『暗号の理論と技術』
第 1～2 刷用正誤表
（2025 年 5 月 30 日現在）

このたびは，標記書籍をお買い求めいただき誠にありがとうございました。
標記書籍に誤りがございました。訂正し，深くお詫び申し上げます。

1 刷の修正箇所

頁数	位置	誤	正
33	10行目	暗号化鍵を攻撃者に送る.	暗号化鍵を敵に送る.
66	「数値例」の可逆元の部分	特に，$f(x)$は二つの環R_p , R_qの両方で可逆で，それらの可逆元はそれぞれ $f_p(x) = x^{13} + x^{11} + x^{10} + x^9 + x^8 - x^6 + x^5 + x^4 + x^3 + x^2 + 1$ $f_q(x) = x^{13} - x^{11} - x^{10} + x^9 + x^8 - x^6 + x^5 - x^4 - x^3 + x^2 + 1$	特に，$f(x)$は二つの環R_p , R_qの両方で可逆で，それらの可逆元はそれぞれ $f_p(x) = x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^4 + x^3 + x^2$ $f_q(x) = 21x^{15} + 20x^{14} + 9x^{13} + 15x^{12} + 12x^{11} + 24x^{10} + 28x^9 + 16x^8 + 30x^7 + 18x^6 + 21x^5 + 11x^4 + 6x^3 + 16x^2 + 29x + 4$
184 ～ 199	アルゴリズム 6.1 ～ 6.12		アルゴリズム 6.1 ～ 6.12 の全てにおいて、 「Input」となっているのを「出力」とする
211	下から5～6行目	暗号プロトコルに特化したツールとして、モデル検査に基づく安全性自動検証ではProVerif[4] やTamarin Prover[5]、定理証明器に基づく計算機支援安全性証明ではEasyCrypt[6] やCryptoVerif[7] などが知られている.	暗号プロトコルに特化したツールとして、安全性自動検証ではProVerif[4] やTamarin Prover[5]、計算機支援安全性証明ではEasyCrypt[6]CryptoVerif[7]などが知られている.

<table>
<tr>
<td>252</td>
<td>図8.5，左側の真理値表</td>
<td>
<table>
<tr><th>w_a</th><th>w_b</th><th>w_c</th></tr>
<tr><td>0</td><td>0</td><td>0</td></tr>
<tr><td>0</td><td>1</td><td>0</td></tr>
<tr><td>1</td><td>0</td><td>1</td></tr>
<tr><td>1</td><td>1</td><td>1</td></tr>
</table>
</td>
<td>
<table>
<tr><th>w_a</th><th>w_b</th><th>w_c</th></tr>
<tr><td>0</td><td>0</td><td>0</td></tr>
<tr><td>0</td><td>1</td><td>0</td></tr>
<tr><td>1</td><td>0</td><td>0</td></tr>
<tr><td>1</td><td>1</td><td>1</td></tr>
</table>
</td>
</tr>
<tr>
<td>260</td>
<td></td>
<td>定義8.4：(k,n)しきい値型秘密分散法I；(k,n)しきい値法；(k,n) しきい値法Π_{SSS} は，秘密空間S，シェア空間V および分散アルゴリズムShareと復元アルゴリズムReconst の組からなる．
• Share(s) → $\boldsymbol{v}$：秘密情報$s \in S$を入力として，n 個のシェア$\boldsymbol{v} = (v_0,\ldots, v_{n-1}) \in V_n$ を出力する．
• Reconst($\boldsymbol{v}_I$) → s': $\boldsymbol{v}_I = \{v_i\}_{i\in I}$ を入力として，秘密$s' \in S$ を出力する．

特に，(k,n)しきい値法の安全性要件は以下のように整理される．

定義8.5： (k,n)しきい値法の安全性要件；$P = \{P_0,\ldots, P_{n-1}\}$ をパーティの集合とし，シェアv_i をパーティP_i が持つものとする．$\Gamma = \{A \mid A \in 2^P, |A| \geq k\}$ とする．Γ をアクセス集合と呼ぶ．秘密分散法Π_{SSS} が安全な(k,n)しきい値法であるとは，以下を満たすことをいう．
• 正当性：アクセス集合に含まれるパーティのシェアから確率1で秘密が復元できる．すなわち，$\{P_{i_0},\ldots,P_{i_{m-1}}\} \in \Gamma$ であるならば，$\Pr[\mathrm{Reconst}(v_{i_0},\ldots, v_{i_{m-1}}) = s] = 1$ を満たす．
• 秘匿性： アクセス集合に含まれないパーティのシェアか</td>
<td>定義8.4：(k,n)しきい値型秘密分散法I；(k,n)しきい値法；(k,n) しきい値法Π_{SSS} は，秘密空間M，シェア空間S および分散アルゴリズムShareと復元アルゴリズムReconst の組からなる．
• Share(m) → $\boldsymbol{s}$：秘密情報$m \in M$を入力として，n 個のシェア$\boldsymbol{s} = (s_0,\ldots, s_{n-1}) \in S_n$ を出力する．
• Reconst($\boldsymbol{s}_I$) → m': $\boldsymbol{s}_I = \{s_i\}_{i\in I}$ を入力として，秘密$m' \in M$を出力する．

特に，(k,n)しきい値法の安全性要件は以下のように整理される．

定義8.5： (k,n)しきい値法の安全性要件；$P = \{P_0,\ldots, P_{n-1}\}$ をパーティの集合とし，シェアs_i をパーティP_i が持つものとする．$\Gamma = \{A \mid A \in 2^P, |A| \geq k\}$ とする．Γ をアクセス集合と呼ぶ．秘密分散法Π_{SSS} が安全な(k,n)しきい値法であるとは，以下を満たすことをいう．
• 正当性：アクセス集合に含まれるパーティのシェアから確率1で秘密が復元できる．すなわち，$\{P_{i_0},\ldots,P_{i_{m-1}}\} \in \Gamma$ であるならば，$\Pr[\mathrm{Reconst}(s_{i_0},\ldots, s_{i_{m-1}}) = m \mid \mathrm{Share}(m) = (s_0,\ldots, s_{n-1})] = 1$ を満たす．
• 秘匿性： アクセス集合に含まれないパーティのシェアか</td>
</tr>
</table>

		らは秘密が復元できない．すなわち，任意のs に対して，$\{P_{i_0},\ldots,P_{i_{m-1}}\} \notin \Gamma$ であるならば，$\Pr[S = s \mid V_{i_0} = v_{i_0},\ldots, V_{i_{m-1}} = v_{i_{m-1}}] = \Pr[S = s]$ を満たす． ただし，大文字のS および各V_iは，秘密情報および各シェアに対応する確率変数とする． 上記の秘匿性について，この定義は秘密情報sとシェアの組$v_{i_0},\ldots, v_{i_{m-1}}$が確率的に……	らは秘密が復元できない．すなわち，任意のm に対して，$\{P_{i_0},\ldots,P_{i_{m-1}}\} \notin \Gamma$ であるならば，$\Pr[M = m \mid S_{i_0} = s_{i_0},\ldots, S_{i_{m-1}} = s_{i_{m-1}}] = \Pr[M = m]$ を満たす． ただし，大文字のM および各S_iは，秘密情報および各シェアに対応する確率変数とする． 上記の秘匿性について，この定義は秘密情報mとシェアの組$s_{i_0},\ldots, s_{i_{m-1}}$が確率的に……
261	3行目	この方式では，$f(0) = s$（秘密情報）と	この方式では，$f(0) = m$（秘密情報）と
276	下から2行目	4. $[z] := [z_0] \vee \cdots \vee [z_{n-1}]$ を計算する．	4. $[z] := 1 - [z_0] \vee \cdots \vee [z_{n-1}]$ を計算する．