Enumeration of Permutation Binomials over Finite Fields

St.Petersburg Department of Steklov Institute of Mathematics
Nikolay N. Vasiliev
&
St.Petersburg State Polytechnical University
Valeria O. Nikolaenko

Dubna, July, 2009
Introduction

• RSA cipher function is a monomial \((x^m \mod p)\) which permutes ring \(\mathbb{Z}/p\mathbb{Z}\)

• RSA can be generalized by replacing monomials with polynomials

• Polynomials must be
  – defined over finite ring
  – invertible for existing of decipher algorithm
  – efficient computable for high speed of cipher algorithm

• The main aim of this work is to construct tables of permutation binomials in connection with the possibility of using them in RSA instead of monomials
History

• In 1988 and 1993, R. Lidl and G.L.Mullen listed seventeen open problems and conjectures involving PPs. Among them:
  • Find new classes of PPs over GF(q)
  • Find the way to use them in cryptography
  • Consider the binomial \( f(x) = x^i + ax^j \). Determine conditions on \( i, j, a \) and \( q \) so that \( f(x) \) permutes \( F_q \)

• In 2008 E. Shadrin listed permutation binomials over prime fields \( F_p \)
Theoretical Aspects

- Let $p$ be a prime, $n$ be a positive integer, and $F_q = GF(p^n)$ be the finite field of order $q = p^n$.

- Let $\phi(x)$ be an arbitrary function from $F_q$ to $F_q$. Then $\phi(x)$ can be written as a polynomial $f(x)$ over $F_q$ with $\deg(f) < q$ from the Lagrange Interpolation Formula.

- A polynomial $f(x)$ in $F_q[x]$ is called a permutation polynomial (PP), if $f(x)$ permutes $F_q$ as a polynomial function.
Finite fields arithmetic
- The element of a field GF(p^n) represented by a polynomial of degree less than n with the coefficients in subfield GF(p) = Z/pZ
- Operations in finite field correspond to multiplication and addition in field F_p[x]/f(x), where f(x) – is irreducible polynomial over GF(p)

Implementation
- The element of a field is an array of integers
- Addition – elementwise addition modulo p
- Multiplication – as for polynomials, result is reduced with f(x)

Optimizations
- Results caching
- For binary fields (of kind GF(2^n)) operations over arrays rewritten to binary operations over integer numbers
Test for Permutation

- **Hermite Criterion:** $f(x)$ is a PP over $F_q$ if and only if
  - $f(x)$ has exactly one root over $F_q$, and
  - for each integer $t$ with $1 \leq t \leq q - 2$ and with $t \not\equiv 0 \pmod{p}$ the reduction of $(f(x))^t \pmod{x^q - x}$ has degree $\leq q - 2$

  - Hermite Criterion checking time complexity is at least $O(q^2)$ and space complexity is $O(q)$

- **Straight examination of all values**
  - For binomial to get its value at arbitrary point cost $O(1)$
  - To get all values cost $O(q)$ by time and $O(q)$ by space
Permutation Binomials
Enumeration. Theory

- The monomial $x^n$ is a PP if and only if $(n, q - 1) = 1$

- $a x^i + b x^j$ is a PP over $F_q$ if and only if $x^i + a^{-1} bx^j$ is a PP over $F_q$, so we consider the binomial such as $f(x) = x^i + a \cdot x^j$, $a$ from $F_q^*$

- If $i \mid q-1$, then $f(x)$ is not a PP

- If $(-a)^s = 1$, where $s = \frac{q - 1}{(q - 1, i - j)}$, then $f(x)$ is not a PP

- If $(i, j) = e > 1$, then $f(x) = h(x^e)$, where $h(x) = x^{i/e} + a \cdot x^{j/e}$, then $f(x)$ is a PP if and only if both $h(x)$ and $x^e$ are PPs

- If $f(x)$ is a PP then $\deg(f(x)) < q - 1$
Permutation Binomials
Enumeration. Implementation

- In general the complexity of enumeration is $O(q^4)$
  - $q^3$ – total amount of binomials
  - $O(q)$ – time complexity of permutation check

- Improving enumeration by using symmetries. By single PB $f(x)$ we can create the series of PB by
  - substitution of $x^e$, where $(e, q - 1) = 1$
  - substitution of $k \cdot x$, where $k \neq 0$
Inverse Polynomial

- **Lagrange Interpolation Formula**

  \[
  f_{\text{inv}}(x) = \sum_{j=0}^{q} j \cdot l_j(x), \quad \text{where} \quad l_j(x) = \prod_{i=0, i \neq j}^{q} \frac{x - f(i)}{f(j) - f(i)}
  \]

- **Simplification for PPs**

  \[
  x^p - x = (x - a) \cdot (x^{p-1} + ax^{p-2} + a^2 x^{p-3} + \ldots + a^{p-2} x), \text{ where } a \neq 0
  \]

  \[
  f_{\text{inv}} = \sum_{i=0}^{q-1} (-i) \cdot \prod_{j=0, j \neq i}^{q-1} (x - f(j)) = \sum_{i=0}^{q-1} (-i) \frac{x^q - x}{x - f(i)} = \\
  \sum_{i=1}^{q-1} (-i) \cdot (x^{q-1} + f(i)x^{q-2} + f(i)^2 x^{q-2} + \ldots + f(i)^{q-2} x) = \sum_{k=1}^{q-1} x^k \sum_{i=1}^{q-1} (-i) \cdot (f(i))^{q-k-1}
  \]

  \[
  a_k = \sum_{i=1}^{q} - (f(i))^{q-k-1} \cdot i
  \]
Permutations

- Every PP defines a permutation and vise versa

- A permutation defines the graph – the composition of simple cycles

- If two PPs define isomorphic graphs then they are conjugate if \( f(x) \) and \( g(x) \) – PPs with isomorphic graphs, then there exists PP \( h(x) \): \( f(x) = g(h(x)) \)

- The order of permutation \( \pi \) in symmetric group equals to least common multiple of its cycle lengths
Permutation orders

1. Suppose we want to decode a message $I$
2. Let $f(x)$ be a PP, used in cipher
3. Then all we know is just the code of a message $f(I)$ and the coding function $f(x)$, which can hardly be inverted
4. By repeating the coding algorithm we may find the order of permutation defined by $f(x)$ (let name it $\pi$)
5. Then the initial message will exactly $(f(I))^{\pi^{-1}}$, that's why the orders of permutations are very important characteristics of the usability of PP in RSA
6. The lower the order the easier it is to break the cipher
Young Diagrams

- Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ be a not increasing sequence, then a Young Diagram is a finite collection of boxes, or cells, arranged in bottom-justified columns, with the $i$-th column size equals to $a_i$.

**Averaged Young Diagrams for PBs**

- The red line on a graph shows the limiting shape of Young Diagram from uniform distribution.
- Colorful points – are front corners of Young Diagrams for PBs.
**PB Properties**

- **Invariant with respect to Frobenius automorphism**
  
  Frobenius automorphism $F(x)$ over field $GF(p^n)$ is $F(x) = x^p$

  Binomials with coefficients in simple subfield and only they appear to be invariant with respect to Frobenius automorphism, i.e. substitution of $x^p$ and raising to $p$ power are equivalent

- **Continuation of permutations from simple subfields**

  1. If PB has coefficients from simple subfield, it permutes this subfield
  2. Experimentally was shown that the contrary fact is not always true

  **Example:**
  $x^8+25\cdot x - PB$ over $GF(29)$
  $x^8+29^k\cdot x^29^k$ for any natural $k$ is not a PB over $GF(29^2)$
Amount of PBs

• Let us throw $q$ times a cube with $q$ facets

• As there exists the correspondence between polynomials and its values due to Lagrange Interpolation Formula there is no difference how to get the polynomial – by its coefficients or by its values

• So the probability to get binomial is equal to $\frac{q^4}{q^q}$

• The probability to get permutation is $\frac{q!}{q^q}$

• It could be expected that the probability to get the PB is approximately:

$$\frac{q^4}{q^q} \cdot \frac{q!}{q^q} = \frac{q!}{q^{2q-4}}$$

• As the number of different throws is $q^q$, then the number of permutation binomials suppose to be equals to

$$\frac{q!}{q^{2q-4}} \cdot q^q = \frac{q!}{q^{q-4}} \approx O\left(\frac{q^{q+0.5}}{e^q \cdot q^{q-4}}\right) = O\left(\frac{q^{4.5}}{e^q}\right)$$

• But in reality amount of PBs is much more greater...
Amount of PBs

<table>
<thead>
<tr>
<th>p/n</th>
<th>Amount of PBs with leading coefficient equals to one</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0 0 0 40 0 3528 0 46848 216432 1471800 0 17219520 0</td>
</tr>
<tr>
<td>3</td>
<td>0 12 300 4064 42240 567648 4773132</td>
</tr>
<tr>
<td>5</td>
<td>0 216 8100 257856 8684200</td>
</tr>
<tr>
<td>7</td>
<td>4 912 72144 3705600</td>
</tr>
<tr>
<td>11</td>
<td>16 5888 931392</td>
</tr>
<tr>
<td>13</td>
<td>8 12432 2708640</td>
</tr>
<tr>
<td>17</td>
<td>24 43584 15569280</td>
</tr>
<tr>
<td>19</td>
<td>66 51552</td>
</tr>
<tr>
<td>23</td>
<td>100 134400</td>
</tr>
<tr>
<td>29</td>
<td>120 273024</td>
</tr>
<tr>
<td>31</td>
<td>224 381184</td>
</tr>
<tr>
<td>37</td>
<td>180 785376</td>
</tr>
<tr>
<td>41</td>
<td>144 1077888</td>
</tr>
<tr>
<td>43</td>
<td>348 1304160</td>
</tr>
<tr>
<td>47</td>
<td>484 2359808</td>
</tr>
<tr>
<td>53</td>
<td>384 3326400</td>
</tr>
<tr>
<td>59</td>
<td>784 4997888</td>
</tr>
<tr>
<td>61</td>
<td>720 5308800</td>
</tr>
<tr>
<td>67</td>
<td>1000 8131840</td>
</tr>
<tr>
<td>71</td>
<td>816 8221824</td>
</tr>
</tbody>
</table>

The absence of PBs over fields GF(2^p), where p = 1, 2, 3, 5, 7, 11, 13 can be explained be the fact that (2^p – 1) – is prime, and the necessary condition of permutation is broken $GCD(i - j, q - 1) = 1$

<table>
<thead>
<tr>
<th>The order of the field</th>
<th>The degree of approximate polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>
### Example of table with PBs

<table>
<thead>
<tr>
<th>Field</th>
<th>№</th>
<th>Binomials</th>
<th>Inverse</th>
<th>Order</th>
<th>Orbit size</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^4$</td>
<td>0</td>
<td>(0,0,0,1) * $x^4 + (0,0,0,1,0) * x^1$</td>
<td>(1,0,1,1) * $x^4 + (0,1,0,1) * x^1$</td>
<td>3</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>(0,0,0,1) * $x^4 + (0,1,0,0) * x^1$</td>
<td>(1,0,1,0) * $x^4 + (1,0,0,0) * x^1$</td>
<td>3</td>
<td>20</td>
</tr>
<tr>
<td>$2^6$</td>
<td>0</td>
<td>(0,0,0,0,1) * $x^4 + (0,0,0,1,0) * x^1$</td>
<td>(0,0,1,1,1,1) * $x^8 + (0,0,0,1,1,1) * x^1$</td>
<td>7</td>
<td>162</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>(0,0,0,0,1) * $x^4 + (0,0,0,1,0,0) * x^1$</td>
<td>(0,0,1,1,1,0) * $x^8 + (0,0,0,1,0,1) * x^1$</td>
<td>7</td>
<td>162</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>(0,0,0,0,1) * $x^8 + (0,0,0,1,0,1) * x^1$</td>
<td>(0,1,0,1,1,0) * $x^8 + (0,1,0,1,0,1) * x^1$</td>
<td>7</td>
<td>162</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>(0,0,0,0,1) * $x^8 + (0,0,1,0,0,0) * x^1$</td>
<td>(0,1,0,1,1,1) * $x^8 + (0,1,0,0,0,1) * x^1$</td>
<td>7</td>
<td>162</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>(0,0,0,0,1) * $x^8 + (0,0,1,0,0,1) * x^1$</td>
<td>(0,1,1,0,0,1) * $x^8 + (0,0,0,1,1,1) * x^1$</td>
<td>7</td>
<td>162</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>(0,0,0,0,1) * $x^8 + (0,0,1,0,1,0) * x^1$</td>
<td>(0,1,1,0,0,0) * $x^8 + (0,0,1,0,1,0) * x^1$</td>
<td>7</td>
<td>162</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>(0,0,0,0,1) * $x^{10} + (0,0,0,1,0,1) * x^1$</td>
<td>(0,0,0,0,1) * $x^{10} + (0,0,1,0,1,1) * x^1$</td>
<td>54</td>
<td>126</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>(0,0,0,0,1) * $x^{10} + (0,0,1,0,0,1) * x^1$</td>
<td>(0,0,0,0,1) * $x^{10} + (0,0,1,1,0,1) * x^1$</td>
<td>54</td>
<td>126</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>(0,0,0,0,1) * $x^{13} + (0,0,0,1,1,1) * x^1$</td>
<td>(0,0,0,0,1) * $x^{13} + (0,0,0,1,0,1) * x^4$</td>
<td>36</td>
<td>126</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>(0,0,0,0,1) * $x^{13} + (0,0,0,1,1,0) * x^1$</td>
<td>(0,0,0,0,1) * $x^{13} + (0,0,0,1,1,1) * x^4$</td>
<td>36</td>
<td>126</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>(0,0,0,0,1) * $x^{16} + (0,0,0,1,0,0) * x^1$</td>
<td>(0,0,0,0,1) * $x^{16} + (0,0,0,1,0,0) * x^1$</td>
<td>6</td>
<td>378</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>(0,0,0,0,1) * $x^{16} + (0,0,0,1,0,1) * x^4$</td>
<td>(0,0,0,0,1) * $x^{16} + (0,0,0,1,0,1) * x^4$</td>
<td>6</td>
<td>378</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>(0,0,0,0,1) * $x^{16} + (0,0,0,1,0,0) * x^1$</td>
<td>(0,0,0,0,1) * $x^{16} + (0,0,0,1,0,0) * x^1$</td>
<td>6</td>
<td>378</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>(0,0,0,0,1) * $x^{16} + (0,0,0,1,0,0) * x^1$</td>
<td>(0,0,0,0,1) * $x^{16} + (0,0,0,1,0,0) * x^1$</td>
<td>6</td>
<td>378</td>
</tr>
</tbody>
</table>
Amount of PBs over GF(p)
Amount of PBs over $\text{GF}(p^2)$

![Graph showing the amount of PBs over GF($p^2$)]

- PB number over GF($p^2$)
- Fitting polynomial of fourth degree

![Graph showing the logarithm of PB number over GF($p^2$)]

- PB over GF($p^2$)
- $4.16 \times x - 1.46$
Amount of PBs over GF(p³)
Results

• The number of permutation binomials depending to field characteristics was studied

• Permutation binomials tables constructed, where binomials with properties listed below marked:
  – binomials, that are invariant with respect to Frobenius automorphism
  – binomials, that have binomial inverse
  – binomials, continuable from simple subfield

• The orders of binomials in symmetric groups found

• Average Young diagrams for permutation cycle lengths were obtained