<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>We need assurance</td>
<td>1</td>
</tr>
<tr>
<td>Factoring large numbers with the TWINKLE device</td>
<td>2</td>
</tr>
<tr>
<td>DES cracking on the Transmogrifier 2a</td>
<td>13</td>
</tr>
<tr>
<td>Modeling the crypto-processor from design to synthesis</td>
<td>25</td>
</tr>
<tr>
<td>A DES ASIC suitable for network encryption at 10 Gbps and beyond</td>
<td>37</td>
</tr>
<tr>
<td>Hardware design and performance estimation of the 128-bit block cipher CRYPTON</td>
<td>49</td>
</tr>
<tr>
<td>Fast implementation of public-key cryptography on a DSP TMS320C6201</td>
<td>61</td>
</tr>
<tr>
<td>How to implement cost-effective and secure public key cryptosystems</td>
<td>73</td>
</tr>
<tr>
<td>Montgomery's multiplication technique: How to make it smaller and faster</td>
<td>80</td>
</tr>
<tr>
<td>A scalable architecture for Montgomery multiplication</td>
<td>94</td>
</tr>
<tr>
<td>Arithmetic design for permutation groups</td>
<td>109</td>
</tr>
<tr>
<td>Fast multiplication in finite fields GF$(2^{N})$</td>
<td>122</td>
</tr>
<tr>
<td>Efficient finite field basis conversion involving dual bases</td>
<td>135</td>
</tr>
<tr>
<td>Power analysis attacks of modular exponentiation in smartcards</td>
<td>144</td>
</tr>
<tr>
<td>DES and differential power analysis</td>
<td>158</td>
</tr>
<tr>
<td>IPA: A new class of power attacks</td>
<td>173</td>
</tr>
<tr>
<td>Security evaluation schemas for the public and private market with a focus on smart card systems</td>
<td>187</td>
</tr>
<tr>
<td>A design of reliable true random number generator for cryptographic applications</td>
<td>204</td>
</tr>
<tr>
<td>Random number generators founded on signal and information theory</td>
<td>219</td>
</tr>
<tr>
<td>A high-performance flexible architecture for cryptography</td>
<td>231</td>
</tr>
<tr>
<td>CryptoBooster: A reconfigurable and modular cryptographic coprocessor</td>
<td>246</td>
</tr>
<tr>
<td>Elliptic curve scalar multiplier design using FPGAs</td>
<td>257</td>
</tr>
<tr>
<td>Highly regular architectures for finite field computation using redundant basis</td>
<td>269</td>
</tr>
<tr>
<td>Low complexity bit-parallel finite field arithmetic using polynomial basis</td>
<td>280</td>
</tr>
<tr>
<td>Resistance against differential power analysis for elliptic curve cryptosystems</td>
<td>292</td>
</tr>
<tr>
<td>Probing attacks on tamper-resistant devices</td>
<td>303</td>
</tr>
<tr>
<td>Fast multiplication on elliptic curves over GF$(2^{m})$ without precomputation</td>
<td>316</td>
</tr>
<tr>
<td>NICE - New Ideal Coset Encryption</td>
<td>328</td>
</tr>
<tr>
<td>Encryption with statistical self-synchronization in synchronous broadband networks</td>
<td>340</td>
</tr>
<tr>
<td>Author Index</td>
<td>353</td>
</tr>
</tbody>
</table>

Table of Contents provided by Blackwell's Book Services and R.R. Bowker. Used with permission.