組み込み型相関電力解析

駒野 雄一† 清水 秀夫† 川村 信一†

†(株) 東芝 研究開発センター コンピュータ・ネットワークラボラトリー
212-8582 川崎市幸区小向東芝町 1

{yuichi1.komano,hideo.shimizu,shinichi2.kawamura}@toshiba.co.jp

あらまし 相関電力解析 (CPA，Correlation Power Analysis) は，暗号実装の消費電力と，既知データ (平文または暗号文) と推測鍵から計算される中間データ候補との相関を計算することにより，暗号実装の秘密鍵を特定する解析手法である．CPA は，暗号演算処理の単位サイズ (8 ビットなど) ごとに部分鍵を特定し，同様の処理を繰り返すことにより秘密鍵のすべてのビット (128 ビットなど) を特定する．

本稿では，CPA の性能を向上する，組み込み型相関電力解析 (BS-CPA, Built-in determined Sub-key CPA) を提案する．BS-CPA は，部分鍵を特定するために中間データ候補を計算する際に，既に特定された部分鍵を利用して信号ノイズ比を向上させる．BS-CPA は，ハードウェアによる暗号実装のように，複数の中間データ (sbox の出力など) が同時に処理される場合に有効な解析手段である．本稿では，DPA contest のデータに BS-CPA を適用し，従来の CPA よりも極めて少ない電力波形で秘密鍵を特定できることを確認する．

Built-in Determined Sub-key Correlation Power Analysis

Yuichi Komano† Hideo Shimizu† Shinichi Kawamura†

†Computer & Network Systems Laboratory, Corporate Research & Development Center,
Toshiba Corporation. 1, Komukai-Toshiba-cho, Saiwai-ku, Kawasaki 212-8582 Japan

{yuichi1.komano,hideo.shimizu,shinichi2.kawamura}@toshiba.co.jp

Abstract Correlation power analysis (CPA) is a well-known attack against cryptographic modules with which an attacker evaluates the correlation between the power consumption and the sensitive data candidate calculated from a guessed sub-key and known data (plaintext or ciphertext). This paper enhances CPA to propose a new general power analysis, *built-in determined sub-key CPA* (BS-CPA), that finds a new sub-key by using the previously determined sub-keys recursively to compute the sensitive data candidate and to increase the signal-to-noise ratio in its analysis. BS-CPA is powerful and effective when the multiple sbox outputs (or corresponding data) are processed simultaneously as in the hardware implementation. We apply BS-CPA to the power consumption traces provided at the DPA contest and succeed in finding DES keys using less traces than the original CPA does.

1 はじめに

サイドチャネル攻撃は，暗号実装の処理時間 [9] や消費電力 [10]，漏洩電磁波 [5] を利用して，痕跡を残すことなく秘密情報を盗みとる解析手法である．Kocher ら [10] が単純電力解析 (simple power analysis, SPA) と (高次) 差分電力解析 ((higher-order) differential power analysis, (HO-)DPA) を提案して以来，攻撃の改良 [11, 3, 14, 4] と対策の提案 [6, 2, 12, 8, 13] が繰り返されている．

相関電力解析 [3] (correlation power analysis, CPA) は (1 次) DPA の改良である．CPA は，推測した部分鍵 (ラウンド鍵の一部) と既知データ (平文または暗号文) から計算される中間データ候補と，暗号実装の消費電力との相関を計算して部分鍵を特定する．CPA や DPA は，理論的な興味だけでなく，暗号実装への現実的な脅威となっている．DPA contest [1] では，様々な解析手法が報告されている．DPA contest は，公開された (8 万を超える) DES のハードウェア実装の電力波形から，より少ない波形で秘密鍵を特定できる解析手法を開発することを競う場である．2009 年 5 月 17 日時点では，改良 CPA により 310 波形で，12-bit の鍵探索をする改良 CPA により 232 波形で，特殊なファイル順番を用いた DPA により 112 波形で，DES の秘密鍵が特定されていた．

DPA contest では，事前に多くの電力波形が公開されているために，解析に都合の良い波形を選別する (順番を並び替える) ことができてしまう．本稿は，そのような事前選別に頼ることのない，汎用的かつ効率的な解析手法を提案する．そのような解析手法を開発することは，暗号実装の安全性評価の効率化にも有効である．また，事前選別した電力波形に本稿で提案する解析手法を適用することで，必要な波形数をさらに削減することも可能である．

提案手法である built-in determined sub-key correlation power analysis (BS-CPA) は，限られた数の消費電力波形を繰り返し利用する．BS-CPA は CPA の拡張攻撃であり，新たな部分鍵を特定するために中間データ候補を計算する際に，既に特定されている部分鍵を利用することで信号ノイズ比 (signal-to-noise ratio, SNR) を向上する．BS-CPA は，ハードウェア実装のように，暗号実装が複数の中間データ (sbox の出力や DES の左出力など) を同時に計算する場合に効果的である．我々は BS-CPA を DPA contest で公開されている電力波形に適用し，波形の事前選別なしに 164 波形[1] で秘密鍵の特定に成功した．さらに，探索区間を絞り込むことにより 143 波形で，ファイルの事前選別を行うことにより 107 波形で秘密鍵を特定できた．これらは，複数のラウンドを利用するなど DES の特性を利用する攻撃を除けば，DPA contest 終了時のカテゴリ 3 と 4 で最良の結果である．

関連研究: Hanley ら [7] は，大きなワード長での CPA を議論している．彼らの目的は解析に必要な消費電力波形の数を減らすことではなく，解析の際の CPA 波形 (相関係数の計算回数) を減らすことである．

DES のハードウェア実装に対する CPA を考えよう．もしも 2^{48} 通りのラウンド鍵すべての CPA 波形が計算できれば，最大の相関値を得て秘密鍵を特定することができるが，これは計算量的に不可能である．彼らは，以下の手順で 2^{11} の CPA 波形で最大の相関を得た．まず最初に 6-bit の (S_1 に対する) 部分鍵を予測して CPA 波形を生成し，相関値が大きい順番に 4 つの鍵候補を推定する．次に，この 4 つの候補を利用して，(S_1 と S_2 に対する) 2 つの部分鍵を推定する．このとき，2 つの部分鍵を特定するためには，通常必要となる 2^{12} の CPA 波形ではなく，$2^6 \times 4$ の CPA 波形を利用することに注意する．この処理を繰り返し，8 個の部分鍵を $2^6 + 7(2^6 \times 4) = 2^{11}$ の CPA 波形で特定することができる．

既に特定された部分鍵を利用して新たな部分鍵を推定する点は，我々の手法と同じである．しかし，彼らの目的は少ない CPA 波形で最大の相関値を得ることであり，必要な電力波形数には言及していない．実際，彼らの手法は (部分鍵の探索順番を固定し) 最初の部分鍵の特定に多くの電力波形が必要となる可能性や，新たな

[1] DPA contest では，100 波形連続して同一の鍵が特定されるときに，攻撃が成功したとみなされる．

部分鍵を探索する際に電力波形を再利用するかどうかについては触れられていない．BS-CPA は，部分鍵を並行して探索し，新たな部分鍵を探索する際に電力波形を巻き戻して，CPA に必要となる電力波形数を戦略的に削減する．

2 記法

$P_i = (p_i(t_1), p_i(t_2), \cdots, p_i(t_m))$ は m 点の電力値を含む i 番目の電力波形をあらわす．

共通鍵暗号の非線形変換 ($sbox$) への CPA を考える．各ラウンドでの sbox の数を n_{sb} であらわす．例えば，DES では $n_{sb} = 8$ であり，AES では $n_{sb} = 16$ とする．sb 番目の sbox を $sbox_{sb}$ であらわす．

CPA は，$sbox_{sb}$ に対応する部分鍵 $key^{(sb)}$ を推測し，$key^{(sb)}$ と i 番目の電力波形に対応する既知データ (平文または暗号文) X_i から ℓ-bit の中間データ候補 $b_i^{(sb)}$ を計算する．一つの sbox における部分鍵の候補数を n_{key} であらわす．例えば，DES では $n_{key} = 64$ であり，AES では $n_{key} = 256$ とする．

次に，CPA は $sbox_{sb}$ と時刻 t_j ごとに鍵候補 key_{sb} について相関値を計算し，相関値が閾値 $th^{(sb)}$ を超えたら部分鍵を特定する．このとき，閾値は鍵候補と時刻を通じての相関値の最大値を利用しても良いし，相関値の 3σ (σ は標準偏差) を利用しても良い．本稿では，DPA contest の基準に従い，閾値として相関値の最大値を利用し，100 波形連続して相関値が最大となるときに鍵の特定に成功したとみなす．

3 CPA

CPA では，時刻 t_j ごとに，鍵候補 $key^{(sb)}$ から計算される中間データ候補 $b_i^{(sb)}$ のハミング距離と電力値 $p_i(t_j)$ との相関値 $\mathsf{cpa}(key^{(sb)}, t_j)$ を以下で計算し，部分鍵を特定する．

$$\frac{1}{n\sigma_{h^{(sb)}}\sigma_{p(t_j)}}\sum_{i=1}^{n}(h_i^{(sb)} - \overline{h^{(sb)}})(p_i(t_j) - \overline{p(t_j)})$$

ただし，$h_i^{(sb)} \in [0, \ell]$ は中間データ候補 $b_i^{(sb)} \in \{0,1\}^\ell$ のハミング距離をあらわす．$\overline{x}$ と σ_x は変数 x の平均値と標準偏差をあらわす．

$$\overline{h^{(sb)}} = \frac{1}{n}\sum_{i=1}^{n} h_i^{(sb)},\ \sigma_h^{(sb)} = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}\left(h_i^{(sb)} - \overline{h^{(sb)}}\right)^2}$$

$$\overline{p(t_j)} = \frac{1}{n}\sum_{i=1}^{n} p_i(t_j),\ \sigma_{p(t_j)} = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}\left(p_i(t_j) - \overline{p(t_j)}\right)^2}$$

4 BS-CPA

BS-CPA は，既に特定された部分鍵 ($key^{(1)}, \cdots, key^{(sb-1)}$ など) を新たな鍵 ($key^{(sb)}$ など) を特定する際に SNR を向上するために用いる．この手法は，ハードウェア実装などのように複数の中間データ (sbox の出力など) が同時に計算されるときに効果的である．

4.1 直観的な説明

従来の DPA や CPA は，$sbox_{sb}$ ごとに $key^{(sb)}$ を独立に計算できるため，プログラミングは容易 (簡明) である．しかし，解析に必要となる電力波形の数を削減する工夫はなされていない．本稿では，電力波形数が少ない場合やファイルを選別できない場合でも部分鍵を効率的に計算できる，汎用的な解析手法を提案する．

SNR について検討する．消費電力は暗号実装が処理する中間データのハミング重み (CPU 処理) または ハミング距離 (CMOS 論理回路) に依存する．ハミング距離とは，2 時刻の中間データの排他的論理和のハミング重みである．以下では，中間データ候補の計算にハミング距離モデルを仮定する．

i 番目の電力波形に対して，時刻 t^* でレジスタが中間データ $y_i^{(1)}, \cdots, y_i^{(n_{sb})}$ を保持し，消費電力に影響を与えていると仮定する．CPA は，攻撃者が中間データ候補 $b_i^{(sb)}$ を推測して電力値 $p(t^*)$ との相関を計算する．

このとき，ある sb に関する $b_i^{(sb)}$ のハミング距離と $p_i(t^*)$ の間で相関が計算されると，他の中間データ $y_i^{(1)}, \cdots, y_i^{(sb-1)}, y_i^{(sb+1)}, \cdots, y_i^{(n_{sb})}$ に起因する電力値は SNR を悪化させるノイズ

成分となる．CPA では，秘密鍵全体を特定するために必要な電力波形数は，各部分鍵 $key^{(sb)}$ を特定するために必要な波形数の最大値 (最悪値) となる．

一般に，鍵候補の推定を複数にすることで SNR を向上できる．部分鍵 key_{sb} と $key_{sb'}$ を同時に推定する場合を考えよう．攻撃者は中間データ $b_i^{(sb)}$ と $b_i^{(sb)'}$ を予測し，それぞれのハミング距離の和と電力値 $p_i(t^*)$ との相関を計算する．このとき，CPA ではノイズとして作用していた中間データ $y_i^{(sb')}$ に起因する電力が，信号成分に変化する．したがって，SNR が向上し，少ない数の電力波形で部分鍵を特定できる．

より多くの部分鍵を同時に予測すれば，SNR が向上して少ない電力波形で部分鍵を特定できる．しかし，予測の数を増やせば部分鍵候補の数が増大し，(相関値など) 計算量が増大する．BS-CPA は，部分鍵の予測は一つとし，既に特定された部分鍵を利用して複数の中間データ候補を計算することで SNR を向上する．この処理を再帰的に繰り返すことで，秘密鍵全体を特定するために必要な電力波形数 (最悪値) を改善する．

4.2 解析手順

部分鍵 $key^{(sb)}$ を特定するために必要な電力波形数は，中間データ $b^{(sb)}$ の電力値への寄与度に依存して sb ごとに異なる．$key^{(sb)}$ を特定するために必要な波形数が最小となる sb は未知なので，BS-CPA は以下の式で相関値 $\mathsf{bs\text{-}cpa}(keys^{(SB)}, key^{(sb)}, t_j)$ を sb について並行に計算する．ここで，$keys^{(SB)}$ と $key^{(sb)}$ は，既に特定された部分鍵と予測する部分鍵をあらわす．

$$\frac{1}{n\sigma_{H^{(SB,sb)}}\sigma_{p(t_j)}}\sum_{i=1}^{n}(H_i^{(SB,sb)}-\overline{H^{(SB,sb)}})(p_i(t_j)-\overline{p(t_j)})$$

ただし，$H_i^{(SB,sb)} \in [0, \ell \times (N+1)]$ は，既に特定された部分鍵 $key^{(SB_1)}, \cdots, key^{(SB_N)}$ と部分鍵候補 $key^{(sb)}$ から計算される中間データ候補 $b_i^{(SB_1)}, \cdots, b_i^{(SB_N)}, b_i^{(sb)} \in \{0,1\}^\ell$ のハミング距離の和をあらわす．記法は 3 節と同様である．BS-CPA の手順を示す．

1. $sb = 1, \cdots, n_{sb}$ に対し $\mathsf{key}[sb] = \phi$ とする
2. $\mathsf{key}[sb] = \phi$ となる sb について以下を並行に実行する
3. $key^{(sb)} = 0, \cdots, n_{key} - 1$ について以下を実行する ($key^{(sb)}$ は並行処理可能)
4. 波形を増やして以下を実行する
5. $\mathsf{bs\text{-}cpa}(keys^{(SB)}, key^{(sb)}, t_j)$ を計算する
6. 部分鍵 $key^{(sb)}$ が特定されたら $\mathsf{key}[sb] = key^{(sb)}$ とおき，ステップ 2 を最初の波形から繰り返す
7. $\mathsf{key}[1], \cdots, \mathsf{key}[sb]$ を出力する

4.3 BS-CPA の変形手法

既に特定された部分鍵を利用して，解析の SNR を向上するアイデアは他の解析手法にも適用できる．例えば，DPA や高次 DPA，ゼロオフセット 2 次 DPA に適用することで，BS-DPA や BS-HO-DPA，BS-ZO-2DPA などが構成できる．特に，解析に多くの電力波形を必要とし，SNR の改善が重要となる高次 DPA には，本手法は有効であると考えられる．

BS-CPA の組み込みのアイデアと，複数の部分鍵の予測 ($key^{(sb)}$ を複数にする) の組み合わせも効果的だが，解析には多くの計算とメモリ領域が必要となる．

5 実験結果

本節では，DPA contest で公開されている DES のハードウェア実装の電力波形を利用して，BS-CPA の有効性を確認する．

5.1 DES のハードウェア実装への適用

DES のハードウェア実装は，ラウンドの左出力と右出力を保持する 2 つの 32-bit レジスタを利用した，ループアーキテクチャで構成されることが多い．図 1 は，DES のデータフローをあらわす．左レジスタ $\mathsf{register}_L$ (右レジスタ $\mathsf{register}_R$) は，各ラウンドで同一のものを用いる．F はラウンド関数をあらわし，4-bit から 6-bit への拡大転置，6-bit の鍵加算，8 個の 6-

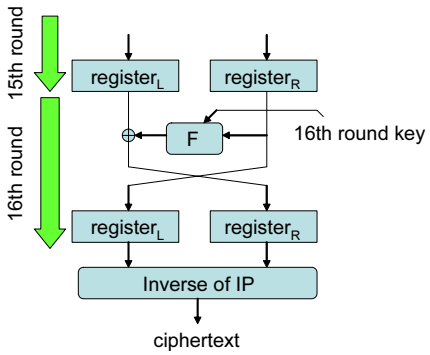

図 1: DES のデータフロー

bit から 4-bit への sbox，32-bit の転置で構成される．

i 番目の電力波形を考えよう．15 ラウンドと 16 ラウンドの終わりに，register$_L$ はラウンドの左出力 $L_{15,i}$ と $L_{16,i}$ をそれぞれ保持する．ここで，$L_{15,i}$ は 16 ラウンドの右出力 $(R_{16,i})$ と 16 ラウンドの F の出力 $F(key^{(sb)}, L_{16,i})$ の排他的論理和に等しい．そこで，16 ラウンドのレジスタのデータ (暗号文) から $L_{15,i}$ の候補を予測して，$L_{16,i}$ との排他的論理和 (ハミング距離) で中間データ候補を計算する．すなわち，

$$b_i^{(sb)} = L_{15,i}^{(sb)} \oplus L_{16,i}^{(sb)} = R_{16,i}^{(sb)} \oplus F^{(sb)}(key^{(sb)}, L_{16,i}) \oplus L_{16,i}^{(sb)}.$$

とする．ここで，$L_{15,i}^{(sb)}$ などは F の置換を考慮し，$sbox_{sb} \in \{sbox_1, \cdots, sbox_8\}$ に対応するデータをあらわす．

BS-CPA では，$n_{sb} \times n_{key} = 8 \times 64$ 個の相関値を同時に計算する．ある部分鍵が特定されたら，波形を最初に巻き戻し，特定された部分鍵を利用して中間データ候補を計算しながら，新たな部分鍵を探索する．

注意: 右レジスタ register$_R$ のハミング距離を利用して中間データ候補を計算することで，さらに SNR を向上できると思われる．register$_R$ は，15 ラウンドと 16 ラウンドの終わりに $R_{15,i} = L_{16,i}$ と $R_{16,i}$ を保持しており，暗号文からハミング距離を計算することが可能ある．DPA contest のデータで右レジスタのデータを利用して解析したところ，処理される時刻が異なるため，解析に必要な電力波形数は削減されなかった．以下では，左レジスタのデータのみを利用して中間データ候補を計算する．

5.2 DPA contest 電力波形への適用

DPA contest は DES のハードウェア実装について，3 種類の電力波形を公開している．我々は以下の条件で解析を行った．

- BS-CPA を用いる
- 部分鍵の予測は 12-bit ではなく 6-bit とする
- 中間データ候補として register$_L$ のハミング距離を用いる
- secmatv1_2006_04_0809 の電力波形を利用する
- データベースのファイル順に従い，ファイルの事前選別は行わない
- すべてのポイントを利用する
- 15 ポイントを 1 ポイントに圧縮する

表 1 に，BS-CPA と CPA の解析結果を示す．どちらの解析手法も，まず $sbox_2$ に対応する部分鍵 $key^{(2)}$ を 65 番目の波形で特定する．2 番目の部分鍵の探索から，解析処理が異なる．

BS-CPA は，電力波形を巻き戻し，$key^{(2)}$ を使って新たな部分鍵を探索し，$key^{(3)}$ を 30 番目の波形で特定する．その後，表 1 に示すように，BS-CPA は再帰的に $key^{(4)}, key^{(7)}, \cdots, key^{(1)}$ を 46, 44, $\cdots$, 48 番目の波形で特定する．これらの最大値は 65 なので，BS-CPA は DES の 16 ラウンドのラウンド鍵 56-bit を 65 波形 (DPA contest の規定では 164 波形で特定することになる．

一方，CPA は既に得られた結果は再利用しない．CPA は $key^{(2)}$ を特定したのち，さらに 13 波形を利用して (75 番目の波形で) $key^{(4)}$ を特定する．そして，順番に $key^{(1)}, key^{(8)}, \cdots, key^{(6)}$ を 90, 91, $\cdots$, 280 番目の波形で特定する．これらの最大値は 280 なので,，CPA が 16 ラウンドのラウンド鍵 56-bit を特定するために必要な電力波形数は 280 (379 波形) となる．

したがって，BS-CPA は CPA よりも少ない電力波形で秘密鍵を特定できることが確認できた．

表 1: BS-CPA と CPA で秘密鍵を特定するために必要な波形数

探索順番	sbox	bs-cpa
1	$sbox_2$	65
2	$sbox_3$	30
3	$sbox_4$	46
4	$sbox_7$	44
5	$sbox_8$	49
6	$sbox_6$	64
7	$sbox_5$	59
8	$sbox_1$	48
max	—	65

発見順番	sbox	cpa
1	$sbox_2$	65
2	$sbox_4$	78
3	$sbox_1$	90
4	$sbox_8$	91
5	$sbox_3$	153
6	$sbox_5$	236
7	$sbox_7$	268
8	$sbox_6$	280
max	—	280

注意: DPA contest の他の結果に従い，解析するポイントを 14450 から 14550 に限定したところ，BS-CPA で秘密鍵を特定するために必要な電力波形数は 65 から 44 (DPA contest の規定では 143 波形) に減らすことができる．さらに，ファイルの事前選別を行うことで，必要な波形数を 8 (107 波形) まで減らすことができる．

参考文献

[1] DPA Contest 2008/2009. `http://www.dpacontest.org/`.

[2] M.-L. Akkar and C. Giraud. An Implementation of DES and AES, Secure against Some Attacks. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *CHES 2001*, volume 2162 of *LNCS*, pages 309–318. Springer, 2001.

[3] E. Brier, C. Clavier, and F. Olivier. Correlation power analysis with a leakage model. In M. Joye and J.-J. Quisquater, editors, *CHES 2004*, volume 3156 of *LNCS*, pages 16–29. Springer, 2004.

[4] S. Chari, J. R. Rao, and P. Rohatgi. Template attacks. In B. S. Kaliski Jr., Ç. K. Koç, and C. Paar, editors, *CHES 2002*, volume 2523 of *LNCS*, pages 13–28. Springer, 2003.

[5] K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic analysis: Concrete results. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *CHES 2001*, volume 2162 of *LNCS*, pages 251–261. Springer, 2001.

[6] L. Goubin and J. Patarin. DES and Differential Power Analysis (The "Duplication" Method). In Ç. K. Koç and C. Paar, editors, *CHES'99*, volume 1717 of *LNCS*, pages 158–172. Springer, 1999.

[7] N. Hanley, R. McEvoy, M. Tunstall, C. Whelan, C. Murphy, and W. P. Marnane. Correlation Power Analysis of Large Word Sizes. In *ISSC*. IET, 2007. Edinburgh, Scotland, UK.

[8] K. Itoh, M. Takenaka, and N. Torii. DPA countermeasure based on the "masking method. In K. Kim, editor, *ICISC 2001*, volume 2288 of *LNCS*, pages 440–456. Springer, 2002.

[9] P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In N. Koblitz, editor, *CRYPTO'96*, volume 1109 of *LNCS*, pages 104–113. Springer, 1996.

[10] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In M. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 388–397. Springer, 1999.

[11] T. S. Messerges. Using second-order power analysis to attack DPA resistant software. In Ç. K. Koç and C. Paar, editors, *CHES 2000*, volume 1965 of *LNCS*, pages 238–251. Springer, 2000.

[12] T. S. Messerges. Securing the AES finalists against power analysis attacks. In B. Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 150–164. Springer, 2001.

[13] K. Schramm and C. Paar. Higher order masking of the aes. In D. Pointcheval, editor, *CT-RSA 2006*, volume 3860 of *LNCS*, pages 208–225. Springer, 2006.

[14] J. Waddle and D. Wagner. Towards efficient second-order power analysis. In M. Joye and J.-J. Quisquater, editors, *CHES 2004*, volume 3156 of *LNCS*, pages 1–15. Springer, 2004.