

Contents

Part I Definitions and First Security Results

1	Introduction: General Definitions	3
1.1	Introduction	3
1.2	General Notation	5
1.3	Block Ciphers	6
1.4	Attack Models	6
1.5	Kerckhoffs’s Principle	8
	References	9
2	Balanced Feistel Ciphers, First Properties	11
2.1	Introduction	11
2.2	Definition of Classical Feistel Ciphers	11
2.3	Signature of Balanced Feistel Networks	14
2.4	Random Feistel Ciphers	15
2.5	Efficient Attacks for One, Two, and Three Rounds	15
2.5.1	KPA for One Round with $q = 1$	16
2.5.2	NCPA for Two Rounds with $q = 2$	16
2.5.3	CCA for Three Rounds with $q = 3$	17
2.6	Conclusion	19
	Problems	19
	References	19
3	The H-Coefficient Method	21
3.1	Six “H-coefficient” Theorems	21
3.1.1	Notation: Definition of H	22
3.1.2	Theorem in KPA	22
3.1.3	Theorems in NCPA	25
3.1.4	Theorem in CPA	25
3.1.5	Theorems in CCA	28
3.1.6	Comments about These Theorems	33

3.2	How to Distinguish Random functions from Random Permutations	34
3.3	Triangular Evaluation on Generic Designs	35
3.4	Example: Exact Values of H for Ψ^r and $q = 2$	35
3.5	Two Simple Composition Theorems in CCA	38
3.5.1	A Simple Mathematical Property	38
3.5.2	A Composition Theorem in CCA with H-Coefficients	39
3.5.3	A Composition Theorem to Eliminate a “hole”	41
3.5.4	Comments about the Composition Theorems	42
	References	43
4	Luby-Rackoff Theorems	45
4.1	Pseudo-Randomness Notions	45
4.2	Results on Ψ^3	47
4.2.1	The “H-Property of Ψ^3 ”	47
4.2.2	“Main Lemma” of Luby and Rackoff for Ψ^3 from the “H-property”	48
4.3	Results on Ψ^4	48
4.3.1	The “H-property” for Ψ^4	48
4.3.2	“Main Lemma” of Luby and Rackoff for Ψ^4 from the “H-property” of Ψ^4	50
4.4	Conclusion: Ψ^3 is Pseudo-Random, Ψ^4 Is Super Pseudo-Random	50
4.4.1	Comments about Luby-Rackoff Theorems	51
4.5	Other Results	52
	Problems	52
	References	53
 Part II Generic Attacks		
5	Introduction to Cryptanalysis and Generic Attacks	57
5.1	Generic Attacks: Distinguishers	57
5.2	2-Point Attacks and φ -Point Attacks and the Variance Method ..	58
5.2.1	General Description of the Attacks	58
5.2.2	Distinguishing Attacks	59
5.3	Attacks with More Than 2^{kn} Computations	60
5.3.1	Attacks on Generators	60
5.3.2	Brute Force Attacks	60
5.3.3	Attack by the Signature	61
5.4	Further Readings	62
	References	62

6	Generic Attacks on Classical Feistel Ciphers	65
6.1	Introduction	65
6.2	Generic Attacks on 1, 2, 3 and 4 Rounds	66
6.2.1	1 Round	67
6.2.2	2 Rounds	67
6.2.3	3 Rounds	67
6.2.4	4 Rounds	68
6.3	Generic Attacks on Ψ^5	69
6.3.1	NCPA on Ψ^5	69
6.3.2	KPA on Ψ^5	69
6.4	Attacks on Ψ^r Generators, $r \geq 6$	70
6.4.1	KPA with r Even	70
6.4.2	KPA with r Odd	71
6.5	Summary of the Best Known Results on Random Feistel Ciphers	72
6.6	Conclusion	72
	Problems	73
	References	73
7	Generic Attacks on Classical Feistel Ciphers with Internal Permutations	75
7.1	Introduction	75
7.2	Generic Attacks for a Small Numbers of Rounds ($r \leq 5$)	76
7.2.1	Generic Attacks on 3-Round Feistel Networks with Internal Permutations	76
7.2.2	Generic Attacks on 4-Round Feistel Networks with Internal Permutations	78
7.2.3	Generic Attacks on 5 Rounds Feistel Networks with Internal Permutations	78
7.3	Generic Attacks for Any Number of Rounds: General Method	79
7.3.1	Computation of the Probabilities	80
7.3.2	All Possible 2-Point Attacks	81
7.3.3	The Attacks	83
7.4	Computation of the H -Coefficients	83
7.4.1	General Ideas for the Computation of the H -Coefficients	83
7.4.2	Exact Formulas for H -Coefficients	85
7.4.3	Exact H -Coefficient Values for $r \leq 5$	89
7.4.4	Table of Leading Terms of $\frac{H \cdot 2^{4n}}{ \mathcal{D}_n ^r} - \frac{1}{1-1/2^{2n}}$ and Example of Attack	91
7.5	Table of Results for Any Number of Rounds	93
	References	94

8	Generic Attacks on Contracting Feistel Ciphers	95
8.1	Definition: Notation.....	95
8.2	Simple Attacks on the First k Rounds.....	97
8.2.1	Attacks on G_k^r for $1 \leq r \leq k - 1$	98
8.3	Generic Attacks When $k = 3$	100
8.3.1	Attacks on 4 Rounds: G_3^4	100
8.3.2	Attacks on 5 Rounds: G_3^5	102
8.3.3	Attacks on 6 Rounds: G_3^6	108
8.3.4	Attacks on 7 Rounds: G_3^7	109
8.3.5	Attacks on G_3^r Generators for $r \geq 8$	110
8.3.6	Summary of the Attacks on G_3^r	112
8.4	Generic Attacks When $k \geq 4$ and $r > k$	112
8.4.1	Attacks for $k + t$ Rounds, with $1 \leq t < k - 1$	113
8.4.2	Attacks for $2k - 1$ Rounds	113
8.4.3	Attacks on Generators	114
8.4.4	Summary of the Results for $r > 4$	115
9	Generic Attacks on Expanding Feistel Ciphers	117
9.1	Notation: Definition—Properties.....	118
9.2	Attacks on the First $k + 2$ Rounds	120
9.2.1	Attacks on F_k^1	121
9.2.2	2-Point NCPA and KPA on F_k^r , $2 \leq r \leq k$	121
9.2.3	2-Point NCPA and KPA on F_k^{k+1}	123
9.2.4	2-Point NCPA and KPA on F_k^{k+2}	124
9.3	Rectangle Attacks for $r \geq k + 3$	125
9.3.1	Notation: First Examples	125
9.3.2	Generation of All Possible Attacks for $k \leq 7$	128
9.3.3	Different Kinds of Rectangle Attacks: R_1 , R_2 , R_3 , and R_4	129
9.3.4	Best KPA Attacks: R_1 , R_2	131
9.3.5	From KPA into NCPA	132
9.3.6	Best NCPA: R_1 , R_2 —Simulations.....	135
9.4	Summary of the Attacks	136
	Problems	138
	References.....	138
10	Generic Attacks on Generalized Feistel Ciphers	139
10.1	Type-1 Feistel Ciphers	139
10.1.1	Notation: Definition	139
10.1.2	Simple Attacks on the First Rounds	140
10.1.3	NCPA and KPA Using the Expectation	142
10.1.4	NCPA and KPA Using the Standard Deviation.....	143
10.1.5	Summary of the Results	146
10.1.6	Signature of Type-1 Feistel Ciphers	146

10.2	Type-2 Feistel Ciphers	147
10.2.1	Notation: Definition	147
10.2.2	KPA	147
10.2.3	NCPA	148
10.2.4	Summary of the Results	150
10.2.5	Signature of Type-2 Feistel Ciphers	150
10.3	Type-3 Feistel Ciphers	151
10.3.1	Notation: Definition	151
10.3.2	KPA	151
10.3.3	NCPA	152
10.3.4	Summary of the Results	152
10.3.5	Signature of Type-3 Feistel Ciphers	153

Part III DES and Other Specific Feistel Ciphers

11	DES and Variants: 3DES, DES – X	157
11.1	Description	157
11.1.1	General Description of <i>DES</i>	157
11.1.2	Design of the Functions F_i	159
11.2	Simple <i>DES</i>	164
11.2.1	Presentation	164
11.2.2	Brute Force Attack	164
11.2.3	Linear Cryptanalysis	165
11.2.4	Biham Type Attack [1]	165
11.2.5	Conclusion on Simple <i>DES</i>	165
11.3	3DES with 2 Keys	165
11.3.1	Presentation	166
11.3.2	Brute Force Attack	166
11.3.3	Merle-Hellman Attack [10]	166
11.3.4	Van Oorschot and Wiener Attack [14]	167
11.3.5	Mitchell Attack [11]	168
11.3.6	Codebook Attack	168
11.3.7	Attack with Partial Decryption	169
11.3.8	Biham Type Attack [1]	169
11.3.9	Related-Key Attack	170
11.3.10	Related-Key Distinguisher	170
11.3.11	Conclusion on 3DES with Two Keys	170
11.4	3DES with Three Keys	170
11.4.1	Presentation	170
11.4.2	Man-in-the-Middle Attack and Refinements by Lucks	171
11.4.3	Codebook Attack	171
11.4.4	Attack with Partial Decryption	171
11.4.5	Biham Type Attack [1]	171
11.4.6	Related-Key Attack	172

11.4.7	Related-Key Distinguisher	172
11.4.8	Conclusion on <i>3DES</i> with Three Keys.....	172
11.5	<i>DES</i> – <i>X</i>	173
11.5.1	Presentation	173
11.5.2	Codebook Attack	173
11.5.3	Linear Cryptanalysis [12]	173
11.5.4	Daemen’s Attack.....	174
11.5.5	Attack with Partial Decryption.....	174
11.5.6	Biham Type Attack	174
11.5.7	Related-Key Attack	174
11.5.8	Related-Key Distinguisher	175
11.5.9	Conclusion on <i>DES</i> – <i>X</i>	175
	Problems	175
	References.....	175
12	GOST, SIMON, BEAR-LION, CAST-256, CLEFIA	177
12.1	Ciphers Based on Balanced Feistel Constructions	177
12.1.1	GOST	177
12.1.2	SIMON	180
12.2	Ciphers Based on Expanding and/or Feistel Constructions	180
12.2.1	BEAR-LION	180
12.2.2	Other Examples of Unbalanced Feistel Ciphers.....	182
12.3	Ciphers Based on Generalized Feistel Constructions	182
12.3.1	CAST-256	182
12.3.2	CLEFIA	184
	References.....	188
 Part IV Advanced Security Results		
13	Proof Beyond the Birthday Bound with the Coupling Technique.....	193
13.1	Feistel Networks as Shuffles	193
13.2	Definition and History of the Coupling Technique	194
13.3	Application to Feistel Ciphers.....	195
13.4	Further Reading	201
	References.....	201
14	Introduction to Mirror Theory.....	203
14.1	Definitions.....	203
14.2	First Properties	207
14.2.1	Typical Theorem in Mirror Theory	209
14.3	Examples	209
14.4	About Computer Simulations	215
14.5	Marshall Hall Jr Theorem and Conjectures of 2008	216
14.5.1	2008 Conjectures	217
14.5.2	Computer Simulations	217

14.6	Examples of Connections Between Mirror Systems and Cryptographic Security of Generic Schemes	218
14.6.1	Xor of 2 Bijections, H Standard Technique	218
14.6.2	Xor of 2 Bijections, H_σ Technique	218
14.6.3	Security of Balanced Feistel Schemes	219
14.6.4	Security of $f(x 0) \oplus f(x 1)$ When f Is a Bijection	219
14.6.5	Other Schemes	220
14.7	Conclusion	220
	References	220
15	“$P_i \oplus P_j$ Theorem” When $\xi_{\max} = 2$	223
15.1	Presentation of “ $P_i \oplus P_j$ Theorem” When $\xi_{\max} = 2$	223
15.2	Security When $\alpha^3 \ll 2^{2n}$	225
15.3	Orange Equations	226
15.3.1	Inclusion-Exclusion Formula for $h_{\alpha+1}$	226
15.3.2	Analysis of the Term $\sum_{i=1}^{2a} B_i $	227
15.3.3	Analysis of the Term $\sum_{i_1 < i_2} B_{i_1} \cap B_{i_2} $	228
15.3.4	General Proof Strategy	229
15.4	Security When $\alpha^4 \ll 2^{3n}$	230
15.4.1	Approximation in $O(\frac{\alpha}{2^n})$ of h'_α	230
15.4.2	Evaluation of $ M_\alpha $	231
15.4.3	Ordering the Equations Such That $\Delta \leq \delta + 1$	232
15.4.4	Security in $\alpha^4 \ll 2^{3n}$ from the Orange Equation, Method 1	233
15.4.5	Security in $\alpha^4 \ll 2^{3n}$ from the Orange Equation, Method 2	234
15.5	The First Purple Equations	236
15.5.1	Inclusion-Exclusion Formula for $h'_{\alpha+1}$	236
15.5.2	Evaluation of $\sum_{i=1}^{2a-4} B_i $	237
15.5.3	Evaluation of $\sum_{i_1 < i_2} B_{i_1} \cap B_{i_2} $	238
15.6	Approximation in $O(\frac{\alpha}{2^n})$ of h''_α and $h_{\alpha-k}$	239
15.7	Security When $\alpha^6 \ll 2^{5n}$	241
15.8	Approximation in $O(\frac{\alpha}{2^n})$ of $h_\alpha^{(d)}$	244
15.9	All the Purple Equations	244
15.9.1	Inclusion-Exclusion for $h_{\alpha+d}^{(d)}$	244
15.9.2	Evaluation of $\sum_{i=1}^{2d(a-2)} B_i $: 1 Equation β_{i_1}	246
15.9.3	Evaluation of $\sum_{i_1 < i_2} B_{i_1} \cap B_{i_2} $: 2 Equations β_{i_1} and β_{i_2}	246
15.9.4	Evaluation of $\sum_{i_1 < i_2 < \dots < i_\varphi} B_{i_1} \cap \dots \cap B_{i_\varphi} $: φ Equations $\beta_{i_1}, \dots, \beta_{i_\varphi}$	247
15.10	Second Purple Equation	250
15.11	Induction on the Deviation Terms	251
15.12	Application with $d = 1$ and $d = 2$	253

15.13	Alternative Proof, Improved Coefficients	254
15.13.1	Sign of the Coefficients	254
15.13.2	Induction by Blocks of 2 Variables	254
15.14	Summary of the Proof	255
	Problems	255
	References	256
16	“$P_i \oplus P_j$ Theorem” on Standard Systems and “$P_i \oplus P_j$ Theorem” with Any ξ_{\max}	257
16.1	Presentation of “ $P_i \oplus P_j$ Theorems” on Standard Systems, and for Any ξ_{\max}	257
16.2	First Results: Security When $a^3 \xi_{\max}^2 \ll 2^{2n}$	259
16.3	Orange Equations	261
16.3.1	Inclusion-Exclusion Formula for $h_{\alpha+1}$	261
16.3.2	Terms in $ B_i $	262
16.3.3	Terms in $ B_{i_1} \cap B_{i_2} $	262
16.3.4	Term in $ B_{i_1} \cap \dots \cap B_{i_\varphi} $: φ Equations β_i	264
16.4	Ordering the Equations Such That $\Delta \leq \delta + \frac{\xi}{2}$	266
16.5	Analysis of the Orange Equations	267
16.5.1	Blue Terms	267
16.5.2	Red Terms	267
16.5.3	Green Terms	268
16.5.4	Solution 1: For Standard Systems, Without Using the Alternating Signs + and –	269
16.5.5	Solution 2: Using the Alternating Signs + and –	269
16.5.6	Conclusion	270
	Reference	270
17	Proofs Beyond the Birthday Bound on Ψ^k with the H-Coefficient Method	271
17.1	Exact Formulas for H and Ψ^k with “frameworks”	271
17.2	Standard Systems Dominate	275
17.2.1	Two Collisions	275
17.2.2	k Collisions	276
17.3	KPA Security for Ψ^4	276
17.3.1	Security in $q \ll 2^n$ Instead of $q \ll \frac{2^n}{n^2}$	281
17.4	CPA Security for Ψ^5	281
17.4.1	Security in $q \ll 2^n$ Instead of $q \ll \frac{2^n}{n^2}$	285
17.5	CCA Security for Ψ^5	285
17.5.1	Case 1: j Is a Direct Query Such That $\exists i < j, R_i = R_j$	285
17.5.2	Case 2: j Is an Inverse Query Such That $\exists i < j, S_i = S_j$	286

17.6	CCA Security for Ψ^6	286
17.6.1	Security in $q \ll 2^n$ Instead of $q \ll \frac{2^n}{n^2}$	287
17.7	Security Results on Ψ^k , $k \geq 6$, with the Composition Theorem ..	287
17.8	Results from Mirror Theory Compared with Results from Coupling on Ψ^k	288
	Problems	289
18	Indifferentiability	291
18.1	Introduction	291
18.2	Formal Definition of Indifferentiability	292
18.3	Five Rounds of Balanced Feistel is not Indifferentiable from an Ideal Cipher	293
18.4	Positive Results	295
18.5	Further Reading	295
	References	296
	Solutions	297
	Reference	309

Feistel Ciphers

Security Proofs and Cryptanalysis

Nachev, V.; Patarin, J.; Volte, E.

2017, XV, 309 p. 39 illus., 6 illus. in color., Hardcover

ISBN: 978-3-319-49528-6