INSTITUTUL DE MATEMATICĂ "SIMION STOILOW" AL ACADEMIEI ROMÂNE

Protocoale Criptografice

Rezumat

Coordonator ştiinţific: :
Ferucio Laurenţiu Ţiplea

Doctorand:
George Teşeleanu

Teză prezentată pentru obţinerea titlului de
Doctor în Informatică

Bucureşti, August 2021

Capitolul 1

Prefaţă

De-a lungul istoriei, rolul principal al criptografiei a fost să păstreze informaţiile sensibile private, chiar şi în prezenţa unui adversar care deţine controlul asupra canalului de comunicaţii. Chiar dacă confidenţialitatea rămâne esenţială pentru criptografie, domeniul s-a extins şi încorporează şi alte obiective, cum ar fi integritatea şi autenticitatea datelor, controlul accesului sau plăţile electronice.

În trecut folosită doar de către armată, criptografia este în prezent utilizată pe scară largă şi oamenii beneficiază de aceasta zilnic, chiar şi fără să o ştie. De exemplu, atunci când cumpăraţi un articol online, un canal securizat este utilizat pentru a procesa tranzacţia şi implicit pentru a asigura confidenţialitatea cardului dumneavoastră de credit. Sau, atunci când comunicăm prin aplicaţii de mesagerie, conversaţiile noastre private sunt protejate folosind criptarea end-to-end. Cu un domeniu de aplicabilitate în creştere, nu este surprinzător faptul că criptografia modernă împleteşte concepte din matematică, informatică, inginerie şi fizică.

Deşi o ştiinţă remarcabilă, criptografia este, de asemenea, o artă. Trebuie să gândim aşa cum ar faceo un atacator, în timp ce apărăm sistemul împotriva ameninţărilor; trebuie să jonglăm între viteză, aplicabilitate şi securitate; trebuie să transformăm concepte cunoscute pentru a le face să corespundă scopului nostru; trebuie să proiectăm concepte de nivel înalt, ţinând cont de cele de nivel scăzut etc. Influenţat de multitudinea de concepte pe care un criptograf trebuie să le gestioneze, în această lucrare abordăm diferite domenii ale criptografiei şi fie luăm rolul proiectantului, fie a atacatorului. Prin prezentarea ambelor feţe ale aceleiaşi monede, ne dorim ca cititorul să înceapă să aprecieze frumuseţea acestei ştiinţe enigmatice şi să înceapă să vadă relaţiile care apar între concepte aparent diferite.

1.1 Structura Tezei

Prezentăm în continuare un scurt rezumat al celor şapte capitole principale conţinute în această lucrare. Unul dintre cele mai dificile lucruri legate de structurarea acestei lucrări a fost interdependenţa unor capitole. Am încercat să prezentăm materialul din această teză într-o ordine logică şi naturală. Mai jos este prezentată structura tezei.

Capitolul 2 abordează criptografia cu chei simetrice şi este împărţit în trei subcapitole. Primul subcapitol conţine o analiză a securităţii cifrului Hill (afin) şi a modurilor de lucru corespunzătoare. Definiţiile şi informaţiile preliminare sunt prezentate în Secţiunea 2.1.1. Partea principală a primului subcapitol constă din Secţiunile 2.1.2 şi 2.1.3 care conţin mai multe modalităţi de clasare a cheilor şi o serie de atacuri care utilizează numai text cifrat. Rezultatele experimentale sunt furnizate în Secţiunea 2.1.4, iar unele direcţii posibile de cercetare sunt prezentate în Secţiunea 2.1.5. Frecvenţele literelor şi atacul asupra cifrului Vigenère utilizate în Secţiunea 2.1.4 sunt prezentate în Anexele A şi B. Câteva metode pentru creşterea complexităţii forţei brute, aplicabile familiei de cifruri flux Grain, sunt prezentate în a doua parte a acestui capitol. Notaţiile utilizate şi specificaţiile tehnice ale familiei de cifruri Grain sunt prezentate în Secţiunea 2.2.1. Secţiunea 2.2.2 conţine o serie de atacuri generice împotriva cifrurilor Grain. În Secţiunea 2.2.3 oferim cititorului o analiză de securitate a schemelor de padding utilizate în cadrul cifrurilor Grain. Câteva idei interesante ce pot fi abordate in viitor sunt prezentate în Secţiunea 2.2.4. Reamintim specificaţile cifrului Grain v1 în Anexa C, cifrului Grain-128 în Anexa D şi cifrului Grain-128a în Anexa E. În această lucrare nu descriem parametrii corespunzători cifrului Grain v0, chiar dacă rezultatele prezentate în această secţiune sunt valabile şi în acest caz. În Anexele F şi G oferim vectori de test pentru algoritmii propuşi. Ultima parte a acestui capitol studiază efectul utilizării cvasigrupurilor izotope cu grupuri la proiectarea structurilor de tip SPN. Astfel, noţiunile preliminare sunt prezentate în Secţiunea 2.3.1. O generalizare a structurilor de tip SPN este introdusă în Secţiunea 2.3.2, iar securitatea sa este studiată în secţiunea 2.3.3.

În Capitolul 3 discutăm mai multe protocoale cu chei publice şi câteva aplicaţii posibile pentru acestea. În primul subcapitol introducem câteva presupuneri de securitate necesare pentru a demonstra securitatea protocoalelor introduse. Protocoalele de tip zero knowledge sunt studiate în a doua parte a acestui capitol. Astfel, reamintim conceptele de bază a protocoalelor de tip zero knowledge în Secţiunea 3.2.1. Inspiraţi de protocolul Unified-Zero Knowledge introdus de Maurer, în Secţiunea 3.2.2 introducem un protocol numit Unified Generic Zero-Knowledge şi demonstrăm că acesta este sigur. Oferim cititorului câteva cazuri particulare ale protocolului UGZK în Secţiunea 3.2.3. O variantă a protocolului care utilizează funcţii hash este prezentată în Secţiunea 3.2.4, împreună cu analiza sa de securitate. Ca o posibilă aplicaţie pentru protocolul UGZK, în Secţiunea

3.2.5 descriem un protocol de autentificare de tip lightweight, discutăm securitatea şi complexitatea acestuia şi prezentăm o serie de implementări optimizate care apar din mici variaţii ale protocolului propus. În Secţiunea 3.2.6 subliniem posibile viitoarele direcţii de lucru. A treia parte a acestui capitol conţine o semnătură digitală inspirată de paradigma UZK a lui Maurer. Noţiunile preliminare necesare sunt prezentate în Secţiunea 3.3.1, iar detaliile exacte ale semnăturii UDS sunt furnizate în Secţiunea 3.3.2. O aplicaţie pentru semnătura UDS este prezentată în a patra parte a acestui capitol. Mai precis, după introducerea noţiunilor preliminare în Secţiunea 3.4.1, introducem în Secţiunea 3.4.2 un protocol de co-semnătură bazat pe protocolul introdus de Ferradi *et. al.* Discutăm câteva probleme deschise în Secţiunea 3.4.3. Două criptosisteme cu cheie publică sunt prezentate în partea a cincea. în Secţiunea 3.5.1 introducem definiţiile, presupunerile de securitate şi criptosistemele utilizate în această secţiune. Mai întâi introducem în Secţiunea 3.5.2 o modificare a schemei de criptare ElGamal generalizată, care va fi utilizată într-un capitol ulterior. Apoi, inspiraţi de schema Joye-Libert PKE şi dorind să obţinem o generalizare relevantă, în Secţiunea 3.5.3 propunem un nou criptosistem bazat pe reziduuri de ordin 2^k, demonstrăm că protocolul este sigur în modelul standard şi analizăm performanţa acestuia în comparaţie cu alte criptosisteme înrudite. Posibile direcţii de cercetare sunt prezentate în Secţiunea 3.5.3.5 şi în Anexa H prezentăm câţiva algoritmi de decriptare optimizaţi pentru schema propusă. Ultima parte a acestui capitol oferă cititorului o aplicaţie a schemei noastre bazate pe criptosistemul Joye-Libert la autentificarea biometrică. Astfel, definiţiile şi presupunerile de securitate sunt prezentate în Secţiunea 3.6.1, iar protocolul nostru de autentificare propus este descris în Secţiunea 3.6.2.

Câteva rezultate utile pentru înțelegerea securităţii criptosistemului bazat pe identitate introdus de Cocks şi a anumitor variaţii ale acestuia sunt furnizate în Capitolul 4. Noţiunile de bază şi schema Cocks sunt prezentate în prima parte a capitolului. A doua parte consideră mulţimi de forma $a + X = \{(a + x) \bmod n \mid x \in X\}$, unde n este un număr prim sau produsul a două numere prime $n = pq$ şi X este o submulţime a lui $\mathbb{Z}_n^*$ ale cărei elemente au un anumit simbol Jacobi modulo factorii primi ai lui n. A treia parte a capitolului conţine două aplicaţii ale rezultatelor menţionate anterior. Prima oferă o analiză detalizată a unor distribuţii legate de criptosistemul IBE introdus de Cocks şi a testului Galbraith, oferind astfel o analiză riguroasă a testul Galbraith. A doua aplicaţie discutată se referă la indistingibilitatea computaţională a unor distribuţii utilizate pentru a demonstra securitatea unor variante ale IBE-ului Cocks. Am reuşit să demonstrăm indistingibilitatea statistică a acestor distribuţii fără nici o presupunere de securitate. Capitolul se încheie cu Secţiunea 4.4.

O metodă neconvenţională pentru a insera backdoor-uri în sistemele criptografice este studiată în Capitolul 5. Noţiunile de bază despre atacurile cleptografice sunt prezentate în Secţiunea 5.1. În prima parte a acestui capitol este descris un atac cleptografic partajat care poate fi implementat în semnătura digitală ElGamal generalizată. Astfel, în Secţiunea 5.2.1 descriem un atac simplificat asupra semnăturii ElGamal generalizată şi apoi acest rezultat îl extindem în Secţiunea 5.2.2. O serie de semnături digitale care permit implementarea atacului nostru sunt furnizate în Secţiunea 5.2.3. Câteva direcţii de cercetare sunt prezentate în Secţiunea 5.2.4 şi un protocol maliţios de co-semnătură este descris în Anexa I. O serie de mecanisme cleptografice adiţionale sunt prezentate în Anexa J. O metodă de infectare a protocolului UZK este studiată în a doua parte a acestui capitol. În Secţiunile 5.3.1 şi 5.3.2 prezentăm o serie de metode cleptografice generice si demonstrăm că acestea sunt sigure. Instanţieri ale atacurilor propuse pot fi regăsite în Secţiunea 5.3.3. Câteva posibile direcţii de cercetare sunt prezentate în Secţiunea 5.3.4. În a treia parte, introducem un model de marketing potrivit pentru vânzarea dispozitivelor infectate. Astfel, o serie de noţiuni preliminarii sunt descrise în Secţiunea 5.4.1. Pe baza algoritmului de criptare ElGamal, o serie de abonamente cleptografice care se potrivesc diferitelor scenarii sunt furnizate în Secţiunile 5.4.2 la 5.4.4. Discutăm câteva probleme deschise în Secţiunea 5.4.5. Canalele hash sunt abordate în ultima parte a capitolului. Prin adaptarea şi îmbunătăţirea mecanismului introdus de Wu, introducem o serie de noi canale hash în Secţiunea 5.5.1. O serie de rezultate experimentale sunt prezentate în Secţiunea 5.5.2, iar câteva aplicaţii sunt furnizate în Secţiunea 5.5.3.

În Capitolul 6 studiem generatoarele de numere (pseudo-)aleatoare. Prima parte a capitolului tratează o vulnerabilitate a generatorul de numere pseudo-aleatoare utilizat de către Adobe Flash Player [1] pentru constant blinding. Introducem noţiunile preliminare necesare în Secţiunea 6.1.1. Mecanismului nostru de recuperare a seed-ului se regaseşte în Secţiunile 6.1.2 şi 6.1.3. Mai precis, aceste două subcapitole conţin o serie de algoritmi utilizaţi pentru a inversa o versiune generalizată a funcţiei hash utilizată în cadrul Flash Player. Rezultatele experimentale sunt prezentate în Secţiunea 6.1.4. Algoritmii auxiliari pot fi regăsiţi în Anexa K. A doua parte conţine o arhitectură care poate fi utilizată pentru a implementa teste de health pentru generatoarele de numere aleatoare. Definiţiile şi noţiunile preliminare sunt prezentate în Secţiunea 6.2.1. Două clase de filtre digitale care amplifică bias-urile deja existente sunt descrise în Secţiunile 6.2.2 şi 6.2.3. Unele aplicaţii posibile sunt prezentate în Secţiunea 6.2.4. În Secţiunea 6.2.5 utilizăm arhitectura propusă pentru surse de zgomot de tip Bernoulli şi prezentăm câteva rezultate experimentale. Modelul teoretic este furnizat în Secţiunea 6.2.6. Unele măsurători mai fine sunt furnizate în Secţiunea 6.2.7. În Secţiunea 6.2.8 propunem unele posibile direcţii de cercetare.

[1] versiunile 24.0.0.221 şi anterioare

Capitolul 7 conţine mai multe protocoale care se încadrează în categoria criptografiei recreaţionale. Astfel, în Secţiunea 7.1 descriem diferite protocoale care vizează rezolvarea problemei milionarilor introdusă de Yao şi furnizăm cititorului analizele de securitate corespunzătoare. În Secţiunea 7.2 prezentăm un set de protocoale care furnizează o soluţie pentru compararea informaţiilor fără a le dezvălui şi discutăm securitatea acestora. În Secţiunea 7.3 descriem un criptosistem cu cheie publică construit prin intermediul unei scheme electrice şi abordăm securitatea acestuia. În Anexa L amintim diverse soluţii criptografice recreaţionale care au apărut în literatură de specialitate, în timp ce în Anexa M prezentăm un protocol generic de criptare cu cheii publice care utilizează diferite sisteme fizice. Protocolul introdus este util pentru prezentarea în cadrul orelor de curs a diferitelor proprietăţi inerente acestor sisteme fizice.

1.2 Articole Publicate

[P1] Mariana Costiuc, Diana Maimuţ, and George Teşeleanu. Physical Cryptography. In *SECITC 2019*, volume 12001 of *Lecture Notes in Computer Science*, pages 156–171. Springer, 2019.

[P2] Diana Maimuţ and George Teşeleanu. Secretly Embedding Trapdoors into Contract Signing Protocols. In *SECITC 2017*, volume 10543 of *Lecture Notes in Computer Science*, pages 166–186. Springer, 2017.

[P3] Diana Maimuţ and George Teşeleanu. A Unified Security Perspective on Legally Fair Contract Signing Protocols. In *SECITC 2018*, volume 11359 of *Lecture Notes in Computer Science*, pages 477–491. Springer, 2018.

[P4] Diana Maimuţ and George Teşeleanu. New Configurations of Grain Ciphers: Security Against Slide Attacks. In *BalkanCrypt 2018*, Communications in Computer and Information Science. Springer, 2018.

[P5] Diana Maimuţ and George Teşeleanu. A Generic View on the Unified Zero-Knowledge Protocol and its Applications. In *WISTP 2019*, volume 12024 of *Lecture Notes in Computer Science*, pages 32–46. Springer, 2019.

[P6] Diana Maimuţ and George Teşeleanu. A New Generalisation of the Goldwasser-Micali Cryptosystem Based on the Gap 2^k-Residuosity Assumption. In *SECITC 2020*, Lecture Notes in Computer Science. Springer, 2020.

[P7] George Teşeleanu. Threshold Kleptographic Attacks on Discrete Logarithm Based Signatures. In *LatinCrypt 2017*, volume 11368 of *Lecture Notes in Computer Science*, pages 401–414. Springer, 2017.

[P8] George Teşeleanu. Random Number Generators Can Be Fooled to Behave Badly. In *ICICS 2018*, volume 11149 of *Lecture Notes in Computer Science*, pages 124–141. Springer, 2018.

[P9] George Teşeleanu. Unifying Kleptographic Attacks. In *NordSec 2018*, volume 11252 of *Lecture Notes in Computer Science*, pages 73–87. Springer, 2018.

[P10] George Teşeleanu. Managing Your Kleptographic Subscription Plan. In *C2SI 2019*, volume 11445 of *Lecture Notes in Computer Science*, pages 452–461. Springer, 2019.

[P11] George Teşeleanu. Reinterpreting and Improving the Cryptanalysis of the Flash Player PRNG. In *C2SI 2019*, volume 11445 of *Lecture Notes in Computer Science*, pages 92–104. Springer, 2019.

[P12] George Teşeleanu. Subliminal Hash Channels. In *A2C 2019*, volume 1133 of *Communications in Computer and Information Science*, pages 149–165. Springer, 2019.

[P13] George Teşeleanu. A Love Affair Between Bias Amplifiers and Broken Noise Sources. In *ICICS 2020*, Lecture Notes in Computer Science. Springer, 2020.

[P14] George Teşeleanu. Cracking Matrix Modes of Operation with Goodness-of-Fit Statistics. In *HistoCrypt 2020*, Linköping Electronic Conference Proceedings. Linköping University Electronic Press, 2020.

[P15] George Teşeleanu. Quasigroups and Substitution Permutation Networks: A Failed Experiment. *Cryptologia*, 2020.

[P16] Ferucio Laurentiu Tiplea, Sorin Iftene, George tese, and Anca-Maria Nica. On the Distribution of Quadratic Residues and Non-residues Modulo Composite Integers and Applications to Cryptography. *Appl. Math. Comput.*, 372, 2020.

[P17] Ferucio Laurenţiu Ţiplea, Sorin Iftene, George Teşeleanu, and Anca-Maria Nica. Security of Identity-Based Encryption Schemes from Quadratic Residues. In *SECITC 2016*, volume 10006 of *Lecture Notes in Computer Science*, pages 63–77, 2016.

Capitolul 2

Criptografie cu Chei Simetrice

Cea mai simplă şi, de asemenea, cea mai comună metodă pentru protejarea confidenţialităţii mesajelor sau pentru autentificarea unei informaţii este utilizarea unei chei secrete comună între expeditor şi receptor. Aceasta metodă se numeşte criptografie cu cheie secretă/simetrică. În acest scenariu, ambii participanţi utilizează funcţii dependente de aceeaşi cheie predeterminată. De obicei, cheia comună este generată aleatoriu.

Se presupune că algoritmii cu cheii simetrice îşi păstrează proprietăţile de securitate atâta timp cât adversarii nu pot deduce cheia utilizată. Acest lucru poate însemna trei lucruri: fie cheia este păstrată în mod sigur de către utilizatorii care o folosesc, fie cheia este suficient de mare pentru a evita atacurile de tip forţă brută sau algoritmul este singur din punct de vedere informaţional. În acest capitol ne vom ocupa de două dintre aspectele menţionate anterior. Mai precis, vom arăta cum cifrul Hill (afin) şi modurile lor corespunzătoare de lucru oferă atacatorului informaţii critice prin intermediul textul cifrat. Apoi vom descrie o metodă pentru extinderea duratei de viaţă a instanţierilor cifrului flux Grain prin creşterea complexităţii corespunzătoare atacurilor de tip forţă brută. În ultima parte, prezentăm cititorului instanţieri echivalente ale structurilor de tip substituţie-permutare.

2.1 Cifrul Hill (Afin)

Două cifruri clasice bazate pe algebră liniară sunt cifrul Hill [144] şi versiunea sa afină [145]. Ambele folosesc matrici inversabile modulo a pentru a cifra mesajele, unde a este dimensiunea alfabetului $\mathcal{A}$. Primul pas al procesului de criptare este codificarea fiecărei litere din text într-un echivalent numeric. Cea mai simplă codificare este `"a"` $= 0$, `"b"` $= 1$ şi aşa mai departe. După codificare, textul este împărţit în blocuri de dimensiunea k şi,

apoi, fiecare bloc este înmulţit cu o matrice inversabilă de dimensiune k. În cazul afin, la rezultat se adună o a doua matrice. După transformarea fiecărui bloc, rezultatul este convertit din nou în litere. Pentru a descifra mesajele, trebuie să efectuaţi paşii de mai sus în sens invers.

Deşi ambele cifruri sunt vulnerabile la atacuri ce utilizează text cunoscut[1], atacuri eficiente ce utilizează numai text cifrat au fost dezvoltate acum doar un deceniu [42] şi numai pentru cifrul Hill cu k mic. Reţineţi că pe măsură ce k creşte atacurile simple de tip forţă brută eşuează. De exemplu, în cazul cifrului Hill cu $a = 26$, avem în jur de 2^{17} chei pentru $k = 2$, 2^{40} chei pentru $k = 3$ şi 2^{73} chei pentru $k = 4$ [42]. Conform [201, 43], dat fiind a şi k se poate calcula numărul exact de matrici inversabile. Menţionăm că, în cazul cifrului Hill afin, efortul de calcul făcut pentru atacurile de tip forţa brută împotriva cifrul Hill este înmulţit cu a^k.

În 2007, Bauer şi Millward [42] au introdus un atac ce utilizează doar text cifrat pentru a ataca cifrul Hill[2], atac ce a fost ulterior îmbunătăţit în [266, 167, 178]. Atacul a fost publicat independent de Khazaei şi Ahmadi [154]. Ideea principală a acestor atacuri este de a face un atac de tip forţă brută pe rândurile cheii, în loc de întreaga matrice, şi apoi de a recupera matricea de decriptare.

În [157], Kiele sugerează utilizarea modurilor de lucru pentru a îngreuna tehnicile algebrice criptanalitice dezvoltate pentru cifrul Hill. Vom arăta în această secţiune cum să adaptăm atacurile descrise în [42, 266, 154] la diferite moduri de operare atât pentru cifrul Hill, cât şi pentru versiunea sa afină. Reţineţi că unele moduri de lucru nu necesită ca cheia să fie inversabilă, astfel că atacul prezentat în [167] nu funcţionează pentru toate modurile de lucru bazate pe Hill. Pentru uniformitate, vom extinde doar atacul lui Yum şi Lee şi vom studia în viitor extinderea [167] la moduri care necesită matrici inversabile. Subliniem că dintre cele trei atacuri [42, 266, 154] atacul lui Yum şi Lee are cel mai bun raport de performanţă per recuperarea mesajelor.

O altă lucrare care a motivat acest studiu este [41]. Autorii [41] presupun că cea de-a patra criptogramă a sculpturii Kryptos [9] este fie criptată utilizând cifrul Hill afin, fie un mod de operare al cifrului. Oferim cititorului un studiu preliminar al acestor presupuneri. Pentru a dovedi sau respinge aceste presupuneri, trebuie să găsim o modalitate de a adapta toate atacurile ce utilizează text cifrat prezentate la versiunile cu codificare secretă ale cifrului Hill (afin) şi a modurilor lor de lucru corespunzătoare. Diverse răspunsuri parţiale pentru versiunea cu codificare secretă a cifrului Hill sunt furnizate în [266].

[1] *i.e.* după ce un număr de mesaje cunoscute sunt criptate, se pot recupera cu uşurinţă cheile de criptare dacă atacatorul are acces la textele cifrat corespunzătoare.

[2] Atacul lui Bauer şi Millward pentru $k = 3$ a fost descris anterior online şi în mod independent de Wutka [257].

2.2 Familia de Cifruri Flux Grain

Familia de cifruri flux Grain constă din patru instanţieri Grain v0 [140], Grain v1 [141], Grain-128 [139] şi Grain-128a [211]. Grain v1 este un finalist al portofoliului hardware eSTREAM [4], o competiţie pentru alegerea cifrurilor flux sigure şi eficiente atât pentru hardware cât şi pentru software.

Designul familiei de cifruri flux Grain include un LFSR. Încărcarea LFSR-ului constă dintr-un vector de iniţializare (IV) şi un anumit şir de biţi P al cărui lungime şi structură depinde de versiunea cifrului. Urmând terminologia utilizată în [39], considerăm că IV-ul este concatenat cu P. Astfel, în toată această secţiune, folosim termenul de *padding* pentru a indica P. Reţineţi că Grain v1 şi Grain-128 folosesc un padding *periodic* şi Grain-128a utilizează un padding *aperiodic*.

În ultimul deceniu, o serie de atacuri împotriva tehnicilor de padding a familiei Grain au apărut în literatura de specialitate [38, 39, 64, 162]. În lumina acestor atacuri, propunem prima analiză de securitate[3] a schemelor de padding generice pentru cifrurile Grain în cazurile *periodic*, precum şi *aperiodic*.

În acest context, problemele care apar sunt strâns legate de impactul asupra securităţii a diferiţilor parametri ai paddingului, cum ar fi poziţia şi structura blocului de padding. Mai mult, în cadrul studiului nostru luăm în considerare atât blocurile de padding *compacte*, cât şi *fragmentate*. Ne referim la schemele originale de padding ale cifrurilor Grain ca fiind compacte (*i.e.* se foloseşte un singur bloc de padding). Considerăm ca padding fragmentat un bloc de padding divizat în blocuri mai mici de lungime egală[4].

Examinând structura paddingului şi analizând versiunile sale compacte şi mai ales fragmentate, studiem de fapt conceptul de a extinde durata de viaţa a cheii. Acesta din urmă ar putea fi realizat prin introducerea unui padding variabil în funcţie de constrângerile adecvate. Prin urmare, întrebarea generală care apare este următoarea: *ce trebuie încărcat în LFSR-urile cifrurilor Grain pentru a obţine instanţieri sigure?*. Reţineţi că studiul nostru este preliminar, luând în considerare doar atacurile de tip slide. Considerăm alte tipuri de atacuri într-un studiu viitor.

Subliniem că găsirea unor atacuri mai bune decât cele prezentate deja în literatură nu intră în scopul acestei secţiuni, deoarece obiectivul nostru principal este de a stabili versiuni personalizate sigure ale cifrului Grain. Prin urmare, munca noastră nu are nicio implicaţie imediată asupra spargerii oricarui cifru din familia Grain. Cu toate acestea, observaţiile noastre devin semnificative fie în scenariul criptografiei de tip lightweight, fie

[3] împotriva atacurilor de tip slide
[4] considerăm că aceste blocuri mai mici sunt răspândite între datele registrului liniar

în cazul unui context de securitate îmbunătăţit (de exemplu, aplicaţii guvernamentale sigure).

Criptografia de tip lightweight se află la intersecţia dintre criptografie, informatică şi inginerie electrică. Astfel, trebuie luate în considerare compromisurile între performanţă, securitate şi cost. Având în vedere astfel de constrângeri şi faptul că dispozitivele încorporate funcţionează în medii ostile, există o nevoie tot mai mare de soluţii de securitate noi şi variate, construite în principal având în vedere actuala tendinţă computaţională. Întrucât familia Grain se află tocmai în categoria primitivelor de tip lightweight, credem că studiul prezentat în secţiunea curentă este de interes pentru industrie şi, în special, pentru organizaţiile guvernamentale.

2.3 Stucturi Substituţie-Permutare Bazate pe Cvasigrupuri

În forma sa de bază, criptanaliza diferenţială [55] prezice modul în care anumite modificări ale textului se propagă printr-un cifru. Când se consideră un cifru ideal, probabilitatea de a prezice aceste modificări este $1/2^n$, unde n este numărul de biţi al datelor de intrare. Astfel, în cazul ideal, este imposibil ca un atacator să folosească aceste predicţii atunci când n este, de exemplu, 128. Din păcate, proiectanţii folosesc estimări teoretice bazate pe anumite ipoteze care nu sunt întotdeauna valabile în practică. Prin urmare, criptanaliza diferenţială este adesea cel mai eficient instrument împotriva algoritmilor criptografici cu cheie simetrică [188].

Cvasigrupurile sunt structuri asemănătoare grupurilor care, spre deosebire de grupuri, nu trebuie să fie asociative şi să posede un element identitate. Utilizarea cvasigrupurilor ca elemente de bază pentru primitive criptografice nu este foarte obişnuită. Totuşi, diverse astfel de criptosisteme pot fi găsite în literatura [164, 117, 116, 35, 90, 160].

În această subsecţiune introducem o generalizare a structurilor substituţie-permutare (SPN) şi studiem securitatea acesteia. Prin înlocuirea operaţiei de grup $\star$ între cheii şi texte (intermediare) cu o operaţie de cvasigrup $\otimes$ am urmărit extinderea utilizării cvasigrupurilor. Din păcate, utilizând criptanaliza diferenţială, demonstrăm că în cazul cvasigrupurilor izotope cu un grup[5] problema atacării unui SPN folosind $\otimes$ se reduce la atacarea unui SPN folosind $\star$ şi o tabelă de substituţie (s-box) diferită de cea iniţială. Astfel, dacă iniţializăm SPN-ul cu un s-box secret aleator, înlocuirea $\star$ cu $\otimes$ nu aduce nici o securitate suplimentară[6]. În cazul s-box-urilor statice, schimbarea $\star$ cu $\otimes$ poate afecta chiar securitatea SPN-ului.

[5] Aceasta este cea mai populară metodă de generare a cvasigrupurilor.

[6] *i.e.* obţinem pur şi simplu o altă instanţă a SPN

Deşi designul prezentat în această lucrare nu este unul de succes, credem că utilitatea sa este dublă. ① Majoritatea rapoartelor ştiinţifice şi lucrărilor publicate apar ca relatări sterile[7] şi acest lucru oferă oamenilor o viziune distorsionată a cercetării ştiinţifice [179, 146, 235, 255]. Acest lucru duce la o viziune care implică faptul că eşecul, serendipitatea şi rezultatele neaşteptate nu sunt o parte normală a ştiinţei [146, 220]. Prin urmare, acest subcapitol oferă studenţilor o indicaţie a proceselor reale de experimentare. ② Rezultatele negative şi direcţiile false sunt rareori raportate [146, 248] şi, prin urmare, oamenii sunt obligaţi să repete aceleaşi greşeli. Prin prezentarea rezultatelor noastre, sperăm să oferim celorlalţi o oportunitate de a afla unde duce această cale. Prin urmare, împiedicându-i să facă aceleaşi greşeli[8].

[7] Autorii îşi prezintă rezultatele ca şi când le-ar fi obţinut într-o manieră simplă şi nu printr-un proces dezordonat.

[8] In [236], autorul îi sfătuieşte pe oameni să îşi noteze greşelile, astfel încât să evite să le comită din nou în viitor.

Capitolul 3

Criptografie cu Chei Publice

Una dintre problemele asociate criptografiei cu cheii simetrice este distribuirea cheilor. O soluţie elegantă pentru acest inconvenient este oferită de criptografia cu cheii publice/asimetrică. Într-un cadru asimetric, un participant posedă o pereche de chei: o cheie publică şi o cheie secretă asociată. Cheia publică este cunoscută de toată lumea şi este legată de identitatea participantului. Folosind cheia publică, orice utilizator poate trimite mesaje proprietarului, în timp ce doar acesta le poate citi folosind cheia sa secretă. Comparativ cu sistemele de chei simetrice[1], în cazul utilizării cheiilor publice nu este nevoie de un canal sigur pentru a disemina cheile publice ale participanţilor. O altă proprietate atractivă a algoritmilor asimetrici este că securitatea lor poate fi, în majoritatea cazurilor, redusă la probleme computaţionale dificile.

Deşi iniţial dezvoltată pentru rezolvarea problemei distribuţiei cheii, criptografia cu cheie publică s-a extins şi încorporează şi alte aplicaţii, cum ar fi schemele de criptare, semnăturile digitale sau protocoalele de tip zero-knowledge. În acest capitol dezvoltăm diverse exemple pentru aplicaţiile menţionate anterior şi le reducem securitatea la unele presupuneri intractabile bine cunoscute.

3.1 Protocoale de Tip Zero-Knowledge

Problema principală abordată de ZKP este reprezentată de *schemele de identificare* (autentificarea unei entităţi). Astfel, bazându-ne pe cel mai important obiectiv pe care îl poate atinge un ZKP, se pot găsi soluţii elegante la diferite probleme care apar în diferite domenii: monede electronice, licitaţii, IoT, autentificare prin parolă şi aşa mai departe.

[1] unde este necesar un canal sigur pentru a distribui cheia de comunicare către participanţi

Un protocol de tip zero-knowledge tipic este format dintr-un prover *Peggy* care posedă o informaţie secretă x asociată cu identitatea ei şi dintr-un verificator *Victor* a cărui sarcină este să verifice dacă *Peggy* deţine cu adevărat x. Două exemple clasice de astfel de protocoale (propuse pentru smartcard-uri) sunt protocolul Schnorr [219] şi protocolul Guillou-Quisquater [131]. Lucrând într-un cadru abstract, Maurer arată în [176] că protocoalele menţionate anterior sunt de fapt instanţieri ale aceluiaşi protocol.

Bazându-ne pe rezultatul lui Maurer, am considerat de mare interes să oferim cititorului o perspectivă generalizată a protocolului Unified Zero-Knowledge (UZK), precum şi o variantă hash a acestuia. O consecinţă importantă a abordării noastre generice este unificarea protocoalelor Maurer [176], Feige-Fiat-Shamir [103] şi Chaum-Everste-Van De Graaf [68]. Mai mult, un caz special al versiunii hash a protocolului nostru este versiunea *h-variant* a schemei Fiat-Shamir [108, 115].

Pe măsură ce paradigma IoT s-a dezvoltat, dispozitivele de tip lightweight[2] au devenit din ce în ce mai populare. Datorită naturii distribuite ale dispozitivelor IoT, este necesară o securitate adecvată pentru ca întreaga reţea să funcţioneze corespunzător. Acum să analizăm cazul reţelelor de senzori wireless (WSN). Natura lightweight a nodurilor senzorilor restricţionează puternic operaţiunile criptografice. Astfel, nevoia de soluţii criptografice specifice devine evidentă. Protocolul de autentificare distribuit asemănător protocolului Fiat-Shamir prezentat în [78] reprezintă un astfel de exemplu. Pe baza acestei construcţii anterioare propunem un protocol generic unificat de tip zero-knowledge. La fel ca rezultatul descris în [78], protocolul nostru poate fi aplicat pentru securizarea WSN-urilor şi, mai general, a soluţiilor legate de IoT. Cu toate acestea, construcţia noastră oferă flexibilitate atunci când alegeţi ipotezele pe care se bazează securitatea sa. O caracteristică secundară a schemei noastre este posibilitatea de a reutiliza certificatele existente la implementarea protocolului de autentificare distribuită.

3.2 Semnături Electronice

În 1986, Fiat și Shamir [108] au descris o tehnică importantă pentru derivarea semnăturilor digitale din protocoalele de tip zero-knowledge. Ideea de bază constă în faptul că semnatarul folosește o funcție hash pentru a crea un verificator virtual. Această tehnică a fost folosită ulterior de Schnorr pentru a-și transforma ZKP într-o semnătură digitală. Semnătura rezultată a fost dovedită sigură în ROM de Pointcheval și Stern [208, 209].

[2] dispozitive cu costuri reduse, cu resurse limitate, fie ele de calcul sau fizice

Cadrul UZK încorporează protocolul Schnorr ZKP. Prin urmare, este firesc să aplicăm transformarea Fiat-Shamir la UZK și astfel să generalizăm semnătura lui Schnorr. Ulterior vom folosi semnătura rezultată ca element principal pentru protocolul de co-semnătură pe care îl propunem în Secțiunea 3.3.2.

3.3 Protocoale de Co-Semnătura

În ultimele decenii au fost propuse diferite scheme de semnare a contractelor care se încadrează în trei categorii diferite de proiectare: *gradual release* [122, 207, 111, 127], *optimistic* [29, 63, 181] şi *concurrent* [71, 104]. Un protocol tipic de co-semnătură implică doi parteneri care nu au încredere unul în altul.

În comparaţie cu paradigmele mai vechi, cum ar fi modelele gradual release sau optimistic, semnăturile concurente nu se bazează pe terţe părţi de încredere şi nu necesită prea multă interacţiune între semnatari. Deoarece astfel de caracteristici sunt mult mai atractive pentru utilizatori, considerăm în continuare protocoalele de co-semnătură şi nu soluţiile mai vechi.

Inspiraţi de perspectiva generică a lui Maurer, am considerat de mare interes extinderea paradigmei sale la protocoalele de semnare a contractelor. Prin urmare, construim ideea principală luând în considerare problema compatibilităţii schemelor care caracterizează sistemele de comunicaţii. Exemplele tipice sunt cazurile utilizării certificatelor într-o infrastructură cu cheii publice şi problema generală a actualizării versiunii unui sistem. Astfel, lucrul într-un cadru general poate reduce erorile de implementare şi poate economisi timp de dezvoltare (şi întreţinere) ale aplicaţilor.

În această secţiune vă prezentăm o clasă de protocoale de co-semnătură şi dovedim securitatea acesteia. Pentru a fi mai precişi, vă propunem o clasă de protocoale de co-semnătură bazată pe UDS (a se vedea Secţiunea 3.2) care păstrează proprietăţile schemei prezentate în [104].

3.4 O Generalizare a Criptosistemului Goldwasser-Micali

Scopul unei scheme de criptare cu cheii publice este de a oferi confidenţialitate, permiţând în acelaşi timp utilizatorilor să distribuie cheile publice utilizând canale nesigure. Prin urmare, numai un utilizator care deţine cheia secretă poate decripta mesajele, în timp ce oricine deţine cheia publică corespunzătoare poate cripta datele pentru a le trimite acestui utilizator. De obicei, proiectarea PKE-urilor se bazează în mod obişnuit pe probleme de calcul intratabile din teoria numerelor.

Autorii [149] au introdus o schemă PKE[3] reprezentând o extensie destul de naturală a criptosistemului Goldwasser-Micali (GM) [123, 124], prima schemă de criptare probabilistică. Criptosistemul Goldwasser-Micali realizează o indistingibilitate a textului cifrat sub ipoteza *reziduurilor pătratice* (QR). În ciuda faptului că este simplă şi elegantă, această schemă este destul de neeconomică în ceea ce priveşte lăţimea de bandă[4]. În literatura de specialitate au fost propuse diferite încercări de generalizare a schemei Goldwasser-Micali pentru a aborda problema menţionată anterior. Schema Joye-Libert poate fi considerată o consecinţă a criptosistemelor propuse în [190] şi [79] şi care suportă criptarea eficientă a mesajelor mai mari.

Inspiraţi de schema Joye-Libert, propunem un nou criptosistem cu cheie publică, îi analizăm securitatea şi oferim cititorului detalii de implementare şi o discuţie despre performanţă. Construim schema propusă de noi pe baza simbolurilor de ordin 2^k. Generalizarea noastră a criptosistemului Joye-Libert foloseşte doi parametri importanţi atunci când vine vorba de funcţiile de criptare şi decriptare: numărul de biţi ai unui mesaj şi numărul primelor distincte ale unui modul public n. Astfel, propunerea noastră nu doar acceptă criptarea mesajelor mai mari (ca în varianta Joye-Libert), ci operează şi pe *un număr variabil de numere mari mari* (în loc de două în cazul Joye-Libert). Ambii parametri pot fi aleşi în funcţie de aplicaţia de securitate dorită.

Schema noastră poate fi privită ca o soluţie flexibilă caracterizată prin capacitatea de a face compromisuri adecvate între viteza de criptare şi extinderea textului cifrat într-un context dat.

3.5 Autentificare Biometrică

În protocoalele de autentificare biometrică, atunci când un utilizator se identifică folosind caracteristicile sale biometrice (captate de un senzor), datele colectate vor varia. Astfel, abordările criptografice tradiţionale (cum ar fi stocarea unei valori hash) nu sunt potrivite în acest caz, deoarece nu sunt tolerante la erori. Ca urmare, protocoalele bazate pe biometrie trebuie construite într-un mod special şi, în plus, sistemul trebuie să protejeze sensibilitatea şi confidenţialitatea caracteristicilor biometrice ale unui utilizator. Un astfel de protocol este propus în [61]. La baza sa stă schema de criptare Goldwasser-Micali. Astfel, o extensie naturală a protocolului din [61] poate fi obţinută folosind generalizarea schemei Joye-Libert. Astfel, descriem un astfel de protocol de autentificare biometrică şi discutăm securitatea acestuia.

[3] reconsiderată în [51]

[4] $k \cdot \log_2 n$ biţi sunt necesari pentru a cripta un mesaj de k biţi, unde n este un modul RSA [123, 124]

Capitolul 4

Criptografie Bazată pe Identitate

Criptografia bazată pe identitate a fost propusă în 1984 de către Adi Shamir [222] care a formulat principiile de bază şi a furnizat o schemă de semnătură bazată pe identitate. În 2000, Sakai, Ohgishi şi Kasahara [216] au propus un protocol de schimb de cheii bazat pe identitate, iar un an mai târziu, Cocks [77] şi Boneh şi Franklin [59] au a propus primele scheme de criptare bazate pe identitate. Schema lui Cocks se bazează pe reziduuri pătratice, în timp ce schema propusă de Boneh şi Franklin se bazează pe perechi biliniare. De atunci, alte câteva scheme de tip IBE bazate pe reziduuri pătratice au fost propuse [60, 147, 31, 76, 99, 100, 148], deşi unele dintre ele nu sunt sigure (consultaţi [246] pentru detalii).

Schema Cocks criptează mesajele bit cu bit şi fiecare bit criptat este format dintr-o pereche de două numere întregi. Decriptarea constă în calcularea simbolului Jacobi a unuia dintre cele două numere întregi din fiecare pereche. Deşi schema IBE a lui Cocks este eficientă numai pentru mesajele mici, este foarte elegantă şi *per se* revoluţionară. Schema a atras interesul multor cercetători [60, 31, 76, 148]. O analiză atentă a [77, 60, 31, 76, 148] arată că numerele întregi de forma $a + r$, unde a este un număr întreg şi r este un reziduu pătratic (modulo un număr întreg n), joacă un rol important în aceste lucrări. În special, se observă ca este importantă cunoaşterea distribuţiei reziduurilor pătratice între toate numerele întregi de forma $a + r$. Un studiu în această direcţie a fost iniţiat de Perron [206] pentru cazul unui modul prim p. Dar, majoritatea aplicaţiilor criptografice ale reziduurilor pătratice necesită utilizarea unui modul compus $n = pq$. Ne confruntăm astfel cu necesitatea extinderii rezultatelor lui Perron la module compuse. Acelaşi lucru a fost susţinut în [31] (consultaţi Secţiunea 2.3 din [31]). Aici autorii au evitat extinderea rezultatelor lui Perron la module compuse cu preţul unor rezultate mai slabe de indistingibilitate (aceaste rezultate vor fi discutate pe deplin în Secţiunea 4.3.1).

Contribuţiile prezentate în acest capitol sunt structurate în două părţi. În prima parte (Secţiunea 4.2) sunt considerate mulţimile de forma $a + X = \{(a + x) \bmod n \mid x \in X\}$, unde n este un număr prim sau produsul a două numere prime $n = pq$, iar X este o submulţime a $\mathbb{Z}_n^*$ ale cărei elemente au un anumit simbol Jacobi modulo factorii primi ai lui n. De exemplu, X poate fi mulţimea tuturor numerelor întregi din $\mathbb{Z}_n^*$ ale căror simbol Jacobi modulo p este 1 şi modulo q este -1 (presupunând $n = pq$); spunem că *şablonul Jacobi* al întregilor din X, în acest caz, este "$+-$". Apoi, având o mulţime de tip $a+X$, calculăm distribuţia reziduuri pătratice, non-reziduuri pătratice etc., în $a+X$. Prezentăm rezultatele obţinute pentru toate şabloanele de lungime Jacobi unu, $+$ şi $-$ (aceastea corespund reziduurilor pătratice şi non-reziduurilor modulo un număr prim) şi şabloane Jacobi de lungime doi, $++$, $--$, $+-$ şi $-+$ (aceastea corespund modulelor care sunt produsul a două numere prime distincte).

Rezultatele prezentate în Secţiunea 4.2 sunt o extensie majoră a proprietăţilor demonstrate de Perron [206], care a studiat doar distribuţia reziduurilor pătratice în mulţimea $a + QR_p$, unde p este un număr prim. Studii conexe cu cele efectuate în Secţiunea 4.3 se regăsesc în [86, 87, 204, 151], unde autorii calculează probabilitatea ca şablonul de lungime ℓ

$$J_p(a)J_p(a+1)\cdots J_p(a+\ell-1)$$

să coincidă cu un şablon dat a priori modulo p, atunci când a este ales aleator din $a \in \mathbb{Z}_p^*$ (p este un număr prim). Astfel, în [204] s-a arătat că numărul întregi a cu proprietatea de mai sus este între $p/2^\ell - \epsilon$ şi $p/2^\ell + \epsilon$, unde $\epsilon = \ell(3 + \sqrt{p})$. Împărţind aceste două limite cu p obţinem probabilitatea ca un întreg a să inducă un şablon Jacobi dat pentru ℓ elemente consecutive. O extensie directă a acestui rezultat la cazul modulelor de tip RSA poate duce la o margine "mult mai mare" decât ϵ. În [151], o extensie la modulele RSA a fost propusă prin generalizarea rezultatelor din [87]. Astfel, autorul a arătat că numărul de întregi a cu proprietatea de mai sus este $n/2^\ell + \mathcal{O}(\sqrt{n} \cdot \log^2 n)$, unde n este un modul RSA şi $1 \leqslant \ell \leqslant (1/2 - \delta)\log_2 n$, pentru $0 < \delta < 1/2$.

Rezultatele dezvoltate în acest capitol sunt diferite de cele menţionate mai sus din cel puţin două motive. În primul rând, am dezvoltat formule exacte şi nu aproximative pentru numărul de întregi cu un şablon Jacobi dat în seturile $a + X$. În al doilea rând, factorul de creştere este arbitrar în toate studiile noastre, în timp ce este unu in toate rezultatele menţionate mai sus.

A doua parte a contribuţilor din acest capitolul (Secţiunea 4.3) subliniază câteva aplicaţii ale rezultatelor dezvoltate în prima parte (Secţiunea 4.2). Există două aplicaţii principale discutate aici. Prima se referă la testul lui Galbraith pentru schema IBE a lui Cocks. Acest test a fost descris pe scurt în mai multe lucrări precum [58, 31, 148], dar unele

afirmaţii nu au fost riguros formulate şi/sau demonstrate. Pe baza rezultatelor dezvoltate în Secţiunea 4.2, am putut face o analiză riguroasă a unor distribuţii ce se regăsesc în schema IBE a lui Cocks şi testul lui Galbraith, oferind astfel o analiză completă a testului Galbraith.

A doua aplicaţie discutată în Secţiunea 4.3 se referă la indistingibilitatea computaţională, presupunând dificultatea problemei reziduurilor pătratice, a unor distribuţii din [31, 76, 148]. Pe baza rezultatelor dezvoltate în Secţiunea 4.2, am putut demonstra indistingibilitatea statistică a acestor distribuţii (fără nicio presupunere computaţională).

Pe lângă aplicaţiile menţionate deja în Secţiunea 4.3, credem că studiul nostru din Secţiunea 4.2 este important şi pentru că contribuie la o mai bună înţelegere a structurii mulţimii $\mathbb{Z}_n^*$ în ceea ce priveşte şabloanele de lungime Jacobi cel mult doi, care sunt frecvent utilizate în criptografie.

Capitolul 5

Atacuri Cleptografice

Deoarece din ce în ce mai multe ţări solicită persoanelor fizice şi furnizorilor să predea parolele şi cheile de decriptare [22], am putea observa o creştere a utilizării *canalelor subliminale*. Canalele subliminale sunt canale secundare de comunicare ascunse în interiorul unui canal de comunicare potenţial compromis. Conceptul a fost introdus de Simmons [226, 227, 228] ca soluţie la *problema prizonierilor*. Problema prizonierilor este următoarea: *Alice* şi *Bob* sunt închişi şi doresc să comunice confidenţial şi nedetectaţi de gardianul lor *Walter* care le impune să citească toate comunicările lor. Reţineţi că *Alice* şi *Bob* pot schimba o cheie secretă înainte de a fi încarceraţi.

Modelele clasice de securitate presupun că algoritmii criptografici dintr-un dispozitiv sunt implementaţi corect şi conform specificaţiilor tehnice. Din păcate, în lumea reală, utilizatorii au un control redus asupra criteriilor de proiectare sau asupra implementării unui modul de securitate. Când foloseşte un dispozitiv hardware, de exemplu un smartcard, utilizatorul presupune implicit că producătorul este onest şi că acesta construieşte dispozitivele conform specificaţiilor furnizate. Ideea unui producător maliţios care deviază de la specificaţiile dispozitivului sau încorporează un backdoor într-o implementare a fost sugerată mai întâi de Young şi Yung [261, 262]. Pentru a demonstra fezabilitatea conceptului, au dezvoltat atacurile de tip *secretly embedded trapdoor with universal protection* (SETUP). Aceste atacuri combină canale subliminale şi criptografia cu cheie publică pentru a recupera în mod neautorizat cheia privată a unui utilizator sau un mesaj. Young şi Yung au presupus un mediu de tip black-box[1], menţionând în acelaşi timp existenţa altor scenarii. Menţionăm că distribuţiile de intrare şi ieşire ale unui dispozitiv cu un mecanism SETUP nu ar trebui să se distingă de distribuţia obişnuită. Cu

[1] Un black-box este un dispozitiv, proces sau sistem, ale cărui intrări şi ieşiri sunt cunoscute, dar structura sa internă sau funcţionarea sa nu sunt cunoscute sau accesibile utilizatorului (*e.g.* dispozitive tamper proof).

toate acestea, dacă dispozitivul este reverse engineered, mecanismul implementat poate fi detectat.

Deşi atacurile de tip SETUP au fost considerate impractice de unii criptografi, evenimentele recente [36, 205] sugerează altfel. În consecinţă, acest domeniu de cercetare pare să fi fost revitalizat [32, 45, 94, 214]. În [47], atacurile de tip SETUP implementate în scheme de criptare simetrice sunt denumite *atacuri de substituţie algoritmică* (ASA). Autorii [47] subliniază faptul că gradul ridicat al complexităţii software-ului open-source (*e.g.* OpenSSL) şi numărul redus de experţi care le revizuiesc fac ASA-urile plauzibile nu numai în modelul black-box. ASA-urile în cazul simetric sunt studiate în continuare în [45, 88] şi, în cazul funcţiilor hash, în [28]. O legătură între *steganografia cu chei simetrice* şi ASA poate fi găsită în [53].

Un exemplu practic de recuperare neautorizată a cheiilor unui utilizator este generatorul Dual-EC, un generator de numere pseudo-aleatoare sigur din punct de vedere criptografic standardizat de NIST. Documentele interne NSA dezvăluite de Edward Snowden [36, 205] indicau un backdoor încorporat în generatorul Dual-EC. După cum sa menţionat în [54], utilizarea generatorului Dual-EC facilitează o terţă parte să recupereze cheia privată a unui utilizator. Un astfel de atac este o aplicaţie naturală a atacurilor prezentate de Young şi Yung. Câteva exemple de atacuri SETUP din lumea reală pot fi găsite în [70, 69]. Bazându-se pe lucrările anterioare [250] şi influenţate de incidentul Dual-EC, [94, 89] oferă cititorilor un cadru formal al generatoarelor de numere pseudo-aleatoare (PRNG).

Un model mai general intitulat *subversion attack* este luat în considerare în [32]. Acest model include atacurile SETUP şi ASA-uri, dar sunt incluse şi atacuri generice de tip malware şi viruşii. Autorii oferă scheme de semnături rezistente la subversiune în modelul propus. Munca lor este extinsă în continuare în [214, 215], unde sunt furnizate soluţii rezistente la subversiune pentru funcţii one-way, scheme de semnături şi PRNG-uri. În [214], autorii subliniază că modelul din [32] presupune că parametrii sistemului sunt generaţi corect (dar acest lucru nu este întotdeauna adevărat). În cazul logaritmului discret, exemple de algoritmi pentru generarea numerelor prime cu backdoor-uri incorporate pot fi găsite în [126, 110].

O metodă diferită pentru protejarea utilizatorilor împotriva atacurilor de subversiune sunt *cryptographic reverse firewalls* (RF). RF reprezintă dispozitive externe de încredere care sanitizează ieşirile aparatelor infectate. Conceptul a fost introdus în [184, 96]. Un RF pentru schemele de semnături este furnizat în [32].

5.1 Atacuri Cleptografice Partajate

În această secţiune, extindem atacurile SETUP introduse Young şi Yung asupra semnăturilor digitale. Introducem primul mecanism SETUP care recuperează cheia secretă a unui utilizator, numai dacă părţile maliţioase decid să facă acest lucru. Presupunem că schemele de semnături sunt implementate într-un black-box echipat cu o memorie volatilă, ştearsă ori de câte ori cineva încearcă să o acceseze.

În cele ce urmează oferim câteva exemple în care poate fi utilă o semnătură cleptografică partajată.

Deoarece documentele semnate digital sunt la fel din punct de vedere legal ca semnăturile pe hârtie, dacă un destinatar primeşte un document semnat de A el va acţiona conform instrucţiunilor lui A. Găsirea cheii private a lui A poate ajuta o agenţie de aplicare a legii să colecteze informaţii suplimentare despre A şi anturajul său. Pentru a proteja cetăţenii de abuzuri, un mandat trebuie emis de o comisie juridică înainte de a începe supravegherea. Pentru a ajuta comisia şi pentru a preveni abuzul, producătorul dispozitivului A poate implementa un mecanism SETUP partajat ℓ din n. Astfel, cheia A poate fi recuperată numai dacă există un cvorum în favoarea emiterii mandatului.

Monedele digitale (*e.g.* Bitcoin) au devenit o alternativă populară la monedele fizice. Tranzacţiile între utilizatori se bazează pe semnături digitale. Când se efectuează o tranzacţie, cheia publică a destinatarului este strâns legată de banii transferaţi. Numai proprietarul cheii secrete poate cheltui banii. Pentru a-şi proteja cheile secrete, utilizatorul poate alege să le stocheze într-un dispozitiv tamper proof, numit portofel hardware. Să presupunem că un grup de entităţi maliţioase reuşeşte să infecteze unele portofele hardware şi implementează un mecanism SETUP partajat ℓ din n. Când ℓ membrii decid, ei pot transfera banii din portofelele infectate fără ştirea proprietarului. Dacă $\ell - 1$ părţi sunt arestate, mecanismul rămâne nedetectabil atât timp cât dispozitivele nu sunt reverse engineered.

În conformitate cu lucrările iniţiale, demonstrăm că mecanismele SETUP partajate nu se pot distinge computaţional de semnăturile obişnuite. În funcţie de semnătura infectată, obţinem securitate în modelul standard sau random oracle (ROM). Pentru obţine acest lucru, folosim o schemă de criptare cu cheii publice (introdusă în Secţiunea 3.5.2) şi schema de partajare a secretelor introdusă de Shamir [221]. Demonstraţiile de securitate în ROM sunt uşor de dedus din demonstraţiile standard de securitate furnizate în acestă secţiune. Astfel, acestea sunt omise.

5.2 Metode Cliptografice Generice

Modelul iniţial propus de Young şi Yung este modelul black-box. Pentru scopurile noastre, acest model este suficient, deoarece protocoalele de tip zero-knowledge pe care le atacăm au fost concepute pentru smartcard-uri. O proprietate importantă este că smartcard-urile infectate ar trebui să aibă intrări şi ieşiri indistingibile de smartcard-urile obişnuite. Cu toate acestea, dacă smartcard-ul este reverse engineered, mecanismul implementat poate fi detectat.

Există două metode pentru a încorpora backdoor-uri într-un sistem: fie prin generarea unor parametri publici speciali (SPP), fie prin infectarea numerele aleatorii (IRN) utilizate de sistem. În cazul sistemelor bazate pe logaritmul discret, SPP şi IRN au fost studiate în [261, 262, 263, 264, 126, 110]. În cazul sistemelor bazate pe factorizare am găsit SPP [83, 261, 262, 265, 264] şi nu IRN.

Folosind acelaşi nivel de abstractizare ca în [176], arătăm cum un atacator (numit *Mallory*) poate introduce un backdoor în protocolul UZK şi poate extrage secretul lui *Peggy*. Când este instanţiat, acest atac oferă o nouă perspectivă asupra atacurilor SETUP. În special, oferim primul atac IRN asupra unui sistem bazat pe factorizare şi primul atac asupra sistemelor construite cu ajutorul reprezentărilor bazate pe radacini de ordinul e. De asemenea, oferim cititorului noi instanţieri ale protocolului unificat al lui Maurer: protocolul Girault, o nou protocol de tip proof of knowledge pentru reprezentări bazate pe logaritmul discret în $\mathbb{Z}_n^*$ şi un protocol bazat pe radacini de ordinul e.

Al doilea atac SETUP pe care îl introducem este o generalizare a atacului introdus de Young şi Yung. Când este instanţiat cu protocolul Schnorr, obţinem rezultatele acestora. De asemenea, oferim alte exemple nementionate de Young şi Yung.

5.3 Abonamente Cleptografice

Unul dintre modelele clasice de afaceri pentru atacurile cleptografice este următorul: un client[2] C plăteşte în avans un producător M, care ulterior va implementa un anumit backdoor într-un dispozitiv tamper proof şi va livra dispozitivul respectiv unei victime. Acest model oferă producătorul un avantaj, deoarece acesta poate taxa clientul fără a implementa backdoor-ul solicitat. Deoarece această tranzacţie este ilegală, clientul nu poate depune plângere şi nu îşi poate recupera legal banii. Astfel, acest lucru ar putea speria unii dintre potenţialii clienţi.

[2] prin definiţie o entitate maliţioasă

Un alt model clasic este următorul: un client plăteşte în avans producătorului jumătate din bani şi restul după ce a verificat corectitudinea backdoor-ului. Dacă producătorul nu ia anumite măsuri de precauţie, atunci clientul este în avantaj. De exemplu, C verifică corectitudinea backdoor-ului, dar nu mai plăteaşte a doua tranşă. Acest lucru poate fi uşor evitat dacă o metodă de dezactivare a backdoor-ului este implementată in M[3]. O posibilă strategie de dezactivare este ca M să trimită către D un input special care instruieşte dispozitivul să şteargă toate probele incriminatoare. O abordare similară este utilizată în [88, 109] pentru a declanşa backdoor-urile.

Ambele abordări clasice prezintă un risc inerent pentru producător: clientul poate dovedi cu uşurinţă că M a implementat în D un backdoor fie prin decriptarea tuturor mesajelor trimise prin dispozitivul respectiv, fie prin dezvăluirea cheilor private stocate în D. Astfel, pentru a produce profit în pofida riscurilor, producătorul trebuie să îi perceapă lui C o taxă mare de încorporare. Acest lucru va speria cu siguranţă anumiţi clienţi constrânşi de resurse (*i.e.* întreprinderi mici care nu au resursele unei mari corporaţii). Pentru a rezolva această problemă, introducem un model bazat pe abonamente adecvat algoritmului de criptare ElGamal.

Modelul nostru se inspiră din serviciile de streaming oferite de companii precum Netflix [6], Amazon [7] şi HBO [8]. Aceste companii oferă acces la conţinutul de streaming în schimbul unei plăţi lunare. În cazul nostru, un client plăteşte pentru un backdoor care îi oferă acces la un număr limitat de mesaje private. Ulterior, clientul trebuie să îşi reînnoiască abonamentul. Acest lucru echilibrează profitul şi factorii de risc pentru producător[4] şi, în consecinţă, M poate reduce taxele de încorporare. Rămâne totuşi un risc: nu există garanţii de livrare a produselor pentru clienţi. Dar acest lucru este minimizat într-un model bazat pe abonament, deoarece obiectivul producătorului este de a menţine clienţii mulţumiţi, astfel încât aceştia să îşi reînnoiască abonamentul[5].

În comparaţie cu modelele clasice, modelul nostru propus are o problemă diferită care trebuie abordată. Clienţii doresc acces la serviciile lor imediat ce plătesc. Dar, tranzacţiile ilegale folosesc în cea mai mare parte criptomonede [75], iar timpul mediu de confirmare pentru acest tip de tranzacţii este mare în unele cazuri (*i.e.* pentru Bitcoin, durează în medie o oră pentru a confirma o tranzacţie [2]). Astfel, pentru a oferi producătorului suficient timp pentru a dezactiva backdoor-ul[6] dacă tranzacţia nu este validă, folosim un mecanism similar cu time-lock puzzles [213].

[3] La fel ca în modelul anterior, tranzacţia este ilegală şi, prin urmare, M nu poate lua măsuri legale împotriva lui C.

[4] M este expus doar pentru o perioadă limitată de timp

[5] Înşelarea unui client va aduce lui M o sumă mică de venituri.

[6] prin intermediul unor mecanisme speciale

Reţineţi că contramăsurile cleptografice generice [214, 215, 135] pot proteja utilizatorii dispozitivului tamper-proof împotriva mecanismelor propuse. Din păcate, cu excepţia cazului în care utilizatorii solicită în mod explicit implementarea acestor mijloace de apărare, producătorul nu este obligat să le implementeze. Astfel, M este liber să implementeze orice mecanism cleptografic.

5.4 Canale Hash

Majoritatea canalelor subliminale sau a atacurilor de tip SETUP folosesc numere aleatorii pentru a transmite informații nedetectate. În consecință, toate contramăsurile propuse se concentrează pe igienizarea numerelor aleatorii utilizate de un sistem. În cazul semnăturilor digitale, o metodă diferită, dar laborioasă pentru inserarea unui canal subliminal într-un sistem este prezentată în [256]. În loc să folosească numerele aleatoare ca purtători de informație, *Alice* folosește hash-ul mesajului pentru a transmite mesajul pentru *Bob*. Pentru a realiza acest lucru, *Alice* face mici modificări la mesaj până când hash-ul are proprietățile dorite. Menţionăm că metoda prezentată în [256] ocolește toate contramăsurile menționate până acum.

Această secțiune studiază o metodă generică care permite prizonierilor să comunice prin semnăturile electronice protejate împotriva canalelor subliminale găsite în [214, 215, 73, 135, 32, 57]. Pentru a ne atinge obiectivul, lucrăm într-un scenariu în care tuturor mesajelor li se aplică un timestamp înaintea semnării. Rețineți că nu încălcăm niciuna dintre ipotezele făcute de propunerile anti-subversiune. Această secţiune este motivată de faptul că majoritatea utilizatorilor nu verifică afirmațiile făcute de producători[7]. Mai mult, utilizatorii nu știu adesea care ar trebui să fie output-urile unui dispozitiv [163]. Un incident notabil în care utilizatorii care nu știau output-urile corecte și au avut încredere în dezvoltatori este incidentul Debian [50].

[7] Producătorii ar putea implementa semnături anti-subversiune doar în scopuri de marketing, în timp ce continuă să infecteze unele dintre dispozitivele produse.

Capitolul 6

Generatoare de Numere (Pseudo-)Aleatoare

Unul dintre elementele esenţiale ale criptografiei sunt generatoarele de numere aleatoare. În special, pentru asigurarea confidenţialităţii sau autenticităţii este vital ca cheile criptografice să fie generate aleatoriu. În plus, majoritatea algoritmilor criptografici sunt randomizaţi.

Generarea numerelor aleatoare prin intermediul proceselor fizice este de obicei consumatoare de timp şi costisitoare, astfel în practică majoritatea aplicaţiilor folosesc generatoare de numere pseudo-aleatoare. Un astfel de generator este un algoritm determinist care primeşte ca input un seed aleatoriu de dimensiuni reduse şi generează o secvenţă de biţi mult mai lungă. Nu toate PRNG-urile sunt potrivite pentru aplicaţii criptografice. Un astfel de exemplu este generatorul folosit de Adobe Flash Player. Unele dintre cerinţele de bază ale securităţii PRNG-urilor sunt: să nu poată fi distins de un RNG real şi să nu se poată recupera starea sa internă pornind de la output-ul său. În prima parte a acestui capitol descriem un algoritm de recuperare a seed-ului pentru Flash Player PRNG.

O metodă populară pentru generarea cheilor criptografice sau a altor input-uri aleatorii este de a avea un pool de entropie care acumulează date dintr-o sursă fizică de zgomot şi un PRNG care îşi updatează periodic starea internă din pool şi produce date cu o rată constantă. Pentru a asigura o funcţionare corectă, înainte de a adăuga date la pool-ul de entropie, acestea se testează statistic. În a doua parte a acestui capitol vom studia o posibilă arhitectură pentru adăugarea datelor în pool. Mai precis, oferim cititorului rezultate experimentale şi un model teoretic pentru arhitectura propusă.

6.1 Flash Player PRNG

Compilatoarele JIT (*e.g.* JavaScript și ActionScript) translatează codul sursă sau bytecode-ul în cod mașină la runtime pentru o execuție mai rapidă. Datorită faptului că scopul compilatoarelor JIT este de a produce date executabile, acestea sunt în mod normal ignorate de mecanismele de tip data execution prevention (DEP[1]) . Astfel, o vulnerabilitate într-un compilator JIT ar putea duce la un exploit nedetectabil de către DEP. Un astfel de atac, numit JIT spraying, a fost propus în [56]. Prin coruperea motorului ActionScript JIT, Blazakis arată cum pot fi scrise instrucţiuni de tip shellcode în memoria executabilă, astfel ocolind mecanismul DEP. Informația cheie este că compilatorul JIT este previzibil și trebuie să copieze unele constante în memoria executabilă. Prin urmare, aceste constante pot codifica instrucțiuni mici și apoi pot controla fluxul către locația următoarei constante.

Pentru a apăra sistemele împotriva atacurilor de tip JIT spraying, Adobe folosește o tehnică numită *constant blinding*. Această metodă împiedică un atacator să își încarce instrucțiunile în constante și astfel blochează rularea scriptului său maliţios. Ideea de la baza constant blinding-ului este de a evita stocarea constantelor în memorie în forma lor originală. În schimb, acestea sunt mai întâi mascate cu un cookie secret generat aleatoriu și apoi stocate în memorie. Dacă cookie-ul secret este generat prin intermediul unei PRNG slab criptografic[2], atacatorul își recapătă capacitatea de a injecta instrucțiuni maliţioase.

În loc să folosească un PRNG demonstrat sigur, designerii Flash Player au încercat să își proiecteze propriul PRNG. Din păcate, în [253, 1] se arată că designul generatorului este defectuos. În [1] este implementat un atac de tip forță brută, în timp ce în [253] este prezentat un atac de tip forță brută mai eficient. Aceste rezultate au fost raportate către Adobe sub codul CVE-2017-3000 [21], iar vulnerabilitatea a fost reparată în versiunea 25.0.0.127.

În această secțiune, îmbunătăţim atacul prezentat în [253] de la o complexitate de timp de $\mathcal{O}(2^{21})$ la una de $\mathcal{O}(2^{11})$. De asemenea, arătăm că, indiferent de parametrii utilizați de PRNG, defectul rămâne. Mai precis arătăm că pentru orice parametru cel mai slab atac de tip forță brută necesită $\mathcal{O}(2^{21})$ operațiuni. În [253] autorii nu prezintă algoritmul complet pentru inversarea PRNG-ului, în timp ce în [1] am găsit algoritmul complet, dar acesta nu a fost optimizat. Pentru completitudine, în Anexa K prezentăm și o versiune optimizată a algoritmului complet. Rețineți că în această secțiune ne concentrăm doar

[1] Mecanismul DEP efectuează verificări suplimentare asupra memoriei pentru a preveni rularea instrucţiunilor maliţioase în cadrul sistemului.

[2] *i.e.* seed-ul utilizat pentru a genera cookie-ul poate fi recuperat într-un timp rezonabil

pe Flash Player PRNG. Pentru mai multe detalii despre atacurile de tip JIT spraying și constant blinding, cititorul poate consulta [33, 56, 212, 253].

6.2 Amplificatoare de Bias

În [264] autorii propun un mecanism interesant care estompează linia dintre ceea ce constituie un troian şi ceea ce nu. Pentru a le detecta mecanismul, un program trebuie să facă o diferenţă cumva între un generator de numere aleatoare (RNG) instabil în mod natural şi unul instabil artificial (obţinut prin intermediul unor transformări matematice). Din câte ştim, [264] este singura lucrare anterioară care discută acest subiect.

Mai exact, în [264] este descris un filtru digital. De obicei, filtrele digitale sunt aplicate RNG-urilor pentru a corecta bias-urile deja existente[3], dar acest filtru are un scop opus. Când este aplicat unor biţi distribuiţi uniform, filtrul este benign. Pe de altă parte, dacă este aplicat unor biţi cu un anumit bias, filtrul amplifică acest bias. Astfel, agravând proprietăţile negative ale RNG-ului.

În această secţiune extindem filtrul din [264][4], prezentăm o nouă clasă de filtre şi discutam câteva noi aplicaţii posibile. Atunci când proiectam un amplificator de bias, trebuie să respectam câteva reguli. Prima spune că, dacă biţii de intrare sunt uniform distribuiţi sau au bias-ul maxim (*i.e.* probabilitatea de a obţine 1 este fie 0, fie 1) filtrul trebuie să menţină bias-ul iniţial. Pentru biţii uniform distribuiţi, această regulă ascunde existenţa amplificatoarelor, atâta timp cât sursa de zgomot funcţionează în conformitate cu parametrii de proiectare iniţiali. Pentru bias maxim, regula este una funcţională. Deoarece RNG-ul este deja complet stricat, schimbarea bias-ului nu are sens (din punct de vedere al proiectării). A doua regulă afirmă că filtrul ar trebui să amplifice bias-ul în direcţia în care este deja. Această regulă îl ajută pe proiectant să amplifice bias-ul într-un mod mai uşor.

Principala aplicaţie pe care o propunem pentru aceste filtre este testarea RNG-urilor (*e.g.* îmbunătăţirea testele de tip health implementate într-un RNG). Standardele recente [158, 249] necesită ca un RNG să poată detecta posibilele defecţiunile şi o astfel de metodă pentru detectarea timpurie poate fi aplicarea unui amplificator şi apoi efectuarea unor teste statistice de tip lightweigh[5]. Pe baza rezultatelor obţinute în Secţiunile 6.2.2 şi 6.2.3, introducem o arhitectură generică pentru implementarea testelor de tip health în Secţiunea 6.2.4.1. Mai precis, aplicând un test de tip lightweight pe biţii amplificaţi,

[3] Se numesc extractoare de numere aleatoare [95].

[4] Filtrul prezentat în [264] corespunde amplificatorului de tip greedy cu parametrul $n = 3$ descris în Secţiunea 6.2.2 .

[5] de exemplu testele descrise în [134]

arhitectura poate detecta abateri de la distribuţia uniformă. Pentru a valida arhitectura noastră, am efectuat mai întâi o serie de experimente pe RNG-uri care generează biţi uniformi independenţi şi identic distribuiţi. Arătăm, de asemenea, că arhitectura noastră poate detecta abaterea de la parametrii iniţiali ai sursei u.i.i.d. În Secţiunea 6.2.5 extindem rezultatele preliminare la sursele de zgomot care au o distribuţie Bernoulli şi arătăm că arhitectura poate detecta, începând din faza de proiectare, sursele grav deviate. Pentru a ne susţine rezultatele, dezvoltăm un model teoretic şi oferim cititorului simulări bazate pe modelul nostru. Menţionăm că modelul nostru teoretic explică, de asemenea, de ce arhitectura noastră poate detecta abaterile de la parametrii iniţiali.

Datorită evenimentelor recente [36, 205, 50, 69] RNG-urile au fost supuse examinărilor publice. Astfel, întrebarea ce tip de mecanisme pot fi puse în aplicare de către o terţă parte maliţioasă pentru a slăbi sau destabiliza un sistem devine naturală. Filtrele de amplificare sunt un posibil mod în care se poate realiza acest lucru. Pe baza mecanismelor de detectare a defecţiunilor propuse în Secţiunea 6.2.4.1, arătăm, de exemplu, modul în care un producător poate manipula arhitectura pentru a deveni maliţioasă.

Capitolul 7

Criptografie Recreaţională

În acest capitol analizăm securitatea unei serii de probleme care pot fi văzute ca jocuri abstracte. Motivaţia noastră principală pentru studierea unor astfel de protocoale este utilitatea lor pedagogică. Menţionăm că nu suntem conştienţi de nicio aplicaţie reală de orice fel. Mai precis, aceste probleme se încadrează în categoria "criptografiei recreaţionale". Deşi recreaţionale, aceste protocoale pot oferi informaţii şi tehnici interesante care pot fi utile pentru înţelegerea conceptelor de bază pe care se bazează aceste protocoale.

Criptografia fizică [130, 44, 191, 218] foloseşte proprietăţile fizice ale sistemelor pentru criptarea şi/sau schimbul de informaţii (*i.e.* fără a utiliza funcţii unidirecţionale). Deşi sunt un instrument didactic foarte interesant, se poate demonstra că unele dintre metodele propuse nu sunt sigure în practică. Astfel, scopul nostru este de a ataca astfel de protocoale fizice folosind metode similare tehnicilor de tip side-channel.

Pe lângă utilitatea pedagogică evidentă, credem că unele dintre schemele abordate în capitolul actual pot fi utilizate cu succes pentru introducerea conceptelor corespunzătoare altor domenii. Oferim cititorului astfel de exemple în următoarele secţiuni.

Deşi unii autori recunosc că protocoalele lor propuse sunt utile doar pentru a se juca cu copiii sau pentru a introduce noi concepte publicului non-tehnic, autorii articolelor [129, 130, 128, 225] susţin că schemele lor pot fi implementate în siguranţă în mod real. În [81], Courtois atacă unul dintre protocoalele propuse în [129], dar autorii contestă rezultatele sale în [130]. Am efectuat în mod independent o simulare a atacului şi rezultatele noastre confirmă afirmaţia lui Courtois.

Bibliografie

[1] A Full Exploit of CVE-2017-3000 on Flash Player Constant Blinding PRNG. https://github.com/dangokyo/CVE-2017-3000/blob/master/Exploiter.as.

[2] Bitcoin: Average Confirmation Time. https://www.blockchain.com/charts/avg-confirmation-time.

[3] C++ Random Library. www.cplusplus.com/reference/random/.

[4] eSTREAM: the ECRYPT Stream Cipher Project. http://www.ecrypt.eu.org/stream/.

[5] Falstad Electronic Circuit. https://www.falstad.com.

[6] Frequently Asked Questions About Netflix Billing. https://help.netflix.com/en/node/41049?ui_action=kb-article-popular-categories.

[7] How to Manage Your Prime Video Channel Subscriptions. https://www.amazon.com/gp/help/customer/display.html?nodeId=201975160.

[8] How to Order HBO: Subscriptios & Pricing Options. https://www.hbo.com/ways-to-get.

[9] Kryptos. https://en.wikipedia.org/wiki/Kryptos.

[10] Left Shift and Right Shift Operators. https://docs.microsoft.com/en-us/cpp/cpp/left-shift-and-right-shift-operators-input-and-output?view=vs-2017.

[11] mbed TLS. https://tls.mbed.org.

[12] Mining Hardware Comparison. https://en.bitcoin.it/wiki/Mining_hardware_comparison.

[13] NIST SP 800-22: Download Documentation and Software. https://csrc.nist.gov/Projects/Random-Bit-Generation/Documentation-and-Software.

[14] Non-Specialized Hardware Comparison. https://en.bitcoin.it/wiki/Non-specialized_hardware_comparison.

[15] OpenMP. https://www.openmp.org/.

[16] Safe Prime Database. https://2ton.com.au/safeprimes/.

[17] Source Code for the Actionscript Virtual Machine. https://github.com/adobe-flash/avmplus/tree/master/core/MathUtils.cpp.

[18] The Diffie-Hellman Key Exchange Using Paint. https://www.youtube.com/watch?v=3QnD2c4Xovk.

[19] The GNU Multiple Precision Arithmetic Library. https://gmplib.org/.

[20] Using the GNU Compiler Collection. https://gcc.gnu.org/onlinedocs/gcc/Integers-implementation.html.

[21] Vulnerability Details: CVE-2017-3000. https://www.cvedetails.com/cve/CVE-2017-3000/.

[22] World Map of Encryption Laws and Policies. https://www.gp-digital.org/world-map-of-encryption/.

[23] FIPS PUB 186-4: Digital Signature Standard (DSS). Technical report, NIST, 2013.

[24] Michel Abdalla, Mihir Bellare, and Phillip Rogaway. DHAES: An Encryption Scheme Based on the Diffie-Hellman Problem. *IACR Cryptology ePrint Archive*, 1999/7, 1999.

[25] Michel Abdalla, Mihir Bellare, and Phillip Rogaway. The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES. In *CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 143–158. Springer, 2001.

[26] Carlisle Adams, Pat Cain, Denis Pinkas, and Robert Zuccherato. RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). Technical report, Internet Engineering Task Force, 2001.

[27] Gorjan Alagic and Alexander Russell. Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts. In *EUROCRYPT 2018*, volume 10212 of *Lecture Notes in Computer Science*, pages 65–93. Springer, 2017.

[28] Ange Albertini, Jean-Philippe Aumasson, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Malicious Hashing: Eve's Variant of SHA-1. In *SAC 2014*, volume 8781 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 2014.

[29] N. Asokan, Matthias Schunter, and Michael Waidner. Optimistic Protocols for Fair Exchange. In *CCS 1997*, pages 7–17. ACM, 1997.

[30] American Bankers Association et al. Working Draft: American National Standard X9. 62-1998 Public Key Cryptography for the Financial Services Industry. Technical report, 1998.

[31] Giuseppe Ateniese and Paolo Gasti. Universally Anonymous IBE Based on the Quadratic Residuosity Assumption. In *CT-RSA 2009*, volume 5473 of *Lecture Notes in Computer Science*, pages 32–47. Springer, 2009.

[32] Giuseppe Ateniese, Bernardo Magri, and Daniele Venturi. Subversion-Resilient Signature Schemes. In *CCS 2015*, pages 364–375. ACM, 2015.

[33] Michalis Athanasakis, Elias Athanasopoulos, Michalis Polychronakis, Georgios Portokalidis, and Sotiris Ioannidis. The Devil is in the Constants: Bypassing Defences in Browser JIT Engines. In *NDSS 2015*. The Internet Society, 2015.

[34] Jean-Philippe Aumasson, Itai Dinur, Luca Henzen, Willi Meier, and Adi Shamir. Efficient FPGA Implementations of High-Dimensional Cube Testers on the Stream Cipher Grain-128. *IACR Cryptology ePrint Archive*, 2009/218, 2009.

[35] Shahram Bakhtiari, Reihaneh Safavi-Naini, and Josef Pieprzyk. A Message Authentication Code Based on Latin Squares. In *ACISP 1997*, volume 1270 of *Lecture Notes in Computer Science*, pages 194–203. Springer, 1997.

[36] James Ball, Julian Borger, and Glenn Greenwald. Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security. *The Guardian*, 6, 2013.

[37] József Balogh, János A Csirik, Yuval Ishai, and Eyal Kushilevitz. Private Computation Using a PEZ Dispenser. *Theoretical Computer Science*, 306(1-3):69–84, 2003.

[38] Subhadeep Banik, Subhamoy Maitra, and Santanu Sarkar. Some Results on Related Key-IV Pairs of Grain. In *SPACE 2012*, volume 7644 of *Lecture Notes in Computer Science*, pages 94–110. Springer, 2012.

[39] Subhadeep Banik, Subhamoy Maitra, Santanu Sarkar, and Turan Meltem Sönmez. A Chosen IV Related Key Attack on Grain-128a. In *ACISP 2013*, volume 7959 of *Lecture Notes in Computer Science*, pages 13–26. Springer, 2013.

[40] Manuel Barbosa, Thierry Brouard, Stéphane Cauchie, and Simao Melo De Sousa. Secure Biometric Authentication with Improved Accuracy. In *ACISP 2008*, volume 5107 of *Lecture Notes in Computer Science*, pages 21–36. Springer, 2008.

[41] Craig Bauer, Gregory Link, and Dante Molle. James Sanborn's Kryptos and the Matrix Encryption Conjecture. *Cryptologia*, 40(6):541–552, 2016.

[42] Craig Bauer and Katherine Millward. Cracking Matrix Encryption Row by Row. *Cryptologia*, 31(1):76–83, 2007.

[43] Friedrich Ludwig Bauer. *Decrypted Secrets: Methods and Maxims of Cryptology*. Springer, 2002.

[44] Tim Bell, Harold Thimbleby, Mike Fellows, Ian Witten, Neil Koblitz, and Matthew Powell. Explaining Cryptographic Systems. *Computers & Education*, 40(3):199–215, 2003.

[45] Mihir Bellare, Joseph Jaeger, and Daniel Kane. Mass-Surveillance without the State: Strongly Undetectable Algorithm-Substitution Attacks. In *CCS 2015*, pages 1431–1440. ACM, 2015.

[46] Mihir Bellare, Chanathip Namprempre, and Gregory Neven. Security Proofs for Identity-Based Identification and Signature Schemes. *Journal of Cryptology*, 22(1):1–61, 2009.

[47] Mihir Bellare, Kenneth G. Paterson, and Phillip Rogaway. Security of Symmetric Encryption Against Mass Surveillance. In *CRYPTO 2014*, volume 8616 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 2014.

[48] Mihir Bellare and Phillip Rogaway. Minimizing the Use of Random Oracles in Authenticated Encryption Schemes. In *ICICS 1997*, volume 1334 of *Lecture Notes in Computer Science*, pages 1–16. Springer, 1997.

[49] Mihir Bellare and Phillip Rogaway. Introduction to Modern Cryptography. https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf, 2005.

[50] Luciano Bello. DSA-1571-1 OpenSSL—Predictable Random Number Generator. https://www.debian.org/security/2008/dsa-1571, 2008.

[51] Fabrice Benhamouda, Javier Herranz, Marc Joye, and Benoît Libert. Efficient Cryptosystems from 2^k-th Power Residue Symbols. *Journal of Cryptology*, 30(2):519–549, 2017.

[52] Côme Berbain, Henri Gilbert, and Alexander Maximov. Cryptanalysis of Grain. In *FSE 2006*, volume 4047 of *Lecture Notes in Computer Science*, pages 15–29. Springer, 2006.

[53] Sebastian Berndt and Maciej Liśkiewicz. Algorithm Substitution Attacks from a Steganographic Perspective. In *CCS 2017*, pages 1649–1660. ACM, 2017.

[54] Daniel J. Bernstein, Tanja Lange, and Ruben Niederhagen. Dual EC: A Standardized Back Door. In *The New Codebreakers*, volume 9100 of *Lecture Notes in Computer Science*, pages 256–281. Springer, 2016.

[55] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In *CRYPTO 1990*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1991.

[56] Dionysus Blazakis. Interpreter Exploitation. In *WOOT 2010*. USENIX Association, 2010.

[57] Jens-Matthias Bohli, Maria Isabel Gonzalez Vasco, and Rainer Steinwandt. A subliminal-free variant of ECDSA. In *IH 2006*, volume 4437 of *Lecture Notes in Computer Science*, pages 375–387. Springer, 2006.

[58] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public Key Encryption with Keyword Search. In *EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 506–522. Springer, 2004.

[59] Dan Boneh and Matthew K. Franklin. Identity-Based Encryption from the Weil Pairing. In *CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.

[60] Dan Boneh, Craig Gentry, and Michael Hamburg. Space-efficient Identity Based Encryption Without Pairings. In *FOCS 2007*, pages 647–657. IEEE Computer Society, 2007.

[61] Julien Bringer, Hervé Chabanne, Malika Izabachéne, David Pointcheval, Qiang Tang, and Sébastien Zimmer. An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication. In *ACISP 2007*, pages 96–106. Springer, 2007.

[62] Xavier Bultel, Jannik Dreier, Pascal Lafourcade, and Malika More. How to explain modern security concepts to your children. *Cryptologia*, 41(5):422–447, 2017.

[63] Christian Cachin and Jan Camenisch. Optimistic Fair Secure Computation. In *CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 93–111. Springer, 2000.

[64] Christophe Cannière, Özgül Küçük, and Bart Preneel. Analysis of Grain's Initialization Algorithm. In *AFRICACRYPT 2008*, volume 5023 of *Lecture Notes in Computer Science*, pages 276–289. Springer, 2008.

[65] Anne Canteaut, Pascale Charpin, and Hans Dobbertin. Weight Divisibility of Cyclic Codes, Highly Nonlinear Functions on F_{2^m}, and Crosscorrelation of Maximum-Length Sequences. *SIAM J. Discrete Math.*, 13(1):105–138, 2000.

[66] Héctor Martín Cantero, Sven Peter, and Segher Bushing. Console Hacking 2010–PS3 Epic Fail. In *27th Chaos Communication Congress*, 2010.

[67] Charalambos A Charalambides. *Enumerative Combinatorics*. Chapman and Hall/CRC, 2002.

[68] David Chaum, Jan-Hendrik Evertse, and Jeroen Van De Graaf. An Improved Protocol for Demonstrating Possession of Discrete Logarithms and Some Generalizations. In *EUROCRYPT 1987*, volume 304 of *Lecture Notes in Computer Science*, pages 127–141. Springer, 1987.

[69] Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Joshua Fried, Shaanan Cohney, Matthew Green, Nadia Heninger, Ralf-Philipp Weinmann, Eric Rescorla, and Hovav Shacham. A Systematic Analysis of the Juniper Dual EC Incident. In *CCS 2016*, pages 468–479. ACM, 2016.

[70] Stephen Checkoway, Ruben Niederhagen, Adam Everspaugh, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, Hovav Shacham, and Matthew Fredrikson. On the Practical Exploitability of Dual EC in TLS Implementations. In *USENIX Security Symposium*, pages 319–335. USENIX Association, 2014.

[71] Liqun Chen, Caroline Kudla, and Kenneth G. Paterson. Concurrent Signatures. In *EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 287–305. Springer, 2004.

[72] Benoît Chevallier-Mames. An Efficient CDH-Based Signature Scheme with a Tight Security Reduction. In *CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 511–526. Springer, 2005.

[73] Jong Youl Choi, Philippe Golle, and Markus Jakobsson. Tamper-Evident Digital Signature Protecting Certification Authorities Against Malware. In *DASC 2006*, pages 37–44. IEEE, 2006.

[74] Jae Cha Choon and Jung Hee Cheon. An Identity-Based Signature from Gap Diffie-Hellman Groups. In *PKC 2003*, volume 2567 of *Lecture Notes in Computer Science*, pages 18–30. Springer, 2003.

[75] Nicolas Christin. Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. In *WWW 2013*, pages 213–224. ACM, 2013.

[76] Michael Clear, Hitesh Tewari, and Ciarán McGoldrick. Anonymous IBE from Quadratic Residuosity with Improved Performance. In *AFRICACRYPT 2014*, volume 8469 of *Lecture Notes in Computer Science*, pages 377–397. Springer, 2014.

[77] Clifford Cocks. An Identity Based Encryption Scheme Based on Quadratic Residues. In *IMACC 2001*, volume 2260 of *Lecture Notes in Computer Science*, pages 360–363. Springer, 2001.

[78] Simon Cogliani, Bao Feng, Houda Ferradi, Rémi Géraud, Diana Maimuţ, David Naccache, Rodrigo Portella do Canto, and Guilin Wang. Public Key-Based Lightweight Swarm Authentication. In *Cyber-Physical Systems Security*, pages 255–267. Springer, 2018.

[79] Josh Cohen and Michael Fischer. A Robust and Verifiable Cryptographically Secure Ellection Scheme (extended abstract). In *FOCS 1985*, pages 372–382. IEEE Computer Society Press, 1985.

[80] Mariana Costiuc, Diana Maimuţ, and George Teşeleanu. Physical Cryptography. In *SECITC 2019*, volume 12001 of *Lecture Notes in Computer Science*, pages 156–171. Springer, 2019.

[81] Nicolas T. Courtois. Cryptanalysis of Grigoriev-Shpilrain Physical Asymmetric Scheme With Capacitors. *IACR Cryptology ePrint Archive*, 2013/302, 2013.

[82] Richard Crandall and Carl Pomerance. *Prime Numbers: A Computational Perspective*. Number Theory and Discrete Mathematics. Springer, 2005.

[83] Claude Crépeau and Alain Slakmon. Simple Backdoors for RSA Key Generation. In *CT-RSA 2003*, volume 2612 of *Lecture Notes in Computer Science*, pages 403–416. Springer, 2003.

[84] Paul Crowley. Mirdek: A Card Cipher Inspired by "Solitaire". http://www.ciphergoth.org/crypto/mirdek/.

[85] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer Science & Business Media, 2013.

[86] Harold Davenport. On the Distribution of Quadratic Residues (mod p). *Journal of the London Mathematical Society*, s1-6(1):49–54, 1931.

[87] Harold Davenport. On the Distribution of Quadratic Residues (mod p). *Journal of the London Mathematical Society*, s1-8(1):46–52, 1933.

[88] Jean Paul Degabriele, Pooya Farshim, and Bertram Poettering. A More Cautious Approach to Security Against Mass Surveillance. In *FSE 2015*, volume 9054 of *Lecture Notes in Computer Science*, pages 579–598. Springer, 2015.

[89] Jean Paul Degabriele, Kenneth G. Paterson, Jacob CN Schuldt, and Joanne Woodage. Backdoors in Pseudorandom Number Generators: Possibility and Impossibility Results. In *CRYPTO 2016*, volume 9814 of *Lecture Notes in Computer Science*, pages 403–432. Springer, 2016.

[90] József Dénes and A Donald Keedwell. A New Authentication Scheme Based on Latin Squares. *Discrete Mathematics*, 106:157–161, 1992.

[91] Itai Dinur, Tim Güneysu, Christof Paar, Adi Shamir, and Ralf Zimmermann. An Experimentally Verified Attack on Full Grain-128 Using Dedicated Reconfigurable Hardware. In *ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 327–343. Springer, 2011.

[92] Itai Dinur and Adi Shamir. Breaking Grain-128 with Dynamic Cube Attacks. In *FSE 2011*, volume 6733 of *Lecture Notes in Computer Science*, pages 167–187. Springer, 2011.

[93] Hans Dobbertin. One-to-One Highly Nonlinear Power Functions on GF(2^n). *Appl. Algebra Eng. Commun. Comput.*, 9(2):139–152, 1998.

[94] Yevgeniy Dodis, Chaya Ganesh, Alexander Golovnev, Ari Juels, and Thomas Ristenpart. A Formal Treatment of Backdoored Pseudorandom Generators. In *EUROCRYPT 2015*, volume 9056 of *Lecture Notes in Computer Science*, pages 101–126. Springer, 2015.

[95] Yevgeniy Dodis, Rosario Gennaro, Johan Håstad, Hugo Krawczyk, and Tal Rabin. Randomness Extraction and Key Derivation Using the CBC, Cascade and HMAC Modes. In *CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 494–510. Springer, 2004.

[96] Yevgeniy Dodis, Ilya Mironov, and Noah Stephens-Davidowitz. Message Transmission with Reverse Firewalls—Secure Communication on Corrupted Machines. In *CRYPTO 2016*, volume 9814 of *Lecture Notes in Computer Science*, pages 341–372. Springer, 2016.

[97] Vasily Dolmatov and Alexey Degtyarev. GOST R 34.10-2012: Digital Signature Algorithm. Technical report, Internet Engineering Task Force, 2013.

[98] Morris Dworkin. Recommendation for Block Cipher Modes of Operation. Methods and Techniques. Technical report, NIST, 2001.

[99] Ibrahim Elashry, Yi Mu, and Willy Susilo. Jhanwar-Barua's Identity-Based Encryption Revisited. In *NSS 2014*, volume 8792 of *Lecture Notes in Computer Science*, pages 271–284. Springer, 2014.

[100] Ibrahim Elashry, Yi Mu, and Willy Susilo. An Efficient Variant of Boneh-Gentry-Hamburg's Identity-Based Encryption Without Pairing. In *WISA 2014*, volume 8909 of *Lecture Notes in Computer Science*, pages 257–268. Springer, 2015.

[101] Taher ElGamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[102] Ronald Fagin, Moni Naor, and Peter Winkler. Comparing Information Without Leaking It. *Communications of the ACM*, 39(5):77–85, 1996.

[103] Uriel Feige, Amos Fiat, and Adi Shamir. Zero-Knowledge Proofs of Identity. *Journal of Cryptology*, 1(2):77–94, 1988.

[104] Houda Ferradi, Rémi Géraud, Diana Maimuţ, David Naccache, and David Pointcheval. Legally Fair Contract Signing Without Keystones. In *ACNS 2016*, volume 9696 of *Lecture Notes in Computer Science*, pages 175–190. Springer, 2016.

[105] Houda Ferradi, Rémi Géraud, Diana Maimuţ, David Naccache, and Amaury de Wargny. Regulating the Pace of von Neumann Correctors. *Journal of Cryptographic Engineering*, pages 1–7, 2017.

[106] Amos Fiat. Batch RSA. In *CRYPTO 1989*, volume 435 of *Lecture Notes in Computer Science*, pages 175–185. Springer, 1989.

[107] Amos Fiat. Batch RSA. *J. Cryptology*, 10(2):75–88, 1997.

[108] Amos Fiat and Adi Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *CRYPTO 1986*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer, 1986.

[109] Marc Fischlin, Christian Janson, and Sogol Mazaheri. Backdoored Hash Functions: Immunizing HMAC and HKDF. *IACR Cryptology ePrint Archive*, 2018/362, 2018.

[110] Joshua Fried, Pierrick Gaudry, Nadia Heninger, and Emmanuel Thomé. A Kilobit Hidden SNFS Discrete Logarithm Computation. In *EUROCRYPT 2017*, volume 10210 of *Lecture Notes in Computer Science*, pages 202–231. Springer, 2017.

[111] Juan Garay, Philip MacKenzie, Manoj Prabhakaran, and Ke Yang. Resource Fairness and Composability of Cryptographic Protocols. In *TCC 2006*, volume 3876 of *Lecture Notes in Computer Science*, pages 404–428. Springer, 2006.

[112] Rosario Gennaro, Hugo Krawczyk, and Tal Rabin. Secure Hashed Diffie-Hellman over Non-DDH Groups. In *EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 361–381. Springer, 2004.

[113] Marc Girault. An Identity-based Identification Scheme Based on Discrete Logarithms Modulo a Composite Number. In *EUROCRYPT 1990*, volume 473 of *Lecture Notes in Computer Science*, pages 481–486. Springer, 1990.

[114] Marc Girault, Guillaume Poupard, and Jacques Stern. On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order. *Journal of Cryptology*, 19(4):463–487, 2006.

[115] Marc Girault and Jacques Stern. On the Length of Cryptographic Hash-Values Used in Identification Schemes. In *CRYPTO 1994*, volume 839 of *Lecture Notes in Computer Science*, pages 202–215. Springer, 1994.

[116] Danilo Gligoroski, Smile Markovski, and Svein Johan Knapskog. The Stream Cipher Edon80. In *New Stream Cipher Designs*, volume 4986 of *Lecture Notes in Computer Science*, pages 152–169. Springer, 2008.

[117] Danilo Gligoroski, Smile Markovski, and Ljupco Kocarev. Edon-R, An Infinite Family of Cryptographic Hash Functions. *I.J. Network Security*, 8(3):293–300, 2009.

[118] Eu-Jin Goh and Stanisław Jarecki. A Signature Scheme as Secure as the Diffie-Hellman Problem. In *EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 401–415. Springer, 2003.

[119] Dirk Goldhahn, Thomas Eckart, and Uwe Quasthoff. Building Large Monolingual Dictionaries at the Leipzig Corpora Collection: From 100 to 200 Languages. In *LREC 2012*, volume 29, pages 31–43. European Language Resources Association (ELRA), 2012.

[120] Oded Goldreich. *Foundations of Cryptography: Volume 1, Basic Tools*. Cambridge University Press, 2007.

[121] Shafi Goldwasser. Cocks' IBE Scheme. Bilinear Maps. MIT Lecture Notes: "6876: Advanced Cryptography", 2004.

[122] Shafi Goldwasser, Leonid Levin, and Scott A. Vanstone. Fair Computation of General Functions in Presence of Immoral Majority. In *CRYPT0 1990*, volume 537 of *Lecture Notes in Computer Science*, pages 77–93. Springer, 1991.

[123] Shafi Goldwasser and Silvio Micali. Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information. In *STOC 1982*, pages 365–377. ACM, 1982.

[124] Shafi Goldwasser and Silvio Micali. Probabilistic Encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.

[125] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The Knowledge Complexity of Interactive Proof Systems. *SIAM J. Comput.*, 18(1):186–208, 1989.

[126] Daniel Gordon. Designing and Detecting Trapdoors for Discrete Log Cryptosystems. In *CRYPTO 1992*, volume 740 of *Lecture Notes in Computer Science*, pages 66–75. Springer, 1993.

[127] S. Dov Gordon, Carmit Hazay, Jonathan Katz, and Yehuda Lindell. Complete Fairness in Secure Two-Party Computation. *Jornal of the ACM*, 58(6):1–37, December 2011.

[128] Dima Grigoriev, Laszlo B. Kish, and Vladimir Shpilrain. Yao's Millionaires' Problem and Public-Key Encryption Without Computational Assumptions. *Int. J. Found. Comput. Sci.*, 28(4):379–390, 2017.

[129] Dima Grigoriev and Vladimir Shpilrain. Secure Information Transmission Based on Physical Principles. In *UCNC 2013*, volume 7956 of *Lecture Notes in Computer Science*, pages 113–124. Springer, 2013.

[130] Dima Grigoriev and Vladimir Shpilrain. Yao's Millionaires' Problem and Decoy-Based Public Key Encryption by Classical Physics. *Int. J. Found. Comput. Sci.*, 25(4):409–418, 2014.

[131] Louis C. Guillou and Jean-Jacques Quisquater. A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory. In *EUROCRYPT 1988*, volume 330 of *Lecture Notes in Computer Science*, pages 123–128. Springer, 1988.

[132] Stuart Haber and W Scott Stornetta. How to Time-Stamp a Digital Document. In *CRYPTO 1990*, volume 537 of *Lecture Notes in Computer Science*, pages 437–455. Springer, 1990.

[133] D. Halliday, R. Resnick, and J. Walker. *Fundamentals of Physics*. John Wiley & Sons, 2010.

[134] Mike Hamburg, Paul Kocher, and Mark E Marson. Analysis of Intel's Ivy Bridge Digital Random Number Generator. Technical report, Rambus, 2012.

[135] Lucjan Hanzlik, Kamil Kluczniak, and Mirosław Kutyłowski. Controlled Randomness - A Defense against Backdoors in Cryptographic Devices. In *MyCrypt 2016*, volume 10311 of *Lecture Notes in Computer Science*, pages 215–232. Springer, 2016.

[136] Dan Harkins and Dave Carrel. RFC 2409: The Internet Key Exchange (IKE). Technical report, Internet Engineering Task Force, 1998.

[137] Sam Hasinoff. Solving Substitution Ciphers. https://people.csail.mit.edu/hasinoff/pubs/hasinoff-quipster-2003.pdf.

[138] Philip Hawkes and Luke O'Connor. XOR and Non-XOR Differential Probabilities. In *EUROCRYPT 1999*, volume 1592 of *Lecture Notes in Computer Science*, pages 272–285. Springer, 1999.

[139] Martin Hell, Thomas Johansson, Alexander Maximov, and Willi Meier. A Stream Cipher Proposal: Grain-128. In *ISIT 2006*, pages 1614–1618. IEEE, 2006.

[140] Martin Hell, Thomas Johansson, and Willi Meier. Grain - A Stream Cipher for Constrained Environments. Technical Report 010, ECRYPT Stream Cipher Project Report, 2005.

[141] Martin Hell, Thomas Johansson, and Willi Meier. Grain: A Stream Cipher for Constrained Environments. *International Journal of Wireless and Mobile Computing*, 2(1):86–93, May 2007.

[142] Florian Hess. Efficient Identity Based Signature Schemes Based On Pairings. In *SAC 2002*, volume 2595 of *Lecture Notes in Computer Science*, pages 310–324. Springer, 2002.

[143] Howard M Heys. A Tutorial on Linear and Differential Cryptanalysis. *Cryptologia*, 26(3):189–221, 2002.

[144] Lester S Hill. Cryptography in an Algebraic Alphabet. *The American Mathematical Monthly*, 36(6):306–312, 1929.

[145] Lester S Hill. Concerning Certain Linear Transformation Apparatus of Cryptography. *The American Mathematical Monthly*, 38(3):135–154, 1931.

[146] Susan M Howitt and Anna N Wilson. Revisiting "Is the Scientific Paper a Fraud?". *EMBO Reports*, 15(5):481–484, 2014.

[147] Mahabir Prasad Jhanwar and Rana Barua. A Variant of Boneh-Gentry-Hamburg's Pairing-Free Identity Based Encryption Scheme. In *INSCRYPT 2008*, volume 5487 of *Lecture Notes in Computer Science*, pages 314–331. Springer, 2009.

[148] Marc Joye. Identity-Based Cryptosystems and Quadratic Residuosity. In *PKC 2016*, volume 9614 of *Lecture Notes in Computer Science*, pages 225–254. Springer, 2016.

[149] Marc Joye and Benoît Libert. Efficient Cryptosystems from 2^k-th Power Residue Symbols. In *EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 76–92. Springer, 2013.

[150] Marc Joye and Benoît Libert. Efficient Cryptosystems from 2^k-th Power Residue Symbols. *IACR Cryptology ePrint Archive*, 2013/435, 2014.

[151] Benjamin Justus. The Distribution of Quadratic Residues and Non-Residues in the Goldwasser-Micali Type of Cryptosystem. *Journal of Mathematical Cryptology*, 8(8):115–140, 2014.

[152] Jonathan Katz and Nan Wang. Efficiency Improvements for Signature Schemes With Tight Security Reductions. In *CCS 2003*, pages 155–164. ACM, 2003.

[153] Charlie Kaufman, Paul Hoffman, Yoav Nir, Parsi Eronen, and Tero Kivinen. RFC7296: Internet Key Exchange Protocol Version 2 (IKEv2). Technical report, Internet Engineering Task Force, 2014.

[154] Shahram Khazaei and Siavash Ahmadi. Ciphertext-Only Attack on $d \times d$ Hill in $O(d13^d)$. *Information Processing Letters*, 118:25–29, 2017.

[155] Shahram Khazaei, Mehdi Hassanzadeh, and Mohammad Kiaei. Distinguishing Attack on Grain. Technical Report 071, ECRYPT Stream Cipher Project Report, 2005.

[156] Tanya Khovanova. One-Way Functions. https://blog.tanyakhovanova.com/2010/11/one-way-functions/.

[157] William A Kiele. A Tensor-Theoretic Enhancement to the Hill Cipher System. *Cryptologia*, 14(3):225–233, 1990.

[158] Wolfgang Killmann and Werner Schindler. A Proposal for: Functionality Classes for Random Number Generators, version 2.0. Technical report, BSI, 2011.

[159] Simon Knellwolf, Willi Meier, and María Naya-Plasencia. Conditional Differential cryptanalysis of NLFSR-Based Cryptosystems. In *ASIACRYPT 2010*, volume 6477 of *Lecture Notes in Computer Science*, pages 130–145. Springer, 2010.

[160] Czesław Kościelny. A Method of Constructing Quasigroup-Based Stream-Ciphers. *Applied Mathematics and Computer Science*, 6:109–122, 1996.

[161] Daniel Kucner and Mirosław Kutyłowski. Stochastic kleptography detection. In *Public-Key Cryptography and Computational Number Theory*, pages 137–149, 2001.

[162] Özgül Küçük. Slide Resynchronization Attack on the Initialization of Grain 1.0. http:www.ecrypt.eu.org/stream, 2006.

[163] Robin Kwant, Tanja Lange, and Kimberley Thissen. Lattice Klepto - Turning Post-Quantum Crypto Against Itself. In *SAC 2017*, volume 10719 of *Lecture Notes in Computer Science*, pages 336–354. Springer, 2017.

[164] Xuejia Lai and James L Massey. A Proposal for a New Block Encryption Standard. In *EUROCRYPT 1990*, volume 473 of *Lecture Notes in Computer Science*, pages 389–404. Springer, 1991.

[165] Xuejia Lai, James L Massey, and Sean Murphy. Markov Ciphers and Differential Cryptanalysis. In *EUROCRYPT 1991*, volume 547 of *Lecture Notes in Computer Science*, pages 17–38. Springer, 1991.

[166] Butler W Lampson. A Note on the Confinement Problem. *Communications of the ACM*, 16(10):613–615, 1973.

[167] Tom Leap, Tim McDevitt, Kayla Novak, and Nicolette Siermine. Further Improvements to the Bauer-Millward Attack on the Hill Cipher. *Cryptologia*, 40(5):452–468, 2016.

[168] Chae Hoon Lim and Pil Joong Lee. A Study on the Proposed Korean Digital Signature Algorithm. In *ASIACRYPT 1998*, volume 1514 of *Lecture Notes in Computer Science*, pages 175–186. Springer, 1998.

[169] Yehuda Lindell. Fast Secure Two-Party ECDSA Signing. In *CRYPTO 2017*, volume 10402 of *Lecture Notes in Computer Science*, pages 613–644. Springer, 2017.

[170] James Lyons. Practical Cryptography, http://practicalcryptography.com/.

[171] Diana Maimuţ and George Teşeleanu. A Unified Security Perspective on Legally Fair Contract Signing Protocols. In *SECITC 2018*, volume 11359 of *Lecture Notes in Computer Science*, pages 477–491. Springer, 2018.

[172] Diana Maimuţ and George Teşeleanu. New Configurations of Grain Ciphers: Security Against Slide Attacks. In *BalkanCrypt 2018*, Communications in Computer and Information Science. Springer, 2018.

[173] Diana Maimuţ and George Teşeleanu. A Generic View on the Unified Zero-Knowledge Protocol and its Applications. In *WISTP 2019*, volume 12024 of *Lecture Notes in Computer Science*, pages 32–46. Springer, 2019.

[174] Diana Maimuţ and George Teşeleanu. A New Generalisation of the Goldwasser-Micali Cryptosystem Based on the Gap 2^k-Residuosity Assumption. In *SECITC 2020*, Lecture Notes in Computer Science. Springer, 2020.

[175] John Malone-Lee and Nigel P. Smart. Modifications of ECDSA. In *SAC 2002*, volume 2595 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2002.

[176] Ueli Maurer. Unifying Zero-Knowledge Proofs of Knowledge. In *AFRICACRYPT 2009*, volume 5580 of *Lecture Notes in Computer Science*, pages 272–286. Springer, 2009.

[177] Kevin McCurley. A Key distribution System Equivalent to Factoring. *Journal of cryptology*, 1(2):95–105, 1988.

[178] Tim McDevitt, Jessica Lehr, and Ting Gu. A Parallel Time-memory Tradeoff Attack on the Hill Cipher. *Cryptologia*, 42(5):1–19, 2018.

[179] Peter Medawar. Is the Scientific Paper a Fraud? *The Listener*, 70(12):377–378, 1963.

[180] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC press, 1996.

[181] Silvio Micali. Simple and Fast Optimistic Protocols for Fair Electronic Exchange. In *PODC 2003*, pages 12–19. ACM, 2003.

[182] Markus Michels, David Naccache, and Holger Petersen. GOST 34.10-A Brief Overview of Russia's DSA. *Computers & Security*, 15(8):725–732, 1996.

[183] Microprocessor, MS Committee, et al. IEEE Standard Specifications for Public-Key Cryptography. *IEEE Computer Society*, 2000.

[184] Ilya Mironov and Noah Stephens-Davidowitz. Cryptographic Reverse Firewalls. In *ASIACRYPT 2015*, volume 9057 of *Lecture Notes in Computer Science*, pages 657–686. Springer, 2015.

[185] Arjan J. Mooij, Nicolae Goga, and Jan Willem Wesselink. *A Distributed Spanning Tree Algorithm for Topology-Aware Networks*. Technische Universiteit Eindhoven, Department of Mathematics and Computer Science, 2003.

[186] Tal Moran and Moni Naor. Polling with Physical Envelopes: A rigorous Analysis of a Human-Centric Protocol. In *EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 88–108. Springer, 2006.

[187] Tal Moran and Moni Naor. Basing Cryptographic Protocols on Tamper-Evident Seals. *Theoretical Computer Science*, 411(10):1283–1310, 2010.

[188] Nicky Mouha. On Proving Security against Differential Cryptanalysis. In *CFAIL 2019*, 2019.

[189] David M'Raïhi, David Naccache, David Pointcheval, and Serge Vaudenay. Computational Alternatives to Random Number Generators. In *SAC 1998*, volume 1556 of *Lecture Notes in Computer Science*, pages 72–80. Springer, 1998.

[190] David Naccache and Jacques Stern. A New Public Key Cryptosytem Based on Higher Residues. In *CCS 1998*, pages 59–66. ACM, 1998.

[191] Moni Naor, Yael Naor, and Omer Reingold. Applied Kid Cryptography or How to Convince Your Children You Are Not Cheating. http://www.wisdom.weizmann.ac.il/~naor/PAPERS/waldo.pdf.

[192] Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. In *FOCS 1997*, pages 458–467. IEEE Computer Society, 1997.

[193] Moni Naor and Omer Reingold. Number-Theoretic Constructions of Efficient Pseudo-Random Functions. *Journal of the ACM*, 51(2):231–262, 2004.

[194] Melvyn B. Nathanson. *Elementary Methods in Number Theory*. Graduate Texts in Mathematics. Springer, 2000.

[195] Koki Nishigami and Keiichi Iwamura. Geometric pairwise key-sharing scheme. In *SECITC 2018*, volume 11359 of *Lecture Notes in Computer Science*, pages 518–528. Springer, 2018.

[196] Kaisa Nyberg. Perfect Nonlinear S-boxes. In *EUROCRYPT 1991*, volume 547 of *Lecture Notes in Computer Science*, pages 378–386. Springer, 1991.

[197] Kaisa Nyberg and Rainer A. Rueppel. A New Signature Scheme Based on the DSA Giving Message Recovery. In *CCS 1993*, pages 58–61. ACM, 1993.

[198] Luke O'Connor. On the Distribution of Characteristics in Bijective Mappings. In *EUROCRYPT 1993*, volume 765 of *Lecture Notes in Computer Science*, pages 360–370. Springer, 1994.

[199] Luke O'Connor. On the Distribution of Characteristics in Bijective Mappings. *Journal of Cryptology*, 8(2):67–86, 1995.

[200] Tatsuaki Okamoto. Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes. In *CRYPTO 1992*, volume 740 of *Lecture Notes in Computer Science*, pages 31–53. Springer, 1992.

[201] Jeffrey Overbey, William Traves, and Jerzy Wojdylo. On the Keyspace of the Hill Cipher. *Cryptologia*, 29(1):59–72, 2005.

[202] Pascal Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *Eurocrypt 1999*, volume 1592 of *Lecture Notes in Computer Science*, pages 223–238. Springer, 1999.

[203] Kenneth G. Paterson. ID-Based Signatures from Pairings on Elliptic Curves. *Electronics Letters*, 38(18):1025–1026, 2002.

[204] René Peralta. On the Distribution of Quadratic Residues and Nonresidues Modulo a Prime Number. *Mathematics of Computation*, 58(197):433–440, 1992.

[205] Nicole Perlroth, Jeff Larson, and Scott Shane. NSA Able to Foil Basic Safeguards of Privacy on Web. *The New York Times*, 5, 2013.

[206] Oskar Perron. Bemerkungen über die Verteilung der quadratischen Reste. *Mathematische Zeitschrift*, 56(2):122–130, 1952.

[207] Benny Pinkas. Fair Secure Two-Party Computation. In *EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 87–105. Springer, 2003.

[208] David Pointcheval and Jacques Stern. Security Proofs For Signature Schemes. In *EUROCRYPT 1996*, volume 1070 of *Lecture Notes in Computer Science*, pages 387–398. Springer, 1996.

[209] David Pointcheval and Jacques Stern. Security Arguments for Digital Signatures and Blind Signatures. *Journal of Cryptology*, 13(3):361–396, 2000.

[210] Jean-Jacques Quisquater, Myriam Quisquater, Muriel Quisquater, Michaël Quisquater, Louis Guillou, Marie Annick Guillou, Gaïd Guillou, Anna Guillou, Gwenolé Guillou, and Soazig Guillou. How to Explain Zero-Knowledge Protocols to Your Children. In *CRYPTO 1989*, volume 435 of *Lecture Notes in Computer Science*, pages 628–631. Springer, 1990.

[211] Martin Ågren, Martin Hell, Thomas Johansson, and Willi Meier. Grain-128a: A New Version of Grain-128 with Optional Authentication. *International Journal of Wireless and Mobile Computing*, 5(1):48–59, December 2011.

[212] Elena Reshetova, Filippo Bonazzi, and N. Asokan. Randomization Can't Stop BPF JIT spray. In *NSS 2017*, volume 10394 of *Lecture Notes in Computer Science*, pages 233–247. Springer, 2017.

[213] Ronald L Rivest, Adi Shamir, and David A Wagner. Time-lock Puzzles and Timed-release Crypto. Technical report, MIT, 1996.

[214] Alexander Russell, Qiang Tang, Moti Yung, and Hong-Sheng Zhou. Cliptography: Clipping the power of kleptographic attacks. In *ASIACRYPT 2016*, volume 10032 of *Lecture Notes in Computer Science*, pages 34–64. Springer, 2016.

[215] Alexander Russell, Qiang Tang, Moti Yung, and Hong-Sheng Zhou. Destroying Steganography via Amalgamation: Kleptographically CPA Secure Public Key Encryption. *IACR Cryptology ePrint Archive*, 2016/530, 2016.

[216] Ryuichi Sakai, Kiyoshi Ohgishi, and Masao Kasahara. Cryptosystems Based on Pairings. In *SCIS 2000*, 2000.

[217] Conrad Sanderson and Ryan Curtin. Armadillo: A Template-Based C++ Library for Linear Algebra. *Journal of Open Source Software*, 1(2):26, 2016.

[218] Bruce Schneier. The Solitaire Encryption Algorithm. https://www.schneier.com/academic/solitaire/.

[219] Claus-Peter Schnorr. Efficient Identification and Signatures For Smart Cards. In *CRYPTO 1989*, volume 435 of *Lecture Notes in Computer Science*, pages 239–252. Springer, 1989.

[220] Martin A Schwartz. The Importance of Stupidity in Scientific Research. *Journal of Cell Science*, 121(11):1771–1771, 2008.

[221] Adi Shamir. How to Share a Secret. *Communications of the ACM*, 22(11):612–613, 1979.

[222] Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In *CRYPTO 1984*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1985.

[223] Victor Shoup. Sequences of Games: A Tool for Taming Complexity in Security Proofs. *IACR Cryptology ePrint Archive*, 2004/332, 2004.

[224] Victor Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2008.

[225] Vladimir Shpilrain. Decoy-Based Information Security. *Groups Complexity Cryptology*, 6(2):149–155, 2014.

[226] Gustavus J. Simmons. The Subliminal Channel and Digital Signatures. In *EUROCRYPT 1984*, volume 209 of *Lecture Notes in Computer Science*, pages 364–378. Springer, 1984.

[227] Gustavus J. Simmons. Subliminal Communication is Easy Using the DSA. In *EUROCRYPT 1993*, volume 765 of *Lecture Notes in Computer Science*, pages 218–232. Springer, 1993.

[228] Gustavus J Simmons. Subliminal Channels; Past and Present. *European Transactions on Telecommunications*, 5(4):459–474, 1994.

[229] Simon Singh. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor, 2000.

[230] Jonathan DH Smith. Four Lectures on Quasigroup Representations. *Quasigroups Related Systems*, 15:109–140, 2007.

[231] Paul Stankovski. Greedy Distinguishers and Nonrandomness Detectors. In *INDOCRYPT 2010*, volume 6498 of *Lecture Notes in Computer Science*, pages 210–226. Springer, 2010.

[232] Neal Stephenson. *Cryptonomicon*. Arrow, 2000.

[233] Douglas R Stinson. *Cryptography: Theory and Practice*. CRC press, 2005.

[234] Fatih Sulak. New Statistical Randomness Tests: 4-bit Template Matching Tests. *Turkish Journal of Mathematics*, 41(1):80–95, 2017.

[235] Terence Tao. Ask Yourself Dumb Questions - and Answer Them! https://terrytao.wordpress.com/career-advice/ask-yourself-dumb-questions-and-answer-them/.

[236] Terence Tao. Use The Wastebasket. https://terrytao.wordpress.com/career-advice/use-the-wastebasket/.

[237] George Teşeleanu. Threshold Kleptographic Attacks on Discrete Logarithm Based Signatures. In *LatinCrypt 2017*, volume 11368 of *Lecture Notes in Computer Science*, pages 401–414. Springer, 2017.

[238] George Teşeleanu. Random Number Generators Can Be Fooled to Behave Badly. In *ICICS 2018*, volume 11149 of *Lecture Notes in Computer Science*, pages 124–141. Springer, 2018.

[239] George Teşeleanu. Unifying Kleptographic Attacks. In *NordSec 2018*, volume 11252 of *Lecture Notes in Computer Science*, pages 73–87. Springer, 2018.

[240] George Teşeleanu. Managing Your Kleptographic Subscription Plan. In *C2SI 2019*, volume 11445 of *Lecture Notes in Computer Science*, pages 452–461. Springer, 2019.

[241] George Teşeleanu. Reinterpreting and Improving the Cryptanalysis of the Flash Player PRNG. In *C2SI 2019*, volume 11445 of *Lecture Notes in Computer Science*, pages 92–104. Springer, 2019.

[242] George Teşeleanu. Subliminal Hash Channels. In *A2C 2019*, volume 1133 of *Communications in Computer and Information Science*, pages 149–165. Springer, 2019.

[243] George Teşeleanu. A Love Affair Between Bias Amplifiers and Broken Noise Sources. In *ICICS 2020*, Lecture Notes in Computer Science. Springer, 2020.

[244] George Teşeleanu. Cracking Matrix Modes of Operation with Goodness-of-Fit Statistics. In *HistoCrypt 2020*, Linköping Electronic Conference Proceedings. Linköping University Electronic Press, 2020.

[245] George Teşeleanu. Quasigroups and Substitution Permutation Networks: A Failed Experiment. *Cryptologia*, 2020.

[246] Ferucio Laurenţiu Ţiplea, Sorin Iftene, George Teşeleanu, and Anca-Maria Nica. Security of Identity-Based Encryption Schemes from Quadratic Residues. In *SECITC 2016*, volume 10006 of *Lecture Notes in Computer Science*, pages 63–77, 2016.

[247] Ferucio Laurentiu Tiplea, Sorin Iftene, George Teseleanu, and Anca-Maria Nica. On the Distribution of Quadratic Residues and Non-residues Modulo Composite Integers and Applications to Cryptography. *Appl. Math. Comput.*, 372, 2020.

[248] Peter Truran. *Practical Applications of the Philosophy of Science: Thinking About Research*. Springer Science & Business Media, 2013.

[249] Meltem Sönmez Turan, Elaine Barker, John Kelsey, Kerry McKay, Mary Baish, and Mike Boyle. NIST DRAFT Special Publication 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation. Technical report, NIST, 2012.

[250] Umesh V. Vazirani and Vijay V. Vazirani. Trapdoor Pseudo-random Number Generators, with Applications to Protocol Design. In *FOCS 1983*, pages 23–30. IEEE, 1983.

[251] Milan Vojvoda, Marek Sỳs, and Matú Jókay. A Note on Algebraic Properties of Quasigroups in Edon80. Technical report, eSTREAM report 2007/005, 2007.

[252] John Von Neumann. Various Techniques Used in Connection with Random Digits. *Applied Math Series*, 12:36–38, 1951.

[253] Chenyu Wang, Tao Huang, and Hongjun Wu. On the Weakness of Constant Blinding PRNG in Flash Player. In *ICICS 2018*, volume 11149 of *Lecture Notes in Computer Science*, pages 107–123. Springer, 2018.

[254] Greg Ward. A Recursive Implementation of the Perlin Noise Function. In *Graphics Gems II*, pages 396–401. Elsevier, 1991.

[255] Donald R Weidman. Emotional Perils of Mathematics. *Science*, 149(3688):1048–1048, 1965.

[256] Chuan-Kun Wu. Hash channels. *Computers & Security*, 24(8):653–661, 2005.

[257] Mark Wutka. The Crypto Forum, http://s13.zetaboards.com/Crypto/topic/123721/1/.

[258] Akihiro Yamaguchi, Takaaki Seo, and Keisuke Yoshikawa. On the Pass Rate of NIST Statistical Test Suite for Randomness. *JSIAM Letters*, 2:123–126, 2010.

[259] Song Y. Yan. *Number Theory for Computing.* Theoretical Computer Science. Springer, 2002.

[260] Andrew C. Yao. Protocols for Secure Computations. In *SFCS 1982*, pages 160–164. IEEE Computer Society, 1982.

[261] Adam Young and Moti Yung. The Dark Side of "Black-Box" Cryptography or: Should We Trust Capstone? In *CRYPTO 1996*, volume 1109 of *Lecture Notes in Computer Science*, pages 89–103. Springer, 1996.

[262] Adam Young and Moti Yung. Kleptography: Using Cryptography Against Cryptography. In *EUROCRYPT 1997*, volume 1233 of *Lecture Notes in Computer Science*, pages 62–74. Springer, 1997.

[263] Adam Young and Moti Yung. The Prevalence of Kleptographic Attacks on Discrete-Log Based Cryptosystems. In *CRYPTO 1997*, volume 1294 of *Lecture Notes in Computer Science*, pages 264–276. Springer, 1997.

[264] Adam Young and Moti Yung. *Malicious Cryptography: Exposing Cryptovirology.* John Wiley & Sons, 2004.

[265] Adam Young and Moti Yung. Malicious Cryptography: Kleptographic Aspects. In *CT-RSA 2005*, volume 3376 of *Lecture Notes in Computer Science*, pages 7–18. Springer, 2005.

[266] Dae Hyun Yum and Pil Joong Lee. Cracking Hill Ciphers with Goodness-of-Fit Statistics. *Cryptologia*, 33(4):335–342, 2009.

[267] Haina Zhang and Xiaoyun Wang. Cryptanalysis of Stream Cipher Grain Family. *IACR Cryptology ePrint Archive*, 2009/109, 2009.

[268] Yuliang Zheng. Digital Signcryption or How to Achieve Cost (Signature & Encryption) $\ll$ Cost (Signature)+ Cost (Encryption). In *CRYPTO 1997*, volume 1294 of *Lecture Notes in Computer Science*, pages 165–179. Springer, 1997.

[269] Yuliang Zheng and Hideki Imai. How to Construct Efficient Signcryption Schemes on Elliptic Curves. *Information Processing Letters*, 68(5):227–233, 1998.

[270] Yuliang Zheng and Jennifer Seberry. Immunizing Public Key Cryptosystems Against Chosen Ciphertext Attacks. *IEEE Journal on Selected Areas in Communications*, 11(5):715–724, 1993.

[271] Shuangyi Zhu, Yuan Ma, Jingqiang Lin, Jia Zhuang, and Jiwu Jing. More Powerful and Reliable Second-Level Statistical Randomness Tests for NIST SP 800-22. In *ASIACRYPT 2016*, volume 10031 of *Lecture Notes in Computer Science*, pages 307–329. Springer, 2016.