An end-to-end user two-way authenticated double encrypted messaging scheme based on hybrid RSA for the future internet architectures

Aniruddha Bhattacharjya*, Xiaofeng Zhong and Jing Wang

Tsinghua National Laboratory for
Information Science and Technology,
Department of Electronic Engineering,
Tsinghua University,
Beijing, China
Email: li-an15@mails.tsinghua.edu.cn
Email: zhongxf@tsinghua.edu.cn
Email: wangj@tsinghua.edu.cn
*Corresponding author

Abstract: In future internet architectures, end-to-end (E2E) secured personal messaging is essential. So here an E2E user two-way authenticated double encrypted messaging architecture based on hybrid RSA for private messaging is proposed. Our P2P protocol works over TCP protocol for creating direct connections in between, with IPv4 broadcast options to discover peers on the same LAN. Our protocol implements perfect forward secrecy using Diffie-Hellman key exchange with renegotiation capability in every session with optimal asymmetric encryption padding and random salts. For making hybrid RSA with double encryption, in encryption level, main RSA is integrated with efficient RSA to give more statistical complexity. In the decryption process, the CRT is used for very high efficiency with integration with shared RSA. Our architecture also gives a hassle-free, secure, peer-to-peer, strong and reliable platform with E2E encryption for private messaging and it can also work with future internet architectures.

Keywords: Chinese remainder theorem; CRT; Diffie-Hellman; perfect forward secrecy; PFS; optimal asymmetric encryption padding; OAEP; shared RSA; efficient RSA; hybrid RSA.

Reference to this paper should be made as follows: Bhattacharjya, A., Zhong, X. and Wang, J. (2018) 'An end-to-end user two-way authenticated double encrypted messaging scheme based on hybrid RSA for the future internet architectures', *Int. J. Information and Computer Security*, Vol. 10, No. 1, pp.63–79.

Biographical notes: Aniruddha Bhattacharjya is with Tsinghua National Laboratory for Information Science and Technology, Department of Electronics Engineering, Tsinghua University, Beijing, China, as a Chinese Government PhD Scholar. His research interests are cryptography, network security, RFID-based architectures and middleware, security in fixed and wireless networks, applications of cryptography and IoT securities. He obtained the ICDCN 2010 PhD forum fellowship. He obtained the best paper award in ACM ICC 2016, in Cambridge University, UK. He is working as IEEE mentor

and ACM faculty sponsor since 2012. He is a member of 34 IEEE societies and various IEEE technical committees. He has published 26 papers and two US patents are pending.

Xiaofeng Zhong received his PhD in Information and Communication System from Tsinghua University in 2005. He has been an Associate Professor in the Department of Electronic Engineering of Tsinghua University. He researches in the field of mobile network, including the users' behaviours and traffic model analysis, MAC and network protocol design and resource management optimisation. He has published more than 30 papers and own seven patents.

Wang Jing received his BS and MS in Electronic Engineering from Tsinghua University, Beijing China in 1983 and 1986, respectively. He has been on the faculty at the Tsinghua University since 1986. Currently, he is a Professor of the School of Information Science and Technology. He serves as the Vice Director of Tsinghua National Lab for Information Science and Technology. His research interests are in the area of wireless communications, including transmission and networking technologies of 4G/5G. He has published more than 150 conference and journal papers.

1 Introduction

The security is fundamental for the application areas in all future internet architectures and it is conclusive that, the elementary end-to-end (E2E) security services with instance freshness of secret keys between two communicating entities, authentication and confidentiality are obligatory. Any kind of information communicated both ways in the network must be secured E2E. Modadugu and Rescorla (2004) have signposted that the use of IPSec may not be apposite in some circumstances, like, in CoAP that necessitates lightweight security. For reason of the asymmetry of the system, there are further security concerns around E2E security such as defending the constrained network from flooding and replay attacks ever since devices in the LLN have considerably less computational resources and memory when equated to internet devices. Through our scrutiny and exploration, providing E2E security is not so petty, principally due to many likely usage scenarios, i.e., CoAP/CoAP, DTLS/DTLS and HTTP/CoAP, TLS/DTLS facilitated by a 6LBR, that have dissimilar restraints and necessities. So in the scenario of personal peer to peer messaging in the future internet architectures, with existing internet architectures, we need very much strong, reliable and efficient peer-to-peer private messaging scheme. Numerous researches have been carried to offer an E2E secure communication like:

1 by use of ECC cryptography

2 by means of specific hardware

3 by using a trusted third party

4 by use of external digital certificates

5 by passwords, etc.

So in case of personal peer to peer messaging context, we have proposed an E2E user two-way authenticated double encrypted messaging architecture based on hybrid RSA for

the future internet architectures which can be incorporated in Choicenet, NEBULA, eXpressive Internet Architecture (XIA) along with sourceless network architecture, CERNET and binding of CoAP with datagram transport layer security (DTLS). RSA, which is one of the most popular asymmetric ciphers, still has weaknesses from various attacks – chosen ciphertext attacks, brute force key search, timing attacks, mathematical attacks, etc. So in our survey we found many variants of RSA (Pointcheval, 1999; Vuillaume, 2003; Boneh and Shacham, 2002; Ju et al., 2008; Hinek, 2007; Kaminaga and Yoshikawa, 2015; Pointcheval, 1999; Padhye, 2006; Aboud et al., 2008; Xiao et al., 2015), which gives better security and strong RSA for future use. Some of the variants are efficient RSA, dependent RSA, Carmichael RSA, shared RSA, multiprime RSA, common prime RSA, CRT-RSA, rebalanced CRT-RSA, etc. (Pointcheval, 1999; Vuillaume, 2003; Boneh and Shacham, 2002; Ju et al., 2008; Hinek, 2007; Kaminaga and Yoshikawa, 2015; Pointcheval, 1999; Padhye, 2006; Aboud et al., 2008; Xiao et al., 2015; Bhattacharjya et al., 2016). They can be further integrated to make hybrid RSA. Hybrid RSA can be an obligatory for E2E security, in IM cases and in communication in future internet architectures scenario.

2 Present scenarios and motivations

DTLS (Kothmayr, 2013; Rescorla and Modadugu, 2006; Fischl et al., 2010; Hartke and Tschofenig, 2014; Kothmayr et al., 2012) is in practice with TLS (Modadugu and Rescorla, 2004; Dierks and Rescorla, 2006) with added features to compact with the untrustworthy nature of UDP communications. AES/CCM is accepted as the cryptographic algorithm, to upkeep fundamental security necessities in the current CoAP (Bormann et al., 2012; Shelby et al., 2012, 2014) specification. Security against replay attacks may also be accomplished in the context of DTLS, using a dissimilar nonce value for each secured CoAP packet (Bormann et al., 2012; Shelby et al., 2012, 2014). An important feature of CoAP security using DTLS (Kothmayr, 2013; Rescorla and Modadugu, 2006; Fischl et al., 2010; Hartke and Tschofenig, 2014; Kothmayr et al., 2012) is that elliptic curve cryptography (ECC) (SECG, 2014) is accepted to provision the raw public key and certificates security modes. A standard-based security architecture with two-way authentication was projected in (Fischl et al., 2010; Seggelmann et al., 2012; Kothmayr et al., 2013). The authentication is accomplished during a fully authenticated DTLS handshake and depending on an exchange of X.509 certificates encompassing RSA keys, which they have implemented (Fischl et al., 2010; Seggelmann et al., 2012; Kothmayr et al., 2013). RSA has the multiplicative property that the encryption of the product of two plaintext messages is the identical as the product of the encryptions of two plaintext messages. That is, for plaintext messages x_1 and x_2, we have $enc_K(x_1x_2) = enc_K(x_1) * enc_K(x_2)$. This property, often named the homomorphic property of RSA, follows from the basic properties of modular multiplication. Exploiting this homomorphic property of RSA, Davida (1982) showed that main RSA is insecure against a chosen ciphertext attack. A simplification of the attack by Judy Moore is as follows – suppose an adversary is given a cipher text $c = m^e \bmod N$ and wants to compute m. Selecting a random $a \in Z_N$, the adversary asks for the plaintext of the cipher text $c_0 = ca^e \bmod N$. Since

$$\begin{aligned} m_0 &= c_0^d \bmod N \\ &= (ca^e)^d \bmod N \\ &= c^d a^{ed} \bmod N \\ &= ma \bmod N \end{aligned}$$

The adversary can simply compute $m = m_0 a^{-1} \bmod N$, to recover the desired plaintext. So protection from chosen cipher text attack is very much essential now a days. Though RSA is the most widespread public key cryptosystem, still it suffers from lots of attacks. Also RSA suffers from low modular complexity with effortlessness and speediness problem and real-time key negotiation between each peers problem and parallel protection to sniffing attacks. Also asymptotic very low speed of decryption of RSA is also very irrelevant in present and future internet scenarios; we need more and more efficient RSA schemes.

So in the past, lots of variants of RSA (Pointcheval, 1999; Vuillaume, 2003; Boneh and Shacham, 2002; Ju et al., 2008; Hinek, 2007; Kaminaga and Yoshikawa, 2015; Pointcheval, 1999; Padhye, 2006; Aboud et al., 2008; Xiao et al., 2015) were proposed, to tackle some of the attacks. So combining two or three or many of them and making a hybrid RSA system, will be a very relevant, as it can give us stronger, more reliable and more efficiency in real time scenarios, like personal peer to peer messaging in the future internet architectures like Choicenet, NEBULA, XIA (http://www.nets-fia.net/) along with sourceless network architecture (Braun and Crowcroft, 2014), CERNET and with binding of CoAP with DTLS (Pointcheval, 2013; Rescorla and Modadugu, 2006; Fischl et al., 2010; Hartke and Tschofenig, 2014; Kothmayr et al., 2012).

Now a day, we are having many IM applications and protocols, they have pitfalls also. They need either centralised security system or trusted third party or password protections or SSL-based solutions or use of some digital certificates. But we need a distributed system, replacing single point failure with own security and authentication, which is purely E2E. Also we need a system replacing backlogs of SSL/TLS without any trusted third party. We need a scheme which affords a hassle-free, secure, peer-to-peer, unconventionally strong and reliable platform with E2E-encryption, for people and organisations, who are concerned about their privacy and security, in a distributed environment, where multiple server and multiple clients can communicate in a peer to peer manner with strong, reliable and efficient E2E security.

All these factors compel us, to propose an E2E user two-way authenticated double encrypted messaging architecture based on hybrid RSA for the future internet architectures and existing architectures.

3 Design and implementation

Our scheme is a stack of three different protocol layers as shown in Figure 1. Our hybrid RSA peer-to-peer private messaging scheme is having an E2E encryption protocol, which works in connection layer. Being a peer-to-peer messaging partner, the architecture users connect to each other directly to exchange messages over an E2E encrypted channel without any centralised system of contact. It works with double authentication with perfect forward secrecy (PFS) using Diffie-Hellman (D-H). Sniffing attacks and real-time

key negotiation between each peers, is resolved by PFS using D-H in our hybrid RSA scheme.

Figure 1 Hybrid RSA messaging scheme protocol stack (see online version for colours)

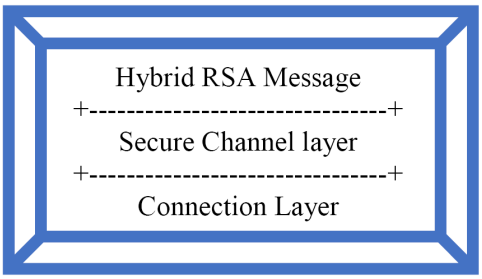
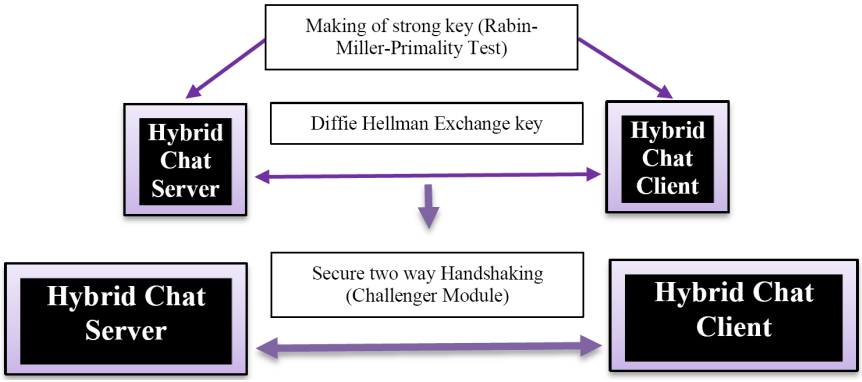


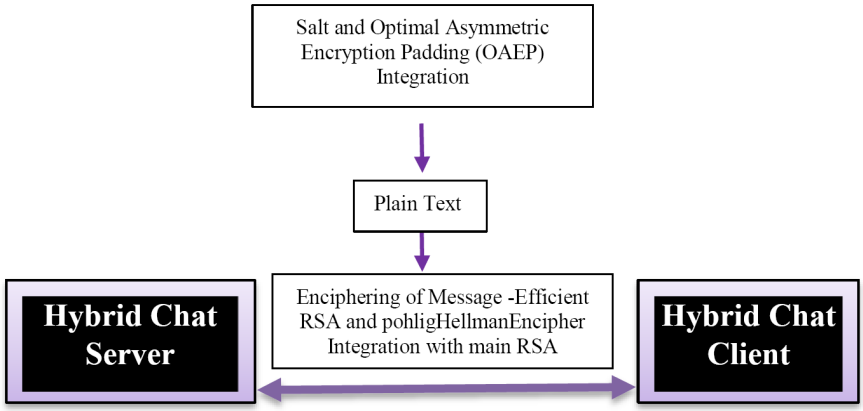
Figure 2 Making of keys and secure two-way handshaking (see online version for colours)



The connection layer is responsible for creating and receiving TCP connections from peers available in local area network (LAN). It offers TCP relay functionality. The Virtual channel in our connection layer streams, provide E2E encrypted tunnel from one peer to another for transporting secure, reliable and strong chat messages. Each chat network essentials a single secure channel stream connection for every peer in the chat group, forming a full mesh network topology. The connection-commencing peer necessitates opening a virtual data channel to our Chat network recognised by IP address used. In the E2E security scenario in future internet architecture's communication, we need to implement full mesh topology, our architecture is making it happened. Our architecture uses IPv4 broadcast options, to discover peers on the same LAN. The handshake protocol is aimed to detect replica TCP connections using peer ID that is IP address. A secure channel ensures real-time E2E encryption during hybrid RSA messaging. Then hybrid RSA layer takes responsibility of strong, efficient and reliable and hassle free secure messaging. Both peers are mandatory to exchange keys at initial stage as shown in Figure 2, to mutually authenticate each other before the secure channel starts communication. The secure channel protocol that is D-H key exchange protocol protects the keys in transit, averting identity release to passive sniffing attacks at network level. In our architecture, the protocol also offers secrete mutual peer key renegotiation capability.

In a situation if any peer try to start secure channel key exchange, every time a new secret mutual shared key will be exchanged. Renegotiation is initiated inevitably by any of the peers on the basis of reconnections. In our architecture, challenger class takes care about the peer to peer architecture and if any third peer comes for communicating messages apart from authenticated peers, it has to wait unless until the hybrid server release the first peer, but still it will be able to do the socket connection only to the RSA hybrid server. We used Rabin-Miller primality test for all of our pseudo random number, generated by pseudo random number generator to check that they are prime and not prime. We use this test as it is based on the properties of strong pseudo primes, it is very unique. These Rabin-Miller primality tested prime numbers are used in all of our cipher, where strong and big prime numbers are needed. Then we use D-H key exchange protocol to generate the common shared key, which is used like a two-way mutual authentication in our architecture and these keys are used in the later communication. After these, secure handshaking is done to initiate pure peer to peer that is E2E user personal messaging initiation. After handshaking is done, then again challenger class do the mutual authentication by exchanging the shared keys generated by D-H key exchange protocol as shown in Figure 2. For second layer authentication, we use hybrid RSA as shown in Figure 3. In our hybrid RSA as shown in Figure 3, salt and optimal asymmetric encryption padding (OAEP) integration is done with text messages before encryption process starts to battle the chosen plaintext attack.

Figure 3 Hybrid encryption process (see online version for colours)



Then actual messaging starts with hybrid encryption. We make hybrid RSA in case of encryption and decryption both. In the encryption, we first integrate main RSA with Pohlig-Hellman encipher and with efficient RSA for more and more strong and statistical complexity. In efficient RSA with Euler phi function, Euler's totient is used. The totient is denoted using the Greek symbol phi ϕ. The totient of n, $\phi(n) = (p - 1) \cdot (q - 1)$, where $n = p * q$, where p and q are two primes. Beastliness of this cipher is that the totient is the count of the number of elements that have their *gcd* with the modulus equal to 1. This expresses us to a key equation regarding the totient and prime numbers: $p \in P$, $\phi(p) = p - 1$.

In this RSA variant, the efficient RSA, definition for the Euler phi function is used as below in equation (1)

$$\phi(n, h) = \left(p^h - p^0\right)\left(p^h - p^1\right)\ldots\left(p^h - p^{h-1}\right) + \left(q^h - q^0\right)\left(q^h - q^1\right)\ldots\left(q^h - q^{h-1}\right) \quad (1)$$

where h is randomly picked among the integers mod n, ever since this function is in use only the in the key generation process and the encryption and decryption processes are identical to the original RSA, the computational rate due to encryption and decryption will not be different ominously from the original RSA. So our hybrid RSA encryption is also having the encryption complexity $(3n_e - 2)(n^2 + 2)$.

Our hybrid RSA works very effortlessly and speedily with the use of extended Euclidean algorithm in the efficient RSA. For example, if h is taken as 1, the phi function becomes like equation (2).

$$\phi(n, 1) = (p - 1) + (q - 1) \quad (2)$$

The public key e in this case should be picked in such means that $gcd(e, \phi(n, 1)) = 1$. The private key d should be ϕ selected such that $e \cdot d = 1 \bmod \phi(n, 1)$. The encryption of message M will be executed as $C = M^e \bmod n$ and the decryption of the cipher text will be executed as $M = C^d \bmod n$. This way, our hybrid encryption is stronger, reliable with double encryption with Pohlig-Hellman encipher and with efficient RSA integration with main RSA. So also for effortlessness and speediness of RSA encryption problem, we are using efficient RSA with Euler phi function with the extended Euclidean algorithm in our hybrid RSA without any extra cost, here our hybrid RSA encryption complexity is also $(3n_e - 2)(n^2 + 2)$.

In our decryption, we integrate the basic RSA scheme with the shared RSA, which is another variant of RSA. It actually uses the modulus n which is a product of two large numbers p and q. The encryption exponent e is selected in that way so that it is co-prime to n. Although the decryption is more complex and statistically problematic as there are added parties who join in this scheme. We actually adopt that there are x parties and the prime factors of n stand unidentified to all person. Each party P_i now solitary recognises the tuple $< p_i, q_i, d_i >$ and retains it furtive from other parties. Furthermore, the following four conditions in equation (3) prerequisite to be fulfilled in this cipher:

$$\begin{aligned}
&1 \quad p \text{ is a large prime number and } p = p_1 + p_2 + \ldots + p_x = \sum\nolimits_{i=1}^{x} p_i \\
&2 \quad q \text{ is a large prime number and } q = q_1 + q_2 + \ldots + q_x = \sum\nolimits_{i=1}^{x} q_i \\
&3 \quad \text{the decryption exponent } d = d_1 + d_2 + \ldots + d_x = \sum\nolimits_{i=1}^{x} d_i \\
&4 \quad ed = 1 \bmod \phi(n).
\end{aligned} \quad (3)$$

In the shared RSA, the encryption and decryption carry on as follows: the encryption is done as in the original RSA as $c = m^e \bmod n$. The decryption ensues as follows: each party with a decryption exponent d_i computes $m_i = c^{d_i} \bmod n$ and then and there bring out m_i to all other parties. For this complexity reason, it is very difficult and challenging for each party to recover d_i when it is given m_i and c. We get the plaintext as in equation (4).

$$\begin{aligned}
&m = \prod\nolimits_{i=1}^{x} m_i \\
&m_1 m_2 \ldots m_3 \equiv c^{d_1} c^{d_2} c^{d_3} \ldots c^{d_x} \bmod n \equiv c^d \bmod n
\end{aligned} \quad (4)$$

So by using the shared RSA, our hybrid RSA (integration of main RSA and the shared RSA) decryption became stronger and complex and more challenging and difficult to be broken in our architecture. So we are using shared RSA with main RSA (our new hybrid RSA) for more and more modular complexity in our proposed scheme.

The CRT-RSA is a different variant of RSA where the Chinese remainder theorem (CRT) is always in use to decrypt the RSA cipher text to the plaintext. Essentially, the decryption algorithm is deferred with TEXTBOOK RSA with the following method:

Given a cipher text $c = m^e \bmod N$, first we compute

$$c_p = c_p^d \bmod p$$

$$c_q = c_q^d \bmod q$$

where $d_p \equiv d(\bmod p - 1)$ and $d_q \equiv d(\bmod q - 1)$, then we calculate the plaintext message m using Garner's algorithm

$$m = c_q + \left(q^{-1} \bmod p\right)\left(c_p - c_q\right)q.$$

CRT is recognised to decrease the RSA computation by use of the divide-and-conquer technique. Using the condition existing in (Vuillaume, 2003; Boneh and Shacham, 2002), we guesstimate the complexity of each technique as the function of the number of operations requisite. Basic algorithms to calculate exponentiations of the form $C^d \bmod n$ take time $O(\log dM(n))$, where $M(n)$ is the cost of multiplying two n-bit integers and can be as $O(\log^2 n)$. When $d = O(n)$, all these algorithms take time $O(\log^3 n)$. On the other side, CRT RSA has $d_p = d_q = O(\sqrt{(n)})$ (so that $\log d_p = \log d_q \; \forall = O(\log (n)/2)$), for an overall cost of $O(2(\log (n)/2)^3)$. The theoretical speedup of CRT-RSA relating to plain RSA is as shown in equation (5).

$$S_{RSA} = \log^3 n \Big/ 2\left(\log (n)/2\right)^3 = 4 \tag{5}$$

We use the CRT in our hybrid RSA decryption, to get

$$m = \left(m_p q\left(q^{-1} \bmod p\right) + m_q p\left(p^{-1} \bmod q\right)\right) \bmod pq = c^d \bmod N$$

due to $m = m_p \bmod p$ and $m = m_q \bmod q$.

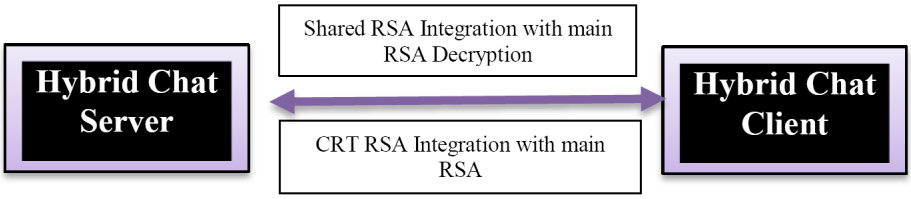
Complexity of our hybrid RSA decryption algorithm is $3n^2/4 + 7n^2/2 + O(n^2)$.

Table 1 Cost estimation comparison of RSA and hybrid RSA

Variants	*Speed-up for n = 1,024 bits*
RSA	1.0
Mpower	2.54
Mprime	1.89
Rebalanced	3.02
Rprime	3.88
Batch	2.78
Hybrid RSA decryption	3.98

The complexity of encryption algorithm is the identical to the original RSA. But the complexity of decryption is $2O(\log^3 N^{1/2}) + 4O(\log^2 N^{1/2})$. If we precalculate $p - 1 \bmod q$ and $q - 1 \bmod p$, the complexity of decryption is around $2O(\log^3 N^{1/2})$. Cost estimation comparisons of variants of RSA and our hybrid RSA scheme decryptions are here in Table 1 (where b = 4(no. of messages), k = 3 (no. of primes), s = 160 in appropriate applicability). The improvement of the hybrid RSA decryption is that it shortens the modular exponentiation executed in the decryption phases of our hybrid scheme and contributes more efficiency in our architecture. So this way our hybrid RSA decryption as shown in Figure 4 makes the decryption more and more efficient.

Figure 4 Hybrid decryption process (see online version for colours)



In chosen plaintext attack (Hinek, 2007), attack can be severe when the plaintext space is small. The attacker at first try to encrypts all plaintext messages and then by matching which of the cipher texts matches the given cipher text c, they do severe attacks and can hamper and breakdown our security. This attack cannot be effortlessly being made if the message space is very considerable. A correlated attack also called short plaintext attack can be through when the message is small even if the cipher text can be as big as n. These two attacks can be protected by integrating OAEP with our main RSA with some random salts added on runtime with synchronise time gap. So in our architecture in the hybrid encryption, we added random salts and integrate OAEP before the hybrid RSA encryption starts, to tackle the dangerous chosen cipher text attacks. These randomly added digits are removed after decryption.

So this way our E2E user two-way authenticated double encrypted messaging architecture based on hybrid RSA for the future internet architectures, is much more secure, reliable and efficient. The peer-to-peer communication nature is the basic requirements for any future and existing internet architectures messaging, so our architecture can be incorporated in any kind of personal messaging architecture.

Our architecture will work fine with Choicenet (http://www.nets-fia.net/). In Choicenet, the essential idea is to provision choice as the key concentrating aspect of the architecture and it allows user to choose their options. So in our architecture, if this hybrid server is installed in the Choicenet, so the hybrid server can chose which peer, he will talk at present and which should wait in queue, so it is like personal messaging as per choice. As our peer-to-peer protocol works over TCP protocol for creating direct connections between peers, so it will use IPv4 broadcast option to discover peers on the Choicenet architecture as per need.

The NEBULA (http://www.nets-fia.net/) gives us access to application-selectable services and network abstractions, so as it supports multipath routing, so multiple user

can use our architecture with our peer-to-peer protocol nature for their private secure, reliable and strong messaging as an application selectable service which is a basic service by NEBULA.

The XIA (http://www.nets-fia.net/) is actually reconnoitering the technical defies in creating a single network that deals inherent support for communication among current communicating principals – including hosts, content, and services – while accepting unknown future entities. So wherever human personal messaging is needed in this architecture we can use our API of hybrid RSA server and clients for peer-to-peer security and reliable communication.

For sourceless network architecture (Braun and Crowcroft, 2014), the architecture works fine with four cases:

1 IPv4 to IPv4

2 SNA to IPv4

3 IPv4 to SNA

4 SNA to SNA.

So in our case as our peer-to-peer protocol works over TCP protocol for creating direct connections between peers in IPV4, so it will use IPv4 broadcast to discover peers in SNA. It will work fine whether the case is any of the four cases as described above.

Also, we already saw in the work of Fischl et al. (2010), Seggelmann et al. (2012) and Kothmayr et al. (2013) that they carry out two-way authentication security scheme for the future internet architectures based on current internet standards, specifically the DTLS protocol. Their security scheme is based on the RSA, and workings on top of standard low power communication stacks. So our hybrid RSA scheme can also be easily incorporated in the binding of CoAP with DTLS.

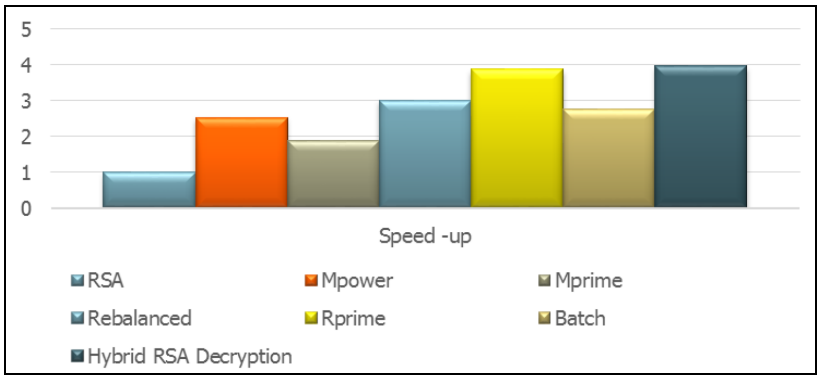
Our E2E user two-way authenticated double encrypted messaging architecture based on hybrid RSA for the future internet architectures has been implemented in Java. We used the NetBeans IDE 8.0.2 and Java Cryptography Extension (JCE). Prime generator class is developed with Rabin-Miller probabilistic primality test. We have used D-H key exchange protocol for generation of the common shared key from output of our Prime generator class for two-way mutual authentication in our architecture and these keys are used in the later communication. After these, secure handshaking is done to initiate pure peer to peer that is E2E user personal messaging initiation. After handshaking is done then again challenger class do the mutual authentication by exchanging the shared keys generated by D-H key exchange protocol as shown in Figure 2.

Hybrid RSA chat server and client class are designed as a main part of the architecture. Plain message as a block is fed into the hybrid RSA algorithm (consisting of efficient RSA with Euler phi function variant integration and Pohlig-Hellman encipher with salt and padding) for encryption as shown in Figure 3. This efficient RSA incorporation is constructing our architecture in such a way that, it become some more computationally difficult. Chosen plaintext attack and short plaintext attacks can be protected in our architecture by integrating OAEP with our main RSA added with some random salts on runtime in synchronise time gap in the encryption process. The salting process adds some random digits to the plaintext before encryption and the padding manner which adds some random digits to the commencement and end of the plaintext

message afore encryption starts, so a large plaintext can be made as shown in Figure 3. So in our architecture in the hybrid encryption, we added random salts and OAEP to tackle this dangerous chosen ciphertext attacks. These randomly added digits can be removed after decryption. So as a whole the Efficient RSA with Rabin-Miller strong primality test integration and Hellman encipher with salt and OAEP integration makes it strong and reliable in enciphering.

In our decryption, we integrate the main RSA scheme with the shared RSA, which makes our hybrid decryption more complex and statistically problematic. So by using the shared RSA, our hybrid RSA (integration of main RSA and the shared RSA) decryption has become stronger, more complex, more challenging and difficult to be broken. The CRT-RSA is an altered variant of RSA, where the CRT is every time in use to decrypt the RSA cipher text to the plaintext. The enhancement of the CRT-RSA is that it shortens the modular exponentiation executed in the decryption phases and contributes more efficiency in our architecture. So this way the CRT-RSA integration in our Hybrid RSA decryption, makes the decryption more and more efficient like almost four times faster than normal RSA. This efficiency of our hybrid RSA compare to other RSA variants, is very much essential for existing and future internet architectures as shown in Figure 5 (where $b = 4$ (no. of messages), $k = 3$ (no. of primes), $s = 160$ in appropriate applicability).

Figure 5 Cost estimation comparisons of variants of RSA and our hybrid RSA scheme (see online version for colours)



Some of the implementation scenarios are here:

1 our hybrid RSA three clients wants to chat with me (hybrid chat server) shown in Figure 6

2 three hybrid RSA clients are connected for messaging with me (hybrid chat server) but only one is able to start secure, reliable and efficient chat in a peer-to-peer manner and others are connected and have to wait for starting of hybrid RSA messaging as shown in Figure 7

3 now first two have closed connections after chat finished and now third one connected and starts messaging in pure peer-to-peer manner as shown in Figure 8

Figure 6 One hybrid RSA three clients wants to chat with me (hybrid chat server) (see online version for colours)

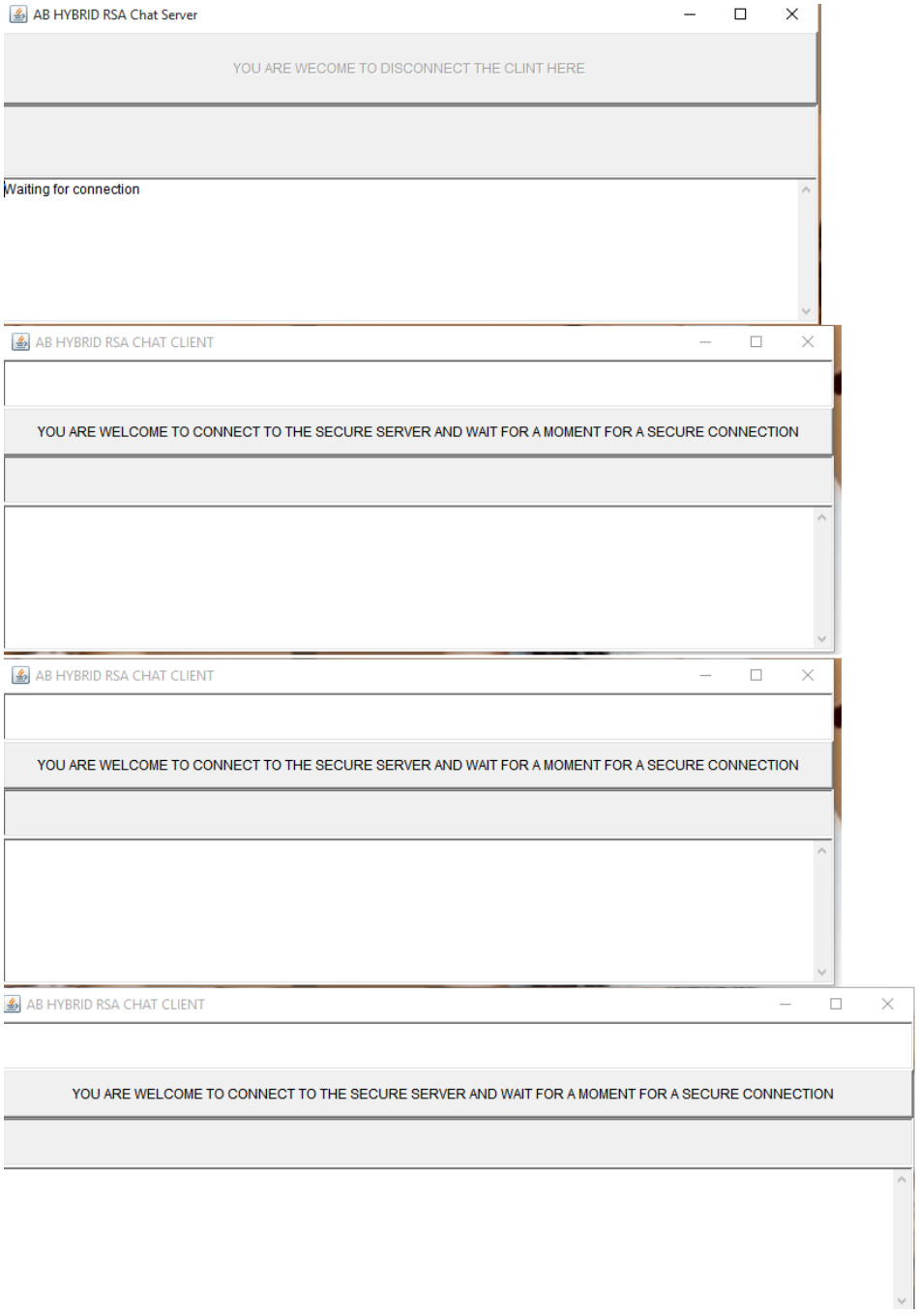


Figure 7 Three hybrid RSA clients are connected for messaging with me (hybrid chat server) but only one is able to start secure, reliable and efficient chat in a peer-to-peer manner (see online version for colours)

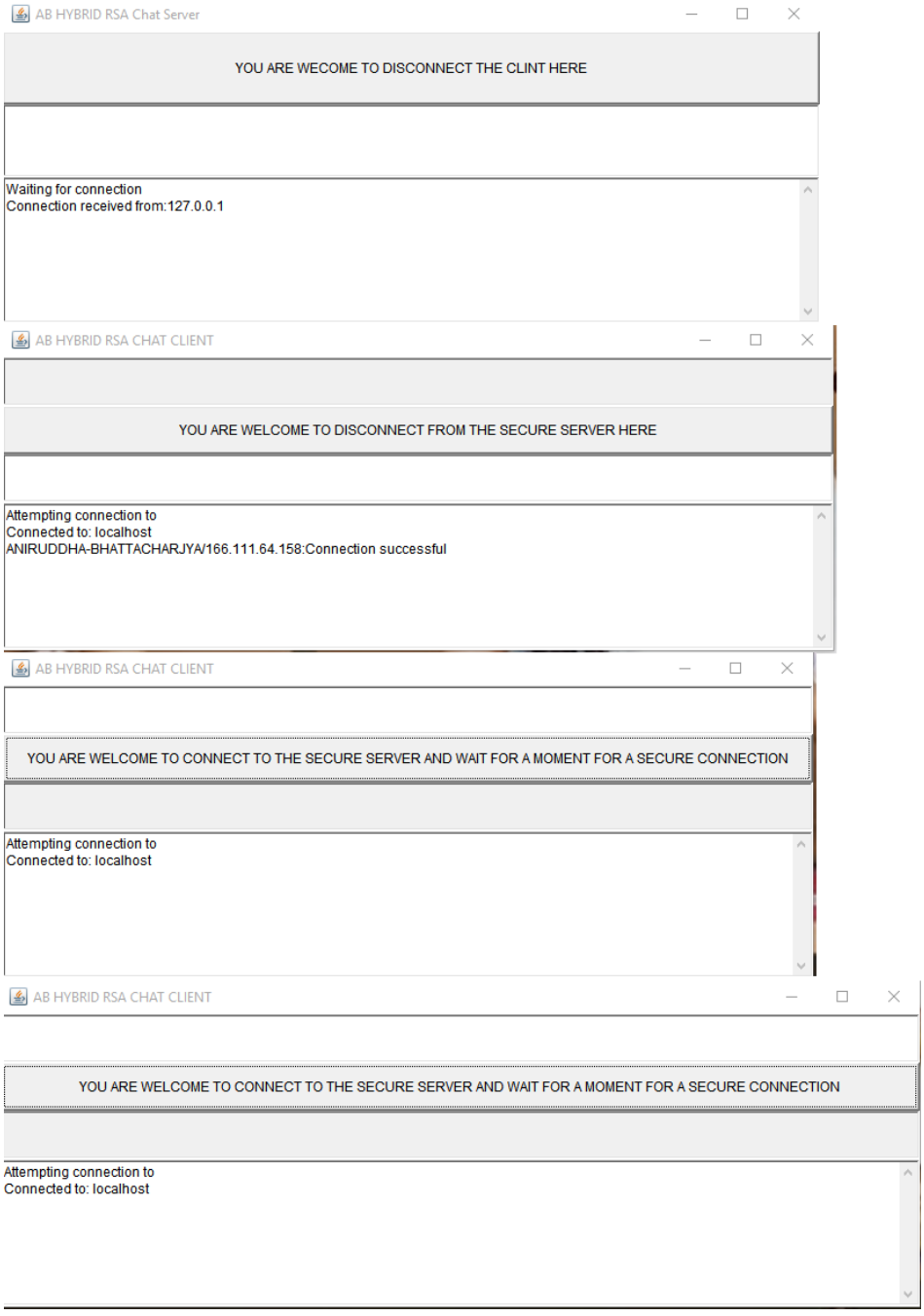
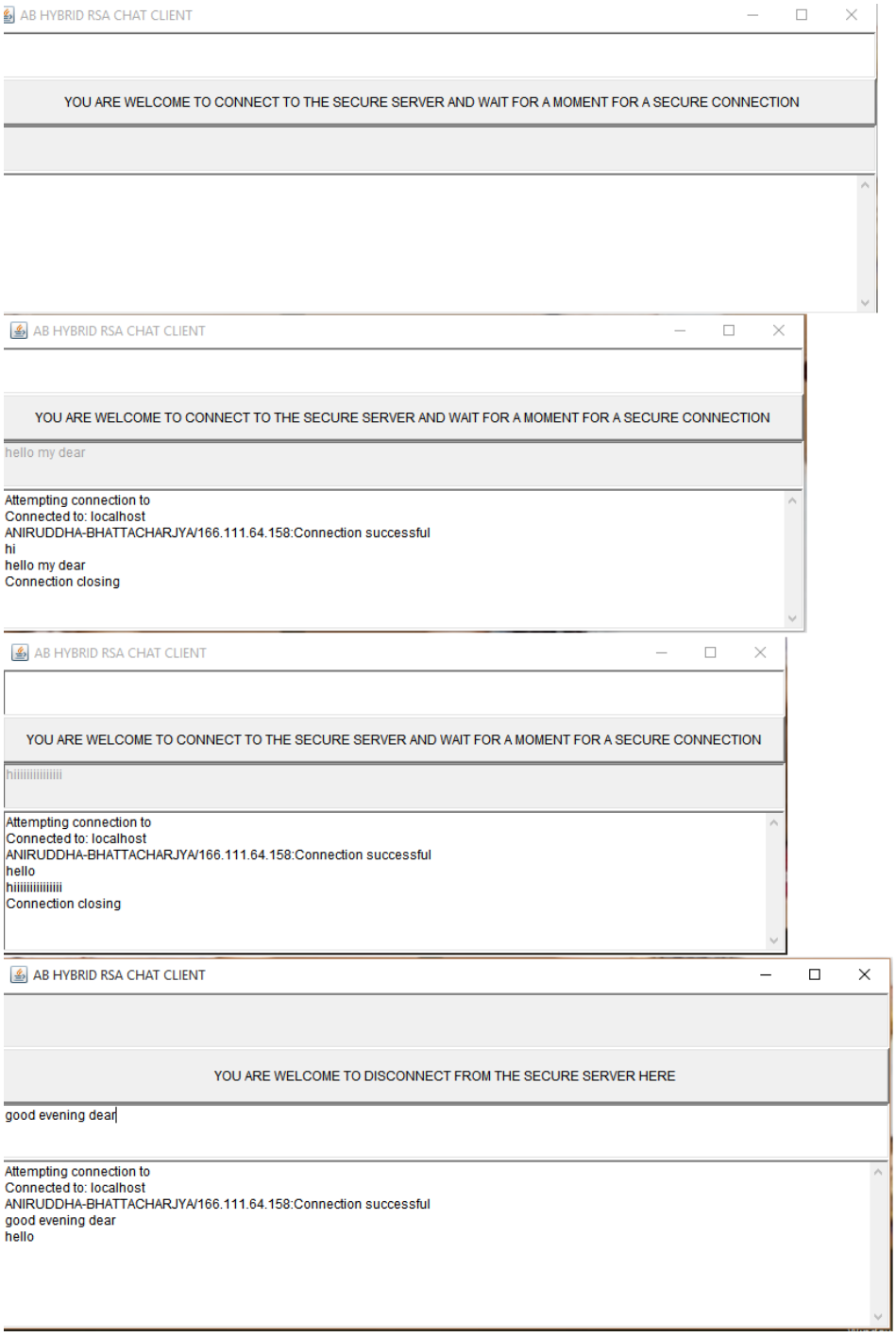


Figure 8 Now first two have closed connections after chat finished and now third one connected and starts messaging in pure peer-to-peer manner (see online version for colours)



4 Conclusions

We are in an era, where around 10 billion devices are presently interconnected to the internet, and it is already predicted that it will rise to 16 billion by 2020. Any kind of personal information communicated both ways in the network must be secured E2E. The shield of data and privacy of users is one of the significant challenges in the future internet architectures, deficiency of confidence about privacy will consequence in reduced acceptance among users and hence is one of the motivating factors in the triumph of the future internet architectures. So in the scenario of personal messaging in the future internet architectures with existing Internet architectures, we need very strong, reliable and efficient messaging models. So, our E2E user two-way authenticated double encrypted messaging architecture based on hybrid RSA for the future internet architectures can be incorporated in the Choicenet, NEBULA, XIA, sourceless network architecture, with scenario of binding of CoAP with DTLS and off course with existing Internet architectures. Low modular complexity with effortlessness and speediness problem is resolved by our hybrid RSA. The parallel protection to Sniffing attacks and real-time key negotiation between each peer is resolved by PFS using D-H integration in our hybrid RSA scheme. Our hybrid RSA use Rabin-Miller primality test for strong primes, it is very unique. Our hybrid RSA messaging scheme is strong, secure and reliable with integration of efficient RSA with Rabin-Miller strong primality test integration and Hellman encipher with salt and OAEP in encryption level and in decryption level shared RSA with CRT-RSA gives efficiency and statistical complexity. We are achieving almost four times efficient decryption which is very much essential for all existing internet architectures and future internet architectures. Our implementation allows ubiquitous and automatic encryption available to all users without any need of understanding the complications involved. Our architecture also affords a hassle-free, secure, peer-to-peer, unconventionally strong and reliable platform with E2E-encryption for people and organisations who are concerned about their privacy and security. We have our own two-way authentications for peers and then hybrid RSA encryption, so in a scenario where no need of use of any password (like – MSN Messenger, AOL Instant Messenger, ICQ and Yahoo Instant Messenger), our scheme can be used. In a scenario where external digital certificates are used, our scheme can work without external digital certificates, as we have our own hybrid RSA security, authentication and highly efficient architecture with very strong confidentiality. In a scenario where there is need of any third party [like instant messaging key exchange (IMKE) protocol], our hybrid RSA scheme can work well as no need of third party authentication, variants of RSA integrations gives more reliability, more efficiency and more strong scheme.

We, in near future, will work on more efficiency of our scheme, balancing with security and strong privacy aspects. Also we will try to incorporate our scheme in near future internet architectures with a perfect balance of privacy, security, efficiency and stronger authentication.

Acknowledgements

This work is supported by Key Laboratory of Universal Wireless Communications (Beijing University of Posts and Telecommunications), Ministry of Education, China (No. KFKT-2014101), National S&T Major Project (2015ZX03002010-002) and National Natural Science Foundation of China (No. 61631013).

References

Aboud, S.J., Alfayoumi, M.A., Alfayoumi, M. and Jabbar, H. (2008) 'An efficient RSA public key encryption scheme', *Proc, 5th International Conf. on Information Technology: New Generations (ITNG)*, Las Vegas, pp.127–130.

Bhattacharjya, A., Zhong, X. and Wang, J. (2016) 'Strong, efficient and reliable personal messaging peer to peer architecture based on hybrid RSA', *Proceedings of the International Conference on Internet of Things and Cloud Computing (ICC 2016)*, 22–23 March, The Møller Centre, Churchill College, Cambridge, UK, ISBN 978-1-4503-4063-2/16/03, DOI http://dx.doi.org/10.1145/2896387.2896431.

Boneh, D. and Shacham, H. (2002) 'Fast variants of RSA', *CryptoBytes*, Vol. 1, No. 5, pp.1–9.

Bormann, C., Castellani, A. and Shelby, Z. (2012) 'CoAP: an application protocol for billions of tiny internet nodes', *IEEE Internet Comput.*, March/April, Vol. 1, No. 2, pp.62–67.

Braun, B.M. and Crowcroft, J. (2014) *SNA: Sourceless Network Architecture*, Technical report, UCAM-CL-TR-849, March, Computer Laboratory, ISSN 1476-2986.

Davida, G.I. (1982) *Chosen Signature Cryptanalysis of the RSA (MIT) Public Key Cryptosystem*, Technical Report TR-CS-82-2, Department of Electrical Engineering and Computer Science, University of Wisconsin, Milwaukee.

Dierks, T. and Rescorla, E. (2006) *The Transport Layer Security (TLS) Protocol Version 1.1*, RFC 4346.

Fischl, J., Tschofenig, H. and Rescorla, E. (2010) *Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)*, RFC 5763, May, IETF.

Hartke, K. and Tschofenig, H. (2014) *A DTLS 1.2 Profile for the Internet of Things*, draft-hartke-dice-profile-03, IETF.

Hinek, M.J. (2007) *On the Security of Some Variants of RSA*, PhD dissertation, University of Waterloo, Canada.

Ju, F. et al. (2008) 'Summary of internet privacy research', *Information Studies: Theory & Application*, Vol. 2008, No. 1, pp.110–111.

Kaminaga, M. and Yoshikawa, H. (2015) 'Double counting in 2t-ary RSA precomputation reveals the secret exponent', *IEEE Transactions on Information Forensics and Security*, July, Vol. 10, No. 7, pp.1394–1401.

Kothmayr, T., Schmitt, C., Hu, W., Brunig, M. and Carle, G. (2012) 'A DTLS based end-to-end security architecture for the future internet architectures with two way authentication', *Proc. 37th IEEE Conf. LCN Workshops*, pp.956–963.

Kothmayr, T., Schmitt, C., Hu, W., Brunig, M. and Carle, G. (2013) 'DTLS based security and two-way authentication for the internet of things', *Ad Hoc Netw.*, November, Vol. 11, No. 8, pp.2710–2723.

Modadugu, N. and Rescorla, E. (2004) 'The design and implementation of datagram TLS', *Proc. NDSS*.

Padhye, S. (2006) 'On DRSA public key cryptosystem', *The International Arab Journal of Information Technology*, October, Vol. 3, No. 4.

Pointcheval, D. (1999) 'New public key cryptosystem based on the dependent-RSA problem', *Proceedings of Eurocrypt'99*, LNCS 1592, pp.239–254, Springer-Verlag, Berlin-Heidelberg.

Rescorla, E. and Modadugu, N. (2006) *DTLS: Datagram Transport Layer Security*, RFC 4347.

SECG (2014) *Elliptic Curve Cryptography – SEC 1* [online] http://www.secg.org (accessed November 2014).

Seggelmann, R., Tüxen, M. and Rathgeb, E. (2012) *Strategies to Secure End-to-End Communication – And Their Application to SCTP-Based Communication*, December, to appear.

Shelby, Z., Hartke, K. and Bormann, C. (2014) *The Constrained Application Protocol (COAP)*, RFC 7252, June, Internet Engineering Task Force.

Shelby, Z., Hartke, K., Bormann, C. and Frank, B. (2012) *Constrained Application Protocol (CoAP)*, Internet draft, draft-ietf-core-coap-09 (work in progress), March, IETF.

Vuillaume, C. (2003) *Efficiency Comparison of Several RSA Variants*, Master's thesis, Darmstadt University of Technology.

Xiao, Z., Wang, Y. and Jiang, Z. (2015) 'Research and implementation of four-prime RSA digital signature algorithm', *2015 IEEE ICIS*, 28 June to 1 July, Las Vegas, USA.