International Journal of Computer Science and Applications,
©Technomathematics Research Foundation
Vol. 11, No. 1, pp. 18 – 36, 2014

THE EFFICIENCY OF ENCRYPTION ALGORITHMS IN EAX MODE OF OPERATION IN IPSEC-BASED VIRTUAL PRIVATE NETWORKS FOR STREAMING RICH MULTIMEDIA DATA

ALEXANDER USKOV

Computer Science and Information Systems, Bradley University, 1501 W Bradley Avenue
Peoria, Illinois, 61625, U.S.A.
auskov@bradley.edu
http://cs.bradley.edu

The characteristics of encryption/decryption algorithms (ciphers) and modes of their operation (modes) have significant influence on security and performance of computer networks. The common modes of cipher operation such as ECB, CBC, OFB, CFB, CTR and XTS provide various levels of data confidentiality; however, those modes do not provide integrity and authenticity of encrypted data, and, therefore, do not efficiently protect data against non-authorized access and/or malicious modification/tampering. The newest generation of cipher modes – authenticated encryption with associated data (AEAD) modes – provides confidentiality, integrity and authenticity of data in a single cryptographic scheme. This paper presents the outcomes of research project on ciphers' efficiency in one of the most promising AEAD cryptographic schemes – the EAX mode - in IPsec-based mobile virtual private networks for streaming rich multimedia data.

Keywords: ciphers; EAX mode; efficiency; VPN; IPsec.

1. Introduction

1.1. *Current status of Internet security*

In accordance with the recent report by Symantec [Symantec (2014)], "… in 2013, there were 8 data breaches that netted hackers 10 million or more identities, the largest of which was a massive breach of 150 million identities. In contrast, 2012 saw only 1 breach larger than 10 million identities. Mobile users are storing sensitive files online (52%), store work and personal information in the same online storage accounts (24%) and sharing logins and passwords with families (21%) and friends (18%), putting their data and their employers' data at risk. Yet only 50% of these users take even basic security precautions. … The most commonly exploited vulnerabilities relate to SSL and TLS protocol renegotiation".

According to the 2013 report by the well-known in IT security area Ponemon Institute [Ponemon Institute (2013)], "… in the IT environment, mobility and third party applications are the greatest security risks. 75% of respondents - 676 IT security practitioners - say mobile devices such as smart phones represent the greatest risk of potential IT security risk within the IT environment. The percentage of respondents who identified the use of cloud computing resources as a major concern has increased from 28

% to 44%. 55% say the increased use of mobile platforms is a threat to the organization, up from 47% last year“ (Fig. 1).

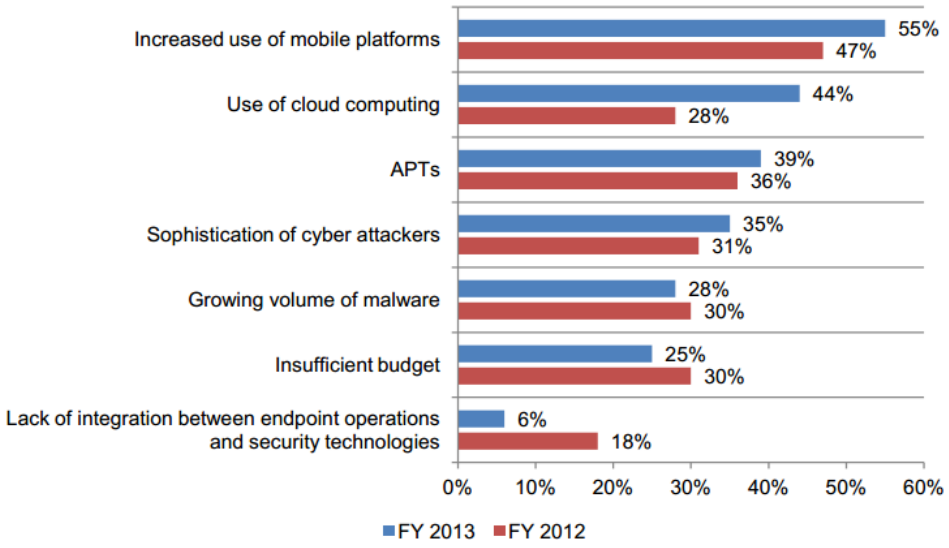

Fig. 1. IT security risks of greatest concern to the organization (three choices permitted) [Ponemon Institute (2013)]

Additionally, the 2014 report by Cisco [Cisco (2014)] reads “Malicious exploits are gaining access to web hosting servers, nameservers, and data centers. Threat alerts grew 14% year over year; new alerts (not updated alerts) are on the rise. Java comprises 91% of web exploits. 99% of all mobile malware in 2013 targeted Android devices. Android users also have the highest encounter rate (71%) with all forms of web-delivered malware”.

These and multiple additional reports from industry and companies in IT security area clearly show that the security of computer networks, mobile computing, cloud computing, Web and mobile applications, including Web-based streaming rich multimedia (RMM) systems is still one of the user’s biggest concerns [Bergman, et al. (2013)].

1.2. *VPN technology and IPsec stack of protocols*

The integrated use of Virtual Private Network (VPN) technology [Lewis (2006), Bollapragada et al (2005)] and IPsec stack of security protocols [Carmouche (2007), Frankel (2005)] is considered as one of the most efficient approaches to overcome (or, significantly reduce) security-related problems in computer networks for a transfer of confidential data, including rich multimedia (RMM) data (audio, video, graphics, etc.) over the public Internet. In accordance with the Computer Security Institute report [Computer Security Institute (2010)] (Fig. 2), VPN technology provides one of the best

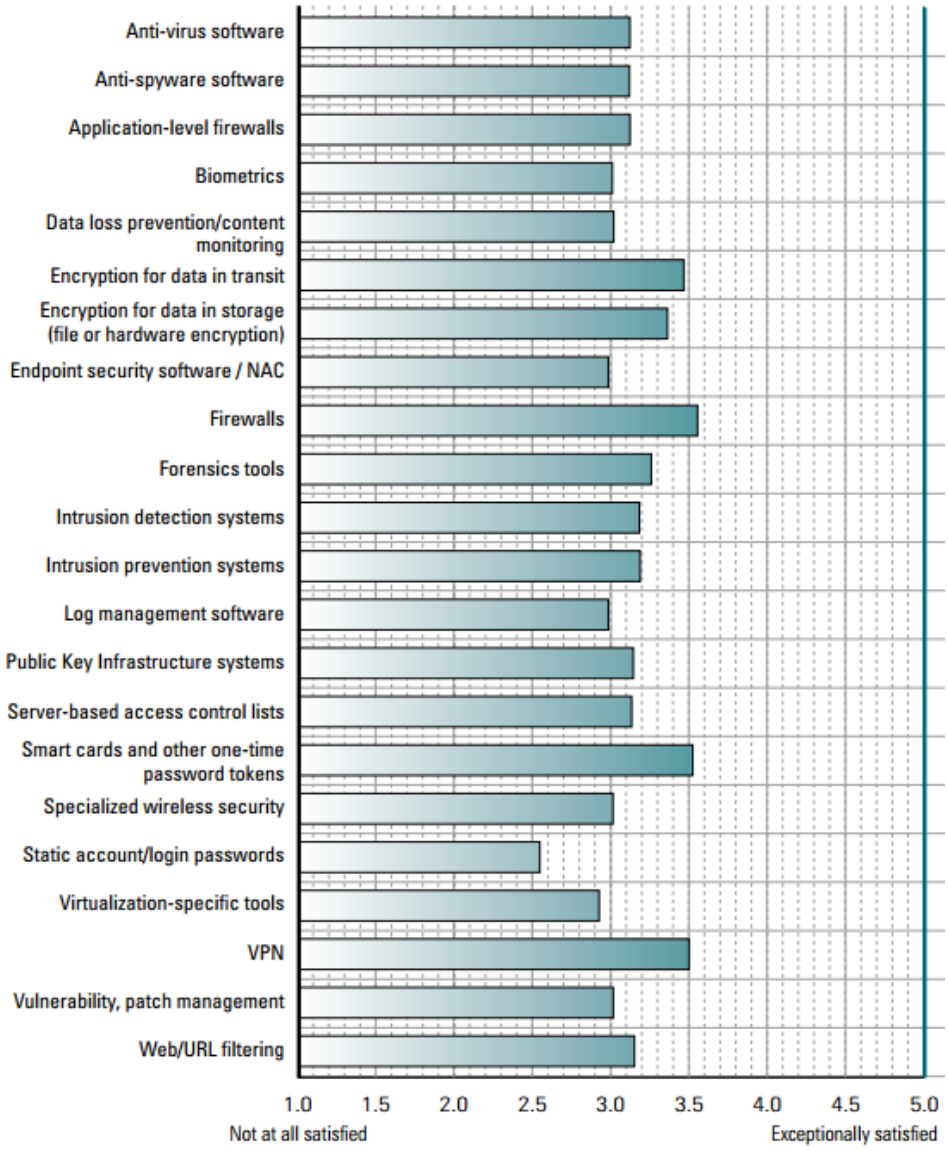

Fig. 2. Satisfaction with security technology [Computer Security Institute (2010)].

user's satisfaction rates in terms of computer network security – 3.50 out of 5.0 points (where 5. 0 corresponds to "exceptionally satisfied" level). The other security technologies with high satisfaction rates include 1) firewalls (3.55 points), 2) encryption for data in transit (3.47 points), 3) smart cards and other one-time password tokens (3.25 points).

The key aspect of mobile VPN (MVPN) design, development and implementation is a set of security, communication and data exchange protocols and mechanisms that use dynamic VPN tunnels to support user mobility and security [Shneyderman and Casati (2002), Bollapragada et al (2005), Uskov (2013)].

IPsec is a framework of open standards for ensuring private secure communications over public Internet Protocol (IP) based networks. It provides security services at the IP layer by enabling a system to select security protocols, identify various encryption and authentication algorithms to be used, and set up cryptographic keys required to provide the requested services [Kent and Seo (2005), Kent (2005a), Kent (2005b)].

1.3. *Modes of operation of encryption algorithm*

The efficiency of VPN tunnel, including performance and security, in IPsec-based MPVN significantly depends on efficiency of its selected components [Mogollon (2007), Bollapragada et al (2005), Uskov (2012), Uskov (2013)], including:

(1) encryption algorithms: encryption algorithms (ciphers) with various parameters such as size of secret key length or data block size; the common popular block ciphers include AES, RC6, RC5, TwoFish, DES, 3DES, IDEA, CAST, Camellia, etc.;
(2) modes of cipher operation;
(3) integrity algorithms: hash algorithms, or, integrity algorithms, including MD5, SHA-1, SHA-2, SHA-256, SHA-384, SHA-512, etc;
(4) authentication algorithms: message authentication code (MAC) and hashed message authentication code (HMAC) algorithms such as HMAC(MD5), HMAC(SHA-1), HMAC(SHA-2), HMAC(SHA-256), etc.

The common modes of operation such as electronic codebook (ECB), cipher-block chaining (CBC), output feedback (OFB), cipher feedback (CFB), counter mode (CTR), and XTS [Dworkin (2001), IEEE P1619/D16 (2007)] provide various levels of only one characteristic - data confidentiality. However, due to multiple reports on security issues [for example, Bernstein (2013)], those modes of cipher operation are not reliable in terms of data protection against accidental modification or malicious tampering.

The newest 4th generation of cipher modes – authenticated encryption with associated data (AEAD) modes – provides confidentiality, integrity and authenticity assurances on the data in a single cryptographic scheme. The examples of AEAD modern cipher modes include but are not limited to counter mode with CBC-MAC (CCM), a conventional authenticated-encryption (EAX), Offset CodeBook 2 (OCB2), Galois/counter mode (GCM), etc. [NIST (2013)].

1.4. *Research project goal*

The main goal of this research project was to analyze efficiency of encryption algorithms in one of the most promising AEAD cryptographic schemes – the EAX mode - in real-world environments that include 1) IPsec-based MVPNs for streaming RMM data, 2) user's various affordable mobile technical platforms, 3) ready-to-be streamed RMM files

(i.e. webified files with audio, video, animation, simulation, outcomes of recorded computer screen technology, static graphics, text, etc.) of significantly different sizes as test data sets; the examples of files include Web-taped ready-to-be-streamed video lectures with synchronized RMM data [Uskov (2004), Uskov (2005), Uskov (2013)].

The rest of this paper consists of the following parts. In Section 2, a brief description of the EAX mode is provided along with its reported advantages and weaknesses. In Section 3 the technical specifications of the used real-world "practical" RMM research environment are provided, and in Section 4 – obtained research outcomes about efficiency of selected block ciphers in the EAX mode in IPsec-based MVPNs. Finally, in Section 5 conclusions and recommendations of this research project are provided.

This paper complements author's research outcomes regarding ciphers' efficiency in CBC and CTR modes [Uskov (2013), Uskov (2012)] on IPsec-based MVPNs.

2. The EAX mode of cipher operation

2.1. *The EAX mode: encryption and decryption*

The EAX mode is the AEAD type of 2-phase cryptographic scheme - with one pass for achieving privacy and one pass for authenticity of data [Bellare et al (2004)].

In general, given a nonce N, a message M, and a header H, the EAX mode protects the privacy of M and the authenticity of both M and H. The EAX mode is based on both CTR and OMAC (one key message authentication code) modes of operation; the details of encryption and decryption phases under EAX mode are given on Fig. 3 [Bellare et al (2004)].

2.2. *The EAX mode: security*

The EAX mode has provable security It is secure assuming that the block cipher that it uses is a secure pseudorandom permutation (PRP). Security for EAX means indistinguishability from random bits and authenticity of ciphertexts. The security proof relies on a result about the security of a tweakable extension of OMAC in which an adversary can obtain not only a tag for a message of its choice, but also an associated key-stream [Bellare et al (2004)].

2.3. *The EAX mode: strengths and weaknesses*

The EAX mode has a set of reported strengths and weaknesses [Bellare et al (2004), Crypto++ (2013)]; its advantages are as follows:

(1) The EAX mode provides a high performance:
   - (i) it has on-line capability (i.e. it can process streaming data on-the-fly) – this feature is very important for streaming RMM data and systems;
   - (ii) it requires neither complex encodings nor aligned operations;
   - (iii) it uses a s single key that minimizes space and key-schedule operations;
   - (iv) it can pre-process static headers;
   - (v) due to "encrypt-then-authenticate" approach used in the EAX mode, the invalid messages can be rejected at half of the cost of decryption;

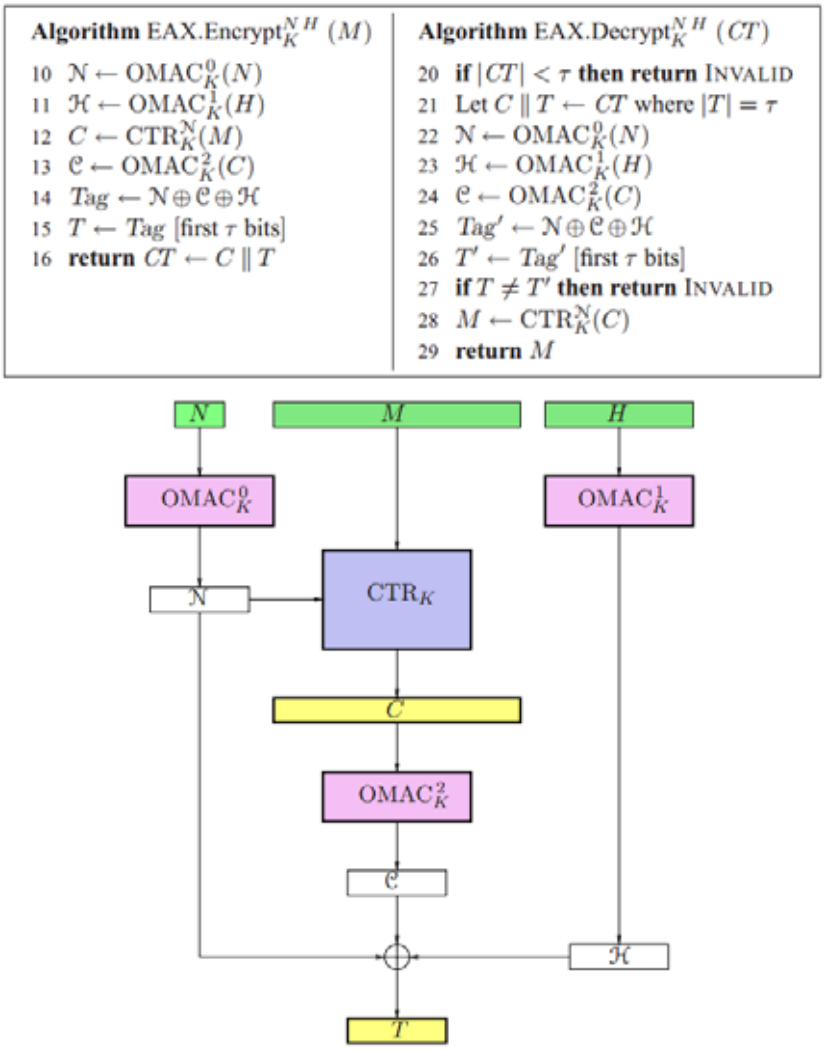

Fig. 3. Encryption and decryption under EAX mode. The plaintext (message) is M, the ciphertext is CT, the key is K, the nonce is N, the header is H and ciphertext CT=C||T. The mode depends on a block cipher E (that CTR and OMAC algorithms implicitly use) and a tag length τ [Bellare et al (2004)].

(2) the EAX mode provides ease of correct use and simplicity of implementation:
   (i) its single cryptographic schema provides all required encoding/decoding procedures;
   (ii) its nonces don't need to be random (what requires additional implementation complexity) – in the EAX nonces should be just non-repeating;
   (iii) due to "encrypt-then-authenticate" approach used in the EAX mode, the invalid messages can be rejected at half of the cost of decryption;
(3) the EAX mode provides ease of correct use and simplicity of implementation:

(i) its single cryptographic schema provides all required encoding/decoding procedures;
(ii) its nonces don't need to be random (what requires additional implementation complexity) – in the EAX nonces should be just non-repeating;
(iii) it directly processes nonces of arbitrary and variable sizes;
(iv) its nonces, headers, and messages can be of any bit length;
(v) a single API for a programmer avoids multiple possible pitfalls (e.g., poor initialization vector (IV) handling, etc.) and coding mistakes;

(4) utilization of the EAX mode is free of charge (i.e. it has no patent encumbrance).

On the other hand, the EAX mode has the following reported weaknesses:

(1) the EAX mode as 2-phase cipher mode is expected to be about slower than 1-phase cipher modes;
(2) the EAX mode is nor parallelizable (what can become a possible issue in light of perspectives of Graphic Processing Unit (GPU) technology use for encoding/ decoding procedures);
(3) the EAX mode is not approved yet by the NIST (National Institute of Standards and Technology, USA).

3. Research environment

3.1. *Encryption algorithms and modes analyzed*

A huge number of various ciphers can be used for an encryption of data to be transferred through a VPN tunnel. In order to narrow a subset of ciphers to be analyzed, the most recent description of the VPN tunneling protocol - Internet Key Exchange, version 2 (IKEv2) [Kaufman (2005)], has been used. It reserves identificators for several ciphers that may be considered as algorithms which most likely will be used in MVPNs in the near future, including the following block ciphers: AES, RC6, RC5, TwoFish, CAST, Camellia, IDEA, DES, and 3DES.

The only EAX mode has been used in the current research project.

3.2. *Test RMM data files used*

One of the objectives of this research project was to analyze the efficiency of ciphers in the EAX mode on RMM ready-to-be-streamed files of significantly different sizes – from 50 to 1,000 MB. The names of RMM test data sets and their exact sizes in bytes are given in Table 1.

Table 1. The names of test RMM data sets and their exact sizes (in bytes).

Test data set name	Exact size of test RMM data set (in Bytes)
5 MB	5,799,936
10 MB	52,126,418
100 MB	104,252,836
150 MB	156,379,254
200 MB	208,505,672

250 MB	260,632,090
1000 MB	1,042,528,360

3.3. *Technical platforms used*

The other objective of this research project was to test the efficiency of ciphers in the EAX mode on various affordable and commonly used mobile technical platforms. A summary of technical platforms used in this research project is presented in Table 2.

Table 2. Specifications of technical platforms used.

Technical platform used	**Name and specs of technical platform used**	**Operating system used**	**CPU mode used**
Technical platform 1 (TP1) - a powerful mobile laptop (of "desktop replacement" type): Dell Latitude Core i5	Intel Dual Core i5-2520M, 2.50GHz, 1066 MHz, Intel 6300 Wireless-N, Intel HD Graphics 3000, 320 GB Hard Drive, 4GB DDR3 ECC SDRAM 1333MHz (2 DIMMs)	Genuine Windows 7 Professional 64-bit	1Proc
			Mproc
		Linux 2.6.39	1Proc
			Mproc
Technical platform 2 (TP2) - a simulation of commonly used netbook (of "thin and light, for everyday mobile computing" type): Asus Seashell 1005PE	1.66GHz Intel N450 Atom Processor, 1GB DDR2 RAM, 2GB, 250 GB SATA Hard Drive (5400RPM), 802.11 b/g/n	Windows 7 Starter operating system	1Proc
			Mproc
		Linux 2.6.39	1Proc
			Mproc
Technical platform 3 (TP3) – used in the current (as of Dec 2013) version of the CRYPTO++ 5.6.0 library	Intel Core 2 1.83 GHz processor	Windows Vista in 32-bit mode	1Proc
		Linux	1Proc

All analyzed ciphers in the EAX mode were coded in C++ and compiled with Microsoft Visual C++ 2005 SP1 (with whole program optimization and optimization for speed).

3.4. *Legend used*

The following legend is used to reflect obtained research outcomes on Fig. 3 and in Tables 3-11:

- Test RMM data set: a name of test RMM data set (file) based on size of RMM ready-to-be-streamed file to be encrypted (5 MB, 50 MB, 100MB, 150 MB, 200 MB, etc.);
- *TIME*: a time (in seconds) needed to encrypt the entire test RMM data set;
- *PERF*: a performance of a particular cipher in *MB/Sec*, where *1 MB* = 1,000,000 *Bytes/sec*. A note: the Crypto++ library [Crypto++ (2013)] uses *MiB* (Mebibyte) unit to measure cipher performance, where 1 *MiB* = 2^20 = 1024x1024=1,048, 576 bytes; as a result, a correction factor of 1.048576 has been used for Crypto++ library data to present it in column # 11 in Table 3;
- *CYCLES*: number of clock cycles needed to encrypt one byte of RMM test data (in *1/Byte*);
- *MEDIAN*: median values of corresponding calculated parameters.

4. Research outcomes

A summary of obtained values of the *PERF* parameter for selected ciphers in the EAX mode on technical platform TP1 (with Windows OS and CPU in 1Proc mode) for RMM test data sets of significantly different sizes is presented on Fig. 4.

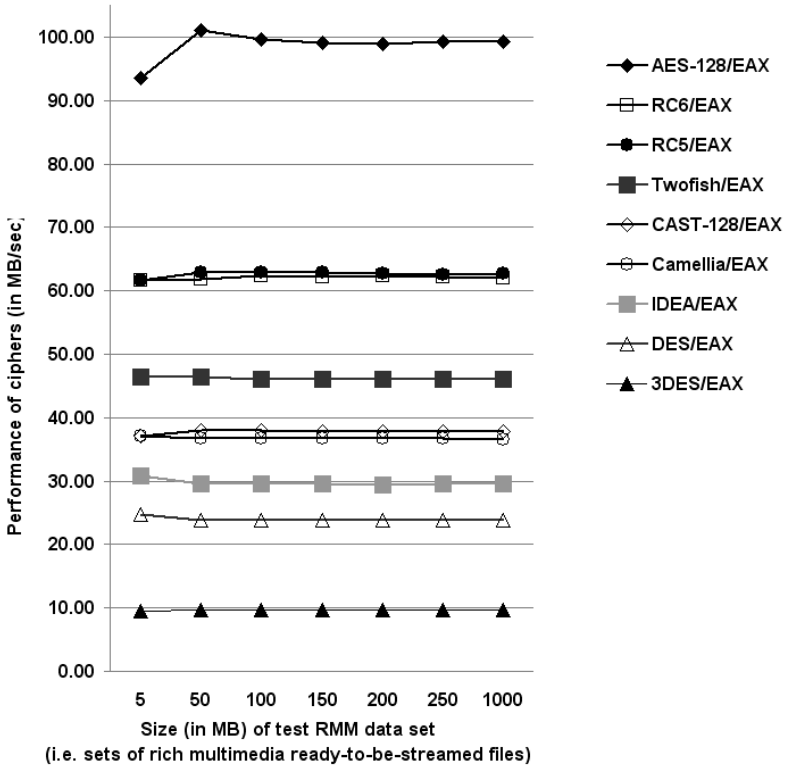

Fig. 4. A summary of cipher efficiency on TP1 technical platform (with Windows OS and in single processor 1Proc mode of CPU operation) in the EAX mode for various RMM data sets: *PERF* parameter

A summary of obtained research outcomes (i.e. calculated values of parameters *PERF* and *CYCLES*) regarding the efficiency of various ciphers in the EAX mode on technical platforms TP1, TP2 and TP3 is presented in Table 3. The median values of calculated parameters *PERF* and *CYCLES* for designated ciphers on technical platforms TP1 and TP2 with Windows and Linux operating systems (OS) in both single processor 1Proc and multi processor MProc modes of CPU operation are given in columns 3-10 in Table 3; the corresponding detailed obtained data are available in Tables 4-11 accordingly. Column # 11 in Table 3 represents the only data available for the EAX mode in Crypto++ library [Crypto++ (2013)].

Table 3. A summary of cipher efficiency in the EAX mode on technical platforms TP1, TP2 and TP3 (a note: only *MEDIAN* values are used in Table 3 in columns 4-11; detailed data for those columns are available in Tables 4-11 below)

		TP1 (powerful Dell laptop)				**TP2 (generic Asus netbook)**				**TP3**
		Windows OS		**Linux OS**		**Windows OS**		**Linux OS**		**Win/ Linux**
Cipher -mode	*Calcula-ted para-meter*	*Modes of CPU operation*								
		1 Proc (table 4)	*M Proc* (table 5)	*1 Proc* (table 6)	*M Proc* (table 7)	*1 Proc* (table 8)	*M Proc* (table 9)	*1 Proc* (table 10)	*M Proc* (table 11)	*1 Proc*
1	2	3	4	5	6	7	8	9	10	11
AES-EAX	*PERF*	98.67	98.28	81.44	81.68	11.61	9.058	13.49	13.56	63.92/ 88.03
	CYCLES	59.71	25.45	30.69	30.60	196.7	383.5	123.1	122.3	27.48/ 23.66
RC6-EAX	*PERF*	62.09	62.32	51.17	51.37	15.09	15.23	20.32	20.42	
	CYCLES	40.26	40.11	48.86	48.66	170.5	176.9	81.84	81.37	
RC5-EAX	*PERF*	62.63	62.81	60.31	59.41	16.83	12.80	25.27	25.80	
	CYCLES	39.91	39.80	41.48	42.07	161.6	338.8	65.87	64.41	
Two-fish-EAX	*PERF*	46.13	46.27	45.26	44.88	10.11	4.347	14.94	14.82	
	CYCLES	54.18	54.02	55.27	55.69	212.8	460.1	111.1	112.0	
CAST-EAX	*PERF*	37.73	38.34	31.42	31.51	10.40	5.769	16.81	16.84	
	CYCLES	66.25	65.24	79.56	79.34	209.5	337.7	98.82	98.61	
Camel-lia-EAX	*PERF*	36.72	36.74	35.69	35.84	9.226	9.305	14.06	14.16	
	CYCLES	68.06	68.04	70.03	69.74	225.9	231.2	118.1	117.2	
IDEA-EAX	*PERF*	29.69	29.72	24.90	25.02	7.155	6.379	9.203	9.261	
	CYCLES	84.20	84.11	100.3	99.89	270.8	331.9	180.4	179.2	
DES-EAX	*PERF*	23.99	24.03	19.52	19.52	5.502	5.351	8.183	8.214	
	CYCLES	104.1	104.0	128.0	128.0	348.3	403.5	202.8	202.1	
3DES-EAX	*PERF*	9.615	9.667	7.355	7.355	2.188	2.224	3.106	3.097	
	CYCLES	260.0	258.6	339.9	339.9	770.8	760.2	534.4	535.9	

Table 4. Ciphers' efficiency in the EAX mode on technical platform TP1 with a) Windows OS, and b) CPU in single processor (1Proc) mode.
(A note: *TIME* calculated parameter is in *Sec*, and *PERF* - in *MB/Sec* units below).

Technical platform: TP1 (Dell laptop) ; OS – Windows XP; CPU mode - 1Proc; cipher mode - EAX								
1	2	3	4	5	6	7	8	9
Test RMM data set	**5MB**	**50 MB**	**100 MB**	**150 MB**	**200 MB**	**250 MB**	**1000 MB**	***MEDIAN***
Cipher / calculated parameter	Mean values of calculated parameters *TIME*, *PERF*, and *CYCLES* (based on at least 3 tests to calculate each mean value below) for each test RMM data set are available in columns ## 2-8, and the final *MEDIAN* values for all test RMM data sets are available in column # 9.							
AES-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.062	0.516	1.047	1.578	2.109	2.625	10.5	
PERF	9.355	101.020	99.573	99.100	98.865	99.288	99.288	98.669
CYCLES	267.244	24.748	25.107	25.227	25.287	25.179	25.179	59.710
RC6-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.094	0.844	1.672	2.516	3.343	4.187	16.797	
PERF	61.701	61.761	62.352	62.154	62.371	62.248	62.066	62.093
CYCLES	40.518	40.479	40.095	40.223	40.083	40.162	40.279	40.263
RC5-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.094	0.828	1.657	2.484	3.328	4.172	16.61	
PERF	61.701	62.955	62.917	62.955	62.652	62.472	62.765	62.631

CYCLES	40.518	39.711	39.735	39.711	39.903	40.018	39.831	39.918
TwoFish-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.125	1.125	2.265	3.391	4.531	5.656	22.671	
PERF	46.399	46.335	46.028	46.116	46.018	46.081	45.985	46.137
CYCLES	53.880	53.955	54.315	54.211	54.327	54.253	54.365	54.187
CAST-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.156	1.375	2.75	4.14	5.516	6.891	27.625	
PERF	37.179	37.910	37.910	37.773	37.800	37.822	37.739	37.733
CYCLES	67.242	65.945	65.945	66.185	66.137	66.099	66.245	66.257
Camellia-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.156	1.422	2.844	4.266	5.688	7.11	28.453	
PERF	37.179	36.657	36.657	36.657	36.657	36.657	36.640	36.729
CYCLES	67.242	68.200	68.200	68.200	68.200	68.200	68.231	68.067
IDEA-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.188	1.766	3.531	5.297	7.078	8.828	35.359	
PERF	30.851	29.517	29.525	29.522	29.458	29.523	29.484	29.697
CYCLES	81.035	84.698	84.674	84.682	84.866	84.679	84.791	84.204
DES-EAX (fixed-size block of data = 8 bytes, size of secret key = 8 bytes)								
TIME	0.235	2.187	4.359	6.547	8.719	10.922	43.656	
PERF	24.681	23.835	23.917	23.886	23.914	23.863	23.881	23.996
CYCLES	101.294	104.889	104.530	104.665	104.542	104.765	104.688	104.196
DES/EDE3-EAX (fixed-size block of data = 8 bytes, size of secret key = 24 bytes)								
TIME	0.61	5.406	10.813	16.234	21.672	27.063	108.265	
PERF	9.508	9.642	9.641	9.633	9.621	9.631	9.629	9.615
CYCLES	262.934	259.274	259.298	259.529	259.849	259.590	259.621	260.014

Table 5. Ciphers' efficiency in the EAX mode on technical platform TP1 with a) Windows OS, and b) CPU in multi processor (MProc) mode.
(A note: *TIME* calculated parameter is in *Sec*, and *PERF* - in *MB/Sec* units below).

Technical platform: TP1 (Dell laptop) ; OS – Windows XP; CPU mode - MProc; cipher mode - EAX								
1	2	3	4	5	6	7	8	9
Test RMM data set	**5MB**	**50 MB**	**100 MB**	**150 MB**	**200 MB**	**250 MB**	**1000 MB**	***MEDIAN***
Cipher / calculated parameter	Mean values of calculated parameters *TIME, PERF*, and *CYCLES* (based on at least 3 tests to calculate each mean value below) for each test RMM data set are available in columns ## 2-8, and the final *MEDIAN* values for all test RMM data sets are available in column # 9.							
AES-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.063	0.531	1.047	1.563	2.094	2.625	10.501	
PERF	92.062	98.167	99.573	100.051	99.573	99.288	99.279	98.285
CYCLES	27.155	25.467	25.107	24.987	25.107	25.179	25.182	25.455
RC6-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.094	0.829	1.672	2.501	3.344	4.187	16.75	
PERF	61.701	62.879	62.352	62.527	62.352	62.248	62.240	62.329
CYCLES	40.518	39.759	40.095	39.983	40.095	40.162	40.167	40.111
RC5-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.093	0.828	1.656	2.484	3.328	4.141	16.578	
PERF	62.365	62.955	62.955	62.955	62.652	62.939	62.886	62.815
CYCLES	40.087	39.711	39.711	39.711	39.903	39.721	39.754	39.800
TwoFish-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.125	1.125	2.25	3.375	4.516	5.641	22.578	
PERF	46.399	46.335	46.335	46.335	46.170	46.203	46.175	46.279
CYCLES	53.880	53.955	53.955	53.955	54.147	54.109	54.142	54.021
CAST-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.141	1.375	2.75	4.125	5.5	6.891	27.547	
PERF	41.134	37.910	37.910	37.910	37.910	37.822	37.845	38.349
CYCLES	60.777	65.945	65.945	65.945	65.945	66.099	66.058	65.245
Camellia-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								

TIME	0.156	1.422	2.844	4.281	5.672	7.093	28.422	
PERF	37.179	36.657	36.657	36.529	36.761	36.745	36.680	36.744
CYCLES	67.242	68.200	68.200	68.439	68.008	68.037	68.156	68.040
IDEA-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.188	1.766	3.531	5.297	7.063	8.812	35.235	
PERF	30.851	29.517	29.525	29.522	29.521	29.577	29.588	29.729
CYCLES	81.035	84.698	84.674	84.682	84.686	84.525	84.494	84.114
DES-EAX (fixed-size block of data = 8 bytes, size of secret key = 8 bytes)								
TIME	0.234	2.187	4.359	6.531	8.719	10.89	43.579	
PERF	24.786	23.835	23.917	23.944	23.914	23.933	23.923	24.036
CYCLES	100.863	104.889	104.530	104.410	104.542	104.458	104.503	104.028
DES/EDE3-EAX (fixed-size block of data = 8 bytes, size of secret key = 24 bytes)								
TIME	0.594	5.406	10.797	16.203	21.594	27.001	108.031	
PERF	9.764	9.642	9.656	9.651	9.656	9.653	9.650	9.667
CYCLES	256.037	259.274	258.914	259.034	258.914	258.995	259.060	258.604

Table 6. Ciphers' efficiency in the EAX mode on technical platform TP1 with a) Linux OS, and b) CPU in single processor (1Proc) mode.
(A note: *TIME* calculated parameter is in *Sec*, and *PERF* - in *MB/Sec* units below).

Technical platform: TP1 (Dell laptop) ; OS – Linux; CPU mode - 1Proc; cipher mode - EAX								
1	2	3	4	5	6	7	8	9
Test RMM data set	**5MB**	**50 MB**	**100 MB**	**150 MB**	**200 MB**	**250 MB**	**1000 MB**	***MEDIAN***
Cipher / calculated parameter	Mean values of calculated parameters *TIME*, *PERF*, and *CYCLES* (based on at least 3 tests to calculate each mean value below) for each test RMM data set are available in columns ## 2-8, and the final *MEDIAN* values for all test RMM data sets are available in column # 9.							
AES-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.07	0.64	1.29	1.92	2.57	3.21	12.84	
PERF	82.856	81.448	80.816	81.448	81.131	81.194	81.194	81.441
CYCLES	30.173	30.695	30.934	30.695	30.815	30.791	30.791	30.699
RC6-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.11	1.03	2.05	3.07	4.09	5.11	20.41	
PERF	52.727	50.608	50.855	50.938	50.979	51.004	51.079	51.170
CYCLES	47.414	49.399	49.159	49.079	49.039	49.015	48.944	48.864
RC5-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.09	0.87	1.75	2.63	3.5	4.37	17.5	
PERF	64.444	59.915	59.573	59.460	59.573	59.641	59.573	60.311
CYCLES	38.794	41.725	41.965	42.045	41.965	41.917	41.965	41.482
TwoFish-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.12	1.17	2.33	3.49	4.66	5.81	23.28	
PERF	48.333	44.552	44.744	44.808	44.744	44.859	44.782	45.260
CYCLES	51.725	56.114	55.874	55.794	55.874	55.730	55.826	55.276
CAST-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.18	1.67	3.33	4.99	6.66	8.33	33.3	
PERF	32.222	31.213	31.307	31.339	31.307	31.288	31.307	31.426
CYCLES	77.587	80.094	79.854	79.774	79.854	79.902	79.854	79.560
Camellia-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.16	1.46	2.92	4.38	5.87	7.34	29.36	
PERF	36.250	35.703	35.703	35.703	35.521	35.508	35.508	35.699
CYCLES	68.966	70.022	70.022	70.022	70.382	70.406	70.406	70.032
IDEA-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.23	2.1	4.19	6.29	8.38	10.49	41.98	
PERF	25.217	24.822	24.881	24.862	24.881	24.846	24.834	24.906
CYCLES	99.139	100.717	100.477	100.557	100.477	100.621	100.669	100.379
DES-EAX (fixed-size block of data = 8 bytes, size of secret key = 8 bytes)								
TIME	0.29	2.68	5.37	8.04	10.72	13.4	53.62	

PERF	20.000	19.450	19.414	19.450	19.450	19.450	19.443	19.522
CYCLES	125.001	128.534	128.773	128.534	128.534	128.534	128.582	128.070
DES/EDE3-EAX (fixed-size block of data = 8 bytes, size of secret key = 24 bytes)								
TIME	0.77	7.12	14.23	21.34	28.46	35.58	142.25	
PERF	7.532	7.321	7.326	7.328	7.326	7.325	7.329	7.355
CYCLES	331.900	341.478	341.238	341.158	341.238	341.286	341.118	339.916

Table 7. Ciphers' efficiency in the EAX mode on technical platform TP1 with a) Linux OS, and b) CPU in multi processor (MProc) mode.
(A note: *TIME* calculated parameter is in *Sec*, and *PERF* - in *MB/Sec* units below).

Technical platform: TP1 (Dell laptop) ; OS – Linux; CPU mode - MProc; cipher mode - EAX								
1	2	3	4	5	6	7	8	9
Test RMM data set	**5MB**	**50 MB**	**100 MB**	**150 MB**	**200 MB**	**250 MB**	**1000 MB**	***MEDIAN***
Cipher / calculated parameter	Mean values of calculated parameters *TIME*, *PERF*, and *CYCLES* (based on at least 3 tests to calculate each mean value below) for each test RMM data set are available in columns ## 2-8, and the final *MEDIAN* values for all test RMM data sets are available in column # 9.							
AES-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.07	0.64	1.28	1.92	2.56	3.19	12.8	
PERF	82.856	81.448	81.448	81.448	81.448	81.703	81.448	81.685
CYCLES	30.173	30.695	30.695	30.695	30.695	30.599	30.695	30.606
RC6-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.11	1.02	2.04	3.05	4.07	5.11	20.37	
PERF	52.727	51.104	51.104	51.272	51.230	51.004	51.180	51.374
CYCLES	47.414	48.920	48.920	48.760	48.800	49.015	48.848	48.668
RC5-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.1	0.88	1.74	2.62	3.5	4.36	17.45	
PERF	57.999	59.235	59.915	59.687	59.573	59.778	59.744	59.419
CYCLES	43.104	42.205	41.725	41.885	41.965	41.821	41.845	42.079
TwoFish-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.13	1.16	2.33	3.48	4.63	5.8	23.17	
PERF	44.615	44.937	44.744	44.937	45.034	44.937	44.995	44.885
CYCLES	56.035	55.634	55.874	55.634	55.514	55.634	55.562	55.698
CAST-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.18	1.66	3.32	4.99	6.63	8.31	33.21	
PERF	32.222	31.401	31.401	31.339	31.449	31.364	31.392	31.510
CYCLES	77.587	79.614	79.614	79.774	79.494	79.710	79.638	79.347
Camellia-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.16	1.46	2.91	4.37	5.83	7.28	29.14	
PERF	36.250	35.703	35.826	35.785	35.764	35.801	35.777	35.844
CYCLES	68.966	70.022	69.782	69.862	69.902	69.830	69.878	69.749
IDEA-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.23	2.09	4.17	6.25	8.35	10.42	41.67	
PERF	25.217	24.941	25.001	25.021	24.971	25.013	25.019	25.026
CYCLES	99.139	100.237	99.997	99.917	100.117	99.949	99.925	99.898
DES-EAX (fixed-size block of data = 8 bytes, size of secret key = 8 bytes)								
TIME	0.29	2.67	5.34	8.2	10.68	13.37	53.42	
PERF	20.000	19.523	19.523	19.071	19.523	19.494	19.516	19.521
CYCLES	125.001	128.054	128.054	131.092	128.054	128.246	128.102	128.086
DES/EDE3-EAX (fixed-size block of data = 8 bytes, size of secret key = 24 bytes)								
TIME	0.78	7.14	14.18	21.28	28.38	35.46	141.86	
PERF	7.436	7.301	7.352	7.349	7.347	7.350	7.349	7.355
CYCLES	336.211	342.437	340.039	340.199	340.279	340.135	340.183	339.926

Table 8. Ciphers' efficiency in the EAX mode on technical platform TP2 with a) Windows OS, and b) CPU in single processor (1Proc) mode.
(A note: *TIME* calculated parameter is in *Sec*, and *PERF* - in *MB/Sec* units below).

Technical platform: TP2 (Asus netbook) ; OS – Windows XP; CPU mode - 1Proc; cipher mode - EAX								
1	2	3	4	5	6	7	8	9
Test RMM data set	**5MB**	**50 MB**	**100 MB**	**150 MB**	**200 MB**	**250 MB**	**1000 MB**	***MEDIAN***
Cipher / calculated parameter	Mean values of calculated parameters *TIME*, *PERF*, and *CYCLES* (based on at least 3 tests to calculate each mean value below) for each test RMM data set are available in columns ## 2-8, and the final *MEDIAN* values for all test RMM data sets are available in column # 9.							
AES-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.422	3.968	8.125	11.9	15.89	20.672	387.235	
PERF	13.744	13.137	12.831	13.141	13.122	12.608	2.692	11.611
CYCLES	120.781	126.364	129.373	126.321	126.507	131.663	616.588	196.799
RC6-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.328	3.047	6.109	9.157	12.203	15.407	385.141	
PERF	17.683	17.107	17.065	17.078	17.086	16.916	2.707	15.092
CYCLES	93.877	97.034	97.273	97.204	97.153	98.129	613.253	170.560
RC5-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.296	2.718	5.437	8.234	10.922	13.656	384.703	
PERF	19.594	19.178	19.175	18.992	19.090	19.086	2.710	16.832
CYCLES	84.718	86.556	86.572	87.406	86.955	86.977	612.556	161.677
TwoFish-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.515	4.578	9.203	13.719	18.391	22.969	384.109	
PERF	11.262	11.386	11.328	11.399	11.337	11.347	2.714	10.111
CYCLES	147.398	145.789	146.538	145.630	146.418	146.293	611.610	212.811
CAST-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.485	4.484	8.953	13.453	17.953	22.375	385.906	
PERF	11.959	11.625	11.644	11.624	11.614	11.648	2.702	10.402
CYCLES	138.812	142.796	142.557	142.807	142.931	142.509	614.471	209.555
Camellia-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.547	5.141	10.14	15.203	20.266	25.329	386.56	
PERF	10.603	10.139	10.281	10.286	10.288	10.290	2.697	9.226
CYCLES	156.557	163.719	161.457	161.383	161.346	161.324	615.513	225.900
IDEA-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.687	6.313	12.609	18.969	25.266	44.032	385.828	
PERF	8.442	8.257	8.268	8.244	8.252	5.919	2.702	7.155
CYCLES	196.626	201.042	200.771	201.360	201.153	280.446	614.347	270.821
DES-EAX (fixed-size block of data = 8 bytes, size of secret key = 8 bytes)								
TIME	0.937	8.625	17.203	25.829	34.454	43.204	501.39	
PERF	6.190	6.044	6.060	6.054	6.052	6.033	2.079	5.502
CYCLES	268.179	274.669	273.920	274.180	274.303	275.172	798.355	348.397
DES/EDE3-EAX (fixed-size block of data = 8 bytes, size of secret key = 24 bytes)								
TIME	2.516	22.782	45.703	68.843	91.125	113.89	653.61	
PERF	2.305	2.288	2.281	2.272	2.288	2.288	1.595	2.188
CYCLES	720.104	725.508	727.721	730.784	725.484	725.380	1040.73	770.816

Table 9. Ciphers' efficiency in the EAX mode on technical platform TP2 with a) Windows OS, and b) CPU in multi processor (MProc) mode.
(A note: *TIME* calculated parameter is in *Sec*, and *PERF* - in *MB/Sec* units below).

Technical platform: TP2 (Asus netbook) ; OS – Windows XP; CPU mode - MProc; cipher mode - EAX								
1	2	3	4	5	6	7	8	9
Test RMM data set	**5MB**	**50 MB**	**100 MB**	**150 MB**	**200 MB**	**250 MB**	**1000 MB**	***MEDIAN***
Cipher /	Mean values of calculated parameters *TIME*, *PERF*, and *CYCLES* (based on at least 3 tests to							

calculated parameter	calculate each mean value below) for each test RMM data set are available in columns ## 2-8, and the final *MEDIAN* values for all test RMM data sets are available in column # 9.							
AES-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.422	3.922	7.829	11.703	35.141	191.296	434.484	
PERF	13.744	13.291	13.316	13.362	5.933	1.362	2.399	9.058
CYCLES	120.781	124.899	124.660	124.230	279.772	1218.38	691.821	383.507
RC6-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.328	3.016	6.015	9.062	12.062	15.079	417.234	
PERF	17.683	17.283	17.332	17.257	17.286	17.284	2.499	15.232
CYCLES	93.877	96.046	95.776	96.195	96.031	96.040	664.355	176.903
RC5-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.297	2.688	5.391	8.11	25.515	183.125	414.235	
PERF	19.528	19.392	19.338	19.282	8.172	1.423	2.517	12.808
CYCLES	85.004	85.601	85.840	86.089	203.135	1166.34	659.579	338.800
TwoFish-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	1.063	10.141	19.532	30.907	40.937	159.641	384.359	
PERF	5.456	5.140	5.338	5.060	5.093	1.633	2.712	4.347
CYCLES	304.241	322.947	311.005	328.085	325.916	1016.77	612.008	460.139
CAST-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	1.016	10.172	20.953	31.563	40.734	22.078	386.734	
PERF	5.709	5.125	4.976	4.955	5.119	11.805	2.696	5.769
CYCLES	290.789	323.934	333.631	335.048	324.300	140.618	615.790	337.730
Camellia-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.547	5.078	9.985	14.985	19.954	24.953	417.329	
PERF	10.603	10.265	10.441	10.436	10.449	10.445	2.498	9.305
CYCLES	156.557	161.712	158.989	159.069	158.862	158.929	664.506	231.232
IDEA-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	1.515	10.094	12.438	18.641	24.891	31.125	487.672	
PERF	3.828	5.164	8.382	8.389	8.377	8.374	2.138	6.379
CYCLES	433.608	321.450	198.048	197.878	198.168	198.239	776.512	331.986
DES-EAX (fixed-size block of data = 8 bytes, size of secret key = 8 bytes)								
TIME	0.922	8.468	16.969	29.797	34.016	43.046	728.312	
PERF	6.291	6.156	6.144	5.248	6.130	6.055	1.431	5.351
CYCLES	263.886	269.669	270.194	316.302	270.815	274.166	1159.67	403.530
DES/EDE3-EAX (fixed-size block of data = 8 bytes, size of secret key = 24 bytes)								
TIME	2.453	22.438	44.859	67.344	89.734	112.094	657.906	
PERF	2.364	2.323	2.324	2.322	2.324	2.325	1.585	2.224
CYCLES	702.073	714.553	714.282	714.871	714.410	713.941	1047.57	760.243

Table 10. Ciphers' efficiency in the EAX mode on technical platform TP2 with a) Linux OS, and b) CPU in single processor (1Proc) mode.
(A note: *TIME* calculated parameter is in *Sec*, and *PERF* - in *MB/Sec* units below).

Technical platform: TP2 (Asus netbook) ; OS – Linux; CPU mode - 1Proc; cipher mode - EAX								
1	2	3	4	5	6	7	8	9
Test RMM data set	**5MB**	**50 MB**	**100 MB**	**150 MB**	**200 MB**	**250 MB**	**1000 MB**	***MEDIAN***
Cipher / calculated parameter	Mean values of calculated parameters *TIME*, *PERF*, and *CYCLES* (based on at least 3 tests to calculate each mean value below) for each test RMM data set are available in columns ## 2-8, and the final *MEDIAN* values for all test RMM data sets are available in column # 9.							
AES-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.42	3.8	7.62	11.43	15.98	19.59	79.02	
PERF	13.809	13.717	13.681	13.681	13.048	13.304	13.193	13.491
CYCLES	120.208	121.013	121.332	121.332	127.223	124.771	125.822	123.100
RC6-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.27	2.48	4.98	7.47	10.8	13.51	54.05	
PERF	21.481	21.019	20.934	20.934	19.306	19.292	19.288	20.322
CYCLES	77.277	78.977	79.296	79.296	85.983	86.047	86.063	81.848

RC5-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.22	1.98	3.94	5.89	8.88	10.95	43.58	
PERF	26.363	26.326	26.460	26.550	23.480	23.802	23.922	25.272
CYCLES	62.966	63.054	62.736	62.524	70.697	69.742	69.392	65.873
TwoFish-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.38	3.4	6.81	10.21	14.38	18.05	72.01	
PERF	15.263	15.331	15.309	15.316	14.500	14.439	14.478	14.948
CYCLES	108.760	108.275	108.434	108.381	114.485	114.963	114.660	111.137
CAST-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.33	3.04	6.07	9.11	12.84	16	64.69	
PERF	17.576	17.147	17.175	17.166	16.239	16.290	16.116	16.815
CYCLES	94.449	96.811	96.652	96.705	102.225	101.906	103.005	98.822
Camellia-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.4	3.62	7.25	10.85	15.27	19.17	77.3	
PERF	14.500	14.400	14.380	14.413	13.655	13.596	13.487	14.061
CYCLES	114.484	115.281	115.441	115.175	121.571	122.096	123.083	118.162
IDEA-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.62	5.59	11.18	16.75	23.13	28.8	115.59	
PERF	9.355	9.325	9.325	9.336	9.015	9.050	9.019	9.203
CYCLES	177.450	178.017	178.017	177.805	184.148	183.431	184.052	180.417
DES-EAX (fixed-size block of data = 8 bytes, size of secret key = 8 bytes)								
TIME	0.7	6.31	12.61	18.9	26.03	31.87	130.23	
PERF	8.286	8.261	8.267	8.274	8.010	8.178	8.005	8.183
CYCLES	200.347	200.946	200.787	200.628	207.236	202.984	207.363	202.899
DES/EDE3-EAX (fixed-size block of data = 8 bytes, size of secret key = 24 bytes)								
TIME	1.83	16.77	33.53	50.23	67.32	84.76	339.47	
PERF	3.169	3.108	3.109	3.113	3.097	3.075	3.071	3.106
CYCLES	523.764	534.052	533.892	533.202	535.962	539.848	540.532	534.465

Table 11. Ciphers' efficiency in the EAX mode on technical platform TP2 with a) Linux OS, and b) CPU in multi processor (MProc) mode.
(A note: *TIME* calculated parameter is in *Sec*, and *PERF* - in *MB/Sec* units below).

Technical platform: TP2 (Asus netbook) ; OS – Linux; CPU mode - MProc; cipher mode – EAX								
1	2	3	4	5	6	7	8	9
Test RMM data set	**5MB**	**50 MB**	**100 MB**	**150 MB**	**200 MB**	**250 MB**	**1000 MB**	***MEDIAN***
Cipher / calculated parameter	Mean values of calculated parameters *TIME*, *PERF*, and *CYCLES* (based on at least 3 tests to calculate each mean value below) for each test RMM data set are available in columns ## 2-8, and the final *MEDIAN* values for all test RMM data sets are available in column # 9.							
AES-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.42	3.8	7.61	11.46	15.26	19.72	78.84	
PERF	13.809	13.717	13.699	13.646	13.664	13.217	13.223	13.568
CYCLES	120.208	121.013	121.173	121.650	121.491	125.599	125.536	122.382
RC6-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.27	2.51	5.02	7.6	10.73	12.71	53.66	
PERF	21.481	20.767	20.767	20.576	19.432	20.506	19.428	20.423
CYCLES	77.277	79.933	79.933	80.676	85.426	80.952	85.442	81.377
RC5-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.22	1.97	3.95	5.93	7.92	10.56	43.37	
PERF	26.363	26.460	26.393	26.371	26.326	24.681	24.038	25.805
CYCLES	62.966	62.736	62.895	62.948	63.054	67.258	69.057	64.416
TwoFish-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.38	3.42	6.94	10.43	14.35	17.92	73.5	
PERF	15.263	15.242	15.022	14.993	14.530	14.544	14.184	14.825
CYCLES	108.760	108.912	110.504	110.717	114.246	114.135	117.033	112.044
CAST-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								

TIME	0.34	3.04	6.1	9.15	12.21	16.05	64.36	
PERF	17.059	17.147	17.091	17.091	17.077	16.239	16.198	16.843
CYCLES	97.311	96.811	97.129	97.129	97.209	102.225	102.479	98.613
Camellia-EAX (fixed-size block of data = 16 bytes, size of secret key = 16 bytes)								
TIME	0.4	3.64	7.26	10.9	14.58	19.06	76.45	
PERF	14.500	14.320	14.360	14.347	14.301	13.674	13.637	14.163
CYCLES	114.484	115.918	115.600	115.706	116.077	121.396	121.730	117.273
IDEA-EAX (fixed-size block of data = 8 bytes, size of secret key = 16 bytes)								
TIME	0.61	5.6	11.21	16.8	22.43	28.62	115.8	
PERF	9.508	9.308	9.300	9.308	9.296	9.107	9.003	9.261
CYCLES	174.588	178.336	178.495	178.336	178.575	182.285	184.386	179.286
DES-EAX (fixed-size block of data = 8 bytes, size of secret key = 8 bytes)								
TIME	0.69	6.31	12.64	18.97	25.26	32.36	129.8	
PERF	8.406	8.261	8.248	8.244	8.254	8.054	8.032	8.214
CYCLES	197.485	200.946	201.265	201.371	201.105	206.105	206.678	202.136
DES/EDE3-EAX (fixed-size block of data = 8 bytes, size of secret key = 24 bytes)								
TIME	1.84	16.8	33.61	50.42	67.56	84.92	339.84	
PERF	3.152	3.103	3.102	3.102	3.086	3.069	3.068	3.097
CYCLES	526.627	535.007	535.166	535.219	537.873	540.867	541.121	535.983

5. Conclusions and recommendations.

The obtained research outcomes enable us to make the following conclusions regarding the efficiency of encryption algorithms in the EAX in terms of encryption of RMM data through real-world IPsec-based MVPN environment:

(1) The AES-128 cipher in EAX mode demonstrated the best overall median (i.e. based on encryption of RMM test data sets of all sizes) performance on technical platform TP1 (i.e. powerful Dell laptop) with both Windows and Linux OS in both single processor 1Proc and multi processor MProc modes of CPU operation (Table 3, columns ## 3-6). The second best ciphers on TP1 platform are RC6 and RC5 ciphers; they demonstrated on average about 38% lower performance than AES-128 cipher in EAX mode.

(2) The RC5 and RC6 ciphers [RSA Security (2005)] in EAX mode demonstrated the best overall median (i.e. based on encryption of RMM files of all sizes) performance on technical platform TP2 (i.e. generic Asus netbook) with both Windows and Linux OS in both single processor 1Proc and multi processor MProc modes of CPU operation (Table 3, columns ## 7-10). The second best ciphers on TP2 are TwoFish and AES-128 ciphers; they demonstrated about 33% (on average) lower performance with Windows OS, and about 47% with Linux OS in comparison with performance of RC6 and RC5 ciphers.

(3) The AES-128 cipher in EAX mode demonstrated on average almost 10 times better performance on TP1 platform rather than on TP2 platform with Windows OS, and about 6 times – with Linux OS (Table 3, data in columns ## 3-10 for the AES-128 cipher).

(4) No significant difference in cipher performances in EAX modes on TP1 or TP2 in 1Proc and MProc modes of CPU operation has been observed (Table 3).

(5) The AES-128 cipher has better cryptographic features than RC6, RC5 or TwoFish ciphers [Nechvatal J. et al. (2000)]. It also demonstrated best performance on

technical platform TP1 and third best performance - on TP2. As a result, it can be recommended for users who need the highest level of cipher efficiency in MVPNs.

Furthermore, a comparative analysis of obtained results (Tables 3-11) and relevant research outcomes about efficiency of the AES cipher in CBC mode [Uskov (2013)] and CTR mode [Uskov (2012)] enables us to make the following additional conclusions:

(6) As expected, the obtained performance of ciphers in 2-phase EAX mode is about twice lower than in 1-phase CTR mode. This is because the EAX mode builds on use of both CTR and OMAC modes (Fig. 2). However, the EAX mode provides data confidentiality, integrity and authenticity in a single cryptographic scheme – this is a crucial feature of cipher efficiency in case of required highly secure transfer of private or strictly confidential data through the MPVN.

(7) The AES-128 cipher in CTR mode provides a satisfactory level of confidentiality and the highest level of performance.

Based on performed research and obtained data, our final recommendations are as follows:

(1) for mobile users who require the highest possible level of security (including data confidentiality, integrity and authenticity) to transfer confidential data through IPsec-based MVPN we strongly recommend to use the AES-128 cipher in the EAX mode;

(2) for mobile users who require satisfactory level of security and highest level of performance we strongly recommend to use the AES-128 cipher in CTR mode.

6. Acknowledgements

The author would like to thank the Office of the Provost and Vice President for Academic Affairs at Bradley University for awarding him with the Caterpillar Fellowship grants in 2011-2014 to perform research on effective IPsec-based VPN.

The author also would like to thank Dr. Steven Dolins, Chair of the Department of Computer Science and Information Systems at Bradley University for providing the author with release time in 2012-2013 to complete the described research project on efficiency of ciphers in EAX mode in IPsec-based MVPN.

References

B'Far, R. (2005). *Mobile Computing Principles,* Cambridge University Press, Cambridge, UK.

Bellare, M., Rogaway, P., Wagner, D. (2004). The EAX Mode of Operation. In Lecture Notes in Computer Science, Volume 3017/2004, 389-407, DOI: 10.1007/978-3-540-25937-4-25.

Bergman, N., Stanfield, M., Rouse, J., Scambray, J. (2013). *Hacking Exposed: Mobile Security Secrets and Solutions,* McGraw-Hill, USA.

Bernstein, D. (2013). Failures of secret-key cryptography, available at http://cr.yp.to/talks/2013.03.12/slides.pdf

Bollapragada, V., Khalid, M., Wainner, S. (2005). *IPSec VPN Design*. Cisco Press, Indianapolis, IN, USA.

Carmouche, J. (2007). *IPsec Virtual Private Network Fundamentals*, Cisco Press, Indianapolis, IN.

CISCO (2014). Cisco 2014 Annual Security Report, available at http://www.cisco.com

Crypto++ (2013). Crypto++ 5.6.0. benchmarks, available at http://www.cryptopp.com/

Dworkin, M. (2001). Recommendations for Block Cipher Modes of Operation, National Institute of Standards and Technology, USA, available at http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

Frankel, S. et al. (2005). Guide to IPsec VPNs: Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology, USA, available at http://csrc.nist.gov/ publications/nistpubs/ 800-77/sp800-77.pdf

Ibrahim, I.K. (2009). *Handbook of Research on Mobile Multimedia*, 2nd ed., Information Science Reference, Hershey, PA, USA.

IEEE P1619/D16 (2007), available at http://grouper.ieee.org/groups/1619/email/pdf00086.pdf

Kaufman, C. (2005). RFC 4306 "Internet Key Exchange (IKEv2) Protocol", available at https://tools.ietf.org/html/rfc4306

Kent, S., K. Seo, K. (2005). RFC 4301 "Security Architecture for the Internet Protocol", available at http://www.ietf.org/rfc/rfc4301.txt

Kent, S. (2005a). RFC 4302 "IP Authentication Header", available at https://tools.ietf.org/html/rfc4302

Kent, S. (2005b). RFC 4303 "IP Encapsulating Security Payload", available at https://tools.ietf.org/html/rfc4303

Krovetz, T., Rogaway, P. (2011). The Software Performance of Authenticated-Encryption Modes, available at http://www.cs.ucdavis.edu/~rogaway/ papers/ae.pdf

Lewis, M. (2006). *Comparing, Designing, and Deploying VPNs*. Cisco Press, Indianapolis, IN.

Moise, A., Beroset, E., Phinney, T., Burns, M. (2011). EAX' Cipher Mode, available at http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/eax-prime/eax-prime-spec.pdf

Mogollon, M. (2007). *Cryptography and Security Services: Mechanisms and Applications*. CyberTech Publishing, Hershey, PA, USA.

Nechvatal J., Barker E., Bassham L., Burr W., Dworkin M., Foti J., Roback E. (2000). Report on the development of the Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S.A., available at http://csrc.nist.gov/archive/ aes/round2/r2report.pdf

NIST (2013). Modes Development, National Institute of Standards and Technology, USA, available at http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html

Ponemon Institute (2013). 2014 State of Endpoint Risk, Ponemon Institute, available at https://www.lumension.com/Lumension/media/graphics/Resources/2014-state-of-the-endpoint/2014-State-of-the-Endpoint-Whitepaper-Lumension.pdf

RSA Security (2005). RSA Security LLC, available at www.rsasecurity.com

Shneyderman, A. , Casati, A. (2002). *Mobile VPN: Delivering Advanced Services in Next Generation Wireless Systems.* Wiley, Indianapolis, IN, USA.

Symantec (2014). Internet Security Threat Report, available at http://www.symantec. com

Uskov, V., Uskov, A. (2004). Blending Streaming Multimedia and Communication Technology in Advanced Web-Based Education, *International Journal Advanced Technology for Learning*, **1**(1) (2004), pp.54-66.

Uskov, V., Uskov, A. (2005): Streaming Media-Based Education: Outcomes and Findings of a Four-Year Research and Teaching Project, *International Journal Advanced Technology for Learning*, **2**(2), pp. 45-57.

Uskov, A. (2012). Information Security of IPsec-Based Mobile VPN: Authentication and Encryption Algorithms Performance, Proceedings of the 11th IEEE international conference on Trust, Security and Privacy in Computing and Communications TrustCom-2012, Liverpool, UK. pp. 1042-1048.

Uskov, A. (2013). IPsec VPN-Based Security of Web-Based Rich Multimedia Systems. Proceedings of the 6th international conference on Intelligent Interactive Multimedia Systems and Services (IIMSS-2013), June 26-28, 2013, Sesimbra, Portugal. IOS Press, ISBN 978-1-61499-261-5, pp. 31-40. DOI: 10.3233/978-1-61499-262-2-31.