Design and Analysis of a New Cryptosystem

J Robert Buchanan

Millersville University of Pennsylvania

November 20, 2014

Outline

- Description of private security parameters and public initialization value.
- High level overview of generation of key stream from private/public values.
- Discussion of mathematical/cryptanalytic questions relevant to this algorithm.

More details found in article linked at

http://eprint.iacr.org/2014/894

of the International Association for Cryptologic Research.

Private Security Parameters

Ordered triple: (c, α, m) where

- c: is an **integer** in the interval $[2^{256}, 2^{1160}]$,
- α: is a **real number** in the interval $[\pi/12, 5\pi/12]$,
- m: is a **real number** in the interval $[4, 65535]$.

Private Security Parameters

Ordered triple: (c, α, m) where

- c: is an **integer** in the interval $[2^{256}, 2^{1160}]$,
- α: is a **real number** in the interval $[\pi/12, 5\pi/12]$,
- m: is a **real number** in the interval $[4, 65535]$.

The private security parameters involve

$$1160 + 54 + 56 = 1270$$

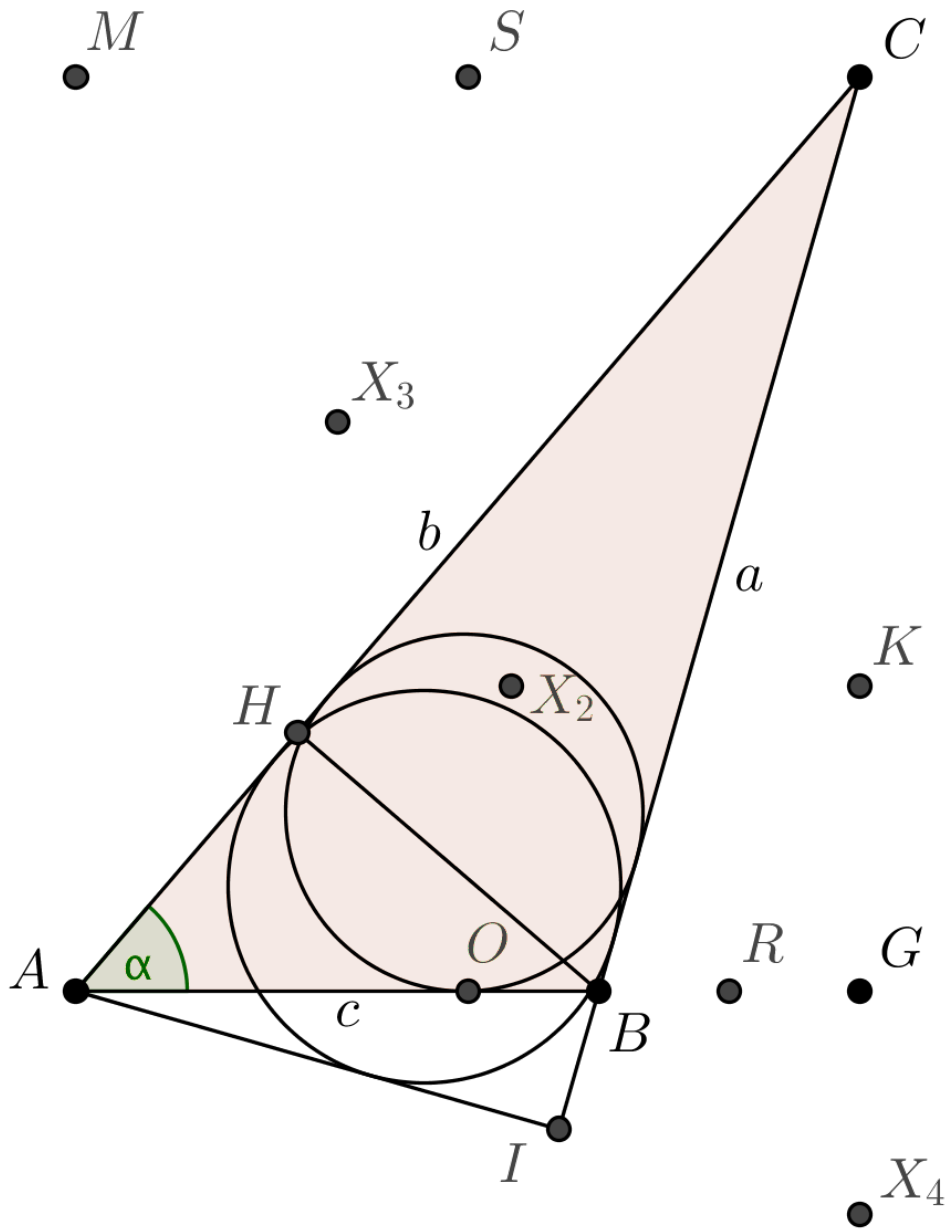
bits of secret state (assuming IEEE-754 double precision floating point format is used to represent α and m).

Two-Dimensional Geometric Form

Once the secret (c, α, m) has been shared, two parties construct $\triangle ABC$ where $\angle CAB = \alpha$, $\|\overline{AB}\| = c$, and $\|\overline{AC}\| = cm$.

The restriction of $4 \leq m \leq 65535$ ensures $\triangle ABC$ is an obtuse scalene triangle.

Example $\triangle ABC$



Miscellaneous Points of $\triangle ABC$

X_2: centroid of $\triangle ABC$

X_3: circumcenter of $\triangle ABC$

X_4: orthocenter of $\triangle ABC$

G: line segment $\overline{AG} = \text{proj}_{\overline{AB}} \overline{AC}$

H: line segment $\overline{BH}$ is height of $\triangle ABC$

I: intersection of $\overline{AX_4}$ and $\overrightarrow{BC}$

K: intersection of line through X_2 parallel to $\overline{AB}$ with $\overline{CG}$

M: intersection of line through A perpendicular to $\overline{AB}$ with line through C parallel to $\overline{AB}$

O: midpoint of $\overline{AG}$

R: midpoint of $\overline{BG}$

S: midpoint of $\overline{CM}$

Public Initialization Value

n: an integer for which $10^8 \leq n < 10^9$

Comments:

- The private security parameters can be re-used a maximum of 9×10^8 times,
- Each value of n creates a different 3D figure from the 2D geometric form previously described.

Irrational Numbers and Mantissas

Define function $f : \mathbb{N} \to [0, 1)$ as

$$f(q) = \sqrt{q} - \lfloor \sqrt{q} \rfloor. \tag{1}$$

When q is prime, $f(q)$ is irrational.

Irrational Numbers and Mantissas

Define function $f : \mathbb{N} \to [0, 1)$ as

$$f(q) = \sqrt{q} - \lfloor \sqrt{q} \rfloor. \tag{1}$$

When q is prime, $f(q)$ is irrational.

Think of $f(q)$ as being expressed in mantissa-exponent form:

$$f(q) = 0.d_1 d_2 d_3 \cdots \times 10^{-b_0}$$

where $d_1 \neq 0$ and $b_0 \geq 0$.

Irrational Numbers and Mantissas

Define function $f : \mathbb{N} \to [0, 1)$ as

$$f(q) = \sqrt{q} - \lfloor \sqrt{q} \rfloor. \tag{1}$$

When q is prime, $f(q)$ is irrational.

Think of $f(q)$ as being expressed in mantissa-exponent form:

$$f(q) = 0.d_1 d_2 d_3 \cdots \times 10^{-b_0}$$

where $d_1 \neq 0$ and $b_0 \geq 0$.

Define function $F(q; N)$ for q prime and $N \in \mathbb{N}$ as

$$F(q; N) = \lfloor f(q) \times 10^{b_0 + \lfloor N \log 16 \rfloor} \rfloor = d_1 d_2 d_3 \cdots d_{\lfloor N \log 16 \rfloor}. \tag{2}$$

Irrational Numbers and Mantissas

Define function $f : \mathbb{N} \to [0, 1)$ as

$$f(q) = \sqrt{q} - \lfloor \sqrt{q} \rfloor. \tag{1}$$

When q is prime, $f(q)$ is irrational.

Think of $f(q)$ as being expressed in mantissa-exponent form:

$$f(q) = 0.d_1 d_2 d_3 \cdots \times 10^{-b_0}$$

where $d_1 \neq 0$ and $b_0 \geq 0$.

Define function $F(q; N)$ for q prime and $N \in \mathbb{N}$ as

$$F(q; N) = \lfloor f(q) \times 10^{b_0 + \lfloor N \log 16 \rfloor} \rfloor = d_1 d_2 d_3 \cdots d_{\lfloor N \log 16 \rfloor}. \tag{2}$$

Comment: $F(q; N)$ converts a prime integer into a pseudorandom sequence of $4N$ bits.

Combining n and $\triangle ABC$

Determine the primes:

$$\begin{aligned} q_1 &= \lceil b \rceil_{\mathbb{P}} = \lceil c\, m \rceil_{\mathbb{P}} \\ p &= \left\lceil \frac{q_1}{n} \right\rceil_{\mathbb{P}} \end{aligned}$$

Comment: the minimum of p is a prime in excess of 4.631×10^{68}.

Combining n and $\triangle ABC$

Determine the primes:

$$\begin{aligned} q_1 &= \lceil b \rceil_{\mathbb{P}} = \lceil c\, m \rceil_{\mathbb{P}} \\ p &= \left\lceil \frac{q_1}{n} \right\rceil_{\mathbb{P}} \end{aligned}$$

Comment: the minimum of p is a prime in excess of 4.631×10^{68}.
Compute $d = F(p; 4050)$, then in hexadecimal

$$(d)_{16} = (F(p; 4050))_{16} = h_1 h_2, h_3 h_4, h_5 h_6, \cdots, h_{4049} h_{4050} \quad (3)$$

a pseudorandom string of 2025 bytes.

Matrix H

Populate a 45×45 matrix H with the bytes of $(d)_{16}$ starting in the center and spiraling clockwise.

$$H = \begin{bmatrix} h_{3873}h_{3874} & & & \cdots & & & h_{3961}h_{3962} \\ & \ddots & & & & \iddots & \\ & & h_{33}h_{34} & h_{35}h_{36} & h_{37}h_{38} & h_{39}h_{40} & h_{41}h_{42} & & \\ & & h_{31}h_{32} & h_{9}h_{10} & h_{11}h_{12} & h_{13}h_{14} & h_{43}h_{44} & & \\ \vdots & & h_{29}h_{30} & h_{7}h_{8} & h_{1}h_{2} & h_{15}h_{16} & h_{45}h_{46} & & \vdots \\ & & h_{27}h_{28} & h_{5}h_{6} & h_{3}h_{4} & h_{17}h_{18} & h_{47}h_{48} & & \\ & & h_{25}h_{26} & h_{23}h_{24} & h_{21}h_{22} & h_{19}h_{20} & h_{49}h_{50} & & \\ & \iddots & & & & & & \ddots & \\ h_{3785}h_{3786} & & & \cdots & & & h_{4049}h_{4050} \end{bmatrix} \tag{4}$$

Diameters and Multipliers (1 of 3)

Process integer d five decimal digits at a time.

$$d \quad = \quad F(p; 4050) = d_1 \cdots d_5 d_6 \cdots d_{10} \cdots d_{4875} d_{4876}$$

Diameters and Multipliers (1 of 3)

Process integer d five decimal digits at a time.

$$\begin{aligned} d &= F(p; 4050) = d_1 \cdots d_5 d_6 \cdots d_{10} \cdots d_{4875} d_{4876} \\ s &= 1 + [d_1 d_2 d_3 d_4 d_5 \pmod{45}] \\ t &= 1 + [d_6 d_7 d_8 d_9 d_{10} \pmod{45}] \end{aligned}$$

Diameters and Multipliers (1 of 3)

Process integer d five decimal digits at a time.

$$\begin{aligned} d &= F(p; 4050) = d_1 \cdots d_5 d_6 \cdots d_{10} \cdots d_{4875} d_{4876} \\ s &= 1 + [d_1 d_2 d_3 d_4 d_5 \pmod{45}] \\ t &= 1 + [d_6 d_7 d_8 d_9 d_{10} \pmod{45}] \end{aligned}$$

- If $H_{s,t}$ is even, let $(k)_{16} = H_{s,t} H_{s,t+1} H_{s,t+2} H_{s,t+3} H_{s,t+4}$.
- If $H_{s,t}$ is odd, let $(k)_{16} = H_{s,t} H_{s+1,t} H_{s+2,t} H_{s+3,t} H_{s+4,t}$.

Diameters and Multipliers (1 of 3)

Process integer d five decimal digits at a time.

$$\begin{aligned} d &= F(p; 4050) = d_1 \cdots d_5 d_6 \cdots d_{10} \cdots d_{4875} d_{4876} \\ s &= 1 + [d_1 d_2 d_3 d_4 d_5 \pmod{45}] \\ t &= 1 + [d_6 d_7 d_8 d_9 d_{10} \pmod{45}] \end{aligned}$$

- If $H_{s,t}$ is even, let $(k)_{16} = H_{s,t} H_{s,t+1} H_{s,t+2} H_{s,t+3} H_{s,t+4}$.
- If $H_{s,t}$ is odd, let $(k)_{16} = H_{s,t} H_{s+1,t} H_{s+2,t} H_{s+3,t} H_{s+4,t}$.

Define
$m_2 = \left(\left[15 \times 10^6 \right] + \left[k \pmod{70 \times 10^6} \right] \right) \times 10^{-8} \in [0.15, 0.85)$
and in a similar fashion define m_3 and m_4.

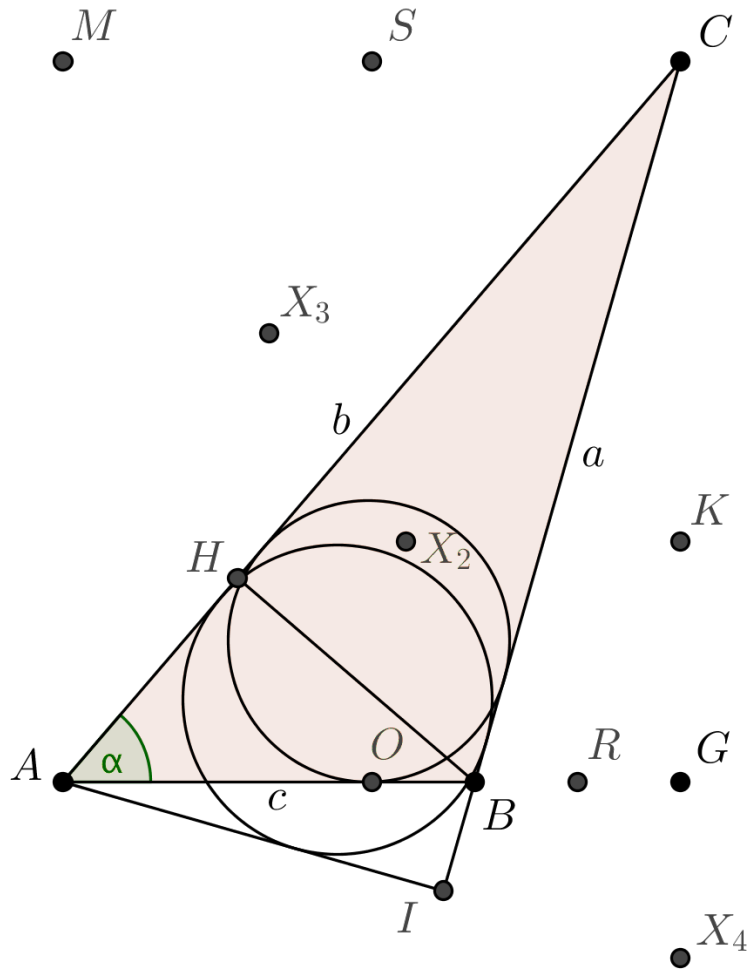
Diameters and Multipliers (2 of 3)

From $\triangle ABC$ find the following values:

$$\varnothing_2 = \frac{2\Delta_{ABC}}{\|\overline{AC}\|}$$

$$\varnothing_3 = \frac{2\Delta_{ACI}}{s_{ACI}}$$

$$\varnothing_4 = \frac{2\Delta_{ABC}}{s_{ABC}}.$$



Diameters and Multipliers (3 of 3)

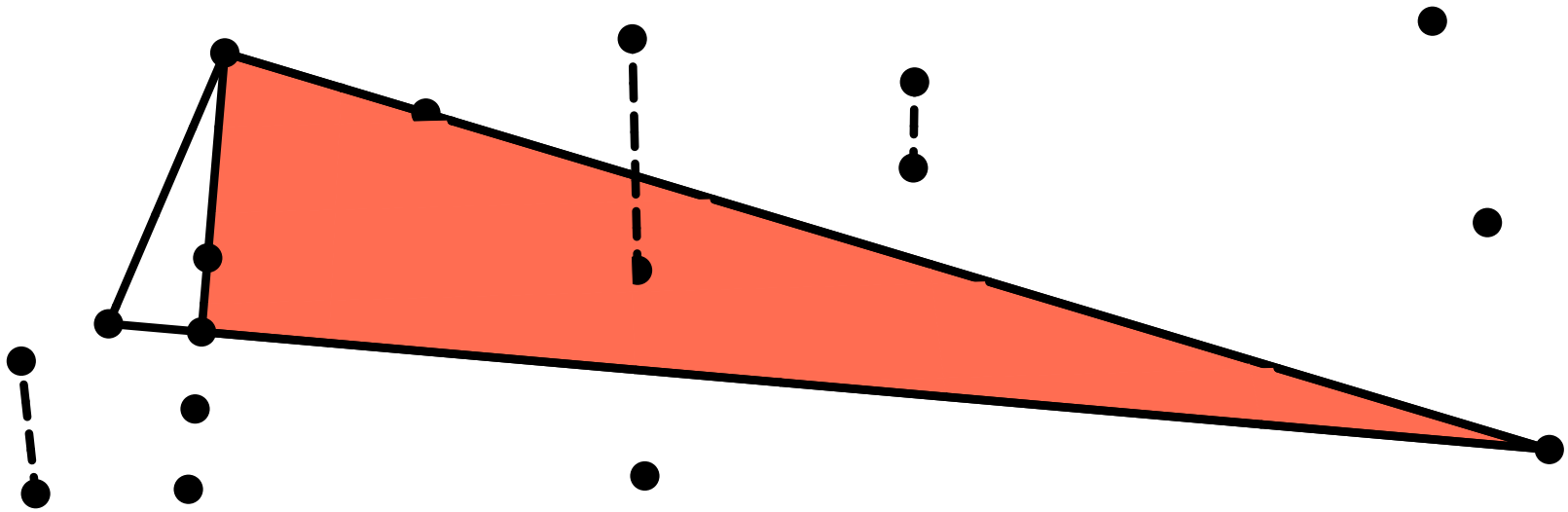
Assuming $\triangle ABC$ lies in the $z = 0$ plane locate the following three points:

Z_2: point above X_2 at altitude $\varnothing_2 m_2$.

Z_3: point above X_3 at altitude $\varnothing_3 m_3$.

Z_4: point above X_4 at altitude $\varnothing_4 m_4$.

3D Geometric Construction



Generation of Primes

Once the 3D geometric figure is constructed, fifteen primes can be calculated from it.

$$\begin{Bmatrix} p_1 & p_2 & p_3 & p_4 & p_5 \\ p_6 & p_7 & p_8 & p_9 & p_{10} \\ p_{11} & p_{12} & p_{13} & p_{14} & p_{15} \end{Bmatrix} = \begin{Bmatrix} \lceil \|\overline{AZ_2}\| \rceil_{\mathbb{P}} & \lceil \|\overline{BZ_2}\| \rceil_{\mathbb{P}} & \left\lceil \|\overline{CZ_2}\| \right\rceil_{\mathbb{P}} & \left\lceil \|\overline{GZ_2}\| \right\rceil_{\mathbb{P}} & \lceil \|\overline{X_3Z_2}\| \rceil_{\mathbb{P}} \\ \left\lceil \|\overline{CZ_3}\| \right\rceil_{\mathbb{P}} & \lceil \|\overline{KZ_3}\| \rceil_{\mathbb{P}} & \lceil \|\overline{MZ_3}\| \rceil_{\mathbb{P}} & \left\lceil \|\overline{SZ_3}\| \right\rceil_{\mathbb{P}} & \lceil \|\overline{X_4Z_3}\| \rceil_{\mathbb{P}} \\ \lceil \|\overline{BZ_4}\| \rceil_{\mathbb{P}} & \left\lceil \|\overline{CZ_4}\| \right\rceil_{\mathbb{P}} & \lceil \|\overline{MZ_4}\| \rceil_{\mathbb{P}} & \left\lceil \|\overline{OZ_4}\| \right\rceil_{\mathbb{P}} & \lceil \|\overline{X_2Z_4}\| \rceil_{\mathbb{P}} \end{Bmatrix}$$

Generation of Primes

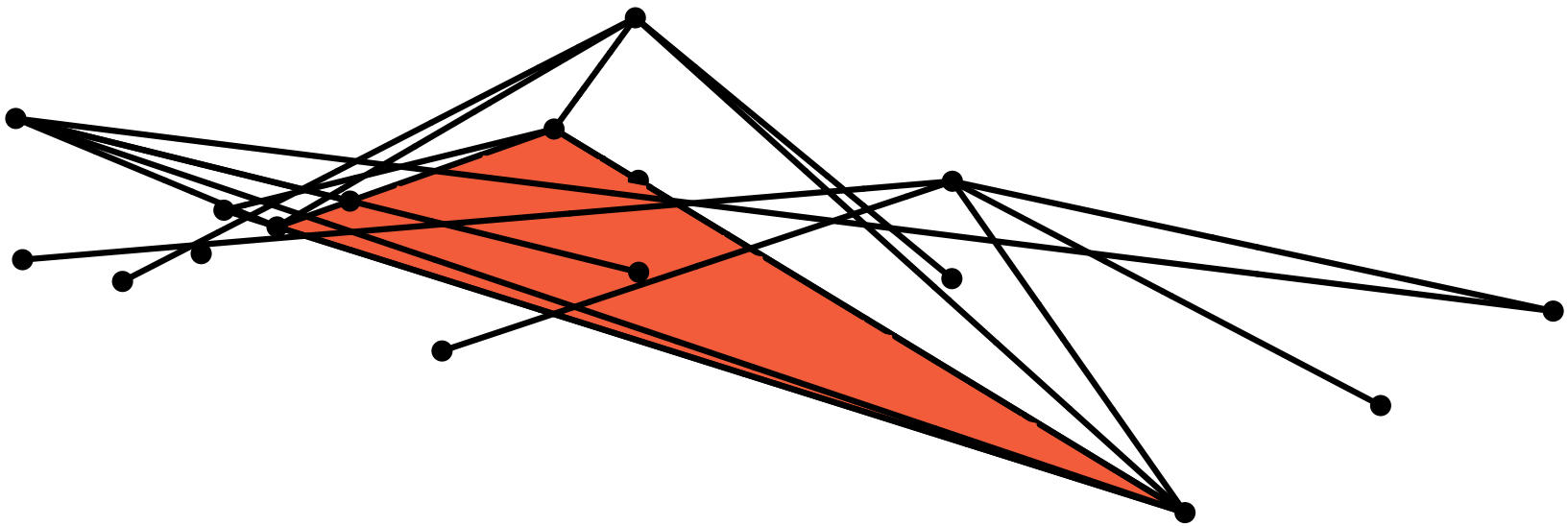
Once the 3D geometric figure is constructed, fifteen primes can be calculated from it.

$$\begin{Bmatrix} p_1 & p_2 & p_3 & p_4 & p_5 \\ p_6 & p_7 & p_8 & p_9 & p_{10} \\ p_{11} & p_{12} & p_{13} & p_{14} & p_{15} \end{Bmatrix} = \begin{Bmatrix} \lceil \|\overline{AZ_2}\| \rceil_{\mathbb{P}} & \lceil \|\overline{BZ_2}\| \rceil_{\mathbb{P}} & \left\lceil \|\overline{CZ_2}\| \right\rceil_{\mathbb{P}} & \left\lceil \|\overline{GZ_2}\| \right\rceil_{\mathbb{P}} & \lceil \|\overline{X_3Z_2}\| \rceil_{\mathbb{P}} \\ \left\lceil \|\overline{CZ_3}\| \right\rceil_{\mathbb{P}} & \lceil \|\overline{KZ_3}\| \rceil_{\mathbb{P}} & \lceil \|\overline{MZ_3}\| \rceil_{\mathbb{P}} & \left\lceil \|\overline{SZ_3}\| \right\rceil_{\mathbb{P}} & \lceil \|\overline{X_4Z_3}\| \rceil_{\mathbb{P}} \\ \lceil \|\overline{BZ_4}\| \rceil_{\mathbb{P}} & \left\lceil \|\overline{CZ_4}\| \right\rceil_{\mathbb{P}} & \lceil \|\overline{MZ_4}\| \rceil_{\mathbb{P}} & \left\lceil \|\overline{OZ_4}\| \right\rceil_{\mathbb{P}} & \lceil \|\overline{X_2Z_4}\| \rceil_{\mathbb{P}} \end{Bmatrix}$$

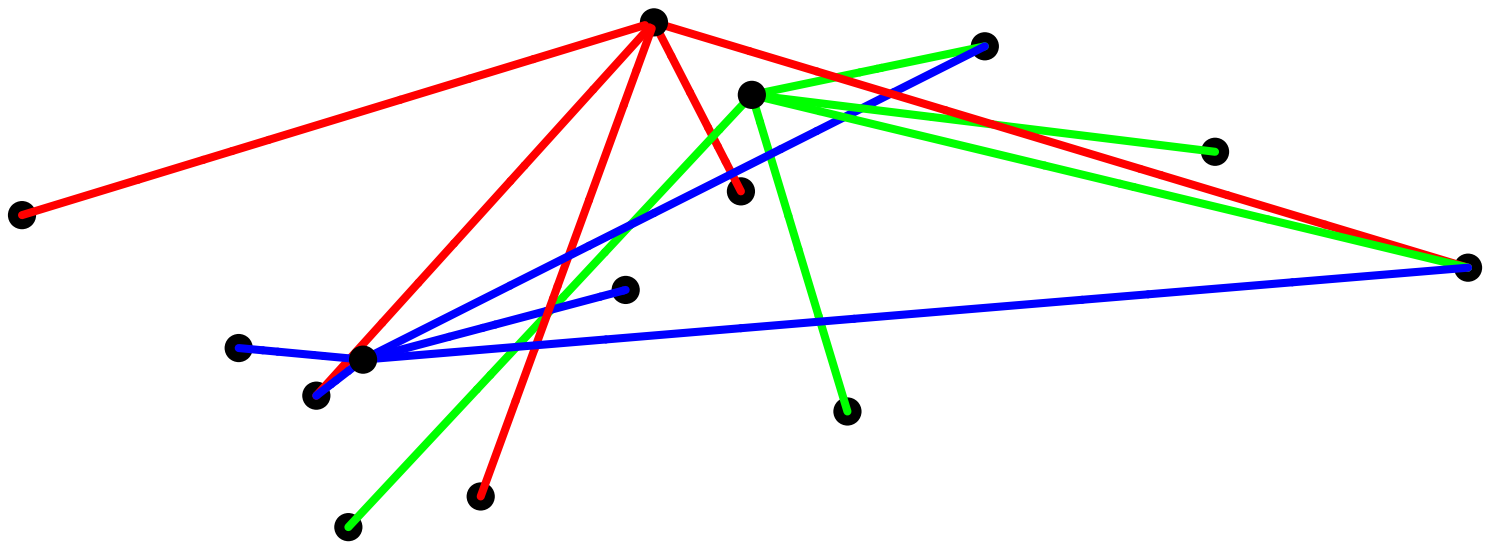
The smallest and largest constructible primes have approximate respective magnitudes of

$$\begin{aligned} P_{\text{min}} &= 1.572 \times 10^{76} \\ P_{\text{max}} &= 1.095 \times 10^{354}. \end{aligned}$$

3D Primes (View 1)



3D Primes (View 2)



Comments

- Endpoint pairings for the line segments used to generate the primes were determined from a large sample of random geometries.
- Pseudorandomness of the generated key stream improves the more primes are calculated, but the rate of improvement beyond the use of fifteen primes declines.
- More primes by calculating additional line segment lengths, or fewer primes by omitting some, or different planar points and circle centers could be used.

Number Theoretic Questions (1 of 2)

1. Is function F from Eq. (2) a one-way function? Given the value of N is $F(q; N)$ invertible? Is function f a one-to-one or many-to-one function? Is function f from Eq. (1) invertible?

Number Theoretic Questions (1 of 2)

1. Is function F from Eq. (2) a one-way function? Given the value of N is $F(q; N)$ invertible? Is function f a one-to-one or many-to-one function? Is function f from Eq. (1) invertible?
2. Function f defined in Eq. (1) maps prime numbers (a countable set) into the irrational numbers (an uncountable set). Can the set of all possible prime numbers which may be generated by the procedure be determined by an attacker so that the set of all possible irrational numbers used in the construction of the key stream can be known as well?

Number Theoretic Questions (1 of 2)

1. Is function F from Eq. (2) a one-way function? Given the value of N is $F(q; N)$ invertible? Is function f a one-to-one or many-to-one function? Is function f from Eq. (1) invertible?
2. Function f defined in Eq. (1) maps prime numbers (a countable set) into the irrational numbers (an uncountable set). Can the set of all possible prime numbers which may be generated by the procedure be determined by an attacker so that the set of all possible irrational numbers used in the construction of the key stream can be known as well?
3. Are there private geometric security parameters and public initialization values which yield all the primes between P_{min} and P_{max}?

Number Theoretic Questions (1 of 2)

1. Is function F from Eq. (2) a one-way function? Given the value of N is $F(q; N)$ invertible? Is function f a one-to-one or many-to-one function? Is function f from Eq. (1) invertible?
2. Function f defined in Eq. (1) maps prime numbers (a countable set) into the irrational numbers (an uncountable set). Can the set of all possible prime numbers which may be generated by the procedure be determined by an attacker so that the set of all possible irrational numbers used in the construction of the key stream can be known as well?
3. Are there private geometric security parameters and public initialization values which yield all the primes between P_{min} and P_{max}?
4. Are the prime numbers generated by this procedure uniformly distributed among the set of prime integers? Is uniformity of distribution important to the security of the system?

Number Theoretic Questions (2 of 2)

5. Given private geometric security parameters (c, α, m) and a public initialization value n, is there an open set (in some non-trivial topology) containing these values such that the image of the open set consists only of a single set of prime integers?
6. Are the fifteen prime integers generated by the procedure described above, necessarily pairwise distinct?
7. Is the procedure which generates the fifteen primes integers a one-way function? In other words, given only the set of fifteen prime integers, can the private geometric security parameters be deduced?

Periodic Pseudorandom Sequence

1. From the next un-used digits of $d = F(p; 4050)$ define

$$\begin{aligned} s &= 1 + [d_{31} \cdots d_{35} \pmod{45}] \\ t &= 1 + [d_{36} \cdots d_{40} \pmod{45}]. \end{aligned}$$

2. If $H_{s,t}$ is even let $(k)_{16} = H_{s,t}H_{s,t+1}H_{s,t+2}H_{s,t+3}$, otherwise let $(k)_{16} = H_{s,t}H_{s+1,t}H_{s+2,t}H_{s+3,t}$.
3. Let $l_1 = 900 + [k \pmod{1500}]$ and find integer $v_1 = F(p_1; l_1)$.
4. Concatenate v_1 with itself to form the l_1-periodic pseudorandom byte sequence

$$\mathbf{v}_1 = x_1x_2, x_3x_4, \ldots, x_{l_1-1}x_{l_1}, x_1x_2, x_3x_4, \ldots, x_{l_1-1}x_{l_1}, \ldots \quad (5)$$

5. Repeat process for $p_2, p_3, \ldots, p_{15}$ giving each pseudorandom byte sequence a unique period.

Pseudorandom Matrix

- Sort the pseudorandom vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{15}\}$ by the SHA-256 hashes of their associated primes $\{p_1, p_2, \ldots, p_{15}\}$.
- Matrix M is assembled from the pseudorandom vectors in SHA-256 order.

$$M = \begin{bmatrix} m_{1,1} & m_{1,2} & m_{1,3} & m_{1,4} & \cdots \\ m_{2,1} & m_{2,3} & m_{2,3} & m_{2,4} & \cdots \\ m_{3,1} & m_{3,2} & m_{3,3} & m_{3,4} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \\ m_{14,1} & m_{14,2} & m_{14,3} & m_{14,4} & \cdots \\ m_{15,1} & m_{15,2} & m_{15,3} & m_{15,4} & \cdots \end{bmatrix}$$

Comments

- SHA-256 hash function is a one-way function.
- Changing one prime p_i inserts v_i in a random position.
- Each p_i may have up to 1500 different representations as v_i.
- Lower bound for the column period of M is 5.354×10^{11} while the upper bound is 4.399×10^{50}.
- Entries in M are pseudorandom bytes.

Partner Matrix

- For $j = 1, 2, \ldots, 15$ define

$$\hat{p}_j = \left[p_j^2 \pmod{\sum_{s=1}^{15} p_s} \right]_{\mathbb{P}}.$$

- Calculate $\hat{v}_j = F(\hat{p}_j; l_j)$ for $j = 1, 2, \ldots, 15$.
- Concatenate $\hat{v}_j$ with itself to form the pseudorandom sequence $\hat{\mathbf{v}}_j$.
- Sort $\{\hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2, \ldots, \hat{\mathbf{v}}_{15}\}$ by the SHA-256 hashes of $\{p_1, p_2, \ldots, p_{15}\}$.
- Let the jth row of matrix L be the jth SHA-256-ordered $\hat{\mathbf{v}}_j$.
- L is another pseudorandom byte matrix having the same structure as M.

Questions Relating to the Matrices

1. The mantissa of the output of function f is converted into an integer having between 900 and 2399 hexadecimal digits. From a knowledge of those limited number of digits, is it possible to determine the prime integer used as input to f?
2. The mantissas are of the output function f are linearly independent over the rationals, but the mantissas are truncated to between 900 and 2399 hexadecimal digits. Do the rows of matrices L and M retain linear independence?
3. The periods of the sequences which make up matrix M are determined by a combination of the private geometric security parameters and the public initialization value. Does knowledge of these periods impart any information about these quantities?
4. The SHA-256 algorithm used to sort the input set of primes is a one-way function. Changing one prime in the input set would change rows in matrices L and M at an unpredictable location - as would inserting a new prime.

Generation of Key Stream: Initial Offset

- Referring to $d = F(p; 4050)$, consume the next ten digits to calculate

$$\begin{aligned} s &= 1 + [d_j d_{j+1} d_{j+2} d_{j+3} d_{j+4} \pmod{45}] \\ t &= 1 + [d_{j+5} d_{j+6} d_{j+7} d_{j+8} d_{j+9} \pmod{45}]. \end{aligned}$$

- If $H(s, t)$ is even let $(w)_{16} = H_{s,t} H_{s,t+1} H_{s,t+2}$, else let $(w)_{16} = H_{s,t} H_{s+1,t} H_{s+2,t}$.
- The initial offset in matrices L and M will then be

$$(s', t') = g(w) \equiv \left(1 + [w \pmod{15}], 1 + \left\lfloor \frac{w}{15} \right\rfloor\right). \quad (6)$$

Generation of Key Stream: First Byte

- The first byte of the pseudorandom key stream is

$$b_1 = G(s', t') \equiv \left(\bigoplus_{j=s'}^{15} m_{j,t'} \right) \oplus \left(\bigoplus_{j=1}^{s'} m_{j,t'+1} \right) \oplus l_{s',t'+1}. \quad (7)$$

where $\oplus$ denotes the bitwise XOR operation.

Generation of Key Stream: First Byte

- The first byte of the pseudorandom key stream is

$$b_1 = G(s', t') \equiv \left(\bigoplus_{j=s'}^{15} m_{j,t'} \right) \oplus \left(\bigoplus_{j=1}^{s'} m_{j,t'+1} \right) \oplus l_{s',t'+1}. \quad (7)$$

  where $\oplus$ denotes the bitwise XOR operation.
- The jth byte is calculated as

$$b_j = G(g(w + j - 1)).$$

Visualization

$$M = \begin{bmatrix}
\cdots & 219 & 5 & 75 & 225 & 225 & \cdots \\
\cdots & 16 & 66 & 3 & 26 & 127 & \cdots \\
\cdots & 108 & 70 & 21 & 79 & 147 & \cdots \\
\cdots & 164 & 203 & 63 & 51 & 64 & \cdots \\
\cdots & 93 & 251 & 4 & 174 & 223 & \cdots \\
\cdots & 123 & 42 & 161 & 36 & 83 & \cdots \\
\cdots & 84 & 124 & 26 & 13 & 59 & \cdots \\
\cdots & 224 & 91 & 91 & 219 & 221 & \cdots \\
\cdots & 157 & 151 & 97 & 51 & 209 & \cdots \\
\cdots & 172 & 245 & 142 & 105 & 200 & \cdots \\
\cdots & 247 & 15 & 63 & 206 & 104 & \cdots \\
\cdots & 246 & 154 & 53 & 235 & 1 & \cdots \\
\cdots & 237 & 70 & 178 & 188 & 136 & \cdots \\
\cdots & 137 & 72 & 208 & 201 & 28 & \cdots \\
\cdots & 83 & 192 & 127 & 147 & 239 & \cdots
\end{bmatrix}$$

If $l_{s',t'+1} = 0$ then $b_1 = 169$.

Comments

- The pseudorandom key stream can be used as a one-time pad.

Comments

- The pseudorandom key stream can be used as a one-time pad.
- The key stream is periodic with period $\text{lcm}(l_1, l_2, \ldots, l_{15})$.

$$5.354 \times 10^{11} < \text{lcm}(l_1, l_2, \ldots, l_{15}) < 4.400 \times 10^{50}$$

Comments

- The pseudorandom key stream can be used as a one-time pad.
- The key stream is periodic with period $\mathrm{lcm}(l_1, l_2, \ldots, l_{15})$.

$$5.354 \times 10^{11} < \mathrm{lcm}(l_1, l_2, \ldots, l_{15}) < 4.400 \times 10^{50}$$

- Evaluation of the key stream by the NIST Statistical Test Suite reveals a high degree of randomness.

Comments

- The pseudorandom key stream can be used as a one-time pad.
- The key stream is periodic with period $\mathrm{lcm}(l_1, l_2, \ldots, l_{15})$.

$$5.354 \times 10^{11} < \mathrm{lcm}(l_1, l_2, \ldots, l_{15}) < 4.400 \times 10^{50}$$

- Evaluation of the key stream by the NIST Statistical Test Suite reveals a high degree of randomness.
- Randomness of the key stream is comparable to the randomness of the quantum photonic source at the Australian National University.

Comments

- The pseudorandom key stream can be used as a one-time pad.
- The key stream is periodic with period $\mathrm{lcm}(l_1, l_2, \ldots, l_{15})$.

$$5.354 \times 10^{11} < \mathrm{lcm}(l_1, l_2, \ldots, l_{15}) < 4.400 \times 10^{50}$$

- Evaluation of the key stream by the NIST Statistical Test Suite reveals a high degree of randomness.
- Randomness of the key stream is comparable to the randomness of the quantum photonic source at the Australian National University.
- Modification of a single row of matrix M alters the entire key stream.

One-time Pads (1 of 2)

- If Alice wants to send Bob the message “HELLO” using a one-time pad, each party will need a strip of paper with the same random string (at least 5 characters long).

$$\text{pad} = \{36, 193, 187, 69, 136\}$$

- Alice encrypts:

	H	E	L	L	O
	72	69	76	76	79
$\oplus$	36	193	178	69	136
	108	132	247	9	199

One-time Pads (1 of 2)

- If Alice wants to send Bob the message “HELLO” using a one-time pad, each party will need a strip of paper with the same random string (at least 5 characters long).

$$\text{pad} = \{36, 193, 187, 69, 136\}$$

- Alice encrypts:

	H	E	L	L	O
	72	69	76	76	79
$\oplus$	36	193	178	69	136
	108	132	247	9	199

- Bob decrypts:

	108	132	247	9	199
$\oplus$	36	193	178	69	136
	72	69	76	76	79
	H	E	L	L	O

One-time Pads (2 of 2)

Advantages:

1. If the pad is truly random, plaintext is encrypted with perfect secrecy.
   - Ciphertext gives no information about plaintext (except maximum length).
   - The entropy in the plaintext is the same as the entropy in the plaintext given the ciphertext.
2. Ciphertext can be decrypted into all possible plaintexts.
3. One-time pad encryption is immune to brute-forcing the key even if a portion of the plaintext is known.

Questions Relating to the Key Stream

1. Calculation of each byte of the key stream depends on entries from each row of matrix M and for each byte two entries from one row are used. Modification (including addition or deletion) of a row of M will alter the entire generated key stream. Differential bit analysis testing finds that any given bit of key stream has equal probability of changing or remaining the same. What are the implications of this to the security of the system?
2. Would interception of a finite segment of the key stream enable an attacker to reconstruct matrix M or matrix L?
3. Does possession of a portion of the key stream enable an attacker to determine the dimensions of matrix M or matrix L?

Cryptanalytic Attack (1 of 2)

In order to learn (c, α, m) an attacker would have to:

1. Determine the period of each row of L or M. This challenge is linked to that of determining the order of the rows in L and M. The period of the key stream is unchanged by a reordering of the rows in these matrices, but the contents of the key stream is changed by a reordering.
2. Determine the entries of matrices L and M from a byte of the key stream.
3. From a row of matrix M (which represents a periodic, truncated approximation to an irrational number) determine the prime integer p_j which produced this row. Similarly from a row of matrix L determine the prime $\hat{p}_j$ which produces this row.
4. From the list of prime integers $\{p_1, p_2, \ldots, p_{15}\}$ determine the set of line segment lengths $\{\|\overline{AZ_2}\|, \|\overline{BZ_2}\|, \ldots, \|\overline{X_2Z_4}\|\}$.

Cryptanalytic Attack (1 of 2)

5. Determine the two-dimensional geometric form from the line segment lengths $\{\|\overline{AZ_2}\|, \|\overline{BZ_2}\|, \ldots, \|\overline{X_2Z_4}\|\}$.
6. Determine the private geometric security parameters (c, α, m) from the two-dimensional geometric form.