

Original citation:

Taramonli, Chryssanthi, Green, Roger and Leeson, Mark S.. (2017) Energy conscious adaptive security scheme : a reliability-based stochastic approach. *Journal of Information Warfare*, 16 (4). pp. 55-72.

Permanent WRAP URL:

<http://wrap.warwick.ac.uk/97159>

Copyright and reuse:

The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions. Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

A note on versions:

The version presented here may differ from the published version or, version of record, if you wish to cite this item you are advised to consult the publisher's version. Please see the 'permanent WRAP URL' above for details on accessing the published version and note that access may require a subscription.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk

Energy Conscious Adaptive Security Scheme: A Reliability-Based Stochastic Approach

C Taramonli¹, MS Leeson², RJ Green²

¹*School of Computing, Electronics and Mathematics
Coventry University
Coventry, UK*

E-mail: sandy.taramonli@coventry.ac.uk

²*School of Engineering
University of Warwick
Coventry, UK*

E-mail: mark.leeson@warwick.ac.uk; roger.green@warwick.ac.uk

Abstract: *The increasing importance of information and communication, which plays a big role in a number of different fields in the modern era, brings with it the need for security. At the same time, encryption, which is an indispensable part of security architecture, is computationally intensive and may require a significant amount of energy consumption. Thus, it is of great importance to provide a sufficient level of security while properly utilizing the available resources. This research suggests a security framework based on the Reliability Function, along with the added ability to dynamically adjust the security level with respect to energy consumption, either according to the severity of the requested service or according to a specified energy threshold.*

Keywords: *Adaptive Security, Low-Energy Encryption, Global Performance Metric, Applied Probability, Reliability*

Introduction

Mobile devices have experienced a period of rapid evolution in recent years, which has brought unprecedented changes in mobile applications. As mobile devices have become increasingly sophisticated, security risks have increased, which has prompted the development of several security schemes for these devices (Guo, Wang & Zhu 2004). The rapid growth of data communications, the complexity of modern communication systems, and the resulting growth of security threats have led to the development of complex and time-consuming security schemes. Encryption, which is the cornerstone of any security system, comes at a significant energy cost (Prasithsangaree & Krishnamurthy 2003). Encryption algorithms, depending on their complexity, may consume a significant amount of computing resources, such as memory, processing time, and battery power. Unfortunately, battery technology has not been able to keep pace with these increasing energy demands; this has led to a considerable decrease in battery life. The key

challenge in providing low-energy encryption solutions is minimising energy consumption while maximising encryption strength. Minimising energy consumption requires the investigation and design of energy-efficient encryption systems. The end goal is to provide a sufficient level of security at the lowest energy cost possible (Chandramouli *et al.* 2006). This paper explores this issue and investigates the performance of the encryption schemes for all available security options.

One possible way to achieve sufficiency of security is by adjusting encryption parameters such as key size, data size, mode of operation, padding, and so forth. Traditional approaches generally deal with ensuring the security and accuracy of the propagated data (Chandramouli *et al.* 2006). Although modern approaches consider the encryption energy cost, existing efforts to examine the energy-cost characteristics of encryption mainly comprise experimentally based comparative approaches which assess the behavioural and energy impacts of the encryption parameters (Elminaam, Kader & Hadhoud 2009; Guo *et al.* 2011; Singh & Maini 2011). It is important to note that energy consumption depends not only on isolated factors, but also on the correlation between factors and their global effect on energy. To achieve low-energy encryption, the balance between minimum energy consumption and maximum encryption strength should be explored: it is essential to consider the relationship between energy consumption and functional encryption parameters. Knowledge about this relationship, as well as about the existence of any dependencies between encryption parameters, will facilitate an adaptive security scheme, with efficient adjustment of encryption parameters to deliver energy-efficient encryption algorithms and protocols. This paper aims to develop a framework that addresses such energy implications and analyses the trade-off between energy consumption and encryption strength. The authors propose an adaptive security scheme that dynamically selects the most efficient encryption possible, allowing for dynamic change of the security mode at the lowest cost of energy. This is based on the Reliability Model that serves as a global quality factor and is used for the evaluation of the available security modes with respect to energy consumption (Taramonli, Green & Leeson 2012).

Relevant Work

In the absence of generally accepted metrics that could be used to analyse and quantify cryptographic strength, Jorstad and Landgrave (1997) suggested a subjective scale for rating the overall strength of an algorithm. Previous work has been focused on comparison-based approaches (Elminaam, Kader & Hadhoud 2009; Guo *et al.* 2011; Singh & Maini. 2011; Potlapally *et al.* 2006) and described the effects of individual adjustments of the encryption parameters on the overall security level with respect to energy consumption. Although such efforts are interesting, there is a demonstrated inherent need to develop global metrics for use in specifying encryption algorithm strength (Jorstad & Landgrave 1997). Several authors have suggested low-cost implementations and lightweight cryptographic protocols (Snader, Kravets & Harris 2016; Vijayan & Raaza 2016; Simplicio *et al.* 2017); however, as ‘green cryptography’ suggests, an attempt should be made to recycle existing cryptographic primitives (Troutman & Rijmen 2009). Furthermore, most authors use the individual performance of the encryption parameters as factors to compare and rank algorithms. However, it does not seem reasonable to consider the overall energy performance of the encryption system in complete isolation from security, since there are prominent trade-offs between those aspects, and the criteria used are not universal. This reality emphasizes the need for a global quality factor and explains the

importance of developing a decision-making framework that evaluates the overall impact of each security mode on energy consumption.

Approach

Knowledge about the optimum selection of the most efficient encryption algorithm under specific security restrictions would help in designing systems that can adjust the security level according to the desired level of strength while taking into consideration the energy implications. Traditional approaches mainly cope with maintaining a high level of confidentiality; along this line, a great deal of effort is put into achieving high degrees of secrecy. However, the significant implication of energy consumption is not considered. Existing approaches that consider the encryption energy costs are mainly based on experimental comparisons of encryption parameters in terms of effectiveness and provide results of their behaviour with respect to their impact on energy consumption. Although such efforts are very interesting, there is a need to develop global metrics for use in specifying the strength of encryption algorithms. The distinguishing feature of the work presented in this paper is the maximisation of encryption system performance by energy consumption management, taking into consideration several interrelated factors. The authors have presented this concept previously (Taramonli, Green & Leeson 2012); this paper further develops an approach for implementing an energy-conscious adaptive-security scheme. As used here, ‘adaptive security’ means that the defined security model reacts to modify the system security based on the desired security level (Alampalayam & Kumar 2003). Moreover, this paper contributes to previous study of the overall influence of the configuration parameters on the energy consumption regarding either the desired security level or the available energy resources. Stochastic considerations in terms of reliability evaluation have been developed to conclude the overall effect of the encryption parameters on energy. The authors are unaware of any other works that attempt to study the overall influence of these configuration parameters on the energy consumption of encryption systems.

Optimisation of energy consumption problems is a challenging task, and here a reliability-based framework is presented for the development of an energy-conscious adaptive-security scheme. This stochastic approach relies on reliability modelling and probabilistic decision making, and has been implemented and tested within the context of a bespoke energy conservation framework. Simulation tests were carried out on an Intel Core i3 3GHz CPU computer with 3GB of RAM and the 32-bit Windows 7 Home Premium OS. For testing purposes, several performance data-streams were collected, including the encryption time and CPU process time. The Sun Netbeans IDE platform for Java application development was used as the platform of the implementation. The R language (Jones, Maillardet & Robinson 2014) was used for data manipulation, calculation, and graphical display. Stochastic data analysis was applied to simulation outputs to provide the reliability metric, facilitating the evaluation of the overall impact of the interrelated encryption parameters on energy consumption and delivering a global performance metric to illuminate the balance between encryption strength and energy consumption. The encryption procedure was simulated 100 times for all 576 combinations of four encryption parameters for the five algorithms. The encryption time ranged between $74 \mu s$ and $2.7 ms$, while the energy consumption ranged between $26 nJB^{-1}$ and $17.6 \mu JB^{-1}$.

Although the method employed is generic, for simulation purposes the authors considered five encryption algorithms, namely AES, DES, 3DES, RC2, and Blowfish. Here, some parameter choices were the same for all algorithms, namely the block cipher modes ECB, CBC, OFB, and CFB; data block sizes of 16, 1024, 2048, and 4096; padding scheme with noPadding, ISO101126, and PKCS5. The key sizes used were different for each algorithm as shown in **Table 1**, below.

The computation of energy consumption uses the technique described in Naik and Wei (2001), where energy consumption was represented by the product of the total number of encryption clock cycles taken and the average current drawn by each CPU clock cycle to deliver the basic encryption cost in units of ampere-cycles. To calculate the total energy cost, this basic ampere-cycle encryption cost was divided by the processor clock frequency and multiplied by the processors' operating voltage to produce the energy cost in Joules.

Algorithm	Key size
AES	128, 192, 256
DES	56
3DES	112, 168
Blowfish	56, 112, 256
RC2	40, 64, 128

Table 1: Key size variation

Reliability

A Reliability Function represents the probability that, for a given time, the system will survive (Gnedenko, Pavlov & Ushakov 1999). For illustration purposes, system S is considered that consists of individual subsystems S_1 , S_2 , S_3 , and S_4 connected in series, as shown in **Figure 1**, below. These subsystems have independent individual lifetimes, not necessarily coming from the same probability distribution. Each subsystem consists of several components, C_a , C_b , and C_c , connected in parallel with each other.

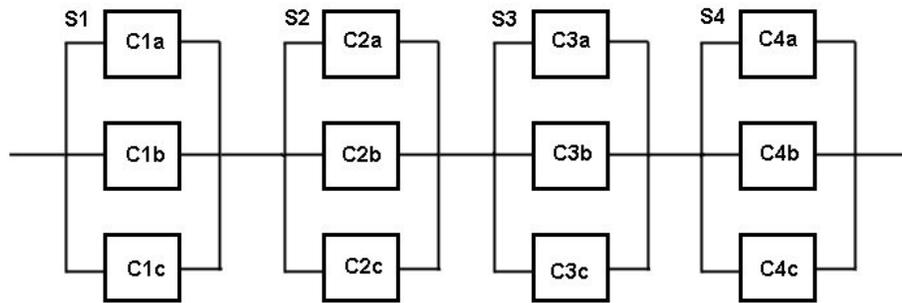


Figure 1: Encryption system S

For the above system, the Reliability Function is:

$$R(t) = P(T > t) = P(T_1 > t, T_2 > t, T_3 > t, T_4 > t) = \prod_{n=1}^4 P(T_n > t) \quad (1)$$

where T represents the total lifetime of the system, while T_1 , T_2 , and T_3 stand for the lifetime of subsystems S_1 , S_2 , and S_3 , respectively (Taramonli, Green & Leeson 2012).

The Reliability Function is the complement of the Cumulative Distribution Function (CDF). If modelling the time to fail, the CDF represents the probability of failure, and the Reliability Function represents the probability of survival. Thus, the CDF increases from zero to one as the value of t increases, and the Reliability Function decreases from one to zero as the value of t increases (Ayyub & McCuen 2011). The CDF is thus:

$$F(t) = 1 - R(t) = P(T_1 \leq t, T_2 \leq t, T_3 \leq t, T_4 \leq t) = \prod_{n=1}^4 P(T_n \leq t) \quad (2)$$

An equivalent formulation in terms of encryption can be made by replacing every occurrence of ‘death’ with the completion of the encryption procedure. Empirical distribution of lifetimes of each encryption mode can be easily measured with several simulations running for all possible combinations. A subsystem’s lifetime refers to its execution time when used in the encryption procedure. Each subsystem consists of several components connected in parallel, representing the parameters’ options that can be selected depending on the required security level (Taramonli, Green & Leeson 2012). The lifetime T of the encryption system should be as low as possible, so that the probability that the system has finished the encryption prior to the time threshold t is as high as possible. Thus, for a given time threshold t , the lower the reliability is, the higher the probability will be that the system will have finished the encryption procedure prior to t .

An example system is depicted in **Figure 2**, below, where the encryption algorithm is a set of subsystems connected in series, and each subsystem can be described by an individual encryption parameter. The resulting system comprises units for the key size, the number of rounds unit, and the operation mode. Empirical distributions of system lifetimes can be easily measured with several simulations running for all possible combinations.

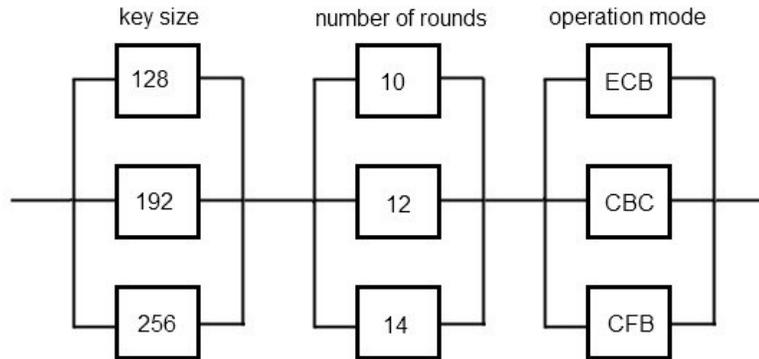


Figure 2: Example encryption system

For the encryption system S , the reliability function as shown in Equation (2) becomes:

$$R(t) = P(T > t) = P(T_1 > t, T_2 > t, T_3 > t) = \prod_{n=1}^3 P(T_n > t) \quad (3)$$

where T represents the total lifetime of the system, while T_1 , T_2 , and T_3 stand for the lifetime of subsystems S_1 , S_2 , and S_3 . A subsystem's lifetime refers to its expected period of use in the encryption procedure. Of interest is the probability that the encryption time of a security mode is low enough to finish the encryption procedure before reaching a target time or consuming less than a target energy value.

Methodology

In security analysis, the CDF function can easily be adopted and treated as a quality factor describing all encryption parameters and their impact on energy consumption. It serves as an indicator of the performance of the encryption parameters with respect to the energy consumption of the overall security system. This forms the basis for the proposed adaptive security scheme that extends the fitting of the model for each security mode accordingly, by properly adjusting functional parameters and always taking into consideration the energy cost. In this way, a metric that indicates the impact of all encryption parameters is developed, and thus a global indicator is derived. The proposed model can be thus considered global, as it is not based on distinct parameters, but, instead, arises from the impact of all the individual encryption parameters on energy consumption.

The suggested adaptive security scheme provides two options for achieving the desired encryption strength at the lowest energy cost:

- For given security requirements for the requested service, the Reliability Function is used to return the most efficient option with respect to energy, for the specific security mode. This can be achieved by excluding the modes that do not meet the security requirements, and by ranking the modes after the elimination based on the reliability or the Empirical Cumulative Distribution Function (ECDF). The higher the ECDF, the higher the probability of finishing the encryption on time.
- In the case of battery-powered devices, for a given energy threshold that derives from the battery level (or energy restrictions), the Reliability Function is used to return the most efficient option with respect to security, for the specific energy threshold. The modes that do not meet the time/energy requirements are excluded, and the rest of the cases are ranked based on the ECDF/Reliability and the selection is made based on this ranking.

Overall, the proposed adaptive security scheme consists of several security modes, each providing a different level of security, depending on the severity of the service requested. Each security mode operates using the appropriate security algorithms and/or primitives. As the energy cost depends on the encryption parameters, each policy will induce a different level of energy consumption.

Using the ECDF, a probability metric is calculated for a specified energy threshold. In this way, one can either accept or reject the combinations according to the desired level of the probability. Depending on whether they satisfy the requirements or not, a decision will be made. This implies that the combinations that do not meet the given constraints will be eliminated.

A general rule applied to most of the cases is that the highest probability of completing the encryption procedure prior to the time threshold will be selected, meaning that, for the specified threshold, the system will accomplish complete encryption in the most secure mode possible as well as at the lowest energy cost. Depending on the desired reliability, the most secure option will be selected.

By setting a time threshold t for the encryption procedure, one can exclude the cases that do not meet the time or energy constraints and, therefore, the energy limitations that derive either from the available resources or the energy-saving requirements. Since the probability that the system will have finished the encryption procedure on time is given by the ECDF, the higher the ECDF the greater the probability of success and hence of energy consumption less than or equal to the level desired. Given that T represents the total lifetime (or the total encryption time of the encryption system), the highest probability that the encryption time T is less than or equal to t is desired:

$$ECDF(t) = F(t) = P(T \leq t) \rightarrow 1 \quad (4)$$

Therefore, the higher the reliability, the higher is the probability that the system will continue the encryption after the specified time threshold t . Thus, a Reliability equal to 0 would be the optimal probability, since it is desired that the system will operate for as little time as possible and, therefore, consume the lowest energy possible:

$$R(t) = P(T > t) \rightarrow 0 \quad (5)$$

Implementation

When a set time threshold is desired, this can be set by the user, and then the calculation of the reliability metric for all the available security modes can proceed. The system will decide in favour of the mode with the highest security unless otherwise stated. For a specified time threshold $t = 500 \mu s$, some of the cases that will complete the encryption procedure prior to t with a desired lifetime ≥ 0.97 are shown in **Table 2**, below. To complete the concept of the suggested scheme, the process continues by using the ECDF of the five cases in **Table 2** that satisfy the requirements for the specified time threshold.

Case	Algorithm	Mode	Key	Data	Padding	ECDF	Reliability	Mean time (μs)	Mean Energy (nJB^{-1})
4	AES	CBC	128	2048	NoPadding	1.00	0.00	293	38
6	AES	CBC	256	2048	NoPadding	0.99	0.01	324	42
119	DES	OFB	56	2048	NoPadding	0.97	0.03	444	58
312	BF	ECB	256	2048	ISO	0.97	0.03	427	56
374	RC2	CFB	64	2048	PKCS5	0.97	0.03	379	50

Table 2: 500 μs threshold

Figure 3, below, depicts the behaviour of the estimated ECDF function which depends on the encryption time, as taken from the simulation for the five cases mentioned above.

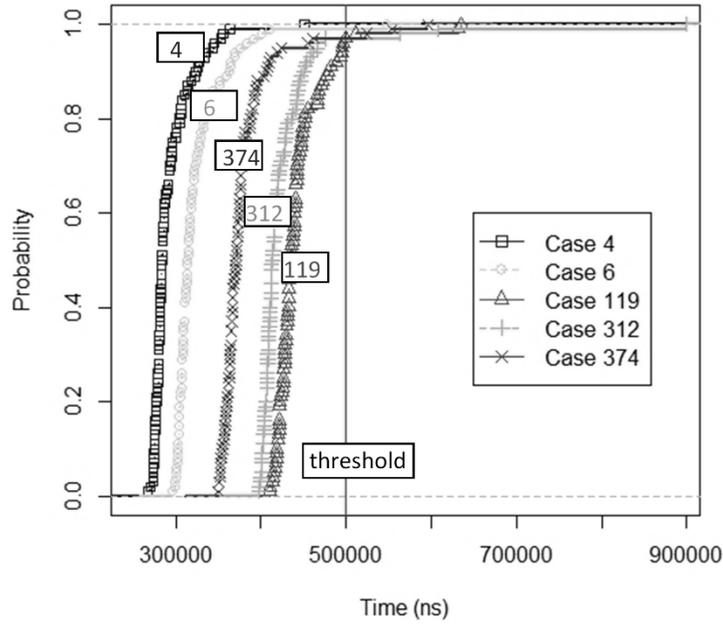


Figure 3: ECDF for sample cases 4, 6, 119, 321, 374

The area on the left side of the vertical line—which is the specified time threshold t —represents the probability that for the given time threshold the encryption procedure will be completed. Specifically, analysing the ECDF probability as illustrated in **Figure 3**, one can extract the result that for Case 4: $P(T \leq 500) = 1$; for Case 6: $P(T \leq 500) = 0.99$; for Cases 119, 312, and 374: $P(T \leq 500) = 0.97$.

Figure 4, below, shows the performance of Case 4 in terms of encryption time. The resulting ECDF and Reliability are presented, illustrating their reciprocal relationship. For the specified time threshold $t = 500 \mu s$, the ECDF tends to 1, while the Reliability Function tends to 0. This can be easily explained by comparing **Figures 3** and **4**, where one can observe that regarding the ECDF, which describes the probability of the encryption time, the maximum observed time is $450 \mu s$. For this reason, the ECDF probability tends to 1, while reliability tends to 0.

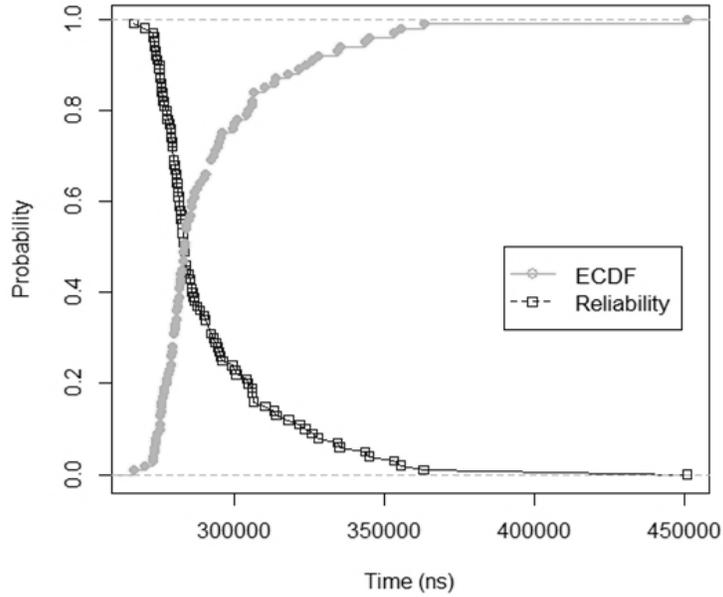


Figure 4: ECDF and Reliability—Case 4

Turning to an ideal encryption-performance scenario where the ECDF is 1 (and Reliability is 0) for time threshold t , a time threshold is set for a time such that $P(T \leq t) = 1$, which will here be $500 \mu s$ and increase it to $550 \mu s$. For example, considering Case 6 from the previous scenario, the probability of finishing before $500 \mu s$ is 0.99; increasing the time threshold by $50 \mu s$ makes the probability that Case 6 will finish before $550 \mu s$ equal to 1. This time threshold increase incurs an energy cost of $13.5 \mu J$ (8.7%) from the model for the extra 10% encryption time, which is the cost of certainty of encryption. This reinforces the idea of the energy consumption and encryption strength trade-off, which provides the user the optimal security mode selection at the lowest energy cost.

The proposed adaptive security scheme evaluates the performance of several encryption algorithms and functional variation of their parameters with respect to energy consumption. Its methodology includes all possible combinations of the encryption functional parameters ranked regarding the quality of the security, whilst also allowing for sorting security modes with respect to the level of energy consumption. At its most fundamental, this scheme determines a probability for each combination of functional parameters based on their impact on energy consumption. In **Table 2**, for example, one can not only see the ranking of a sample of the 576 cases, but also a quantitative comparison of the latter, that is, Case 4 is 3% more likely to finish the encryption prior to the time threshold t than Case 119 and so on.

Results

When a system has not been configured to differentiate between the security hierarchy of the requested services, all the propagated data will be encrypted using the same encryption scheme. Thus, the mode that meets the requirements of the most crucial service is selected, so that an adequate level of security is guaranteed. However, it is not always necessary to encrypt data with a higher level of security strength than is needed, as this might result in unnecessary time and energy consumption.

In the example presented in the previous section, for the encryption of a 2 kB of data, the user aims to encrypt prior to the 500 μs threshold, with probability ≥ 0.97 . Consider that apart from the time/energy requirements, the user also desires a high level of security. Assuming that AES is adequate for the user's security requirements, according to **Table 2** the available options for this encryption process are Cases 4 and 6, which differ only in the key size. However, given that both options provide an adequate level of security, Case 4 runs at a saving of 4 nJB^{-1} . Although this might be negligible for one encryption, using the appropriate parameters could save a significant amount of energy over many encryptions.

Let n be the number of encryptions and X be a random variable with mean μ and variance σ^2 that represents the encryption time of a security mode. Let $S = \sum_{i=1}^n X_i$ be the overall encryption time of the n encryptions. Since X_1, \dots, X_n are i.i.d., from Central Limit Theorem (CLT), S approaches a normal distribution (Milton & Arnold 2002). Hence, the ECDF of \hat{S} converges in distribution to

$$S \sim N(n\mu, n\sigma^2) \text{ as } n \rightarrow \infty \quad (6)$$

From Equation (6), it can be derived that for Case 4 in Table 2, \hat{S}_4 converges to $S_4 \sim N(n\mu_4, n\sigma_4^2)$ as $n \rightarrow \infty$, where $n = 1000$, $\mu_4 = 2.93 \times 10^5 \text{ ns}$, $\sigma_4^2 = 6.61 \times 10^8 \text{ ns}$, $\mu_{S_4} = n\mu_4 = 2.9 \times 10^8 \text{ ns}$ and $\sigma_{S_4}^2 = n\sigma_4^2 = 6.61 \times 10^{11} \text{ ns}$.

Figure 5, below, illustrates a point-to-point comparison of the theoretical distribution of S_4 and the approximate of \hat{S}_4 as generated from $\hat{S}_4 = \sum_{i=1}^n X_{i,j}$, where $j \in \{1, \dots, m = 10000\}$ and $X_i \sim ECDF_4$ with mean μ_i and variance σ_i^2 , $\forall i \in \{1, \dots, n\}$. As shown in the histogram, \hat{S}_4 is distributed evenly around the mean, with most of the frequencies gathered in the centre, indicating that \hat{S}_4 follows the normal distribution. Hence, the approximation of \hat{S}_4 is good, since the theoretical density maps the histogram. The Q-Q plot indicates that \hat{S}_4 follows the normal curve as well since the data points lie close to the diagonal line. Similarly, for Case 6, \hat{S}_6 converges to $S_6 \sim N(n\mu_6, n\sigma_6^2)$ as $n \rightarrow \infty$, where $n = 1000$, $\mu_6 = 3.24 \times 10^5 \text{ ns}$, $\sigma_6^2 = 1.05 \times 10^9 \text{ ns}$, $\mu_{S_6} = n\mu_6 = 3.24 \times 10^8 \text{ ns}$ and $\sigma_{S_6}^2 = n\sigma_6^2 = 1.05 \times 10^{12} \text{ ns}$.

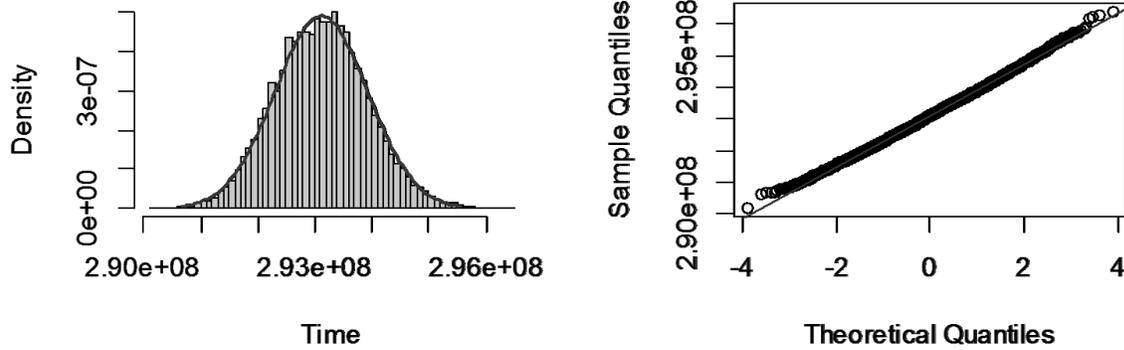


Figure 5: Theoretical S_4 vs. estimated \hat{S}_4 distribution

Figure 6, below, illustrates a comparison of the theoretical distribution of S_6 and the approximate version \hat{S}_6 as generated from $\hat{S}_6 = \sum_{i=1}^n Y_{i,j}$, where $j \in \{1, \dots, m = 10000\}$ and $Y_i \sim ECDF_6$ with mean μ_i and variance σ_i^2 , $\forall i \in \{1, \dots, n\}$. Again, the figure indicates that the distribution of the sum approaches a normal distribution. The Q-Q plot indicates that \hat{S}_6 is a good fit as well, as the data points do not deviate from the diagonal line. Therefore, by fixing all encryption parameters that meet the user requirements and by distinguishing the key size, Cases 4 and 6 are compared.

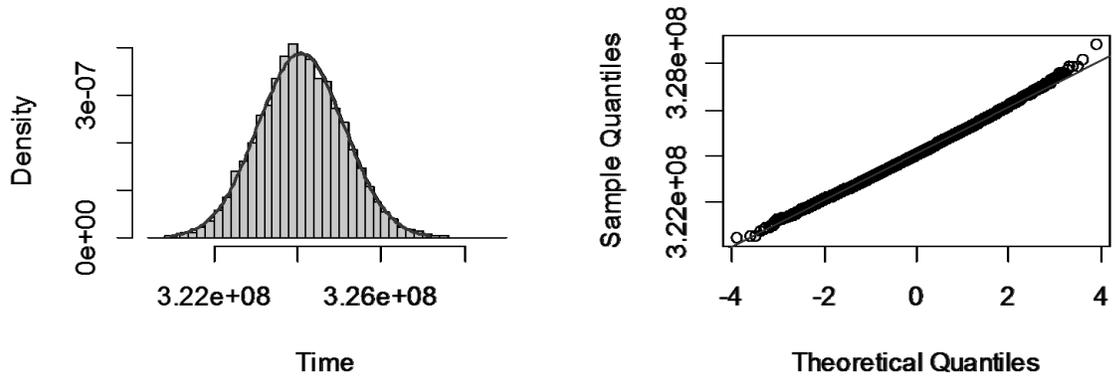


Figure 6: Theoretical S_6 vs estimated \hat{S}_6 distribution

Figure 7, below, illustrates the contrast of the two encryption modes. As expected, S_4 has a smaller mean compared to S_6 , $\mu_{S_4} = 2.93 \times 10^8 s < \mu_{S_6} = 3.2410^8 s$, as well as smaller variance, $\sigma_{S_4}^2 = 6.61 \times 10^{11} s^2 < \sigma_{S_6}^2 = 1.05 \times 10^{12} s^2$. In terms of n encryptions, this difference could be translated to 10% more time for encryption with mode 6 than with mode 4.

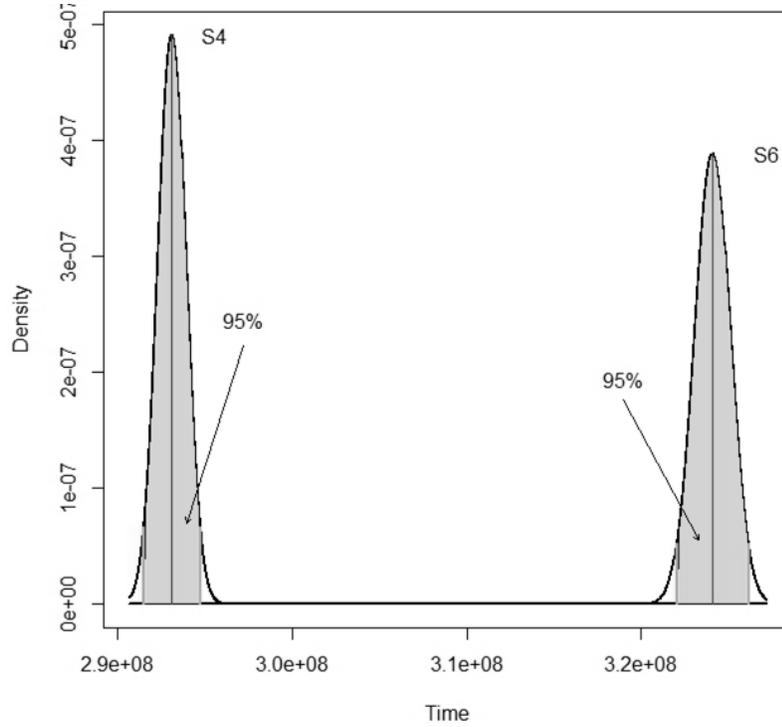


Figure 7: S_4 vs S_6 density plot

Additionally, for an observation that follows the distribution of S_4 , the probability that the overall encryption time of n services will take values from the following ranges is

$$P\left(S_4 \in (\mu_{S_4} - 3\sigma_{S_4}, \mu_{S_4} + 3\sigma_{S_4})\right) \approx 0.99 \quad (7)$$

$$P\left(S_4 \in (\mu_{S_4} - 2\sigma_{S_4}, \mu_{S_4} + 2\sigma_{S_4})\right) \approx 0.95 \quad (8)$$

$$P\left(S_4 \in (\mu_{S_4} - \sigma_{S_4}, \mu_{S_4} + \sigma_{S_4})\right) \approx 0.68 \quad (9)$$

As it has been shown, by encrypting n times under Case 6 parameterisation, it is expected that the overall encryption time will be 10% higher than the Case 4 parameterisation. Knowledge of the distributions of S_4 and S_6 provides further understanding regarding the deviation of the encryption time from the mean by computing the confidence intervals as shown in Equations (7-9).

There follows an analysis that will enable the user not only to rank security cases, but also to quantify and mathematically evaluate the selection among the available options. This will allow a user to predict the encryption time/energy saving s/he could achieve and make inference on how likely the predictions are to be true. Therefore, the distribution of the difference between the time of n encryptions from Case 4 and 6 will be investigated.

Let $W_1 = S_6 - S_4$ be a random variable that represents the difference of two independent random variables, where $S_6 \sim N(n\mu_6, n\sigma_6^2)$ and $S_4 \sim N(n\mu_4, n\sigma_4^2)$. The characteristic function of a random variable X is defined by

$$\varphi_x(t) = E(e^{itX}) \quad (10)$$

and has the property that uniquely characterizes the probability function of Papoulis & Pillai (2002). Hence, from Equation (10) the characteristic function of a normal r.v. with expected value μ and variance σ^2 is given by:

$$\varphi_x(t) = \exp(it\mu - \frac{\sigma^2 t^2}{2}) \quad (11)$$

Thus, from Equation (11),

$$\begin{aligned} \varphi_{W_1}(t) &= \varphi_{S_6 - S_4}(t) \\ &= \varphi_{S_6}(t) \varphi_{S_4}(t) \quad (\text{by independence}) \end{aligned} \quad (12)$$

Also, by symmetry $-S_4 \sim N(-n\mu_4, n\sigma_4^2)$ (Papoulis & Pillai 2002), Equation (12) results in

$$\begin{aligned} \varphi_{W_1}(t) &= \exp\left\{itn\mu_6 - n\sigma_6^2 \frac{t^2}{2}\right\} \cdot \exp\left\{itn\mu_4 - n\sigma_4^2 \frac{t^2}{2}\right\} \\ &= \exp\left\{itn\mu_6 - n\sigma_6^2 \frac{t^2}{2} + itn\mu_4 - n\sigma_4^2 \frac{t^2}{2}\right\} \\ &= \exp\{itn(\mu_6 - \mu_4) - t^2 n(\sigma_6^2 + \sigma_4^2)\} \end{aligned} \quad (13)$$

Hence, from (13), W_1 follows the normal distribution

$$W_1 \sim N(n(\mu_6 - \mu_4), n(\sigma_6^2 + \sigma_4^2)) \quad (14)$$

The distribution of the difference between the time of n encryptions for Cases 4 and 6 is illustrated in **Figure 8**, below.

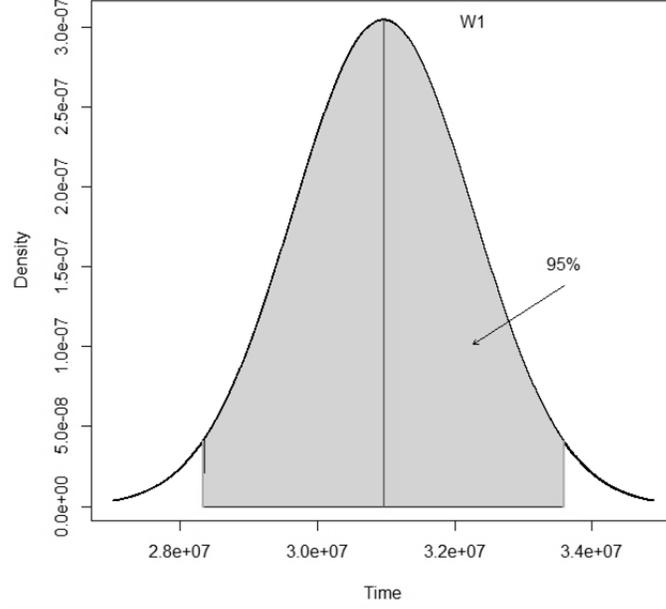


Figure 8: W_1 density plot

It is shown that 95% of the shaded area is inside the range $\mu_{W_1} \pm 2\sigma_{W_1} = (2.8 \times 10^7s, 3.3 \times 10^7s)$ as stated in Equation (9), while from Equation (8), 99% of the area under the curve lies within $\mu_{W_1} \pm 3\sigma_{W_1} = (2.7 \times 10^7s, 3.4 \times 10^7s)$. This reveals that the likelihood that n services, which have been encrypted using security mode 4, will finish prior to n services which have been encrypted using security mode 6, is very low, since $P(W_1 < 0) \rightarrow 0$.

As expected, the results show that between S_4 and S_6 , the former should be selected for services whose security requirements are satisfied, since it provides greater efficiency than S_6 .

There now follows an examination of an adaptive scenario to illustrate the adaptability of the proposed scheme. In the scenario, the user has requested k services to be encrypted using mode 4 and $(n - k)$ using mode 6. Let $Q_1 = Z_6 + Z_4 = \sum_{i=1}^k X_i + \sum_{j=1}^{n-k} Y_j$ where $Z_6 = \sum_{i=1}^k X_i \sim N(k\mu_6, k\sigma_6^2)$, $Z_4 = \sum_{j=1}^{n-k} Y_j \sim N((n - k)\mu_4, (n - k)\sigma_4^2)$, $X_i \sim ECDF_6$, $i \in \{1, \dots, k\}$, with $\mu_6, \sigma_6^2 < \infty$, $Y_j \sim ECDF_4$, $j \in \{1, \dots, n - k\}$, with $\mu_4, \sigma_4^2 < \infty$. In addition, X_i are i.i.d., Y_j are i.i.d. and X_i, Y_j independent $\forall i, j$. Similar to Equation (12) and by independence and because

$$\begin{aligned}
 \varphi_{Q_1}(t) &= \varphi_{Z_6}(t) \cdot \varphi_{Z_4}(t) \\
 &= \exp\left\{itk\mu_6 - k\sigma_6^2 \frac{t^2}{2}\right\} \cdot \exp\left\{it(n - k)\mu_4 - (n - k)\sigma_4^2 \frac{t^2}{2}\right\} \\
 &= \exp\left\{itk\mu_6 - k\sigma_6^2 \frac{t^2}{2} + it(n - k)\mu_4 - (n - k)\sigma_4^2 \frac{t^2}{2}\right\} \\
 &= \exp\left\{it(k\mu_6 + (n - k)\mu_4) - \frac{t^2}{2}(k\sigma_6^2 + (n - k)\sigma_4^2)\right\}
 \end{aligned}$$

the overall encryption time Q_1 of the compound scenario is distributed according to

$$Q_1 \sim N(k\mu_6 + (n - k)\mu_4, k\sigma_6^2 + (n - k)\sigma_4^2) \quad (15)$$

The density of Q_1 for $k = 200$ encryptions under mode 4 and $n - k = 800$ encryptions under mode 6 is illustrated in **Figure 9**, below.

For the compound mode, it is expected that the overall encryption time will be 8% higher than mode 4 and 2% less than mode 6. Furthermore, from Equation (8), the time interval that assures the user's overall encryption time will lie within $(3.16 \times 10^8 s, 3.2 \times 10^8 s)$ with probability 0.95. This provides statistical confidence that with high probability the right 2.5% tail of Q_1 will not overlap with the left 2.5% tail of S_6 , since

$$P(Q_1 > \mu_{S_6} - 2\sigma_{S_6}) \approx 0.6 \times 10^{-10} \rightarrow 0 \quad (16)$$

and

$$P(S_6 < \mu_{Q_1} + 2\sigma_{Q_1}) \approx 0.7 \times 10^{-20} \rightarrow 0 \quad (17)$$

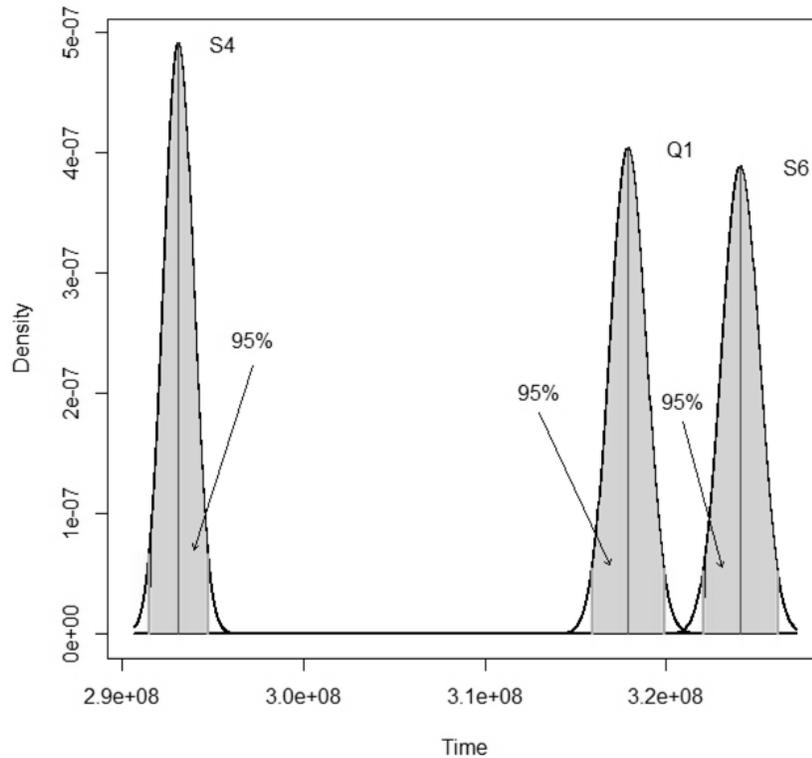


Figure 9: Q_1, S_4, S_6 density plot

Hence, with a 95% probabilistic level of confidence, time predictions belonging to the set of the 2.5% best-case scenarios for S_6 do not to overlap with those lying in the 2.5% worst-case scenarios for the compound mode. Therefore, S_4 and S_6 can be considered as benchmarks for the user customization options and decisions regarding the mode selection, since the distributions of S_4 and S_6 provide an upper and lower bound on the customisation of security. The user can make

inferences and predict the expected times for the different encryptions according to the severity of each service. Depending on the allocation of the k and the $n - k$ services to different encryption modes, the user can customize security according to need.

This section highlighted the benefits of deploying the Reliability Model for the decision-making for the selection of the most effective security mode. As discussed, the investigation of the probability that a single encryption will be completed prior to a given threshold is feasible using the ECDF derived from the simulations. This acts as an indicator that can be used as a performance metric for the corresponding security mode.

The asymptotic distribution of n encryptions of the two cases that were assumed to meet users' security requirements has been investigated. The approximate distribution of the overall execution time of n encryptions as calculated by applying CLT, is a normal distribution $N(\mu, \sigma^2)$ with parameters μ equal to n times the mean execution time of a single encryption and σ^2 equal n times the variance of the execution time of a single encryption. It must be noted that the general form of the normal distribution as shown in Equation (6) is applicable to any case by properly adjusting the parameters μ and σ^2 . The compound scenario presented in this section can be used as a decision-making policy for the allocation of k encryptions to a specific security mode and $n-k$ encryptions to another one. This policy could also be further extended to include more security modes. The distribution of the overall encryption time of the n encryptions would be normal and the corresponding μ and σ^2 values could be used to derive the compound mode distribution.

Conclusions and Future Work

This paper proposes an adaptive security scheme that takes a novel approach to low-energy encryption. The method described relies on the use of the CDF as a global performance indicator. The performance of five encryption algorithms was evaluated based on the encryption time, energy consumption, and the encryption parameter variation, taking into consideration the overall impact of the encryption parameters on energy consumption. CDF was used as a global indicator for the optimal security mode selection among algorithms and encryption parameters. An adaptive security scheme that results in the most efficient security mode, aiming for the highest security level possible at the lowest energy cost, was suggested. This stochastic approach, based on Reliability Methods, was presented.

The proposed methodology provides the user the ability to predict the energy consumption as the number of encryptions n scales up, by examining the distribution of the security modes. The latter acts as a benchmark, and predictions regarding the saving in the overall encryption time of those modes can be made based on the distribution of their difference. A saving of up to 10% in terms of energy or time was shown for an example user specification, by means of the appropriate parameter selection.

There are several open-ended problems extending beyond this work that offer interesting research opportunities. One suggestion for future work entails further examining the extreme values and their influence on decision-making. Hence, although the Reliability Function by default deals with the right tail of the distribution, as part of future work, an investigation into more detailed aspects of the distribution of those extremes would be useful. Another possibility for future work is to include more encryption algorithms in the system. The resulting scheme would allow for the

optimum selection among a plethora of options and hence provide a more generic decision-making tool. Moreover, examining algorithms other than those described in this paper would provide an interesting point of comparison for further evaluation.

References

Alampalayam, SP & Kumar, A 2003, 'An adaptive security model for mobile agents in wireless networks', *Proceedings of the IEEE Global Telecommunications Conference, 2003 (GLOBECOM '03)*, vol. 3, pp. 1516-21.

Ayyub, BM & McCuen, RH 2011, *Probability, statistics, and reliability for engineers and scientists*, 3rd edn, CRC Press, Boca Raton, FL, U.S.A.

Chandramouli, R, Bapatla, S, Subbalakshmi, KP & Uma, RN 2006, 'Battery power-aware encryption', *ACM Transactions on Information and System Security (TISSEC)*, vol. 9, no. 2, pp. 162-80.

Elminaam, DSA, Kader, HMA & Hadhoud, MM 2009, 'Energy efficiency of encryption schemes for wireless devices', *International Journal of Computer Theory and Engineering*, vol. 1, no. 3, p. 302.

Gnedenko, B, Pavlov, IV & Ushakov, IA 1999, *Statistical reliability engineering*, John Wiley & Sons, New York, NY, U.S.A.

Guo, C, Wang, HJ & Zhu, W 2004, November, 'Smart-phone attacks and defences', *Proceedings of the Third Workshop on Hot Topics in Networks (HotNets-III) ACM SIGCOMM*, pp. 223-34.

Guo, Z, Jiang, W, Sang, N & Ma, Y 2011, 'Energy measurement and analysis of security algorithms for embedded systems', *Proceedings of the IEEE/ACM International Conference on Green Computing and Communications (GreenCom)*, pp. 194-99.

Jones, O, Maillardet, R & Robinson, A 2014, *Introduction to scientific programming and simulation using R*, CRC Press - Taylor and Francis Group, Boca Raton, FL, U.S.A.

Jorstad, ND & Landgrave, TS 1997, 'Cryptographic algorithm metrics', *Proceedings of the National Institute of Standards and Technology 20th National Information Systems Security Conference*.

Milton, JS & Arnold, JC 2002, *Introduction to probability and statistics: Principles and applications for engineering and the computing sciences*, 4th edn, McGraw-Hill Inc., New York, NY, U.S.A.

Naik, K & Wei, DS 2001, 'Software implementation strategies for power-conscious systems', *Mobile Networks and Applications*, vol. 6, no. 3, pp. 291-305.

Papoulis, A & Pillai, SU 2002, *Probability, random variables, and stochastic processes*, Tata McGraw-Hill Education, Columbus, OH, U.S.A.

Potlapally, NR, Ravi, S, Raghunathan, A & Jha, NK 2006, 'A study of the energy consumption characteristics of cryptographic algorithms and security protocols', *IEEE Transactions on Mobile Computing*, vol. 5, no. 2, pp. 128-43.

Prasithsangaree, P & Krishnamurthy, P 2003, 'Analysis of energy consumption of RC4 and AES algorithms in wireless LANs', *Proceedings of the 2003 IEEE Global Telecommunications Conference (GLOBECOM '03)*, vol. 3, pp. 1445-49.

Simplicio, MA Jr, Silva, MV, Alves, RC & Shibata, TK 2017, 'Lightweight and escrow-less authenticated key agreement for the Internet of Things', *Computer Communications*, vol. 98, pp. 43-51.

Singh, SP & Maini, R 2011, 'Comparison of data encryption algorithms', *International Journal of Computer Science and Communication*, vol. 2, no. 1, pp. 125-27.

Snader, R, Kravets, R & Harris, AF III 2016, 'Cryptocop: Lightweight, energy-efficient encryption and privacy for wearable devices', *Proceedings of the 2016 Workshop on Wearable Systems and Applications*, pp. 7-12.

Taramonli, C, Green, RJ & Leeson, MS 2012, 'Energy conscious adaptive security scheme for optical wireless', *Proceedings of the 14th International IEEE Conference on Transparent Optical Networks (ICTON)*, pp. 1-4.

Troutman, J & Rijmen, V 2009, 'Green cryptography: Cleaner engineering through recycling', *IEEE Security & Privacy*, vol. 7, no. 4, pp. 71-73.

Vijayan, K & Raaza, A 2016, 'A novel cluster arrangement energy efficient routing protocol for wireless sensor networks', *Indian Journal of Science and Technology*, vol. 9, no. 2.