PLOS | ONE

RESEARCH ARTICLE

AIB-OR: Improving Onion Routing Circuit Construction Using Anonymous Identity-Based Cryptosystems

Changji Wang[1,2,4]*, **Dongyuan Shi**[3,4], **Xilei Xu**[3,4]

1 National Pilot School of Software, Yunnan University, Kunming, China, **2** Yunnan Key Laboratory of Software Engineering, Yunnan University, Kunming, China, **3** School of Information Science and Technology, Sun Yat-sen University, Guangzhou, China, **4** Guangdong Key Laboratory of Information Security Technology, Sun Yat-sen University, Guangzhou 510275, China

* wchangji@gmail.com

Citation: Wang C, Shi D, Xu X (2015) AIB-OR: Improving Onion Routing Circuit Construction Using Anonymous Identity-Based Cryptosystems. PLoS ONE 10(3): e0121226. doi:10.1371/journal.pone.0121226

Academic Editor: Gaoxi Xiao, Nanyang Technological University, SINGAPORE

Received: August 31, 2014

Accepted: January 29, 2015

Published: March 27, 2015

Data Availability Statement: All relevant data are within the paper.

Funding: National Natural Science Foundation of China (Grant No. 61173189, http://www.nsfc.gov.cn/), Yunnan Province Software Engineering Key Laboratory Project (Grant No. 2015SE203), the Foundation for Innovative Research Team of Yunnan University, and Guangdong Province Information Security Key Laboratory Project (http://ist.sysu.edu.cn/). The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Abstract

The rapid growth of Internet applications has made communication anonymity an increasingly important or even indispensable security requirement. Onion routing has been employed as an infrastructure for anonymous communication over a public network, which provides anonymous connections that are strongly resistant to both eavesdropping and traffic analysis. However, existing onion routing protocols usually exhibit poor performance due to repeated encryption operations. In this paper, we first present an improved anonymous multi-receiver identity-based encryption (AMRIBE) scheme, and an improved identity-based one-way anonymous key agreement (IBOWAKE) protocol. We then propose an efficient onion routing protocol named AIB-OR that provides provable security and strong anonymity. Our main approach is to use our improved AMRIBE scheme and improved IBOWAKE protocol in onion routing circuit construction. Compared with other onion routing protocols, AIB-OR provides high efficiency, scalability, strong anonymity and fault tolerance. Performance measurements from a prototype implementation show that our proposed AIB-OR can achieve high bandwidths and low latencies when deployed over the Internet.

Introduction

The rapid development of network technology has made anonymous communication an increasingly important security requirement for many network applications [1]. While end-to-end encryption can protect the data content of communications from unauthorized access, it does not conceal all the relevant information that two communicating parties are communicating. For example, routing information is still transmitted in the clear because routers need to know packets' destinations in order to route them in the right direction. Traffic analysis can also be done by watching particular data moving through a network, by matching the amount

Competing Interests: The authors have declared that no competing interests exist.

of data, or by examining coincidences, such as connections opening and closing at about the same time.

In many situations, it is highly desirable or indispensable for users to be able to preserve the communications anonymity. For example, an abrupt change in the traffic pattern may indicate some forthcoming activities in a tactical military communication network. This can be extremely dangerous in that adversaries can easily identify critical network nodes and then launch targeted attacks on them. In addition, people have a strong desire to remain anonymous when pursuing sensitive information in order to avoid unnecessary trouble.

Over the years, a large number of anonymity networks have been proposed and some have been implemented. Among them, onion routing has been widely employed as an infrastructure for private communication over a public network.

Related Work

Identity-Based Cryptography. To simplify certificate management in tradition public key infrastructure, Shamir [2] first introduced the concept of identity-based public key cryptography, where an entity's public key can be publicly computed from his recognizable identity information, such as a complete name or an e-mail address, while the corresponding private key is generated by a trusted third party named as private key generator (PKG).

The first practical and secure identity-based encryption (IBE) scheme was constructed from bilinear pairings by Boneh and Franklin [3]. Since then, various IBE schemes, identity-based signature schemes and identity-based key agreement (IBKA) protocols have been proposed [4].

For example, considering a situation where a sender would like to encrypt a message for t receivers, the sender must encrypt the message t time using conventional IBE schemes. To improve the performance, Baek et al. [5] introduced the notion of multi-receiver IBE scheme, and proposed an efficient provably secure multi-receiver IBE scheme from bilinear pairings. To guarantee receiver's privacy, Boyen and Waters [6] proposed an anonymous IBE scheme, where the ciphertext does not leak the identity of the recipient.

Later, Fan et al. [7] introduced the concept of anonymous multi-receiver IBE (AMRIBE) scheme and proposed an efficient AMRIBE scheme from bilinear parings. In an AMRIBE scheme, one can examine whether himself is a selected receiver or not. Nobody, except the sender, knows who the other selected receivers are. Subsequently, Chien [8] pointed out that Fan et al.'s AMRIBE scheme only provides receiver anonymity for outsider attackers or non-selected receivers, and presented an improved AMRIBE scheme. However, only heuristic arguments for security proofs are presented. Tseng et al. [9] proposed a new AMRIBE scheme that was proved to be semantically secure against adaptive chosen ciphertext attacks in the random oracle model under the Gap-BDH assumption.

Sakai et al. proposed the first non-interactive IBKA protocol from bilinear pairing, where the established key consists of only one participant's identity-based private key and the other participant's identity. Thus, the established key can not be used as a session key because it always establishes the same (secret) key for the same entities in each run of the protocol. Kate et al. [10] extended Sakai et al.'s IBKA protocol, and proposed an identity-based one-way anonymous key agreement (IBOWAKE) protocol to provide unconditional anonymity for participants by replacing the identities of the participants by pseudonyms. Unfortunately, Kate et al. IBOWAKE protocol is insecure against man-in-the-middle (MIMA) attack because it can not authenticate the communication entities.

Certificateless Cryptography. The concept of certificateless public key cryptography was first introduced by Al-Riyami and Paterson [11], which combines the advantages of traditional

certificate-based public key cryptography and identity-based public key cryptography. In a certificateless cryptosystem, the key generation center (KGC) does not have access to the entity's private key, the KGC derives a partial private key from the entity's identity and the master secret key. The entity then combines the partial private key with some secret information to generate the actual private key. Thus, certificates are not considered necessary anymore to guarantee the authenticity of public keys in traditional certificate-based public key cryptography, and at the same time the private key is not fully determined by the KGC to prevent the inherent key escrow problem in identity-based public key cryptography.

Certificateless public key cryptography has received a significant attention in recent years, several certificateless encryption schemes, certificateless signature schemes and certificateless key agreement protocols were presented. For example, Catalano et al. [12] introduced the concept of anonymous certificateless key agreement and proposed two constructions.

Attribute-Based Encryption. Attribute-based encryption (ABE) was first introduced by Sahai and Waters [13] with the original goal of providing an error-tolerant IBE that uses biometric identities. ABE can be viewed as an extension of the notion of IBE in which user identity is generalized to a set of descriptive attributes instead of a single string specifying the user identity. Compared with IBE, ABE has significant advantage as it achieves flexible one-to-many encryption instead of one-to-one, it is envisioned as a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control.

ABE have drawn extensive attention from both academia and industry in recent years, many ABE schemes have been proposed [14–16] and several cloud-based secure systems using ABE have been developed [17–19]. There are two types of ABE depending on which of private keys or ciphertexts that access policies are associated with.

In a key-policy attribute-based encryption (KP-ABE) system, ciphertexts are labeled by the sender with a set of descriptive attributes, and users' private keys are issued by the trusted attribute authority are associated with access policies (also called access structures) that specify which type of ciphertexts the key can decrypt. In a ciphertext-policy attribute-based encryption (CP-ABE) system, when a sender encrypts a message, they specify a specific access policy in terms of access structure over attributes in the ciphertext, stating what kind of receivers will be able to decrypt the ciphertext. Users possess sets of attributes and obtain corresponding secret attribute keys from the attribute authority, such a user can decrypt a ciphertext if his/her attributes satisfy the access policy associated with the ciphertext.

Onion Routing. Onion routing was first proposed by Reed, Syverson and Goldschlag [20, 21]. In onion routing, for a given connection, the sender selects a sequence of routers, known as a circuit, that will be used to forward the sender's traffic. The sender establishes a circuit by first directly opening a circuit with the first router, and then iteratively extending the circuit by sending message over the existing circuit. Messages are encrypted with the key of each router in the circuit in the reverse order that the routers appear. Like someone peeling an onion, each onion router removes a layer of encryption to uncover routing instructions, and sends the message to the next router where this is repeated. This prevents these intermediary nodes from knowing the origin, destination, and contents of the message.

In the original onion routing protocol [22], each onion router is equipped with a pair of public and private key. The source uses the public keys of the intermediate routers with the top layer encrypted with the public key of the router immediately next to the source. The intermediate routers then use their own corresponding private keys to decrypt the packet and obtain the information about the next hop in the network. The packets thus routed and forwarded by each intermediate genuine node, eventually reach the destination. The advantage here is that if any one of the routers is compromised by an adversary, even then, the other components remain beyond the reach, because of being encrypted using a different public key. However, it is

evident that a sender is required to encrypt a message as many times as is the number of intermediate onion routers.

Kate et al. [10] presented a pairing-based onion routing (PB-OR) protocol by using an IBOWAKE protocol. Catalano et al. [12] then proposed a certificateless onion routing (CL-OR) protocol by using an anonymous certificateless key agreement protocol. Later, Catalano et al. [23] proposed a fully non-interactive onion routing protocol with forward secrecy by using a forward-secure IBE scheme. Recently, Doshi et al. [24] proposed an onion routing circuit construction called attribute-based onion routing (AB-OR) using the Bethencourt et al. CP-ABE scheme [15]. Here the access policy is boolean formula over routers' identities and the access policy is sent in the clear along with the ciphertext. Thus, AB-OR provides neither recipient anonymity nor route anonymity.

Motivation and Our Contributions

Compared to the original onion routing protocol, onion routing protocols proposed in recent years have greatly improved in terms of efficiency and anonymity. However, there are still three drawbacks in the existing onion routing protocols.

- Failure tolerance is relatively poor. The palsy of any one of the intermediate onion router will result in the palsy of the entire onion routing process.
- Recipient anonymity is not strong enough. The last onion router will know the identity of the recipient.
- Communication anonymity is weak. Each intermediate onion router needs to know the identity of the next hop router on the path, which impairs the communication anonymity.

In this paper, we first improve Kate et al.'s IBOWAKE protocol [10] and Tseng et al.'s AMRIBE scheme [9], then we propose a new onion routing circuit construction called anonymous identity-based onion routing (AIB-OR) by integrating our improved IBOWAKE protocol with AMRIBE scheme in onion routing circuits construction. Compared to PB-OR and CL-OR, our proposed AIB-OR achieves both efficiency improvement and anonymity enhancement. This paper makes three primary contributions in the field of anonymous communication.

- The efficiency of onion routing circuit construction is improved. The performance of AIB-OR surpasses those of PB-OR and CL-OR, requiring significantly less computation and fewer network communications. Unlike existing onion routing protocols, Our proposed AIB-OR only requires the sender to encrypt the message twice, irrespective of the number of intermediate onion routers.
- Failure tolerance of onion routing circuit construction is provided. The sender can select any one of the path through which to forward the packet out of the multiple paths at its disposal in the proposed AIB-OR.
- Anonymity of onion routing circuit construction is enhanced. The sender, the recipient and the intermediate onion routers are anonymous to others, no one knows the real identities and location of the sender, the intermediate onion routers, or the recipient. Adversaries cannot trace a packet flow back to its sender or the recipient. Nobody, except the sender, knows the real routing path between the sender and the recipient.

Paper Organization

The rest of this paper is organized as follows. Some necessary preliminary work and our improved IBOWAKE protocol and AMRIBE scheme are introduced in Section 2. The proposed AIB-OR model and construction are described in Section 3. Efficiency and security analysis of our AIB-OR are discussed in Section 4. Performance test of PB-OR and our AIB-OR are explained in Section 5. Finally, we conclude our work in Section 6.

Preliminary Work

Notations

To facilitate further description, we introduce notations in Table 1.

Bilinear Group Generator and Complexity Assumptions

Definition 1 *The bilinear group generator $\mathcal{G}$ is an algorithm that takes as input a security parameter κ and outputs a bilinear group $(q,\mathbf{G}_1,\mathbf{G}_2,\hat{e},P)$, where q is a prime of size 2^κ, $\mathbf{G}_1$ and $\mathbf{G}_2$ are cyclic groups of order q, P is a generator of $\mathbf{G}_1$, and $\hat{e}:\mathbf{G}_1\times\mathbf{G}_1\rightarrow\mathbf{G}_2$ is a bilinear map with the following properties:*

- *Bilinearity: For $a, b \xleftarrow{\$} \mathbf{Z}_q^*$, we have $\hat{e}(aP, bP) = e(P, P)^{ab}$.*
- *Non-degeneracy: $\hat{e}(P, P)$ is a generator of $\mathbf{G}_2$.*
- *Computability: For $P_1, P_2 \xleftarrow{\$} \mathbf{G}_1$, there is an efficient algorithm to compute $\hat{e}(P_1, P_2)$.*

Definition 2 (Bilinear Diffie-Hellman Assumption) *The BDH assumption in a prime order bilinear group $(q, \mathbf{G}_1, \mathbf{G}_2, \hat{e}, P)$ generated by $\mathcal{G}(1^\kappa)$ is that if a tuple $\langle P, aP, bP, cP\rangle \in \mathbf{G}_1^{(4)}$ is given for unknown $a, b, c \xleftarrow{\$} \mathbf{Z}_q^*$, there is no probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ can compute $\hat{e}(P, P)^{abc} \in \mathbf{G}_2$ with non-negligible advantage* [3].

Definition 3 (Decisional Bilinear Diffie-Hellman Assumption) *The DBDH assumption in a prime order bilinear group $(q, \mathbf{G}_1, \mathbf{G}_2, \hat{e}, P)$ generated by $\mathcal{G}(1^\kappa)$ is that if a tuple $\langle P, aP, bP, cP, T\rangle \in \mathbf{G}_1^{(4)}\tilde{n}\mathbf{G}_2$ is given for unknown $a, b, c \xleftarrow{\$} \mathbf{Z}_q^*$ and $T \xleftarrow{\$} \mathbf{G}_2$, there is no PPT adversary $\mathcal{A}$ can decide whether $T = \hat{e}(P, P)^{abc}$ with non-negligible advantage* [4].

Table 1. Notations.

Symbol	Description
$x \xleftarrow{\$} \mathbf{S}$	Pick an element x uniformly at random from the set $\mathbf{S}$
κ	The system security parameter
Π	A semantically secure symmetric encryption scheme
len	The key length of Π
$E_k(m)$	Encrypt a message m under Π with a session key $k \in \{0, 1\}^{len}$
$D_k(c)$	Decrypt a ciphertext c under Π with a session key $k \in \{0, 1\}^{len}$
H_0	Hash function $H_0 : \{0,1\}^* \rightarrow \mathbf{G}_1^*$
H_1	Hash function $H_1 : \mathbf{G}_2 \rightarrow \mathbf{Z}_q^*$
H_2	Hash function $H_2 : \mathbf{Z}_q^* \rightarrow \{0,1\}^{len}$
H_3	Hash function H_3:{0, 1}$^* \rightarrow$ {0, 1}^{2len}

doi:10.1371/journal.pone.0121226.t001

Definition 4 (Gap Bilinear Diffie-Hellman Assumption) *The Gap-BDH assumption in a prime order bilinear group* $(q, \mathbf{G}_1, \mathbf{G}_2, \hat{e}, P)$ *generated by* $\mathcal{G}(1^\kappa)$ *is that if a tuple* $\langle P, aP, bP, cP\rangle \in \mathbf{G}_1^{(4)}$ *is given for unknown* $a, b, c \xleftarrow{\$} \mathbf{Z}_q^*$, *there is no PPT adversary* $\mathcal{A}$ *can compute* $\hat{e}(P, P)^{abc} \in \mathbf{G}_2$ *with the help of the DBDH oracle with non-negligible advantage. The DBDH oracle means that given a tuple* $\langle P, aP, bP, cP, T\rangle \in \mathbf{G}_1^{(4)} \tilde{n} \mathbf{G}_2$, *outputs 1 if* $T = \hat{e}(P, P)^{abc}$ *and 0 otherwise* [9].

Our Improved IBOWAKE Protocol

Kate et al. [10] proposed an IBOWAKE protocol that was proved to be secure in the random oracle model under the BDH assumption. The core idea of Kate et al.'s IBOWAKE protocol is to replace the identity hashes with pseudonyms generated by users, and each user can randomly generate many possible pseudonyms and the corresponding private keys.

To avoid impersonation and MIMA attacks, it is desirable that only the pseudonym with valid certificate can be used as an encryption key during an anonymous communication session. For privacy purposes, we require that the PKG will not know the real pseudonym of an entity and the corresponding certificate. Our improved IBOWAKE protocol is described as follows.

- **Setup**: The PKG runs $\mathcal{G}(1^\kappa)$ to get $(q, \mathbf{G}_1, \mathbf{G}_2, \hat{e}, P)$, chooses $s \xleftarrow{\$} \mathbf{Z}_q^*$, computes $P_{pub} = sP \in \mathbf{G}_1$. Finally, the PKG sets the master secret key $msk = s$ and the system parameters $mpk = \langle q, \mathbf{G}_1, \mathbf{G}_2, \hat{e}, P, P_{pub}, H_0\rangle$.
- **Extract**: Given a user's identity ID, the PKG computes $Q_{\mathrm{ID}} = H_0(\mathrm{ID})$ and $d_{\mathrm{ID}} = sQ_{\mathrm{ID}}$. Finally, the PKG sends the user's private key d_{ID} to the user via a secure channel.
- **PNGen**: An entity X chooses $k_X \xleftarrow{\$} \mathbf{Z}_q^*$, computes $\mathrm{PN}_X = k_X P$ and $sk_{\mathrm{PN}_X} = k_X P_{pub} = s\mathrm{PN}_X$. Finally, the entity X sets PN_X and sk_{PN_X} as his pseudonym and the corresponding private key, respectively.
- **BlindCert** An entity X with a pseudonym PN_X chooses $r_X \xleftarrow{\$} \mathbf{Z}_q^*$, generates a masked pseudonym by computing $PN'_X = r_X H_0(PN_X)$, X then sends PN'_X to the PKG. The PKG computes $\sigma'_X = sPN'_X$ and sends the signature σ'_X to X. Upon receiving σ'_X, X verifies σ'_X by checking $\hat{e}(\sigma'_X, P) = \hat{e}(PN'_X, P_{pub})$. If the equation holds, X then computes $\sigma_X = r_X^{-1}\sigma'_X = sH_0(PN_X)$, and obtains his pseudonym certificate $\langle \mathrm{PN}_X, \sigma_X\rangle$. Anyone can verify entity X's pseudonym certificate $\langle \mathrm{PN}_X, \sigma_X\rangle$ by testing $\hat{e}(\sigma_X, P) = \hat{e}(H_0(\mathrm{PN}_X), P_{pub})$.
- **Key Agreement**: Suppose Alice wants to perform a session key agreement with Bob. Alice knows Bob's identity ID_B and wishes to remain anonymous to Bob, Alice and Bob perform the following steps:
  - Alice generates her pseudonym PN_X and gets her pseudonym certificate $\langle \mathrm{PN}_A, \sigma_A\rangle$ by performing the **PNGen** algorithm and the **BlindCert** algorithm, respectively.
  - Alice computes the session key $K_{A,B} = \hat{e}(sk_{\mathrm{PN}_A}, Q_{\mathrm{ID}_B})$. Alice then sends her pseudonym certificate $\langle \mathrm{PN}_A, \sigma_A\rangle$ to Bob.
  - Upon receiving Alice's pseudonym certificate $\langle \mathrm{PN}_A, \sigma_A\rangle$, Bob verifies Alice's pseudonym certificate by testing $\hat{e}(\sigma_A, P) = \hat{e}(H_0(\mathrm{PN}_A), P_{pub})$. If the equation holds, Bob then computes the corresponding session key $K_{A,B} = \hat{e}(\mathrm{PN}_A, d_{\mathrm{ID}_B})$ by using his private key d_{ID_B}.

Note that the **BlindCert** algorithm is in fact a blind Boneh-Lynn-Shacham (BLS) signature scheme [25], which is proved to be existentially unforgeable under adaptive chosen-message attacks under the computational Diffie-Hellman assumption in the random oracle model.

Our Improved AMRIBE Scheme

Tseng et al. [9] proposed an AMRIBE scheme that was proved to be semantically secure against adaptive chosen ciphertext attacks in the random oracle model under the Gap-BDH assumption.

Tseng et al.'s AMRIBE scheme [9] is an extension of Boneh and Franlin's IBE scheme [3] to multiple recipients scenario. Rapid enhanced-security asymmetric cryptosystems transform (REACT) [26] is an important tool for any asymmetric encryption schemes to achieve IND-CCA secure from IND-CPA secure. We apply the REACT transformation in Tseng et al.'s AMRIBE scheme to further improve the efficiency without compromising security.

- **Setup**: The PKG runs $\mathcal{G}(1^{\kappa})$ to get $(q,\mathbf{G}_1,\mathbf{G}_2,\hat{e},P)$, chooses $s \xleftarrow{\$} \mathbf{Z}_q^*$, computes $P_{pub} = sP \in \mathbf{G}_1$. Finally, the PKG sets $msk = s$ and $mpk = \langle q,\mathbf{G}_1,\mathbf{G}_2,\hat{e},P,P_{pub},H_0,H_1,H_2,H_3,\Pi\rangle$.
- **Extract**: Given a user's identity ID, the PKG computes $Q_{\mathrm{ID}} = H_0(\mathrm{ID})$ and $d_{\mathrm{ID}} = sQ_{\mathrm{ID}}$. Finally, the PKG sends the user's private key d_{ID} to the user via a secure channel.
- **Encrypt**: To encrypt a message $m \in \{0,1\}^*$ for t receivers with identities $\mathbf{ID} = \{ID_i\}_{i=1}^t$, the sender chooses $r, k \xleftarrow{\$} \mathbf{Z}_q^*$, computes $U = rP$, $T = rP_{pub}$, $Q_{\mathrm{ID}_i} = H_0(\mathrm{ID}_i)$ and $v_i = H_1(\hat{e}(Q_{\mathrm{ID}_i}, T))$ for $1 \le i \le t$, and constructs a polynomial $f(x)$ with degree t as

$$f(x) = \prod_{i=1}^{t}(x - v_i) + k \bmod q = c_0 + c_1 x + \ldots + c_{t-1}x^{t-1} + x^t.$$

  The sender then computes $W = E_{H_2(k)}(m)$ and $\lambda = H_3(m, k, c_0, c_1, \ldots c_{t-1}, U, W)$. Finally, the sender sets the ciphertext $C = \langle c_0, c_1, \ldots, c_{t-1}, U, W, \lambda\rangle$.
- **Decrypt**: Upon receiving a ciphertext $C = \langle c_0, c_1, \ldots, c_{t-1}, U, W, \lambda\rangle$ that is encrypted using identities $\mathbf{ID} = \{ID_i\}_{i=1}^t$, a selected receiver with identity $\mathrm{ID}_j \in \mathbf{ID}$ first computes $v_j = H_1(\hat{e}(d_{\mathrm{ID}_j}, U))$, $k' = f(v_j) = c_0 + c_1 v_j + \cdots + c_{t-1}v_j^{t-1} + v_j^t \ mod\ q$ and $m' = D_{H_2(k')}(W)$. The receiver then sets $\lambda' = H_3(m', k', c_0, c_1, \ldots c_{t-1}, U, W)$, and tests whether $\lambda' = \lambda$ holds or not. If it does not hold, the recipient rejects the ciphertext. Otherwise, the recipient outputs m as the decryption of C.

The AIB-OR Protocol

The system model for our proposed AIB-OR protocol is illustrated as Fig. 1, in which the round represents the users and the rectangle represents the onion routers. Assume that there are $t-1$ onion routers between the sender and the receiver along the routing path. We denote the i-th router in the path by OR_i where $1 \le i \le t-1$. Unlike existing onion routing protocols, we will distinguish users and routers in our AIB-OR.

The proposed AIB-OR protocol involves a trusted PKG whose responsibility is to initialize system parameters and to issue identity-based private keys and blind pseudonym certificates for all participants. The PKG runs the setup algorithm in AMRIBE scheme, sets the master key $msk = s$, and publishes the system parameters $mpk = \langle q,\mathbf{G}_1,\mathbf{G}_2,\hat{e},P,P_{pub},H_0,H_1,H_2,H_3,\Pi\rangle$.

Circuit Construction

When the sender would like to send a message $m \in \{0,1\}^{\ell}$ to the designated recipient with identity ID_R anonymously and securely, he performs the following steps:

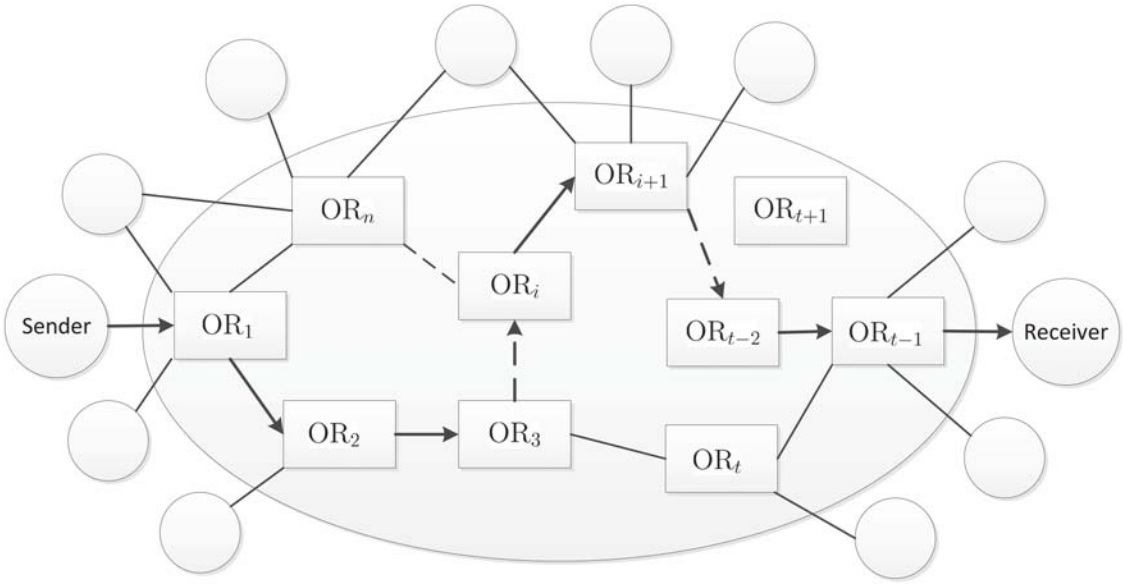

Fig 1. System Model of Onion Routing.

doi:10.1371/journal.pone.0121226.g001

1. The sender generates his pseudonym PN_S and gets his pseudonym certificate $\langle PN_S, \sigma_S \rangle$ by performing the **PNGen** algorithm and the **BlindCert** algorithm, respectively.
2. The sender runs the **Key Agreement** algorithm of our improved IBOWAKE protocol, gets the session key $K_{S,R} = \hat{e}(sk_{PN_S}, Q_{ID_R})$, and encrypts message m using a symmetric encryption algorithm (such as Advanced Encryption Standard, AES) with the session key $K_{S,R}$ to get the ciphertext C_0. Note that the seesion key is used to encrypt data and is valid only for the duration of the communication.
3. The sender then constructs a circuit by selecting an ordered subset of onion routers from a generally known set of onion routers. We denote the identities of selected subset of onion routers by $\{ID_i\}_{i=1}^{t-1}$, where ID_{t-1} is the identity of onion router closest to the designated receiver.
4. The sender encrypts the inner ciphertext C_0 for identities $\{ID_i\}_{i=1}^{t-1} \cup ID_R$ by applying the **Encrypt** algorithm of our improved AMRIBE scheme to get the outer ciphertext C_1.
5. Finally, the sender transmits the onion packet $ONI \triangleq (seq, \langle PN_S, \sigma_S \rangle, C_1)$ to the first onion router OR_1 along the path.

Decrypt by Onion Router

When an onion router OR_i receives the onion packet, it processes the onion packet as follows.

1. The onion router OR_i checks whether the packet has already been received or not by using the field *seq* as the unique identifier for the packet. If there is an entry with the same *seq* field in its local routing table, it simply discards the onion packet. Otherwise it inserts a new record (seq, OR_{i-1}, ttl) into the local routing table.
2. The onion router OR_i decrypts the ciphertext C_1 of the onion packet with its private key d_{ID_i} by running the **Decrypt** algorithm of our improved AMRIBE scheme. If the decryption

fails, the OR_i just discards the packet without forwarding. Otherwise, the OR_i forwards the onion packet to all the connecting onion routers and users except the previous onion router (whom it gets the packet from).

Decrypt by the Recipient

When a user receives the onion packet, he performs the same operations as the onion routers. Note that a user can not decrypt the ciphertext C_1 of the onion packet with his private key unless he is the designated recipient. If he is not the designated recipient, he simply discards the packet. Otherwise, he is the designated recipient, and he can further decrypt the inner ciphertext C_0 with the session key $K_{S,R} = \hat{e}(\mathrm{PN}_S, d_{\mathrm{ID}_R})$ and get the plaintext m.

Security and Efficiency Analysis

In this section, we explain how the proposed AIB-OR protocol meets the sender anonymity, recipient anonymity, route anonymity and failure tolerance, and analyze why the proposed AIB-OR protocol can greatly reduce computational and communications costs. In the following, all analyzes and discussions are based on the onion routing example illustrated in Fig. 2.

- **Sender Anonymity**: The sender constructs circuit using its one-time pseudonym in our AIB-OR protocol, which ensures sender anonymity.
- **Recipient Anonymity**: In existing onion routing protocols, if an adversary compromised the onion router OR_{10}, then he knows the address or identity of the recipient. In our AIB-OR protocol, the sender encrypts the inner ciphertext for multiple identities $\{ID_i\}_{i=1}^{t-1} \cup ID_R$ by applying AMRIBE scheme, which provides privacy protection for the recipient and the onion routers in the circuit.
- **Route Anonymity**: In the circuit construction given in PB-OR and CL-OR, the sender sends to each onion router a pseudonym and a message symmetrically encrypted with the session

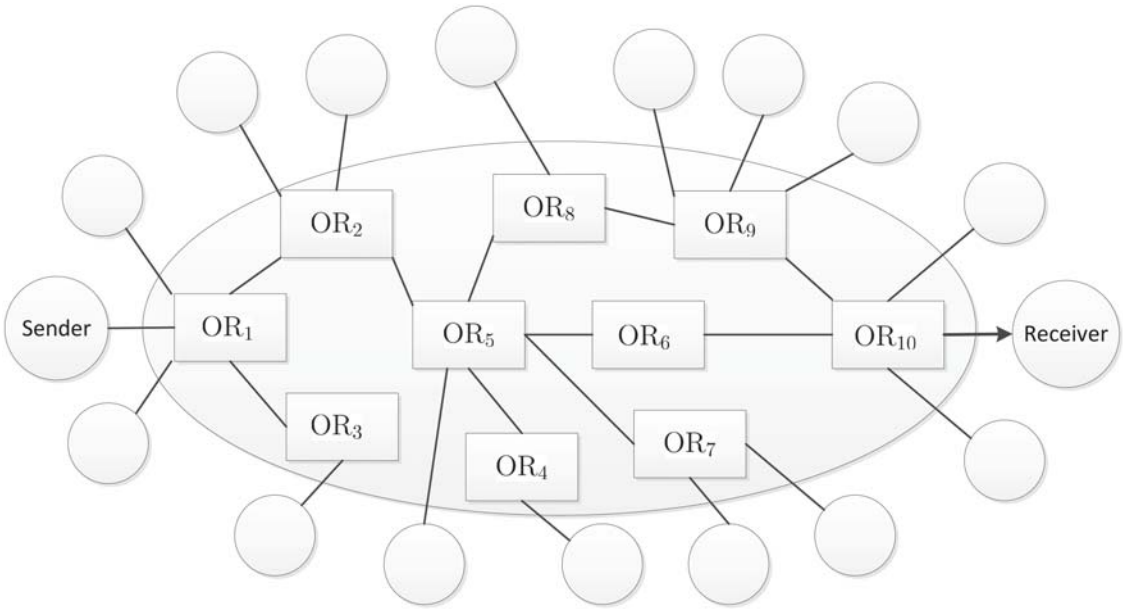

Fig 2. Example of Onion Routing.

doi:10.1371/journal.pone.0121226.g002

key K_i. The session key K_i is generated by a non-interactive anonymous key agreement protocol, and the message contains the identity of the next node in the circuit. Thus every onion router in the circuit knows the address or identity of both the previous onion router and the next onion router. In the circuit construction of our AIB-OR protocol, the sender encrypts the inner ciphertext for multiple identities $\{ID_i\}_{i=1}^{t-1} \cup ID_R$ by applying AMRIBE scheme, which ensures none of the onion routers knows who is the next onion router or user since every onion router sends message to all the connecting onion routers and users except the previous onion router.

- **Failure Tolerance**: Assume that sender sends a message to the receiver using the routing path Sender → OR_1 → OR_2 → OR_5 → OR_6 → OR_{10} → Recipient. If there is something wrong with OR_6, the message will be discarded after OR_5 in the existing onion routing protocols. In our AIB-OR protocol, the sender can add both the identity of OR_8 and OR_9 to the recipient collection. In this way, both OR_8 and OR_9 can decrypt the ciphertext with their own private key, respectively. If OR_6 failed, the message can still be transferred to the receiver following the path Sender → OR_1 → OR_2 → OR_5 → OR_8 → OR_9 → OR_{10} → Recipient. This will bring extra overhead in circuit construction since the sender needs to construct higher order polynomial. Here we assume the sender has sufficient knowledge of routing paths leading to the recipient and the sender make a tradeoff between efficiency and failure tolerance to decide the actual routing path.
- **Message Consistency**: We assume the adversaries have complete control over some part of the network, but not all parts of the network, since this cannot be possible for large network with thousands of network links. It may look like the message is not changing at every hop in the path so this may give path information to an attacker. However, attackers do not know the next hop in the path in our AIB-OR. So there is nearly no possibility for adversaries to get the whole path information by utilizing techniques such as traffic analysis, unless they are watching the entire network. In addition, our AIB-OR, unlike PB-OR and CL-OR, provides message integrity detection by verifying the value of λ.
- **Forward Secrecy**: To achieve forward secrecy in PB-OR and CL-OR, onion routers' keys are required to be changed frequently, this implies a significant computational effort for the PKG. In contrast our AIB-OR, none of the onion routers can decrypt the inner ciphertext and know who is the next onion router or user. To achieve forward secrecy in our proposed AIB-OR, only the sender's pseudonym or the recipient's key is required to be changed.
- **Communication Cost**: At first glance, our AIB-OR protocol will bring higher network overhead since each onion router forwards the onion packet to all the connecting onion routers and users except the previous onion router. In fact, out of all only onion routers in the circuit can decrypt and the remaining will discard the onion packet. In Fig. 2, when OR_5 receives an onion packet from OR_2, it will send the onion packet to the onion routers OR_4, OR_6, OR_7, OR_8 and a user, respectively. However, only OR_6 can decrypt the onion packet and others will discard it since they can not decrypt the onion packet. In addition, the size of the onion packet is shorter than those of PB-OR and CL-OR.
- **Storage Cost**: Both onion routers and users are given an identity-based private key from the trusted PKG, which can be used to decrypt the ciphertext encrypted by AMRIBE scheme as well as symmetric encryption algorithm with the session key $K_{S,R}$, thus the overhead of key management is greatly reduced. In addition, for an onion router or a user who receives the same packet for the second time, they can check the field *seq* in the packet against entries in the local routing table. If there is a matching record in the routing table, the onion router or

user will discard the packet. A time to live field (*ttl*) is set in the local routing table, so that the entry can be removed from the local routing table when the *ttl* reaches zero.

- **Computation Cost**: In the PB-OR and CL-OR, a sender is required to perform symmetric encryption operation t times if there are t onion routers in the path. In our AIB-OR, a sender is only required to perform symmetric encryption operation 2 times irrespective of number of onion routers in the path. Our AIB-OR, like PB-OR and CL-OR, each intermediate onion router is required to perform one bilinear pairing and one symmetric decryption operations. Note that, message is actually transmitted from the last onion router to the designated recipient in the clear text both in the PB-OR and CL-OR. Thus, the recipient does not need to perform any operations in PB-OR and CL-OR. Obviously, this would lead to the disclosure of messages and exposure of recipient identity. Our AIB-OR, unlike existing onion routing protocols, the user and the onion router is different, and the recipient is required to perform two bilinear pairing and two symmetric decryption operations.

We compare the security properties, computational and communications costs on circuit construction in PB-OR, CL-OR and our AIB-OR. The comparison is summarized in Table 2. We denote by t, $|m|$, $|\mathrm{ID}|$, $|\mathbf{G}_1|$ and $|\mathbf{Z}_q^*|$ the number of onion routers in the circuit, the bit-length of a plaintext, an identity, an element in group $\mathbf{G}_1$, and an element in group $\mathbf{Z}_q^*$, respectively. We denote by e_1, e_2, p, E, D the computation cost of an exponentiation in $\mathbf{G}_1$, an exponentiation in $\mathbf{G}_2$, a bilinear pairing in $(\mathbf{G}_1,\mathbf{G}_2)$, a encryption operation and a decryption operation in Π, respectively. Other operations are omitted in the following analysis since their computation cost is trivial.

Performance Test

We conducted several experiments to compare AIB-OR with PB-OR in terms of computation cost and bandwidth overhead. The experiments were run on a machine with 2GB of RAM, and hosted on 2.00GHz. We implement our algorithms based on Charm-Crypto Framework (version 0.42) [27] and Pairing-Based Crypto (PBC) library [28].

In our experiment, we use symmetric bilinear groups over supersingular elliptic curves of type A [28], where an element in $\mathbf{G}_1$ can be represented by 512 bits. We choose AES-256 as the symmetric encryption algorithm, and the number of onion routers is chosen to be from 5 to 20, and the packet size is chosen to be 512 bytes.

Table 2. Comparison among our AIB-OR, PB-OR and CL-OR.

	PB-OR [10]	CL-OR [12]	AIB-OR
Sender Cost	$tp+tE+te_1+te_2$	$tE+5te_1$	$(t+1)p+2E+2e_1$
OR Cost	$1p+1D$	$3e_1+1D$	$1p+1D$
Onion Packet Size	$\|m\|+(t-1)\|\mathrm{ID}\|+t\|\mathbf{G}_1\|$	$\|m\|+(t-1)\|ID\|+t\|\mathbf{Z}_q^*\|$	$\|m\|+(t+1)\|\mathbf{Z}_q^*\|+\|\mathbf{G}_1\|$
Recipient Anonymity	No	No	Yes
Sender Anonymity	Yes	Yes	Yes
OR Anonymity	Partial	Partial	Complete
Fault Tolerance	No	No	Yes
Forward Secrecy	Yes	Yes	Yes
Message Integrity	No	No	Yes
MIMA Resistance	No	No	Yes

doi:10.1371/journal.pone.0121226.t002

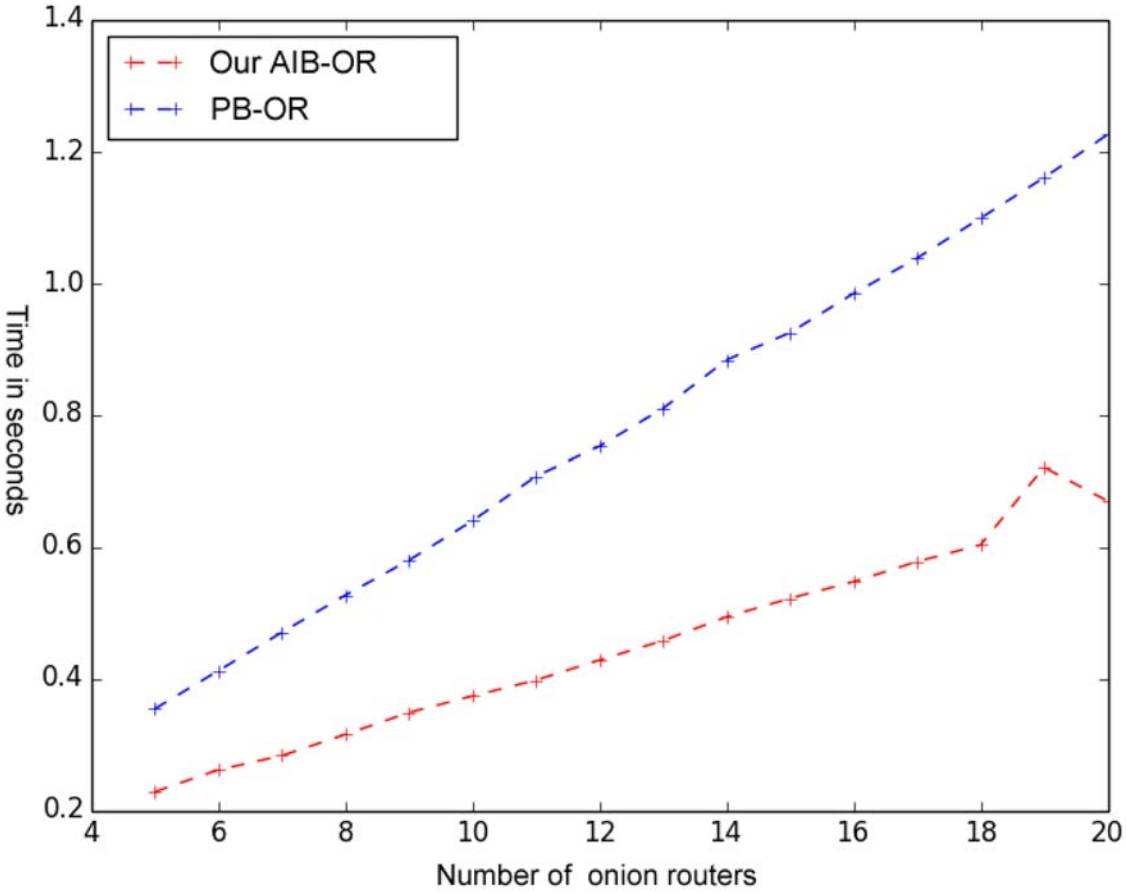

Fig 3. Comparison of Circuit Construction Cost.

doi:10.1371/journal.pone.0121226.g003

The time cost of circuit construction is measured on encryption time run by the source node, decryption time run by all the intermediate nodes in the circuit and decryption time run by the destination node. Fig. 3 shows the comparison of computation time required by the sender in PB-OR [10] and our AIB-OR. As shown in the figure, the computation time required by the sender in our AIB-OR is shorter than in PB-OR for the same number of onion routers. Moreover, the growth rate of computation time required by the sender in our AIB-OR is slower than in PB-OR.

For PB-OR, the size of onion packets becomes larger with the increase in the number of onion routers. For the intermediate routers, the closer to the destination node, the higher bandwidth overhead will be. There is no such problem in our AIB-OR. Fig. 4 shows the comparison of onion packet size in PB-OR [10] and in our AIB-OR. As shown in the figure, the size of onion packet in our AIB-OR is shorter than in PB-OR. Moreover, the growth rate of onion packet size in our AIB-OR is slower than in PB-OR.

Conclusion

In this paper, we propose a new approach for circuit construction in onion routing anonymity networks by using our improved anonymous multi-receiver identity-based encryption scheme and our improved anonymous identity-based one-way key agreement protocol. Compared to

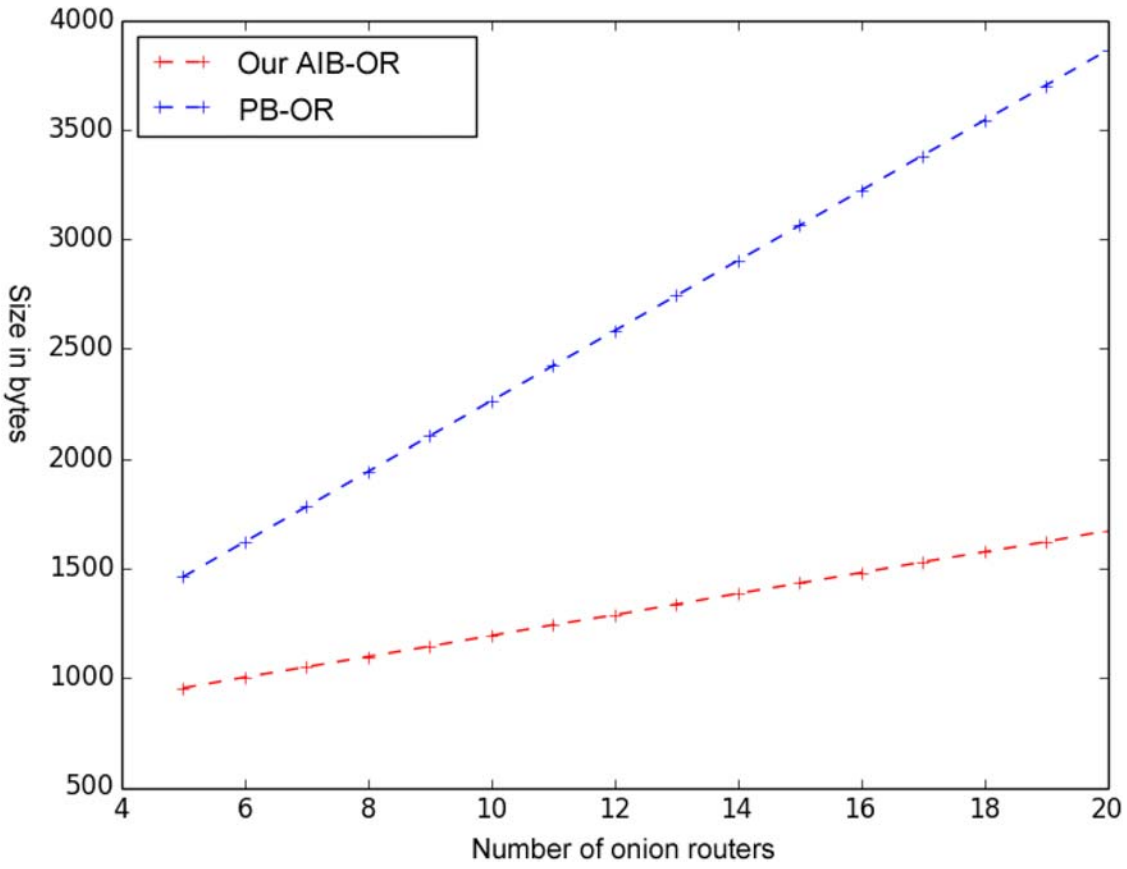

Fig 4. Comparison of Onion Packet Size.

doi:10.1371/journal.pone.0121226.g004

existing approach for circuit construction in onion routing anonymity networks, our approach provides high efficiency, scalability, strong anonymity and fault tolerance. Performance experiment shows that our proposed approach uses significantly less computation and communication than that of paring-based onion routing.

Acknowledgments

The authors would like to thank the editors and the anonymous reviewers of this paper for their valuable comments and suggestions while at the same time helping us to improve the English spelling and grammar throughout the manuscript.

Author Contributions

Conceived and designed the experiments: CJW DYS XLX. Performed the experiments: DYS XLX. Analyzed the data: CJW DYS. Contributed reagents/materials/analysis tools: CJW DYS. Wrote the paper: CJW.

References

1. Ren J and Wu J. Survey on Anonymous Communications in Computer Networks. Computer Communications. 2010, 33(4): 420–431.

2. Shamir A. Identity-Based Cryptosystems and Signature Schemes. Advances in Cryptology – CRYPTO 1984, Lecture Notes in Computer Science Volume 196, 1985, pp. 47–53.
3. Boneh D and Franklin M. Identity-Based Encryption from the Weil Pairing. Advances in Cryptology—CRYPTO 2001, Lecture Notes in Computer Science Volume 2139, 2001, pp. 213–229. doi: 10.1007/3-540-44647-8_13
4. Baek J, Newmarch J, Safavi-naini R and Susilo W. A Survey of Identity-Based Cryptography. Proceedings of Australian Unix Users Group Annual Conference, 2004, pp. 95–102.
5. Baek J, Safavi-Naini R and Susilo W. Efficient Multi-receiver Identity-Based Encryption and Its Application to Broadcast Encryption. Public Key Cryptography—PKC 2005, Lecture Notes in Computer Science Volume 3386, 2005, pp. 380–397. doi: 10.1007/978-3-540-30580-4_26
6. Boyen X and Waters B. Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles). Advances in Cryptology—CRYPTO 2006, Lecture Notes in Computer Science Volume 4117, 2006, pp. 290–307. doi: 10.1007/11818175_17
7. Fan CI, Huang LY and Ho PH. Anonymous Multireceiver Identity-Based Encryption. IEEE Transactions on Computers, 2010, 59(9): 1239–1249. doi: 10.1109/TC.2010.23
8. Chien HY. Improved Anonymous Multi-receiver Identity-based Encryption. The Computer Journal, 2012, 55(4): 439–445. doi: 10.1093/comjnl/bxr086
9. Tseng YM, Huang YH and Chang HJ. CCA-secure Anonymous Multi-receiver ID-based Encryption. The 26th International Conference on Advanced Information Networking and Applications Workshops, 2012, pp. 177–182. doi: 10.1109/WAINA.2012.50
10. Kate A, Zaverucha G and Goldberg I. Pairing-Based Onion Routing. Privacy Enhancing Technologies—PET 2007, Lecture Notes in Computer Science Volume 4776, 2007, pp. 95–112.
11. Al-Riyami SS and Paterson KG. Certificateless Public Key Cryptography. Advances in Cryptology—ASIACRYPT 2003, Lecture Notes in Computer Science Volume 2894, 2003, pp. 452–473. doi: 10.1007/978-3-540-40061-5_29
12. Catalano D, Fiore D and Gennaro R. Certificateless Onion Routing. Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009, pp. 151–160.
13. Sahai A and Waters B. Fuzzy Identity-based Encryption. Advances in Cryptology—EUROCRYPT 2005, Lecture Notes in Computer Science Volume 3494, 2005, pp. 457–473. doi: 10.1007/11426639_27
14. Goyal V, Pandey O, Sahai A and Waters B. Attribute-based Encryption for Fine-grained Access Control of Encrypted Data. Proceedings of the 13th ACM Conference on Computer and Communications Security, 2006, pp. 89–98.
15. Bethencourt J, Sahai A and Waters B. Ciphertext-Policy Attribute-Based Encryption. IEEE Symposium on Security and Privacy, 2007, pp. 321–334. doi: 10.1109/SP.2007.11
16. Waters B. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. Public Key Cryptography—PKC 2011, Lecture Notes in Computer Science Volume 6571, 2011, pp. 53–70. doi: 10.1007/978-3-642-19379-8_4
17. Ibraimi L, Asim M and Petkovic M. Secure Management of Personal Health Records by Applying Attribute-based Encryption. 6th International Workshop on Wearable Micro and Nano Technologies for Personalized Health, 2009, pp.71–74. doi: 10.1109/PHEALTH.2009.5754828
18. Pirretti B, Traynor P, McDaniel P and Waters B. Secure Attribute-based Systems. Journal of Computer Security, 2010, 18(5): 799–837.
19. Wang CJ, Liu X and Li WT. Design and Implementation of a Secure Cloud-based Personal Health Record System Using Ciphertext-policy Attribute-based Encryption. International Journal of Intelligent Information and Database Systems, 2013, 7(5): 389–399. doi: 10.1504/IJIIDS.2013.056381
20. Reed M, Syverson P and Goldschlag D. Anonymous Connections and Onion Routing. IEEE Journal on Selected Areas in Communications. 1999, 16(4): 482–494. doi: 10.1109/49.668972
21. Goldschlag D, Reed M and Syverson P. Onion Routing. Communications of the ACM, 1999, 42(2): 39–41. doi: 10.1145/293411.293443
22. Mauw S, Verschuren JHS and de Vink EP. A Formalization of Anonymity and Onion Routing. European Symposium on Research in Computer Security—ESORICS 2004, Lecture Notes in Computer Science Volume 3193, 2004, pp. 109–124. doi: 10.1007/978-3-540-30108-0_7
23. Catalano D, Raimondo MD, Fiore D, Gennaro R and Puglisi O. Fully Non-interactive Onion Routing with Forward-Secrecy. Applied Cryptography and Network Security—ACNS 2011, Lecture Notes in Computer Science Volume 6715, 2011, pp. 255–273.

24. Nishant D and Devesh J. AB-OR: Improving the Efficiency in Onion Routing Using Attribute Based Cryptography. Computer Networks & Communications—NetCom 2013, Lecture Notes in Electrical Engineering Volume 131, 2013, pp. 425–432.

25. Boneh D, Lynn B and Shacham H. Short Signatures from the Weil Pairing. Journal of Cryptology, 2004, 17(4): 297–319. doi: 10.1007/s00145-004-0314-9

26. Okamoto T and Pointcheval D. REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform. Topics in Cryptology—CT-RSA 2001, Lecture Notes in Computer Science Volume 2020, 2001, pp. 159–174. doi: 10.1007/3-540-45353-9_13

27. Akinyele JA, Garman C, Miers I, Pagano MW, Rushanan M, Green M, et al. Charm: a Framework for Rapidly Prototyping Cryptosystems. Journal of Cryptographic Engineering, 2013, 3(2): 111–128. doi: 10.1007/s13389-013-0057-3

28. Lynn B. The Pairing-Based Cryptography Library. 2014. Available: http://crypto.stanford.edu/pbc/.