it-angriffe-von-terroristen-1511-117529.html
74. http://www.heise.de/newsticker/meldung/JavaScript-Engine-V8-Vorsicht-vor-Math-random-3010353.html
75. http://www.golem.de/news/verschluesselung-punkte-auf-der-falschen-elliptischen-kurve-1511-117643.html
76. http://www.heise.de/newsticker/meldung/House-of-Keys-Millionen-von-Geraeten-mit-kompromittierten-Krypto-Schluesseln-im-Netz-3025416.html
77. http://www.spiegel.de/netzwelt/web/quantenkryptografie-forscher-knacken-datenverschluesselung-a-1068698.html
78. http://www.tecchannel.de/sicherheit/management/1747288/ueber_zufallszahlen_verschluesselung_hintertueren_vista_und_das_nsa/index3.html
79. http://www.golem.de/news/openssl-luecke-die-sache-mit-den-sicheren-primzahlen-1601-118812.html
80. http://www.heise.de/newsticker/meldung/BSI-Audit-OpenSSL-ohne-grosse-Schwachstellen-aber-mit-Entropie-Problemen-3097632.html

81. http://www.heise.de/newsticker/meldung/18-Jahre-lang-vorhersehbare-Zufallszahlen-bei-GnuPG-3300159.html
82. http://www.golem.de/news/dsa-diffie-hellman-primzahlen-koennen-hintertuer-enthalten-1610-123778.html
83. http://www.elektroniknet.de/halbleiter/sonstiges/artikel/104776/
84. http://www.spiegel.de/netzwelt/gadgets/verschluesselung-forscher-beschreiben-methode-fuer-hintertueren-in-chips-a-922853.html
85. https://www.heise.de/security/meldung/Fehler-in-Software-fuer-ZigBee-Funkmodule-erleichtert-Lauschangriff-906983.html
86. http://www.golem.de/news/dan-kaminsky-sichere-zufallszahlen-zum-standard-machen-1408-108469.html
87. https://www.golem.de/news/duhk-angriff-vermurkster-zufallszahlengenerator-mit-zertifizierung-1710-130777.html
88.