Solving a class of ODEs arising in the analysis of a computer security process using generalized hyper-Lambert functions

Panayotis E. Nastou\(^{(a)}\), Yiannis C. Stamatiou\(^{(b,c)}\), Apostolos Tsiakalos\(^{(c)}\)

\(^{a}\)Department of Mathematics, University of the Aegean, Karlovasi, Samos, Greece, 83200
\(^{b}\)Computer Technology Institute and Press - “Diophantus”, University of Patras, N. Kazantzaki, 26504, Rio, Patras, Greece.
\(^{c}\)Department of Mathematics, University of Ioannina, Ioannina, Greece, 45110

ABSTRACT

In this paper, we derive the solution to a class of ordinary differential equations (ODEs) that arise from the theoretical analysis, conducted in a previous work, of a key agreement process stemming from computer security. The analysis led to a new class of ordinary differential equations that resemble the well known class of Abel differential equations of the First Kind except that this new class involves the unknown function in powers greater than three. To the best of our knowledge, no general solution strategy exists for integrating the differential equations in this class towards a solution. We show that the solution to these ordinary differential equations can be expressed, interestingly, through the use of a class of Generalized Hyper-Lambert Functions that naturally generalize the well known Lambert \(W\) function, which frequently arises in the analysis of engineering applications. A key step to the connection of the solution of the differential equations with Generalized Hyper-Lambert Functions is the analysis of the equations into partial fractions in a way that matches the recursive pattern of the definition of these functions.

Keywords: ODEs, Lambert \(W\) function; Generalized Hyper-Lambert functions; Key Agreement.

© 2012 Darbose. All rights reserved.

1. Introduction

The key agreement problem involves two entities whose goal is to agree, secretly, on a shared piece of information in order to use it as a cryptographic key in establishing a secure communication session (e.g. with some shared key cipher). One way to solve the key agreement problem is to assume that each of the two involved entities possess an initially random string and, subsequently, execute a process that will enable them to modify their strings in order to agree on as many positions as possible in the end of the process. If the percentage of positions at which the two strings are the same is sufficiently large after the termination of the process, then it will be easier for the two entities to locate shared pieces of information than it would be using their initial strings, which may differ in many positions.

In [5] a process was proposed by means of which the two entities exchange suitable encodings of randomly chosen substrings of size \(k\) (\(k\) is a parameter) of their strings and delete, in turn, locally one bit position if the number of bits in which the size \(k\) substrings differ is at least \(\lceil k/2 \rceil\). This simple process, that was proposed in [5], is called \(k\)-place elimination process. The idea is to gradually increase, through deletions of non-similar bits, the fraction of positions at which the two strings have the same bits. The theoretical analysis of the process
was conducted by employing Wormald’s theorem which transforms the discrete time evolution equation for the percentage of positions at which the two strings are equal into a continuous time differential equation whose solution can be shown to follow closely the solution of the discrete evolution equation.

The differential equation that results for the case $k = 2$ was analyzed theoretically in [5], where it was shown that the equation belongs to the class of the Abel differential equations of the First Kind, which have the form

$$\frac{dy(t)}{dt} = f_3(t)y(t)^3 + f_2(t)y(t)^2 + f_1(t)y(t) + f_0(t),$$

with $f_i(t), 0 \leq i \leq 3$ complex functions. The solution of the differential equation for $k = 2$ involves the Lambert $W$ function which is defined as follows: for $x \in \mathbb{R}$, the Lambert $W$ function (see [2] for a comprehensive treatment of this function and its properties), denoted by $W(x)$, is defined as the principal branch of the function that satisfies the equation $W(x)e^{W(x)} = x$. For $k > 2$, however, the resulting class of differential equations, although it appears to generalize straightforwardly the class of Abel differential equations of the First Kind, it does not appear to be amenable to some known analytic solution approach.

Using as a departure point, as well as a hint, the fact that for $k = 2$ the solution to the differential equation involves the Lambert $W$ function, in this paper we show how for $k \geq 3$ the solution to resulting differential equations can be written in explicit form using a class of functions generalizing the Lambert $W$ function, called Generalized Hyper-Lambert Functions denoted by $HW(x)$, as defined in [3]. Our solution strategy relies on expanding a rational equation that results from integrating the target differential equation and whose solution is a solution of the given differential equation, into partial fractions. Then we relate the partial fraction expansion with the Generalized Hyper-Lambert functions and derive the solution to the differential equation in explicit form. The accuracy of the derived solution is assessed numerically by performing a comparison with the numerical solution computed directly from the differential equation.

To the best of our knowledge, no systematic treatment of this particular class of differential equation exists in the literature. Our work offers yet another example (see [2]) of the ubiquitous nature of the Lambert $W$ and the Generalized Hyper-Lambert functions $HW$ in many practical engineering problems and applications.

2. The key agreement process

For completeness of exposition, in this section we review briefly the key agreement process given in [5] and state the differential equations that result from the theoretical analysis given in that paper.

Let $E_0$ and $E_1$ be two communicating entities possessing two $n$-bit strings $V_0$ and $V_1$ correspondingly. Let $X(V_0, V_1)$ be the number of bit positions at which the two strings $V_0$ and $V_1$ are, initially, the same. At each step $i$ of the process, one of the two entities selects a random subset of $k$ bit positions from the set of available bit positions $N_i$ (initially this set is equal to $N_0 = \{1, \ldots, n\}$) and sends the $k$ positions as well as the corresponding bits, suitably encoded (see in [5]), to the other entity. If the receiving entity discovers that the two subsets of bit positions differ in at least $\lceil \frac{k}{2} \rceil$ positions, then it sends a message to the sending entity to eliminate from further consideration one bit position which is randomly chosen from the sent $k$ bit positions while also eliminating the same bit position locally. This process continues up to a certain, predetermined number of steps $T$. Since the number of bit positions at which the two entities agree changes during the execution of the process, we denote by $X(V_0, V_1, i)$ or simply $X(i)$ when no confusion arises, the number of bit positions at which the two strings are the same, after the execution of the $i$-th step of the process. Initially, we have $X(V_0, V_1, 0) = X(V_0, V_1)$ or, simply, $X(0)$.

In order to track of the density of bit positions where two strings agree, in [5] the authors employed Wormald’s theorem [7] to model the probabilistic evolution of the algorithm using a deterministic function which stays provably close to the real evolution of the algorithm. What the theorem essentially states is that if we are confronted with a number of (possibly) interrelated random variables (associated with some random process) such that they satisfy a Lipschitz (essentially, smoothness) condition and their expected fluctuation at each time step is known, then the value of these variables can be approximated using the solution of a system of differential equations. Furthermore, the system of differential equations results directly from the expressions for the expected fluctuation.
of the random variables describing the random process (in [1] the interested reader may find a well presented
and readable discussion on the intuition behind the theorem). In the case of the key agreement process
-described above, the theorem states (see [5, 7] for more precise formulations) that we can correlate
$X(i)$ with a continuous time function $x(t)$, which is derived as the solution of a deterministic dif-
ferential equation, so as to have, with high probability, $X(i) = x(i/n) \cdot n + o(n)$.

In [5], the following was proved for the continuous time analog, $x(t)$, of $X(i)$ through the use of
Wormald’s theorem:

**Theorem 2.1.** The differential equation that results from the application of Wormald’s theorem
on the quantity $x(t)$ is the following:

$$\frac{dx(t)}{dt} = \sum_{j=\lfloor \frac{k}{2} \rfloor}^{k} \binom{k}{j} \left(1 - \frac{x(t)}{1-t}\right)^j \left(\frac{x(t)}{1-t}\right)^{k-j}$$

$$+ \sum_{j=\lfloor \frac{k}{2} \rfloor}^{k} \binom{k}{j} \frac{j}{k} \left(1 - \frac{x(t)}{1-t}\right)^j \left(\frac{x(t)}{1-t}\right)^{k-j}$$

$$- \frac{x(t)}{1-t} \sum_{j=0}^{\left\lfloor \frac{k}{2} \right\rfloor - 1} \binom{k}{j} \left(1 - \frac{x(t)}{1-t}\right)^j \left(\frac{x(t)}{1-t}\right)^{k-j}.$$  

(2.1)

Based on the following two lemmas, whose proofs follow by straightforward algebraic manipulations,
we will rewrite (2.1) so as to facilitate its study:

**Lemma 2.2.** For any $l, 0 \leq l \leq k$, and independently of $y$ it holds

$$\sum_{j=l}^{k} \binom{k}{j} y^{j-l} (1-y)^{j-l} \left[1 - \binom{j}{k} - y\right] = -\frac{l}{k} \binom{k}{l}.$$  

Using Lemma 2.2 the following can be proved:

**Lemma 2.3.** Let $h(y)$ be the polynomial, which results from the right-hand side of Equation (2.1)
by replacing the quantity $x(t)/(1-t)$ with $y$:

$$h(y) = -\sum_{j=\lfloor \frac{k}{2} \rfloor}^{k} \binom{k}{j} (1-y)^j y^{k-j} \left(1 - \frac{j}{k}\right)$$

$$- y \sum_{j=0}^{\left\lfloor \frac{k}{2} \right\rfloor - 1} \binom{k}{j} (1-y)^j y^{k-j}.$$  

Then the polynomial $h(y)$ can be written as follows:

$$h(y) = -y + y^{k-\left\lfloor \frac{k}{2} \right\rfloor + 1} (1-y)^{\left\lfloor \frac{k}{2} \right\rfloor} \binom{k-1}{\left\lfloor \frac{k}{2} \right\rfloor - 1}.$$  

(2.2)

Setting

$$y = y(t) = \frac{x(t)}{1-t}$$  

(2.4)

Darbose
we derive the following:
\[
\frac{dx(t)}{dt} = (1 - t) \frac{dy(t)}{dt} - y(t).
\] (2.5)
Combining (2.4) and (2.5) with (2.3) and (2.1), we conclude that (2.1) can be written as follows:
\[
\frac{dy(t)}{dt} = \frac{1}{1 - t} \left[ y(t)^{k - \left\lfloor \frac{k}{2} \right\rfloor + 1} (1 - y(t))^\left\lfloor \frac{k}{2} \right\rfloor \left( k - 1 - \frac{y(t)^{k - \left\lfloor \frac{k}{2} \right\rfloor}}{\left| \frac{k}{2} \right|} \right) \right].
\] (2.6)

3. The general solution
The differential equation (2.6) is of the form
\[
\frac{dy}{dt} = w(y)g(t)
\]
with
\[
w(y) = \left[ y(t)^{k - \left\lfloor \frac{k}{2} \right\rfloor + 1} (1 - y(t))^\left\lfloor \frac{k}{2} \right\rfloor \left( k - 1 - \frac{y(t)^{k - \left\lfloor \frac{k}{2} \right\rfloor}}{\left| \frac{k}{2} \right|} \right) \right]
\]
and \( g(t) = \frac{1}{1 - t} \). Therefore, the differential equation is separable and, consequently, its solution \( y(t) \) can be found by solving the following equation for \( y \) (see, e.g., Murphy, 1960):
\[
\int \frac{dy}{w(y)} = \int g(t) dt + C.
\] (3.1)
After some substitutions in (2.6), and replacing \( y(t) \) with \( y \) for simplicity leaving the dependence on \( t \) implicit, we obtain from (3.1) the following:
\[
\frac{1}{k - \left\lfloor \frac{k}{2} \right\rfloor - 1} \int \frac{dy}{y^{k - \left\lfloor \frac{k}{2} \right\rfloor + 1} (1 - y)^\left\lfloor \frac{k}{2} \right\rfloor} = -\ln(1 - t) + C.
\] (3.2)

3.1 The case \( k = 2 \)
For \( k = 2 \), the differential equation (2.6) becomes:
\[
\frac{dy(t)}{dt} = \frac{1}{1 - t} \left[ y(t)^2 (1 - y(t)) \right]
\] (3.3)
with the solution given, implicitly, by (3.2) with \( k = 3 \):
\[
\int \frac{dy}{y^2(1 - y)} = -\ln(1 - t) + C.
\] (3.4)
The differential equation (3.3) that results for \( k = 2 \) is an instance of the Abel equation of the First Kind and was solved, using a standard methodology (see, for example, [6]), in [5].

**Lemma 3.1.** For \( k = 2 \) the solution of the differential equation given in Theorem 2.1 is the function
\[
x(t) = \frac{1 - t}{W(c(1 - t)) + 1}, c = \left[ \frac{1 - x(0)}{x(0)} \right] e^{\frac{1 - x(0)}{x(0)}}
\] (3.5)
where \( x(0) \) is the percentage of the initial agreement positions.
For \( x \in \mathbb{R} \), the \( W(x) \) function (see [2] for a detailed study of the function and its properties) is defined as the principal branch of the function that satisfies the equation

\[
W(x)e^{W(x)} = x.
\]

(3.6)

The connection with the \( W(x) \) function becomes more apparent by solving Equation (3.4) directly, without resorting to the methodology for solving the general Abel equation of the First Kind. After computing the integral on the left-hand side of (3.4) and exponentiating we obtain the following equation, with \( y = y(t) \):

\[
\left(1 - \frac{1}{y}\right)e^{1/y} = (1 - t)e^{-C}.
\]

(3.7)

Setting \( z = 1/y - 1 \) and multiplying both sides with \(-e^{-1}\) we obtain from the equation above the following:

\[
Ze^{z} = -(1 - t)e^{-C - 1}.
\]

From (3.6) we conclude that the solution to (3.7) is

\[
y(t) = \frac{1}{z + 1} = W[-(1 - t)e^{-C - 1}] + 1.
\]

(3.8)

For \( t = 0 \), the initial condition requires \( y(0) = x(0) \). Thus, solving \( y(0) = x(0) \) for \( C \) we obtain

\[
C = -\ln \left(\frac{-1 + x(0)}{x(0)}\right)x(0) + 1.
\]

Thus

\[
e^{-C - 1} = e^{-\ln \left(\frac{-1 + x(0)}{x(0)}\right)x(0) + 1 - 1} = -\left(1 - \frac{x(0)}{x(0)}\right)e^{\frac{-1 - x(0)}{x(0)}}.
\]

(3.9)

After inserting the expression above for \( e^{-C - 1} \) in (3.8), we are led to the solution (3.5) given in Lemma 3.1.

### 3.2 The cases \( k > 2 \)

In this section we analyze the exponents involved in the integral of the differential equation (2.6) and its solution equation (3.2). We will show that the involved integral can be computed explicitly, in an inductive way, that involves only the operation of addition as well as a set of constants defined recursively. Thus, the computation of the integral can be performed very efficiently and leads to an explicit form.

Let \( s = \lceil k/2 \rceil \). If \( k \) is odd then \( k = 2s - 1 \), while \( k - \lceil k/2 \rceil + 1 = s \). For even \( k \), we have \( k = 2s \), while \( k - \lceil k/2 \rceil + 1 = s + 1 \). Thus, the integrand in (3.2) is equal to

\[
\frac{1}{y^{s+1}(1 - y)^s}, \text{if } k \text{ is even}
\]

or equal to

\[
\frac{1}{y^{s}(1 - y)^{s}}, \text{if } k \text{ is odd},
\]

where \( s = \lceil k/2 \rceil \).

Based on the above analysis, we compute (inductively) the partial fraction expansion of the integrand in (3.2) having as basis the case \( k = 1 \). The proofs of the following two theorems are straightforward and, thus, omitted. They follow, easily, from inspection of the involved quantities.
Theorem 3.2. Let
\[ \frac{1}{y^s(1 - y)^s} = \sum_{i=1}^{s} \frac{A_y,i}{y^i} + \sum_{i=1}^{s} \frac{A_{1-y,i}}{(1 - y)^i} \]
be the partial fraction expansion of the function \( \frac{1}{y^s(1 - y)^s} \).
Then the partial fraction expansion of the function \( \frac{1}{y^{s+1}(1 - y)^{s+1}} \) is given as
\[ \frac{1}{y^{s+1}(1 - y)^{s+1}} = \sum_{i=1}^{s+1} \frac{A'_y,i}{y^i} + \sum_{i=1}^{s} \frac{A'_{1-y,i}}{(1 - y)^i} \]
with \( 1 < i \leq s + 1 \)
\[ A'_{y,1} = \sum_{i=1}^{s} A_{1-y,i} \]
\[ A'_{y,i} = A_{y,i-1} \]
and with \( 1 \leq i \leq s \)
\[ A'_{1-y,i} = \sum_{j=i}^{s} A_{1-y,j}. \]

Theorem 3.3. Let
\[ \frac{1}{y^s(1 - y)^{s-1}} = \sum_{i=1}^{s} \frac{A_y,i}{y^i} + \sum_{i=1}^{s-1} \frac{A_{1-y,i}}{(1 - y)^i} \]
be the partial fraction expansion of the function \( \frac{1}{y^s(1 - y)^{s-1}} \).
Then the partial fraction expansion of the function \( \frac{1}{y^{s+1}(1 - y)^{s}} \) is given as
\[ \frac{1}{y^{s+1}(1 - y)^{s}} = \sum_{i=1}^{s} \frac{A'_y,i}{y^i} + \sum_{i=1}^{s} \frac{A'_{1-y,i}}{(1 - y)^i} \]
with \( 1 < i \leq s \)
\[ A'_{y,1} = \sum_{i=1}^{s} A_{y,i} \]
\[ A'_{1-y,i} = A_{y,i-1} \]
and with \( 1 \leq i \leq s \)
\[ A'_{y,i} = \sum_{j=i}^{s} A_{y,j}. \]
Let us assume that for a particular value of \( k \) we have the integrand
\[
\frac{1}{y^{s+\delta_k} (1-y)^{s}}
\] with \( s = \lceil \frac{k}{2} \rceil \) and
\[
\delta_k = \begin{cases} 
0 & \text{if } k \text{ is odd} \\
1 & \text{if } k \text{ is even}.
\end{cases}
\]

For instance, for \( k = 1 \) we have \( \delta_1 = 0 \) while for \( k = 2 \) we have \( \delta_2 = 1 \). Assume, also, that we have computed its partial fraction expansion (this expression was given above):
\[
\frac{1}{y^{s+\delta_k} (1-y)^{s}} = \sum_{i=1}^{\lceil \frac{s}{2} \rceil} \frac{A'_{y,i}}{y^i} + \sum_{i=1}^{\lceil \frac{s}{2} \rceil} \frac{A'_{1-y,i}}{(1-y)^i}.
\]

Integrating,
\[
\int \frac{1}{y^{s+\delta_k} (1-y)^{s}} \, dy = A'_{y,1} \ln(y) - A'_{1-(y),1} \ln (1-y) - \sum_{i=2}^{\lceil \frac{s}{2} \rceil} \frac{A'_{y,i}}{(i-1)y^{i-1}} + \sum_{i=2}^{\lceil \frac{s}{2} \rceil} \frac{A'_{1-y,i}}{(i-1)(1-y)^{i-1}}.
\] (3.12)

From Theorems 3.2 and 3.3 we have:
\[
A'_{y,1} = A'_{(1-y),1} = \begin{cases} 
\sum_{i=1}^{\lceil \frac{s}{2} \rceil} A_{y,i} & \text{if } k \text{ is odd} \\
\sum_{i=1}^{\lceil \frac{s}{2} \rceil} A_{1-(y),i} & \text{if } k \text{ is even}.
\end{cases}
\] (3.13)

Thus, the integral equation (3.2) becomes, using (3.12) and (3.13), as follows:
\[
- \ln(1-t) + C = \frac{A'_{y,1}}{(\frac{k}{2}-1)^{\frac{k}{2}}} \ln \left( \frac{y}{1-y} \right) - \sum_{i=2}^{\lceil \frac{s}{2} \rceil} \frac{A'_{y,i}}{(i-1)y^{i-1}} \] (3.14)

Let us, now, consider the case \( k = 3 \). We have to solve, for \( y = y(t) \), the equation
\[
\left( 1 - \frac{1}{y} \right)^2 e^{\frac{1}{y} - \frac{1}{y}^\prime} = (1-t)e^{-C}.
\] (3.15)

This time it is not possible to transform (3.15) into a form suitable for the application of the definition of the \( W \) function in (3.6) since, as remarked in [3], the most general form of equation that can be cast into (3.6) is
\[\alpha z^m e^{b z^n} = g(t),\]
with \( m, n \) integers, \( a, b \) complex numbers, and \( g(t) \) a complex function of \( t \). Thus, in [3] an effort was made to generalize the \( W \) function, as given by (3.6). Below we will provide the definitions relevant to the class of Generalized Hyper-Lambert Functions as given in [3]:

\[\mathcal{W} \] Darbose
Definition 3.1. Let $I$ be an index set and $f_i : \mathbb{C} \to \mathbb{C}$ be arbitrary complex functions not vanishing identically. Assuming $m, n \in \mathbb{N}$ such that $m \geq n$ we define $F_{n,m}(z) : \mathbb{N}^2 \times \mathbb{C} \to \mathbb{C}$ as follows:

$$F_{n,m}(z) = \begin{cases} e^{z} & \text{if } n = 1 \\ e^{f_m(z) - (n - 1)f_{n-1,m}(z)} & \text{if } n > 1. \end{cases}$$

(3.16)

Definition 3.2. Let $f_i$ be as in Definition 3.1 and $z \in \mathbb{C}$. Then we define the function $G$ as $G(f_1(z), f_2(z), \ldots, f_k(z); z) = zF_{k+1,k+1}(z)$.

Definition 3.3. Let $f_i$ be as in Definition 3.1, $G$ as in Definition 3.2, and $y \in \mathbb{C}$. Then the function $HW(\{f_i\}_{i \in I}; y)$ is the function which satisfies the following equation:

$$G(\{f_i\}_{i \in I}; HW(\{f_i\}_{i \in I}; y)) = y.$$  

(3.17)

We will, now, solve (3.14) using the class of functions defined by (3.17) in Definition 3.3. For simplicity, we set

$$\Delta = \frac{1}{A_{y,1}} \left[ \left( \frac{k}{2} \right) + S \sum_{i=2}^{k} \frac{A_{y,i}}{(i - 1)y^{i-1}} - \sum_{i=2}^{k} \frac{A'_{y,i}}{(i - 1)(1 - y)^{i-1}} \right],$$

$$S = \frac{\left( \frac{k}{2} - 1 \right)}{A_{y,1}} (-\ln(1 - t) + C).$$

(3.18)

Then, it is straightforward to see that (3.14) can be written as

$$\ln \left( \frac{y}{1 - y} \right) = S + \Delta$$

(3.19)

which can be rewritten as

$$ye^{-\left( \frac{\Delta + S + \ln(1 - y)}{y} \right)} = 1.$$  

(3.20)

Setting $f(y) = -\frac{\Delta + S + \ln(1 - y)}{y}$ and using the functions defined in Definition 3.3 we conclude that the solution to (3.20) is given by $y(t) = HW(f(y); 1)$. Expanding it, we finally obtain

$$y(t) = HW(-\frac{\Delta + S + \ln(1 - y)}{e^y}; 1).$$

(3.21)

4. Numerical computations

In order to assess, numerically, the accuracy of the derived solution we performed a comparison with the numerical solution computed directly from the differential equation. Assuming $x(0) = \frac{1}{2}$, for $k = 3$, the differential equation (2.6) becomes

$$(1 - t) \frac{dy(t)}{dt} = 2y(t)^2(1 - y(t))^2$$

(4.1)

with initial condition $y(0) = \frac{x(0)}{1 - 0} = \frac{1}{2}$ ($t = 0$). By solving Equation (4.1) numerically in the interval $(0, 1)$ using the Maple symbolic and numerical computation software package (see, e.g., [4]), the values of the second column of Table (1) were obtained. Moreover, for $k = 3$, the equations in (3.18) become

Darbose
Table 1: Numerical Solution values and values of the solution based on HW Functions

<table>
<thead>
<tr>
<th>t</th>
<th>differential equation (2.6)</th>
<th>HW (3.21)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>0.5131</td>
<td>0.5131</td>
</tr>
<tr>
<td>0.2</td>
<td>0.5278</td>
<td>0.5278</td>
</tr>
<tr>
<td>0.3</td>
<td>0.5443</td>
<td>0.5443</td>
</tr>
<tr>
<td>0.4</td>
<td>0.5631</td>
<td>0.5631</td>
</tr>
<tr>
<td>0.5</td>
<td>0.5849</td>
<td>0.5849</td>
</tr>
<tr>
<td>0.6</td>
<td>0.6107</td>
<td>0.6107</td>
</tr>
<tr>
<td>0.7</td>
<td>0.6422</td>
<td>0.6422</td>
</tr>
<tr>
<td>0.8</td>
<td>0.6826</td>
<td>0.6826</td>
</tr>
<tr>
<td>0.9</td>
<td>0.7406</td>
<td>0.7406</td>
</tr>
</tbody>
</table>

\[
\Delta = \frac{1}{2y} - \frac{1}{2(1-y)},
\]
\[
S = -\ln(1-t) + C
\]  

(4.2)

and the function \( f \) can be written as follows:

\[
f(y) = -\frac{1}{2y} - \frac{1}{2(1-y)} + C + \ln\left(\frac{1-y}{1-y}\right)e^y.
\]

In order to find a value for constant \( C \), we assume an initial value for \( x(0) \) and then using Equations (4.2) Equation (3.19) is solved for \( t = 0 \). Assuming the same initial value \( x(0) = \frac{1}{2} \) as in numerical solution the constant equals to 0.

Using the Maple program provided in [3] for the computation of the HW functions, the values of the third column of Table 1 were obtained. We observe that the values obtained from numerical computations are equal, within a 4-digit accuracy, to the values obtained from computations based on the HW functions.

5. Conclusions

In this paper we derived, in explicit form, the solution to a class of ordinary differential equations that arose in the theoretical analysis of a randomized key agreement process that was proposed and studied in [5]. The process is parameterized by an integer \( k > 1 \), which denotes the size of substrings examined, in turn, by two communicating parties in order to locate and eliminate positions at which their two, initially, random candidate key bit strings differ.

In [5] one particular instance of the process was analyzed, corresponding for \( k = 2 \), resulting to a solution expressed through the well known Lambert \( W \) function. In our work we showed that the solution of the ordinary differential equation that results from the analysis of the next instances of the process for \( k > 2 \) can be expressed through the the Generalized Hyper-Lambert functions, which naturally generalize the Lambert \( W \) function. An interesting open question for further research would be to examine whether the solution of the ordinary differential equations for the cases \( k \geq 3 \) can also be written through the use of the Generalized Hyper-Lambert functions for more general, than the ones considered in this paper, choices for the coefficient functions that are involved in the ordinary differential equations considered here.
References


