sciendo

BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **21**, No 3
Sofia • 2021 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2021-0028

A Survey on Proxy Re-Signature Schemes for Translating One Type of Signature to Another

Shilpa Chaudhari[1], *Aparna R.*[1], *Archana Rane*[2]

[1]*Department of Computer Science and Engineering, M. S. Ramaiah Institute of Technology* (*Affiliated to VTU*), *Bangalore, Karnataka, India*
[2]*Department of MCA, K. K. Wagh Institute of Engineering Education and Research, Nashik, Maharashtra, India*
E-mails: shilpasc29@msrit.edu aparna@msrit.edu alrane@kkwagh.edu.in

***Abstract*:** *Proxy Re-Signature* (*PRS*) *complements well-established digital signature service. Blaze-Bleumer-Strauss discussed PRS in 1998 for translating a signature on a message from Alice into a signature from Bob on the same message at semi-trusted proxy which does not learn any signing-key and cannot produce new valid signature on new message for Alice or Bob. PRS has been largely ignored since then but it has spurred considerable research interest recently for sharing web-certificates, forming weak-group signatures, and authenticating network path. This article provides a survey summarizing and organizing PRS-related research by developing eight-dimensional taxonomy reflecting the directional feature, re-transformation capability, re-signature key location, delegatee involvement, proxy re-signing rights, duration-based revocation rights, security model environment, and cryptographic approach. Even though multi-dimensional categorization is proposed here, we categorize the substantial published research work based on the eighth dimension. We give a clear perspective on this research from last two-decades since the first PRS-protocol was proposed.*

***Keywords*:** *Signature translation, Proxy Re-Signature, PKI-based re-signature, Identity-based re-signature, Certificateless re-signature, Semi-trusted Proxy.*

1. Introduction

At the inception of the Proxy Re-Signature Scheme (PRS) in 1998, the technical design choices and operational requirements were the differentiating properties. In the last two decades, there has been increasing convergence between normal signature-based security provisioning and PRS expressing many effects ranging from drastic to behind the scene. PRS is different from proxy signature given in M a m b o, U s u d a and O k a m o t o [33] where the proxy is trusted and full rights are given for signing the document on behalf of the user. A semi-trusted proxy exists in PRS wherein some information in contrast to complete authority as in proxy signature is

given to him for re-signing the signed document by the user. The Alice's signature on a message 'm' is transformed using the provided partial information into Bob's signature on the same message at semi-trusted proxy. The proxy cannot, on its own, generate signatures for either Alice or Bob during this process. The first proposal of PRS was published at Eurocrypt'98 by Blaze, Bleumer, and Strauss (BBS) (Blaze, Bleumer and Strauss [3]). Since then, the original proposal has been improved but very little follow up work has been done immediately, to our knowledge. The BBS original construction (Blaze, Bleumer and Strauss [3]) is inefficient with limited required features. At an early stage of the research work, it has been envisaged that the PRS has confused notation. Indeed, the recent years saw a growing range of possible applications of PRS with many new research-works in the literature.

PRS, a critical branch of digital signature, has been first introduced in Blaze, Bleumer and Strauss [3] wherein a semi-trusted proxy acts as a translator to translate a perfectly-valid and publicly-verifiable signature generated on certain message, m, from Alice, denoted as $\sigma_A(m)$, into signature from Bob on the same message, denoted as $\sigma_B(m)$, via re-signature key. Even though BBS scheme supports multi-use, multi-directional, and public proxy for re-signing key, there are no follow-up studies conducted in the literature until the breakthrough work of Ateniese and Hohenberger [2], wherein the authors summarize the formal definition and properties of PRS with the proof about PRS usage in weak group signatures, network path authentication and web certificate sharing. PRS applications can include simple certificate and key management, provide proof for chosen path, inter-operable system with digital rights management. Since then, many PRS schemes have been investigated, which is the topic of this paper. Both signatures generated in PRS can coexist and can be publicly verified as being two signatures from two distinct people on the same message. Semi-trusted proxy in the PRS scheme can convert a single signature into multiple signatures of several and distinct signers, and vice-versa.

A PRS is a tuple of probabilistic/polynomial time algorithms, (KeyGen, REKey, Sign, RESign, Verify) where: KeyGen is the standard key generation process involved in PRS; Sign is the signing algorithm used to generate signature; Verify is the verification algorithm for verifying the received signature at receiver; REKey is the re-signature key generation algorithm which takes sk_A and sk_B as the secret key of A and B, respectively, and generates rk_(A–B) key for the semi-trusted proxy; RESign is the re-signature function that takes rk_(A–B), a signature σ, a message m, and a public key pk_A to generate a new signature σ` on message m corresponding to pk_B. If Verify (pk_A, m, σ`) is successful then accept the message otherwise reject it. The scenario of this process is given in Fig. 1.

The PRS schemes have eight desirable properties in addition to the security and correctness that are either necessary or desirable when it is used in any application. These properties are listed as follows: (1) Unidirectional, (2) Multi-use, (3) Private Proxy, (4) Transparent, (5) Key Optimal, (6) Non-interactive, (7) Non-transitive, (8) Temporary. None of existing PRS schemes satisfies all of these properties. Additional PRS functionalities, possibilities and challenges have generated a considerable amount of research recently, which will be discussed during its comprehensive survey in next sections.

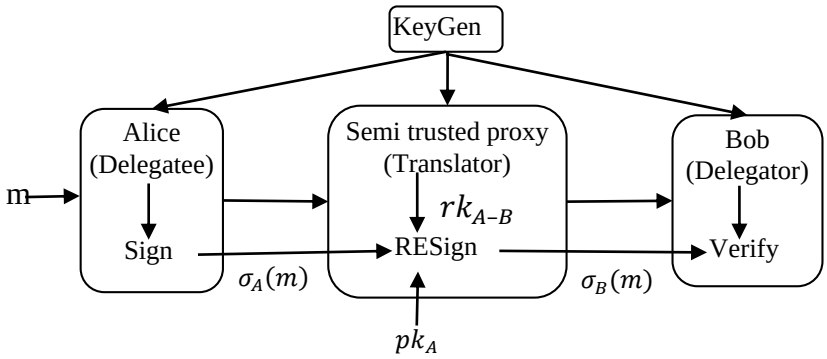

Fig. 1. Components of PRS scheme

Our contributions: Consequently, this significant amount of published research on PRS requires some categorization to provide a convenient overview of the current state of the art. To this end, we have developed multi-dimensional taxonomy to classify the PRS research based on the properties supported in the research work that is given in Section 2. The designed eight dimensions are as follows. (1) Directional feature examined to allows the proxy to transform A's signature to B's in unidirectional or multidirectional. (2) Re-transformation capability to decide whether the transformed signature can be re-transformed or not. (3) Re-signature key location for keeping the generated proxy re-signature key. (4) Delegatee involvement in delegation process to indicate delegatee interaction with delegator during creation of re-signature. (5) Proxy re-signing rights for re-delegation in multi-use feature support for generating the re-signature key. (6) Type of revocation rights based on the duration to minimize renovation overhead. (7) Security model environment to decide whether it is a standard or random model. (8) Cryptographic approach used such as Public Key Infrastructure (PKI), IDentity based (ID-based), and Certificateless (CL). The presented taxonomy allows us to analyze the PRS research trends over time and various properties supported in the work. To illustrate the usefulness of the provided classification, we discuss a detailed survey of the collected research articles from extensive databases available online where PRS based references can be explored according to the designed dimensions and categories of the presented taxonomy.

Our specific contributions are as follows. (1) Design and discuss eight-dimensional taxonomy. (2) Explain the PRS research trends across the eighth dimension – cryptographic approach used. (3) Compare the discussed PRS scheme in each category with respect to eight desirable properties. (4) Discuss the scope of the research on the topic of the paper.

The remaining part of this article is structured in various sections as follows. In Section 2, explains the methodology for creating the PRS research work taxonomy with its dimensions and categories. It also explains the PRS-related research material to analyze and provide trends on the distribution across the proposed dimensions. Section 3 presents a detailed survey of the key research findings and related comparison with respect to eight desirable properties related to the PRS. Section 4 addresses the scope of the research on PRS. Finally, conclusions are drawn in Section 5.

2. Design of PRS taxonomy and classification

The taxonomy provides a classification of the research works on the addressed topic in order to obtain a comprehensive understanding with the state-of-the-art on the selected topic. Taxonomy construction varies from topic to topic but all works in one class given in the taxonomy should be similar in the features or properties. The classification categories should be non-overlapping with well-defined limits between them. The taxonomy designed for PRS related research for analyzing their features and performance include eight dimensions with a number of non-overlapping categories in each dimension. We consider different aspects to be analyzed in each dimension for each classified research article related to PRS. The eight dimensions used for the categorization of PRS schemes are: (1) directional feature examined; (2) re-transformation capability; (3) re-signature key location; (4) delegatee involvement in delegation process; (5) proxy re-signing rights for re-delegation; (6) type of revocation rights based on the duration; (7) Security model environment; (8) cryptographic approach used. We involve all the properties of PRS as part of taxonomy dimension except transparency and key optimal property in the categorization as all the proposed research work on PRS has to support these properties and no further classification is possible. In Transparent proxy property, a user involved in the process does not know the existence of proxy. The input signature of delegatee using Sign algorithm and the corresponding signature generated from ReSign algorithm cannot be linked. In key optimal property, a user is required to protect and store only a small constant amount of secrets such as its corresponding secret keys regardless of how many signature delegations the user gives or accepts. This optimal usage of storage minimizes the safe storage cost for each user. Optimal key storage at a semi trusted proxy could also play a role in supporting this feature.

Each dimension consists of a set of categories used to classify the existing PRS related articles. The presented taxonomy allows us to analyze the PRS research trends over time and various properties supported in the work. The selected article may not be mutually exclusive to the category as it may belong to one or more categories per dimension. The PRS taxonomy illustration in graphical form is given as shown in Fig. 2. We have made an effort to minimize the possible overlap between the existing PRS schemes as per the proposed dimensions in this early stage of defining the classification categories.

The first dimension named as directional features in the proposed PRS taxonomy further classifies the existing research works into two categories depending upon the capability of semi trusted proxy re-sign key during the process of PRS. When semi trusted proxy resigns the A's signature on a message to B's signature on the same message using his re-sign key, if it cannot use same key for resigning B's signature on a particular message to A's signature on that message then it is unidirectional otherwise it is bidirectional. We consider unidirectional and bidirectional PRS as two categories in Dimension-1 using this directional feature of semi trusted proxy resign key. Most of the existing PRS schemes follow either unidirectional or bidirectional. Bidirectional PRS scheme is less secure compared to

unidirectional PRS scheme as the re-sign key of semi-trusted proxy can be recovered by anybody on the network listening to the conversation.

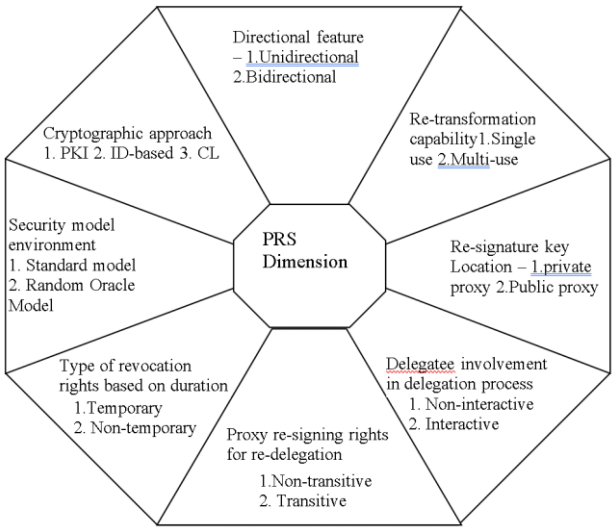

Fig. 2. Graphical illustration of proposed PRS taxonomy

The second dimension named as re-transformation capability in the proposed PRS taxonomy further classifies the existing research works into two categories depending upon the re-transformation capability to decide whether the transformed signature can be re-transformed/re-signed or not. When the generated signature based on signed or re-signed algorithm can be given as input to resign, then that PRS scheme has re-transformation capability, which is called as multi-use property. Otherwise, that scheme is called a single-use property. We consider single-use and multi-use PRS as two categories in Dimension-2 based on this re-transformation feature. Each scheme can be either single-use or multi-use.

The third dimension named as re-signature key Location in the proposed PRS taxonomy further classifies the existing research works into two categories depending upon whether the re-signature key used by a semi trusted proxy can be kept secret by proxy or it can be recomputed by an adversary. When the re-signature key is located at the proxy secretly then the PRS is called a private proxy scheme. When the re-signature key is obtained through the resumption by the adversary passively based on the observation of a proxy then the PRS is called a public proxy scheme.

The fourth dimension named as delegatee involvement in delegation process in the proposed PRS taxonomy further classifies the existing research works into two categories depending upon the delegatee involvement in delegation process. When the delegatee is not involve in the process of delegation where the delegator creates a re-signature key from his select key and public key of delegatee, the process is non-interactive otherwise it is interactive.

The fifth dimension named as proxy re-signing rights for re-delegation in the proposed PRS taxonomy further classifies the existing research works into two categories depending upon the capacity of re-delegation rights given to the semi

trusted proxy. Re-delegation is a need in multi-use feature support in PRS. If proxy alone can re-delegate the re-signing rights, then the PRS is transitive but re-signing rights cannot be re-delegated by the proxy alone hence, the PRS is non-transitive in most of the recent research work. When semi trusted proxy has the re-signing key for A-B and B-C, resigning key A-C cannot be produced by it in non-transitive PRS.

The sixth dimension named as type of revocation rights based on the duration in the proposed PRS taxonomy further classifies the existing research works into two categories depending upon revocation rights. There is a need for revocation of given rights in PRS which includes change of delegator public key after every revocation. To minimize this revocation overhead, temporary delegations are realized assuming the trusted re-signature proxy and appropriate instructions are issued to the proxy.

The seventh dimension named as security model environment in the proposed PRS taxonomy further classifies the existing research works into two categories depending upon the usage of standard or random oracle model. Existence of truly random functions is assumed in the random oracle model wherein all involved parties have access. Random oracle proves that the protocol is secure. Hash function instantiates random oracles due to lack of its efficient existence in reality. A hash function of random oracle environment behaves well enough heuristically as replacement of random oracle but it may trivially insecure also. The protocol only relies on standard cryptographic assumptions during the proof in the standard model. Standard model constructs are nicer from a theoretical perspective and do not rely on random oracles. We consider the standard model based and random oracle model based PRS scheme as two categories in Dimension-7 based on the usage of these security models as an environment.

The eighth dimension named as cryptographic approach used in the proposed PRS taxonomy further classifies the existing research works into four categories depending upon the usage of cryptographic protocols for security provisioning of signature generated. We consider the usage of PKI, ID-based, and CL for PRS as three main categories in Dimension-8 based on the cryptographic approach used. PKI-based PRS schemes requires public key to generate digital signature, which is bound to the corresponding digital certificate issued by a certification authority (CA). Binding of public key to the owner's identity before the usage of the public key at the CA side increases certificate management complexity though the main goal of PRS schemes is to simplify certificate management. The heavy overhead incurred for certificate issuing and management lacks the popularity of PKI based PRS. The required public key for signature is generated effortlessly from the corresponding user's unique identity such as phone number, account number or email address in ID PRS schemes. The Public Key Generator (PKG) has knowledge of the master secret that is used to generate the corresponding private key. Increase in size of signature and verification complexity is the limitations of ID based schemes. Key escrow is the inherent drawback that exists in identity based PRS where proxy has knowledge of user's private key that may be used to damage the essential requirements of PRS. CLPRS is considered a favourable candidate for PRS that overcomes the expensive certificate management of PKI-based PRS and the key escrow of identity-based PRS.

Even though the multi-dimensional categorization is proposed in this paper, we categorize the substantial published research work on as per the eighth dimension shown in Fig. 3 to provide manageable overview of the current state-of the art because a given article may not be mutually exclusive to the category and it may belong to one or more categories per dimension. We have divided three main categories for PRS classification: (1) Usage of PKI for PRS; (2) ID-based PRS; (3) CL PRS. We have surveyed a total fifty existing PRS available in the standard databases such as IEEE, Springer, Science Direct and few from Google scholar. Thirty-three PRS out of fifty use PKI for re-sign key generation. Fourteen PRS out of fifty use ID-based key generation for re-sign keys. Three PRS out of fifty use CL key generation for re-sign keys. Usage of PKI for PRS is further divided into two sub-categories – one for re-sign key generation and other for PRS. The re-sign key can be generated using the standard cryptographic problem that motivates use to divide this category into three classes at next level: (1) Logarithm-based where the PRS uses Diffie-Hellman (DH) assumption for re-sign key generation; (2) Integer factorization based where the PRS uses integer factorization problem for re-sign key generation; (3) Isomorphism of polynomials where the PRS uses quadratic equations for re-sign key generation. Second category for PKI based PRS is further classified into two categories: (1) Threshold PRS where the threshold level for proxies in chain is decided for usage of re-signature generation to support the multi-use property; (2) Conditional delegation where the multi-use property supported for re-signature generation from one proxy to other based on condition. A detailed survey of the PRS collected research illustrates the usefulness of the proposed classification apart from a general research analysis.

3. Literature survey

This section discusses the various categories designed in our taxonomy shown in Fig. 3. Each main category is discussed in a separate subsection.

Table 1. Acronym used for Comparison Parameters

SN	PRS Property as comparison parameter	Corresponding acronym
1	Unidirectional/Bidirectional	U/B
2	Single use/Multi use	S/M
3	Public proxy/Private proxy	Pu/Pr
4	Transparent	T
5	Key optimal	KO
6	Non-Interactive	NI
7	Non-Transitive	NT
8	Temporary	Temp
9	security bases Assumption	SbA
10	Security model environment – Random Oracle Model or Standard security model	(ROM)/(SSM)
11	Computation cost for Sign phase	CCS
12	Computation cost for verify phase	CCV
13	Computation cost for ReSign phase	CCRS

We discuss the comparison among the proposed PRS techniques in particular categories in terms of standard eight properties with two more parameters. Computational cost in ReSign, sign and verify algorithm is also compared theoretically in terms of Exponential (E), Modulation (M), Scalar (S), Pairing (P) and Hash (H) operations. Table 1 provides the acronym used for comparison parameters for the corresponding properties.

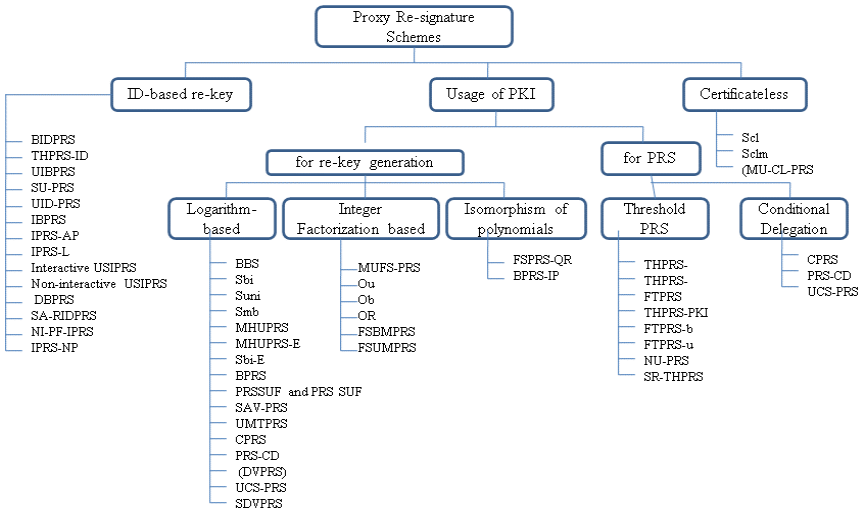

Fig. 3. Taxonomy of PRS

3.1. PKI for PRS

This subsection explains the detailed survey of the PKI based PRS collected research. We do not consider standard eight properties expected for PRS while discussing general research analysis of the paper but we compare them at the end of each category description.

3.1.1. Logarithmic based PKI for PRS

Some papers use logarithm-based PKI for PRS uses DH assumption for re-sign key generation. We discuss such papers in this section. Most of the proposed PRS use DH assumption using bilinear pairing operations.

As mentioned in Section 2, BBS is the first PRS scheme that satisfies limited properties of PRS such as multi use, bidirectional usage and public proxy for re-sign key storage. It has a few security flaws including informal and inefficient definition of BBS paper. Anyone can deduce the re-signature key if signature/re-signature is known to them. Proxy and delegatee can collude to expose the delegator's secret. Authors Ateniese and Hohenberger [2] call BBS scheme as proxy-less as careful observation of the original signature and its transformation helps to recover the information/re-signature key stored at proxy. This endorses proxy rights for anyone after release of the first re-signature. The BBS scheme, being symmetric, can allow Alice to recover Bob's secret key and vice-versa from the publicly known re-

signature key. It guarantees only few limited application security due to these limitations.

Authors A t e n i e s e and H o h e n b e r g e r [2] discuss the eight properties of PRS in addition to the formal definition of PRS and safe storage of re-signature keys at proxy. They propose two PRS schemes called Sbi and Suni based on bilinear maps and Computational DH (CDH) assumption. Sbi is symmetric being bidirectional that is simple and uses private proxy for semi-trusted proxy keys while Suni is asymmetric being unidirectional that provides better security and uses public proxy for its keys. Suni allows signers to use strong and weak secrets for a single public key. Two signature algorithms each at separate levels wherein first level signature can be translated by proxy and level 2 signatures cannot. After their work on these PRS schemes, many PRS schemes have been investigated. It is efficient and secure in the random oracle model. It is only proven secure in the random oracle model. Arbitrary strings public key unrelated to their owner's identity. Complexity of certificate management, though proxy re-signature schemes can be used to simplify certificate management.

PRS scheme of A t e n i e s e and H o h e n b e r g e r [2] and S h a o et al. [43] are existentially unforgeable in random oracle model while Waters approach (W a t e r s [4]), based two PRS schemes given in S h a o et al. [43] are existentially unforgeable in standard model and constructed in bilinear groups with CDH assumption. One of the two PRS schemes uses PKI named as S_{mb} while the other uses an ID named as $S_{id\text{-}mb}$. Both PRS support multi-use and bidirectional properties. Sign and resign algorithms of PRS use two exponentiations in Galois field yielding computationally efficient schemes. It is computationally efficient. Relatively large size of its public parameters and secure with static corruption, not the adaptive corruption limits its functionality.

The simple and clearer security model of unidirectional PRS is discussed in S h a o et al. [42] for various attack particularly the attack with private re-signature key that solves the problems of A t e n i e s e and H o h e n b e r g e r [2] and S h a o et al. [43].

Multi-Hop Unidirectional PRS (MHUPRS) of L i b e r t and V e r g n a u d [31] is existentially unforgeable in random oracle model under the extension of DH assumption as well as in standard model using Waters elegant technique (W a t e r s [4]). The involved proxy translates the signature in one direction and the re-signing on the messages is performed in polynomial number of times. DH-related intractability assumptions are the new demand in of this PRS in bilinear map groups. Strong secret and weak secret for the signers are created from single secret using probability to retain different shapes in terms of first and second level signatures respectively. User can directly generate the signature at specific level if limited number of translators are involved, which is indistinguishable from the signature generated sequentially. Even though it is efficient and secure in the random oracle model as well as in standard model, the size of signature grows linearly with the number of past translations.

Its extension called MHUPRS-E is proposed in C h o w and P h a n [13], wherein the design of generic unidirectional proxy re-signature scheme uses

homomorphic signatures. It also incorporates forward-security into the proxy re-signature paradigm. It is not Strongly Unforgeable.

The authors of Sunitha and Amberker [46], address the open challenge of Ateniese and Hohenberger [2], related to translation of one type of signature generated using Schnorr/ElGamal algorithm to another type of signature generated using RSA algorithm in their proposed PRS, we call it Sbi-E. They prove that none of the secret is compromised during the conversation between delegatee, delegator and proxy signer. It is only proven secure in the random oracle model, arbitrary strings public key unrelated to their owner's identity and complexity of certificate management limits its functionality.

The concept of blind signature protects the original signer's privacy. The authors of (Yu-qiao, Du Ming-hui and Xiao-hua [69]), propose a blind proxy re-signer based on Water in Waters [4] and Bilinear Mapping Re-Signature (BPRS) scheme. The blind signature and blind message is given as input to blind agents in the PRS scheme. It provides security against forged signature attack.

Two strongly unforgeable PRS named as PRS_{SUF} and $PRS2_{SUF}$ – proposed in Vivek et al. [51], based on the static corruption security model of Shao et al. [43] and Water scheme of Waters [4] for strong unforgeability of PRS scheme in standard model. PRSSUF scheme uses transformation technique of Boneh, Shen and Waters [15], and careful random extra parameters. Strengthening the security in as PRS_{SUF} reduced the efficiency due to large number of public parameters. To improve the efficiency, Chameleaon hash function based on generic transformation of FuchunGuo, Yi Mu and Willy Susilo [17], is used in $PRS2_{SUF}$ for generating strongly unforgeable signatures. Tight security reduction of FuchunGuo, Yi Mu and Willy Susilo [17], improves the efficiency. Both schemes provide same PRS properties with different transformation techniques and use bilinear maps based on CDH assumption. But the large number of public parameters used does not allow adaptive corruption of users of the system.

The Server-Aided verification of PRS (SA-PRS) based on Ateniese and Hohenberger [2] for mobile users in cloud environment proposed in Zhiwei Wang and Wei Lv [73] addresses the issue of critical resources availability in cloud for users who are mobile in nature wherein few computations of PRS verification are carried out at cloud server (considered as proxy). Most of the PRS use bilinear pairing-based cryptography, which requires much more computational cost than exponentiation computation. It reduces the elliptic curve based pairing computational load of mobile user verification steps. It uses cloud servers as a proxy for generating the re-signature. Heavy computations of verification are done at cloud servers instead of mobile users who have limited resources. Two SAV-PRS schemes are proposed with minor differences based on the computation of sub-key in the setup phase and rearranging the steps of the execution.

Unidirectional Multiple Time PRS (UMTPRS) using binary hash tree restricts the attacker's forgery in addition to restraining the delegatees abuse and release of revocation overheard (Hong, Gao and Wan [21]). It has a restriction on the number of times re-signature is generated. It is simple, efficient and comparatively shorter length for signature.

Off-line and on-line phases in Divisible On-line/Off-line Proxy Re-Signatures (DO2PRS) improves the real-time efficiency of existing PRS in scenarios where quick response is expected (Yang et al. [65]). Off-line phase pre-computes the statistics before seeing messages to be re-signed that are used in on-line phase after re-signing the message. It uses a chameleon hash function based on the discrete logarithm problem. It is secure without resorting to the random oracle model and requires less computation cost. On-line complexity of our scheme is equivalent to two modular subtractions and two modular multiplications. As this concept of on-line and off-line can be used with any PKI based PRS, we do not include this in our comparison table wherein we compare all PKI-based PRS in terms of standard PRS properties.

Designated Verifier Proxy Re-Signature (DVPRS) uses an existing concept called Designated Verifier Signature (DVS) used in applications that requires "deniable authentication" (Wei, Yang and Mu [56]) in the field of wireless communication. Only designated verifiers are involved in DVS to achieve non-transferability property (Jakobsson, Sako and Impagliazzo [27]). Re-designate verifier algorithm is defined for DVPRS to change designated verifier of DVS at proxy that allows change of signer or verifier. It is very efficient as resign and re-designate-verifier algorithms only require one exponentiation operation. Its security depends on ideal random oracles.

Strong Designated-Verifier Proxy Re-Signature (SDVPRS) (Yang et al. [68]), solves the sender's identity privacy problem in IoT environments. It maintains IoT data transmission integrity in addition to protection of IoT device identity in standard model of Waters [4]. Proxy can change the signer or verifier in DVPRS (Wei, Yang and Mu [56]), but only the designated verifier knows the signer's true identity in SDVPRS. Integrity, unforgeability, non-transferability and signer's identity privacy protection are guaranteed in a single step. Proxy converts IOT device signature into group signature on the same data without identifying the IoT device's identity according to the signature. Verification requires only one pairing operation while length of a signature double compared to Wei, Yang and Mu [56], and requires extra exponentiation operation compared to Wei, Yang and Mu [56].

Signature and encryption operations are done as a single step in signcryption. Signcryption, re-signature and re-encryption is done as a single step in SignReCrypting Proxy Re-Signature (SRCPR) (SnehaKanchan and Narendra Chaudhari [45]). The steps involved include key generation, signcryption, receiving message verification at receiver, decryption as standard flow and re-encryption, re-signature and membership-revocation as optional flow. It is robust, secure, and efficient. Signcryption saves a considerable amount of computational cost. But it has more exponential functions and multiplications.

Table 2 compares the above-discussed logarithmic based PKI for PRS in terms of comparison parameters given in Table 1.

3.1.2. Integer factoring based PKI for PRS

Some papers use Integer factoring-based PKI for PRS uses prime factor assumption for re-sign key generation such as RSA algorithm. We discuss such papers in this section.

Table 2. Comparison of Logarithmic based PKI for PRS

PRS	U/B	S/M	Pu/Pr	T	KO	NI	NT	T	SbA	ROM/ SSM	CC_S	CC_V	CC_{RS}
BBS (Blaze, Bleumer and Strauss [3])	B	M	Pu	Yes	Yes	No	No	No		ROM	Multiple E	3E	Multiple E
Sbi (Ateniese and Hohenberger [2])	B	M	Pr	Yes	Yes	No	No	No	CDH assumption	ROM	H+E	H+P	E
Suni (Ateniese and Hohenberger [2])	U	S	Pu	Yes Not Completely	Yes	Yes	Yes	Yes	CDH and 2-Discrete Logarithm (2-DL) assumptions	ROM	H+E+M	P	4P+10E+11S
Smb (Shao et al. [43])	B	M	Pr	Yes	Yes	No	No	No	Constructed in bilinear groups, and proven secure under the CDH assumption	SSM	2E+S	3P+S	2E+3P+S
MHUPRS (Libert and Vergnaud [31])	U	M	Pu	No	Yes	Yes	Yes	No	DH-like assumptions in bilinear groups	ROM/ SSM	E+H	2P+H	3E
MHUPRS-E (Chow and Phan [13])	U	S	Pr	No	Yes	No	Yes	Yes	CDH	SSM	3E+H	3P+H	6E+H
Sbi-E (Sunitha and Amberker [46])	U	S	Pu	Yes Not Completely	Yes	Yes	Yes	Yes	CDH and 2-Discrete Logarithm (2-DL) assumptions	ROM	H+E	H+P	E
BPRS (Yu-qiao, DuMing-hui and Xiao-hua [69])	U	S	Pr	Yes	Yes	Yes	Yes	Yes	CDH in bilinear groups	SSM	2P+3E+S	P	NONE
PRS_{SUF} and $PRS2_{SUF}$ (Vivek et al. [51])	B	M	Pr	No	Yes	No	No	No	CDH	SSM	2H+3E+S	2P+2H+2E	2H+5E
SAV-PRS (Zhiwei Wang and Wei Lv [73])	U	M	Pr	Yes	Yes	Yes	No	No	elliptic curve in bilinear group	SSM	E+H	4E+H+P	E
UMTPRS (Hong, Gao and Wan [21])	U	S	Pu	Yes	Yes	Yes	Yes	Yes	CDH	ROM	2E+H+S	E+S	H+M+2E+2P
(DVPRS) (Wei, Yang and Mu [56])	B	M	Pr	Yes	Yes	Yes	Yes	No	standard Bilinear DH (BDH) and Decisional Bilinear DH (DBDH) assumptions	ROM	E+P	E+2P	E
SDVPRS (Yang et al. [68])	B	M	Pr	Yes	Yes	Yes	Yes	No	decisional bilinear DH (DBDH) problem and gapbilinear DH (GBDH) problem	SSM	2E+P	2E	E+P
SRCPR (SnehaKanchan and Narendra Chaudhari [45])	U	S	Pr	Yes	Yes	Yes	Yes	No	liner and strong DH assumption with Bilinear group	ROM	E+P	E+2P	E
											E+P	E+2P	E

The basic idea of Multi-Use Unidirectional Forward-Security PRS (MUFS-PRS) (Sunitha and Amberker [36]) extends the key updating algorithm for frequent key changes regularly with the same public key using the hardness of factoring for re-signature and forward security. The author discusses inexpert multi-use bidirectional forward security and multi-use unidirectional forward security schemes with a lot of repetition of information among both. Inexpert

description, generating random secret and frequent increase of re-sign keys complexity limits its usage.

The authors of (S u n i t h a and A m b e r k e r [47]) propose forward-secure PRS as a solution for design of multi-use unidirectional PRS problem using the property of forward-security based on the hardness of factoring. In addition to the translation of one person's signature to another person's signature, the scheme facilitates the signers as well as the proxy to guarantee the security of messages signed in the past even if their secret key is exposed today. It also addresses the open problem of translation of one type of signature algorithm-based signature to another type of signature algorithm-based signature. The authors discuss five PRS schemes (Ou, Ob, OR, Forward-Secure Bi-directional Multi-use Proxy Re-Signature Scheme (FSBMPRS) and, Forward-Secure Unidirectional Multi-use Proxy (FSUMPRS)) – two for re-signature based on unidirectional problem and other three for re-signature based on different signature algorithm. Even though these schemes protect from internal and external (adaptive chosen-message attack) security attacks, it needs separate schemes for separate problems and requires a combined approach.

Table 3 compares the above discussed integer factorization-based PKI for PRS in terms of comparison parameters given in Table 1.

Table 3. Comparison of integer factoring based PKI for PRS

PRS	U/B	S/M	Pu/Pr	T	KO	NI	NT	T	SbA	ROM/SSM	CC_S	CC_V	CC_{RS}
MUFS-PRS (S u n i t h a and A m b e r k e r [36])	U	M	Pr	Yes	Yes	No	Yes	Yes	hardness of factoring	SSM	2E+M+S	Multiple E+s	M+S+Multiple E
Ou (S u n i t h a and A m b e r k e r [47])	U	M	Pr	Yes	Yes	No	Yes	Yes	hardness of factoring	ROM	E+ M+H	E+S+M	E+S+M
Ob (S u n i t h a and A m b e r k e r [47])	B	M	Pr	Yes	Yes	No	No	Yes	hardness of factoring	ROM	E+ M+H	E+S+M	E+S+M+H
OR (S u n i t h a and A m b e r k e r [47])	U	M	Pr	Yes	Yes	No	Yes	Yes	hardness of factoring	ROM	E+ M+H+S	2E+S+M	4E+S+M+H
FSBMPRS (S u n i t h a and A m b e r k e r [47])	B	M	Pr	Yes	Yes	No	Yes	Yes	hardness of factoring	ROM	E+ M+H	2E+S+M	6E+S+M+H
FSUMPRS (S u n i t h a and A m b e r k e r [47])	U	M	Pr	Yes	Yes	No	Yes	Yes	hardness of factoring	ROM	E+ M+H	2E+S+M	5E+S+M+H

3.1.3. Isomorphism of polynomials PKI for PRS

Some papers use quadratic factoring-based PKI for PRS using isomorphism of polynomial assumption for re-sign key generation. The quadratic factoring-based PKI supports the future quantum world. We discuss such papers in this section.

Blind Proxy Re-Signature Scheme Based on Isomorphism of Polynomials (BPRS-IP) (H u i x i a n et al. [25]) based on IP signature of (T a n g and X u [40]) resists quantum attack by keeping the message blind using hash function. Usage of Isomorphism of polynomials helps to keep the delegatee's identity anonymous. The delegate authorizes the proxy signer by altering the random number in the re-signature key generation process. It supports quantum resistance, high efficiency, message blindness, and delegatee anonym with low-power hardware. The size of public key and private key is large.

The quadratic residues problem based PRS proposed in (Y u q i a o and G e [70]) is different from the previous all CDH assumption based PRS. The author initially discusses the bidirectional PRS in quadratic residue problem for proving its security and robustness then he upgrades it with the forward secure PRS scheme in

the same problem. Forward secure PRS greatly reduces the leakage of secret keys. It resists adaptive chosen message attack.

Table 4 compares the above discussed isomorphism of polynomial based PKI for PRS in terms of parameters' comparison given in Table 1.

Table 4. Comparison of isomorphism of polynomial based PKI for PRS

PRS	U/B	S/M	Pu/Pr	T	KO	NI	NT	T	SbA	ROM/SSM	CC_S	CC_V	CC_{RS}
FSPRS-QR (Yuqiao and Ge [70])	B	S	Pu	Yes	Yes	No	No	No	quadratic	ROM	2M+2E+S	S+E	2E+S
BPRS-IP (Huixian et al. [25])	U	M	Pr	Yes	Yes	No	Yes	No	Polynomial Isomorphism problem.	ROM	2H+S	2H+S	5H+S

3.1.4. Threshold PRS

Some papers use threshold value for the number of proxies through which the re-signature is passed and created to support multi-use property for PRS. We discuss such papers in this section.

Key escrow problem in PRS is addressed in (Yang, Cao and Dong [37]) using a group of proxies for signature translation instead of single proxy. The valid re-signature translation into a given signature requires the number of participant proxies that attain the given threshold value based on polynomial interpolation. This threshold PRS proposes two schemes – one based on unidirectional concept of (Ateniese and Hohenberger [2]) called as THPRS-1 and the other – on bidirectional concept of (Shao et al., [43]) called as THPRS-2. The extended version of this paper is given in (Yang, Cao and Dong [62]) wherein the same PRS is described by the authors to distribute the re-signature key to multiple proxies for management. The proposed schemes manage to limit the re-signature proxy's power, to reduce the risk of single point failure, and to enhance the system's robustness. THPRS-1 has secret sharing complexity among more than one semi trusted proxies while THPRS-2 has identity-based computation at each semi-trusted proxy that limits its usage.

Forward security schemes guarantee the past signed data security in presence of attack on today's data signature. Forward secure Threshold PRS (FTPRS) (Xiaodong Yang et al. [59]) combines the advantages of threshold re-signature and forward security wherein the re-sign keys of all involved proxies are updated at regular intervals. This is based on the Pedersen Secret Sharing protocol (Gennaro et al. [38]) for sharing re-sign keys for prescribed periods among all the involved proxies in a group and the Joint-Exp-RSS protocol (Pedersen [48]) for generating random secret value of the particular proxy. PKG generates public parameters and distributes re-sign keys. This is robust, unforgeable, forward secure and unforgettable without relying on random oracle models. Generation of valid PRS is infeasible as the re-sign keys are changed regularly. Generating random secrets and re-sign keys frequently increases complexity.

Improved PRS of (Shao et al. [43]) resists various attacks through collusion resistant threshold PRS (Yang and Wang [63]) wherein the author proposes two schemes – one based on public key embedded in a digital signature called as (THPRS-PKI) and the other is based on identity information of signer called as

(THPRS-ID). Delegator, delegate, trusted dealer and n-semi-trusted proxies are the four parties involved in these threshold PRS with polynomial time algorithms. Trusted dealer obtains the re-signature key of delegate and delegator, which is shared using Shamir's secret sharing (Shamir [1]) along with the verification keys. These keys are distributed to semi-trusted proxies for re-signature. Collision-resistant hash functions are used to create identities and messages of arbitrary length based on bilinear maps. These are unforgeable under a chosen message attack. Security is based on the CDH problem and has a fixed threshold value.

Threshold based PRS protects the re-signature key from internal and external attacks. The previous threshold PRS has fixed threshold values. The authors of (Yang et al. [67]) propose two threshold PRS schemes in standard model based on the flexible threshold values called as FTPRS-b for bidirectional feature and FTPRS-u for unidirectional feature. Flexibility of changing the threshold value and the number of proxies is based on significance of the message to be signed and Chinese Remainder Theorem. Each proxy generates its re-signature key share and corresponding verification key according to variable threshold value. It is existentially unforgeable and robust.

Re-sign key oracle failure possibility increases in game based PRS of (Shao et al. [43]) as both users are corrupted or uncorrupted, that affects proxy. The modified game based PRS of (Hong and Long [20]) called as Novel Unidirectional PRS (NU-PRS) gives normal behavior of proxy through security provisioning to original signature and re-signature in any case of users. Original signature does not change even in case of exposure of a re-sign key. The security of PRS in mobile ad hoc network nodes is provided through mobile agents that have secret sharing and threshold PRS. It is flexible and secure authorization of mobile ad hoc nodes without pairing operations for re-signing and few public parameters but has time consuming pairing operation for verifying the re-signature. Authorized nodes can represent the CA.

The delegator delegates his signing right. Threshold PRS with privacy (SR-THPRS) to n-delegatees wherein at least t-delegatees and a proxy are involved to re-sign (Chen and Lin [9]). The re-signature is designated verifiable by the transformer. The PRS consists of different polynomial time algorithms, which provide secure transmission of keys. Two algorithms among them are not explicitly used: registration for registering delegator with proxy and ASign for signing message by delegator himself. The privacy of the delegatee is considered in the scenario involving multiple delegatees.

As existing Threshold PRS uses bilinear maps that are more time consuming than exponentiation operation, threshold proxy re-signature proposed in (Chen et al. [11]) and combines (k, n) threshold secret sharing (Blaze, Bleumer and Strauss [3]) and the proxy re-signature (Ivan and Dodis [26]). It gives El-Gamal-like solution for threshold proxy re-signature by extending the group-originated Threshold PRS scheme of (Harn [19]) for unidirectional and bidirectional features. The difference lies in the flexible construction using standard cryptographic primitives such as El-Gamal signatures based on discrete logarithm problems. Hence, we do not include this in our comparison table wherein we compare

all PKI-based PRS in terms of standard PRS properties. It requires less computational cost compared to the schemes constructed with bilinear maps.

Table 5 compares the above discussed threshold PRS in terms of comparison parameters given in Table 1.

Table 5. Comparison of threshold PRS

PRS	U/B	S/M	Pu/Pr	T	KO	NI	NT	T	SbA	ROM/SSM	CC_S	CC_V	CC_{RS}
THPRS-1 (Yang, Cao and Dong [37]) (Yang, Cao and Dong [62])	U	M	Pr	Yes	Yes	No	No	No	Constructed in bilinear groups, and proven secure under the CDH assumption.	SSM	4E	3P	4E+3P
THPRS-2 (Yang, Cao and Dong [37]) (Yang, Cao and Dong [62])	B	M	Pu	Yes	Yes	Yes	Yes	Yes	CDH and 2-DL assumptions	ROM	H+S+E+M	2P+H+E	E+2P+H
FTPRS (Xiaodong Yang et al. [59])	B	M	Pr	Yes	Yes	Yes	No	Yes	CDH in bilinear groups	SSM	4E	2P+E	4E+2P
THPRS-PKI (Yang and Wang [63])	B	M	Pr	Yes	Yes	Yes	Yes	Yes	CDH in bilinear groups	SSM	3E+S	2P+2E	4E+2P
FTPRS-b (Yang et al. [67])	B	M	Pu	Yes	Yes	Yes	No	Yes	CDH in bilinear groups	SSM	4E	2P	4E+S
FTPRS-u (Yang et al. [67])	U	M	Pu	Yes	Yes	Yes	No	Yes	CDH in bilinear groups		4E	5P	6E+S+3P
NU-PRS (Hong and Long [20])	U	S	Pr	Yes	Yes	Yes	Yes	Yes	CDH	ROM	H+S+2E	H+S+3P	5E+H+S
SR-THPRS (Chen and Lin [9])	U	S	Pr	Yes	Yes	Yes		Yes	CDH with bilinear map	ROM	H+2E+S	2P+H+2E	3P+2E

3.1.5. Conditional delegation-based PKI PRS

Some papers use delegates to re-sign to the next proxy in the chain to support multi-use property based on the condition. We discuss such papers in this section.

Unidirectional security against static corruption from (Shao et al. [42]) is used in (Vivek and Balasubramanian [50]) to propose Controlled PRS (CPRS) that incorporate conditions (chosen condition attack). Initially corrupted and uncorrupted users are decided in the game between them and adversary. The challenger in the game proves the security of system training and allows adversaries to query various oracles of the system such as Corrupted Key Generation Oracle, Uncorrupted Key Generation Oracle, ReKey Oracle, Uncorrupted Signature Oracle, Re-Signature Oracle considering its limited computation power. It is secure if the adversary comes up with a valid forgery with respect to a condition and a message for an uncorrupted use. However, complexity certificate management and overhead signature verification time limits its functionality.

In Proxy Re-signature Supporting Conditional Delegation (or conditional proxy re-signature) (PRS-CD), the delegate needs not to change its own signature algorithm to support the conditional delegation (Wang [53]). It uses Waters Hash Function and fixed randomness for conditional delegation. It easily achieves the message-based fine-grained delegation and the non-transferable property. Complexity of certificate management and overhead signature verification time limits its functionality.

Owner of WSN employs conditional PRS proposed for the online code dissemination in (Xie et al. [61]) to authorize different tenants for fine-grained accessing privilege of special sub-network. Owner is acting as a proxy to generate a conditional proxy re-signature key for that tenant using cryptographic algorithms.

Tenant verifies the digital re-signature of message m. As this conditional PRS is based on specific constraints of WSN tenants without focusing on the historical proposal of PKI based PRS, we do not include this in our comparison table wherein we compare all PKI-based PRS in terms of standard PRS properties.

Universally composable secure PRS (UCS-PRS) given in (Hong et al. [22]) maintain the protocol security within any context using the universal composability (UC) framework of (Canetti Ran [7]). Game based security definition is similar to (Shao et al. [42]) but does not restrict the corruption of proxies in presence of corrupted and uncorrupted parties. The delegator's and the delegatee's signing keys are protected during the security provisioning. Even though it is secure under the game-based definition while being guaranteed the composition properties, complexity of certificate management and overhead signature verification time limits its functionality.

Table 6 compares the above-discussed Conditional delegation-based PKI PRS in terms of comparison parameters given in Table 1.

Table 6. Comparison of Conditional delegation-based PKI PRS

PRS	U/B	S/M	Pu/Pr	T	KO	NI	NT	T	Cryptography	SbA	ROM/SSM	CC_S	CC_V	CC_{RS}
CPRS (Vivek and Balasubramanian [50])	U	S	Pr	Yes	Yes	Yes	Yes	No	conditional delegation	CDH in bilinear groups	ROM	S+2H	S+4H	4H+S
PRS-CD (Wang [53])	U	M	Pr	Yes	Yes	No	Yes	No	conditional delegation	3-linear map	ROM	4E+H	H+P+2E	2E+P+H
UCS-PRS (Hong et al. [22])		S	Pr	Yes	Yes	Yes	Yes	No	conditional delegation-universal composability	CDH in bilinear groups	ROM	S+2E+H	4E+M+2P	3+SE

3.2. ID-based PRS

This subsection explains the detailed survey of the ID based PRS collected research. We do not consider standard eight properties expected for PRS while discussing general research analysis of the paper but compare them at the end of each category description.

Bidirectional-ID-based PRS (BIDPRS) of (Xiaoming Hu, Zhe Zhang and Yinchun Yang [60]) uses Gentry's identity-based encryption (Gentry [5]) and Hierarchical Identity Based Signature (HIBS) (Au, Liu and Yuen [32]) for optimal signature size and computation. It has the following advantages. (1) Achieves optimal signature size. 2) Optimal computation doesn't need additional algorithm or process to re-signature. 3) Unforgeable in the standard model with a tight security reduction. It has exponential time complexity -four computationally expensive bilinear pairings and security rely on strong difficult problem assumptions.

THPRS-ID (Yang and Wang [63]) is described in a PKI survey.

The Unidirectional ID Based PRS (UIBPRS) scheme (Shao et al. [44]) is based on probabilistic polynomial time algorithms used in (Libert and Vergnaud [31]) and Schnorr's signature (Schnorr [6]). The private keys based on the delegator and delegatee identity are extracted for its usage in unidirectional to translate the delegatee signature to delegator signature. This UIBPRS is initially proposed for single use then modified for multi-use. It has less computation cost and

shorter signature size. It lacks batch verification for reduction in storage and computation cost minimization. 3 pairings in verify algorithm.

The Single Use and unidirectional PRS (SU-PRS) of (Sree Vivek et al. [41]) converts the PKI-based signature of a user to the ID-based signature of the same user using appropriate security model of the problem in random oracle model using PKI based signature scheme of (Dan Boneh, Ben Lynn and Hovav Shacham [14]). Re-signature key is generated from the private key used in PKI and identity of the user. It has defined the security notions and proved the security of the scheme assuming the hardness of the CDH problem in the random oracle model at the cost of four pairings for verification.

Unidirectional ID-based PRS (UID-PRS) of (Menon [34]) discusses the flaws of (Xiaoming Hu, Zhe Zhang and Yinchun Yang [60]) with respect to the Delegator Security violation wherein delegator is honest while proxy and delegatee are colluding to obtain the private key of the delegator and Delegatee Security violation wherein delegate is honest while proxy and delegator is colluding to obtain the private key of the delegatee. Based on the private key, the signature can be generated in either case. The authors of (Menon [34]) propose the solution to these flaws by inducing randomness in the proxy rekeying value using only two of the computationally expensive bilinear pairings.

Six algorithms of Identity-Based Proxy Re-Signature (IBPRS) are system setup to define system parameters such as cyclic group for master secret key with hash function, private key extracting from KGC, generating proxy re-private key from delegator and delegatee private keys, generating signature on message at signer using his private key extracting from KGC, generating re-signature using proxy re-private key and signature verifying at receiver (Huang et al. [24]). Authors of (Hu et al. [23]) modify signature algorithm in this scheme and its aggregate re-sign version as those are not secure. The re-sign algorithm remains the same as in (Huang et al. [24]). It reduces the computational complexity. Signature can be forged without knowing the signer private key.

Arbitrary-sized set of re-signature aggregation using unrestricted aggregate property used in (Wang and Xia [54]) reduces the communication cost in bidirectional ID-based PRS which utilizes full domain hash structure from multi-linear map (Hohenberger, Sahai and Waters [39]). This ID-based PRS with Aggregate Property (IPRS-AP) neither rogues proxy nor allows outside attacker to forge a user signature. Even though it uses unrestricted aggregation to reduce communication cost, it requires numerous system parameters.

Identity-based PRS from Lattice assumptions (IPRS-L) is the first quantum age related scheme that is proven secure under conventional Small Integer Solution (SIS) assumption (Tian [49]). SIS lattice assumption is as hard as approximating several standard lattice problems and intractable even for quantum computers. SampleMat algorithm of (MiaomiaoTian and Liusheng Huang [35]) is employed to extract the user's secret key. Even though it is unforgeable under adaptive chosen message and identity attacks, the size of the signature and secret key is relatively large.

ID-based proxy re-signature without pairing for cloud computing applications is an attractive solution due to processing and power constraints of mobile devices used by a huge number of cloud users (Wang, Xia and He [55]). Quadratic residues are used instead of costly pairing operations similar to (Chai Zhenchuan, Cao Zhenfu and Dong Xiaolei [8]). Interactive and non-interactive versions are proposed for this cloud environment. Computation of re-signature key involves the interaction with the delegate in interactive version while no interaction involved in the non-interactive version. Advantages include no pairing operations and unforgeability with respect to adaptive chosen message and identity attacks while any one can fabricate a signature on arbitrary data.

Identity-Based Blind Proxy Re-Signature Scheme for Data Security (IDBPRS) (Yang et al. [64]) protects data in addition to signature conversion based on PRS of (Shao et al. [43]). The difference between (Pedersen [48]) and (Wang [52]) lies with data security provisioning. No data security is provided in (Wang [52]). Neither Signer nor proxy can obtain details of messages to be signed. It improves signature length and computational cost compared to (Wang [52]).

Existing identity based PRS do not have key revocation functionality for dynamic user management towards removal of compromised users. Revocable Identity-Based Proxy Re-Signature (RIDPRS) and Server-Aided Revocable Identity-Based Proxy Re-Signature (SA-RIDPRS) proposed in (Yang et al. [64]) considers key revocation based on PRS of (Shao et al. [43]). It divides PKG's master key into two parts. Fixed secret keys are generated based on one part of this master key while PKG periodically updates the private keys of non-revoked users based on another part of its master key. Re-sign key is generated from non-revoked user's secret key using re-randomization concept. SA-RIDPRS reduces computational operations at verifiers with limited computing power by relocating the computation on the server with powerful computing capabilities. It is unforgeable against adaptive chosen identity and message attacks.

Non-interactive pairing-free ID-based PRS (NI-PF-IPRS) of (Zhang, Bai and Wang [72]) achieves identity-based privacy and relieves the burden of the end user by avoiding expensive pairing operation and complex certificate management without interacting with other users. It is provably secure under integer factoring problem eg. RSA assumption. Security model used is similar to (Yang et al. [64]) and (Lee and Kim [29]) for showing provable internal and external security. It is secure against inside attack and outside attack in the Ateniese-Hohenberger security model.

Lightweight PRS of (Wang, Xia and He [55]) for resource-constrained devices is analyzed for forgery attacks in (Zhang [71]) with the proposal on improved PRS (IPRS-NP) to address the attacks. Anyone can fabricate the delegatee's signature or the delegator's signature (re-signature) of (Wang, Xia and He [55]). Additionally, delegator's private key leakage exists in non-interactive PRS of (Wang, Xia and He [55]). Random number is introduced during the generation process of re-signing keys to avoid such leakage/attacks. It has the following advantages: no pairing operation, secure against EUF-CID-MA and resist private key leakage of the delegator under the condition that the proxy colludes the delegate.

However, it takes more exponential and multiplicative operations during the computations.

Table 7 compares the above-discussed ID-based PRS in terms of comparison parameters given in Table 1.

Table 7. Comparison of ID-based PRS

PRS	U/B	S/M	Pu/Pr	T	KO	NI	NT	T	Cryp	SbA	ROM/SSM	CC_S	CC_V	CC_{RS}
BIDPRS (Xiaoming Hu, Zhe Zhang and Yinchun Yang [60])	B	M	Pr	Yes	Yes	Yes	No	Yes	ID	q-SDH (Strong DH) assumption	SSM	6E	4E+3P	6E+3P
THPRS-ID (Yang and Wang [63])	B	M	Pr	Yes	Yes	Yes	Yes	Yes	ID	CDH in bilinear groups	SSM	3E	2P	6E+2P
UIBPRS (Shao et al. [44])	U	M	Pr	Yes	Yes	Yes	Yes	No	ID	extended CDH	ROM	E+H	2P+E+2H	4E+H
SU-PRS (Sree Vivek et al. [41])	U	S	Pr	Yes	Yes	No	Yes	No	ID	CDH in bilinear groups	ROM	H+S(PKI)/ 2H+S(IDB)	P+H(PKI)/3P+ 2H(IDB)	S
UID-PRS (Menon [34])	U	M	Pr	Yes	Yes	Yes	No	Yes	ID	CDH and Decisional Bilinear DH	SSM	H+S+P	H+2P+S	2P+S+4H
IBPRS (Huang, Yang, Li and Wang [24]) (Hu et al. [23])	B	S	Pr	Yes	Yes	Yes	Yes	No	ID	discrete logarithmic problem	ROM	3E+H	2H+P	NONE
IPRS-AP (Wang and Xia [54])	B	M	Pr	Yes	Yes	No	Yes	No	Id	multi-linear maps CDH	ROM	Multiple P	Multiple P	NONE
IPRS-L (Tian [49])	B	M	Pr		Yes	No	Yes		Id	lattice assumption - small integer solution	ROM	E=H+S	2H+S	S
Interactive USIPRS (Wang, Xia and He [55])	U	S	Pr	Yes	Yes	No	Yes	No	ID	factoring for quadratic residues	ROM	2E+S	2E+S	3E+S
Non-interactive USIPRS (Wang, Xia and He [55])	U	S	Pr	Yes	Yes	Yes	Yes	No	ID	factoring for quadratic residues	ROM	2E+S	2E+S	3E+3S
IDBPRS (Yang et al. [64])	B	M	Pr	Yes	Yes	Yes	Yes	No	ID	CDH in bilinear groups	SSM	2E	4P	4P+2E
	B	M	Pr	Yes	Yes	Yes	Yes	No	ID		SSM	6E	4P+4E	4P+7E
RIDPRS (Yang et al. [64])	B	M	Pr	Yes	Yes	No	Yes	No	ID	CDH in bilinear groups	SSM	2E	4P	2E+4P
SA-RIDPRS (Yang et al. [64])	B	M	Pr	Yes	Yes	No	Yes	No	ID	CDH in bilinear groups	SSM	2E	4E+P	6E+P
NI-PF-IPRS (Zhang, Bai and Wang [72])	U	S	Pr	Yes	Yes	Yes	Yes - 2 Level	Yes	special properties	integer factoring problem	ROM	3E+2H	3E+2H	4E
IPRS-NP (Zhang [71])	U	S	Pr	Yes	Yes	No	Yes	No	ID	integer factoring for quadratic residues	ROM	3E+2S	3E+2S	3E+S

3.3. CL-PRS

This subsection explains the detailed survey of the certificateless PRS collected research. We do not consider standard eight properties expected for PRS while discussing general research analysis of the paper but compare them at the end of each category description.

The first certificateless PRS scheme, named as $S_{cl,}$ proposed in (Guo et al. [18]) uses certificateless cryptography to solve certificate management problem of PKI based PRS and key escrow problem of ID based PRS. The required public key is

generated from the identity of the user at key generator centre through the computation of the partial private key. Re-sign key is generated from the public key of the involved users in the same way as previous schemes. It provides a solution to the public key replacement and malicious key generator attack. Its Security Analysis provides Correctness, Unforgeable, and External Security. KGC computation is an overhead. Security proof is not given.

The authors of (Xiao and Zhang [58]) provide a solution to the key escrow problem of ID – based PRS and certificate management problem of PKI based PRS through the usage of certificateless public cryptosystem in PRS for addressing public key replacement attack and malicious KGC attack. It is similar to the certificateless PRS of (Guo et al. [18]). The authors do not discuss why to call provably secure PRS.

The author of (Chen et al. [10]) consider flaws of first CL-PRS of (Guo et al. [18]) and CL-blind-PRS of (Feng and Liang [16]) to propose S_{clm} in standard model. They claim that first CL-PRS of (Guo et al. [18]) does not have security proof while CL-blind-PRS of (Feng and Liang [16]) does not provide security to re-key. We do not consider (Feng and Liang [16]) in our survey, as it is not available in the standard database. They propose unforgeable CL-PRS denoted as S_{clm} in standard model using six probabilistic polynomial time algorithms to overcome the deficiencies. It considers replacing the public key without master key and access master key without key replacement adversary with different capabilities. It has the following advantages. 1) Solve the key escrow problem, the complexity management of certificates and has the signature transfer faction. 2) Compared to the existing schemes, it is rather superior in security and efficiency. It takes more time compared with earlier schemes.

Promising Multi-use unidirectional certificateless PRS (MU-CL-PRS) (Wu, Xiong and Jin [57]) is suitable for long signing chains of untrusted user's communication with simple entry of each user to reduce the cost. It achieves unidirectional and multi-use features. The authors discuss the security model of two adversaries' interactive games to prove the less computational cost and communication overhead – malicious third party who can use public key without the master secret key and compromised KGC. It is unforgeable against adaptive chosen message attacks.

Unidirectional certificateless proxy re-signature scheme developed as an independent interest in lightweight and privacy-preserving authentication protocol for mobile payment in the context of IoT (Chen et al. [12]). It proves secure under eCDH assumption in the random oracle model. We do not include this in our comparison table wherein we compare all PKI-based PRS in terms of standard PRS properties. It needs one exponentiation plus two hash operations in sign phase, two bilinear plus two exponentiation operations in verification phase and five exponentiation operators for resigning phase.

Table 8 compares the above-discussed certificateless PRS in terms of comparison parameters given in Table 1.

Table 8. Comparison of certificateless PRS

PRS	U/B	S/M	Pu/Pr	T	KO	NI	NT	T	Cryp	SbA	ROM/SSM	CC_S	CC_V	CC_{RS}
Scl (Guo et al. [18])	B	M	Pr	Yes	Yes	Yes	No	No	CL-PKS	CDH in bilinear groups	SSM	4E+H	4P+H	4E
S_{clm} (Chen et al. [10])	B	M	Pr	Yes	Yes	Yes	Yes	No	CL-PK	CDH with bilinear map	SSM	4E	4P	4E
(MU-CL-PRS (Wu, Xiong and Jin [57])	U	S	Pr	Yes	Yes	Yes	Yes	Yes	CL	eCDH with bilinear pair	ROM	3E+3H	4P +2E+3H	3E

4. Discussion on scope of research in PRS

PRS relieves issues of key management. Although various articles exist in the literature so far in the area of PRS addressing the various issues, there are still some areas that need to be further investigated. These sections discuss the trends and issues in the PRS and provide directions to researchers for promoting their contributions in this area in future.

Recent proposals on PRS formalize security definitions and desirable properties of PRS. PKI-based PRS uses a bounded public key of user with corresponding identity in digital certificate that is issued by CA. As mentioned earlier, it incurs heavy overhead through the certificate distribution, management including revocation, storage and computational cost of certificate verification that limits its uses. There is scope for researchers to reduce this overhead of PKI in PRS. Many PKI based PRS use CDH assumption with bilinear pairing which increases computational cost. Researchers can work on reduction of this cost.

Usage of identity for public key generation at PKG reduces the overhead to certain extent in ID-based PRS. User private keys are generated by PKG using the user's identity that is available with PKG. Even though the need for certificates is eliminated in ID-PRS, it introduces key escrow problems due to PKG dependency requirement for private key generation. ID-PRS cannot offer non-repudiation as PKG can forge any user’s signature in the way that PKI-based PRS can. Usage of threshold or multiple PKG helps to solve the key escrow problem at the extra communication and infrastructure. Compromise of PKG’s master key could be a disaster in ID-based PRS compared to compromise of CA’s signing key in PKI-based PRS. Researchers have scope to improve on these issues of ID-based PRS with the support of the standard PRS properties.

Very little research exists in CL-PRS that neither requires certificates nor have built-in key escrow. User’s private key is based on the secret value selected by that user in CL-PRS. Semi-trusted proxy generates the partial private key to tackle key escrow problems. Key replacement and malicious KGC attacks affect the CL-PRS. Researchers have scope towards addressing these attacks.

5. Conclusions

The PRS scheme was initially designed in 1998 by Blaze, Bleumer, and Strauss for translating a signature on a message from Alice into a signature from Bob on the same message at a semi trusted proxy which does not learn any signing key and cannot produce any new valid signature on new message for Alice or Bob. It had been largely ignored from then but recently it has spurred considerable research interest due to useful features for sharing web certificates, forming weak group signatures, and authenticating a network path. We presented taxonomy and classification of PRS-related articles, which clearly shows that PRS has considerable potential for application in diverse fields of security applications. The proposed taxonomy has proved a convenient means of grouping the available PRS research and giving insight on its contribution in terms of standard properties supported in the PRS scheme, security environment and research approach used. This survey explored published research works in greater depth related to the exploitation of features with respect to cryptographic approach demotions in our taxonomy as a basis for the discussion.

References

1. Shamir, A. How to Share a Secret. – Communication of the ACM, Vol. **22**, 1979, No 11, pp. 612-613.
2. Ateniese, G., S. Hohenberger. Proxy Re-Signatures: New Definitions, Algorithms, and Applications. – In: Proc. of 12th ACM Conference on Computer and Communications Security, ACM, November 2005, pp. 310-319.
3. Blaze, M., G. Bleumer, M. Strauss. Divertible Protocols and Atomic Proxy Cryptography. – In: Proc. of International Conference on the Theory and Applications of Cryptographic Techniques, Berlin, Heidelberg, Springer, May 1998, pp. 127-144.
4. Waters, B. Efficient Identity-Based Encryption without Random Oracles. – In: Proc. of Eurocrypt'05, LNCS 3494, Springer, 2005, pp. 114-127.
5. Gentry, C. Practical Identity-Based Encryption without Random Oracles. – In: Proc. of EUROCRYPT'06, LNCS 4404, Springer-Verlag, 2006, pp. 445-464.
6. Schnorr, C. P. Efficient Identifications and Signatures for Smart Cards. – In: Proc. of CRYPTO'98, LNCS, Vol. **435**, 1998, pp. 239-251.
7. Canetti, Ran. Universally Composable Security: A New Paradigm for Cryptographic Protocols. – In: Proc. of 42nd IEEE Symposium on Foundations of Computer Science, IEEE, 2001.
8. Chai, Zhenchuan, Cao Zhenfu, Dong Xiaolei. Identity Based Signature Scheme Based on Quadratic Residues. – Science in China Series F: Information Sciences, Vol. **50**, 2007, No 3, pp. 373-380.
9. Chen, K. Y., H. C. Lin. Threshold Proxy Re-Signature Scheme with Privacy. – International Journal of Computer and Electrical Engineering, Vol. **5**, 2013, No 1, p. 98.
10. Chen, L., X. Chen, Y. Sun, X. Du. A New Certificateless Proxy Re-Signature Scheme in the Standard Model. – In: Proc. of 7th International Symposium on Computational Intelligence and Design, IEEE, Vol. **1**, 2014, pp. 202-206.
11. Chen, X., Y. Liu, L. Harn, Y. Li, G. Yao. Threshold Proxy Re-Signature: Definition and New Constructions. – Journal of the Chinese Institute of Engineers, Vol. **41**, 2018, No 2, pp. 141-148.
12. Chen, Y., W. Xu, L. Peng, H. Zhang. Light-Weight and Privacy-Preserving Authentication Protocol for Mobile Payments in the Context of IoT. – IEEE Access, Vol. **7**, 2019, pp. 15210-15221.

13. C h o w, S. S., R. C. W. P h a n. Proxy Re-Signatures in the Standard Model. – In: Proc. of International Conference on Information Security, Berlin, Heidelberg, Springer, September 2008, pp. 260-276.
14. B o n e h, D a n, B e n L y n n, H o v a v S h a c h a m. Short Signatures from the Weil Pairing. – Journal of Cryptology, Vol. **17**, 2004, No 4, pp. 297-319.
15. B o n e h, D a n, E m i l y S h e n, B r e n t W a t e r s. Strongly Unforgeable Signatures Based on Computational Diffie-Hellman. – In: Public Key Cryptography. Vol. **240**. 2006. 229 p.
16. F e n g, T., Y. X. L i a n g. Provably Secure Certificate Less Blind Proxy Re-Signatures. – Journal on Communications, Vol. **31**, 2012, No S1, pp. 58-69.
17. F u c h u n, G u o, Y i M u, W i l l y S u s i l o. How to Prove Security of a Signature with a Tighter Security Reduction. – In ProvSec. Vol. **103**. 2009. 90 p.
18. G u o, D., W. P i n g, Y. D a n, Y. X i a o y u a n. A Certificateless Proxy Re-Signature Scheme. – In: Proc. of 3rd IEEE International Conference on Computer Science and Information Technology, Vol. **8**, 2010, pp. 157-161.
19. H a r n, L. Group-Oriented (t, n) Threshold Digital Signature Scheme and Digital Multisignature. – IEE Proceedings-Computers and Digital Techniques, Vol. **141**, 1994, No 5, pp. 307-313. DOI:10.1049/ip-cdt:19941293.
20. H o n g, X., Y. L o n g. A Novel Unidirectional Proxy Re-Signature Scheme and Its Application for MANETs. – Journal of Computers, Vol. **7**, 2012, No 7, pp. 1796-1800.
21. H o n g, X., J. G a o, Z. W a n. Unidirectional Multiple-Times Proxy Re-Signature Scheme. – Information Technology Journal, Vol. **12**, 2013, No 17, pp. 4063-4067.
22. H o n g, X., J. G a o, J. P a n, B. Z h a n g. Universally Composable Secure Proxy Re-Signature Scheme with Effective Calculation. – Cluster Computing, 2017, pp. 1-10.
23. H u, X., Y. L i u, H. X u, J. W a n g, X. Z h a n g. Analysis and Improvement of Certificateless Signature and Proxy Re-Signature Schemes. – In: Proc. of IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC'15), December 2015, pp. 166-170.
24. H u a n g, P., X. Y a n g, Y. L i, C. W a n g. Identity-Based Proxy Re-Signature Scheme without Bilinear Pairing. – Journal of Computer Applications, Vol. **35**, 2015, No 6, pp. 1678-1682.
25. H u i x i a n, L., H. Z h i p e n g, W. L i q i n, P. L i a o j u n. Blind Proxy Re-Signature Scheme Based on Isomorphisms of Polynomials. – IEEE Access, Vol. **6**, 2018, pp. 53869-53881.
26. I v a n, A. A., Y. D o d i s. Proxy Cryptography Revisited. – In: Proc. of 10th Network and Distributed System Security Symposium, Washington, DC: The Internet Society, San Diego, CA, 6-7 February 2003, pp. 514-532.
27. J a k o b s s o n, M., K. S a k o, R. I m p a g l i a z z o. Designated Verifier Proofs and Their Applications. – In: Advances in Cryptology – EUROCRYPT. Springer, 1996, pp. 143-154.
28. J i a n g, M., J. H o u, Y. G u o, Y. W a n g, S. W e i. An Efficient Proxy Re-Signature over Lattices. – In: Proc. of International Conference on Frontiers in Cyber Security, Singapore, Springer, November 2019, pp. 145-160.
29. L e e, E., S. W. K i m. Non-Interactive Conditional Proxy Re-Signature in the Standard Model. – The Computer Journal, Vol. **61**, 2018, No 12, pp. 1772-1782.
30. L e i, Y., M. H u, B. G o n g, L. W a n g, Y. C h e n g. A One-Way Variable Threshold Proxy Re-Signature Scheme for Mobile Internet. – In: Proc. of International Conference on Security and Privacy in New Computing Environments, Cham., Springer, April 2019, pp. 521-537.
31. L i b e r t, B., D. V e r g n a u d. Multi-Use Unidirectional Proxy Re-Signatures. – In: Proc. of ACM Conference on Computer and Communications Security, 2008, pp. 511-520.
32. A u, M., J. L i u, T. Y u e n. Practical Hierarchical Identity Based Encryption and Signature Schemes without Random Oracles. 2006.
http://eprint.iacr.org/2006/368
33. M a m b o, M., K. U s u d a, E. O k a m o t o. Proxy Signatures: Delegation of the Power to Sign Messages. – IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. **79**, 1996, No 9, pp. 1338-1354.
34. M e n o n, T. An Identity Based Proxy Re-Signature Scheme. – International Journal of Engineering and Technology, Vol. **4**, 2012, No 3, p. 303.
35. M i a o m i a o, T i a n, L i u s h e n g H u a n g. Efficient Identity-Based Signature from Lattices. – In: Proc. of IFIP SEC, Springer, 2014, pp. 321-329.

36. S u n i t h a, N. R., B. B. A m b e r k e r. Multi-Use Unidirectional Forward-Secure Proxy Re-Signature Scheme. Department of Computer Science and Engg., Siddaganga Institute of Technology, Tumkur, Karnataka, India, 2009.
37. Y a n g, P., Z. C a o, X. D o n g. Threshold Proxy Re-Signature. – In: Proc. of Performance, Computing and Communications Conference (IPCCC'08), 2008, pp. 450-455.
38. G e n n a r o, R., S. L. J a r e c k i, H. K r a w c z y k, T. R a b i n. Secure Distributed Key Generation for Discrete-Log Based Cryptosystems. – Advances in Cryptology-Eurocrypt'99, LNCS. Vol. **1592**. 1999, pp. 295-310.
39. H o h e n b e r g e r, S., A. S a h a i, B. W a t e r s. Full Domain Hash from (Leveled) Multilinear Maps and Identity-Based Aggregate Signatures. – In: Proc. of 34th International Conference of Cryptology, Vol. **1**, 2013, pp. 494-512
40. T a n g, S., L. X u. Proxy Signature Scheme Based on Isomorphisms of Polynomials. – In: Proc. of Network and System Security (Lecture Notes in Computer Science). Vol. **7645**. Heidelberg, Germany, Springer, 2012, pp. 113-125.
41. V i v e k, S. S r e e, S. S h a r m i l a D e v a S e l v i, C. P a n d u R a n g a n. A Special Purpose Proxy Re-Signature Scheme. Department of Computer Science and Engineering, Indian Institute of Technology, Chennai, India, 2012.
42. S h a o, J., M. F e n g, B. Z h u, Z. C a o, P. L i u. The Security Model of Unidirectional Proxy Re-Signature with Private Re-Signature Key. – In: R. Steinfeld, P. Hawkes, Eds. Information Security and Privacy. ACISP 2010. Lecture Notes in Computer Science. Vol. **6168**. Berlin, Heidelberg, Springer, 2010,
43. S h a o, J., Z. C a o, L. W a n g, X. L i a n g. Proxy Re-Signature Schemes without Random Oracles. – In: Proc. of International Conference on Cryptology in India, Springer, Berlin, Heidelberg, December 2007, pp. 197-209.
44. S h a o, J., G. W e i, Y. L i n g, M. X i e. Unidirectional Identity-Based Proxy Re-Signature. – In: Proc. of IEEE International Conference on Communications, (ICC'11), 2011, pp. 1-5.
45. S n e h a, K a n c h a n, N a r e n d r a S. C h a u d h a r i. SRCPR: SignReCrypting Proxy Re-Signature in Secure VANET Groups. Department of Computer Science and Engineering, IIT Indore, Indore 453552, India, 2018.
46. S u n i t h a, N. R., B. B. A m b e r k e r. Proxy Re-Signature Scheme that Translates One Type of Signature Scheme to Another Type of Signature Scheme. – In: Proc. of International Conference on Network Security and Applications, Berlin, Heidelberg, Springer, July 2010, pp. 270-279.
47. S u n i t h a, N. R., B. B. A m b e r k e r. Proxy Re-Signature Schemes: Multi-Use, Unidirectional & Translations. – Journal of Advances in Information Technology, Vol. **2**, 2011, No 3, pp. 165-176.
48. P e d e r s e n, T. P. Distributed Provers with Applications to Undeniable Signatures. – In: Proc. of Rurocrypt'91, LNCS, Vol. **547**, 1991, pp. 221-238.
49. T i a n, M. Identity-Based Proxy Re-Signatures from Lattices. – Information Processing Letters, Vol. **115**, 2015, No 4, pp. 462-467.
50. V i v e k, S. S., G. B a l a s u b r a m a n i a n. Controlled Proxy Re-Signing-Conditional Proxy Re-Signatures. – In: Proc. of 12th International Joint Conference on e-Business and Telecommunications (ICETE'15), Vol. **4**, July 2015, pp. 186-193.
51. V i v e k, S. S., S. S. D. S e l v i, G. B a l a s u b r a m a n i a n, C. P. R a n g a n. Strongly Unforgeable Proxy Re-Signature Schemes in the Standard Model. – IACR Cryptology ePrint Archive, 2012, p. 80.
52. W a n g, W. An Identity-Based Blind Proxy Re-Signature Scheme. – Computer Applications and Software, Vol. **29**, 2012, No 10, pp. 308-309.
53. W a n g, X. Proxy Re-Signature Supporting Conditional Delegation. – In: Proc. of 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2015, pp. 844-848,
54. W a n g, Z., A. X i a. ID-Based Proxy Re-Signature with Aggregate Property. – Journal of Information Science and Engineering, Vol. **31**, 2015, No 4, pp. 1199-1211.
55. W a n g, Z., A. X i a, M. H e. ID-Based Proxy Re-Signature without Pairing. – Telecommunication Systems, Vol. **69**, 2018, No 2, pp. 217-222.

56. W e i, J., G. Y a n g, Y. M u. Designated Verifier Proxy Re-Signature for Deniable and Anonymous Wireless Communications. – Wireless Personal Communications, Vol. **97**, 2017, No 2, pp. 3017-3030.
57. W u, Y., H. X i o n g, C. J i n. A Multi-Use Unidirectional Certificateless Proxy Re-Signature Scheme. – Telecommunication Systems, 2019, pp. 1-13.
58. X i a o, H., M. Z h a n g. Provably-Secure Certificateless Proxy Re-Signature Scheme. – In: Proc. of International Conference on Intelligent Networking and Collaborative Systems, 2013, pp. 591-594.
59. X i a o d o n g, Y a n g, C a i f e n W a n g, Y u l e i Z h a n g, W e i y i W e i. A New Forward-Secure Threshold Proxy Re-Signature Scheme. College of Mathematics and Information Science, Northwest Normal University, Lanzhou 730070, China, 2009.
60. X i a o m i n g, H u, Z h e Z h a n g, Y i n c h u n Y a n g. Identity Based Proxy Re-Signature Schemes without Random Oracle. School of Computer & Information Shanghai Second Polytechnic University Shanghai, China, 2009.
61. X i e, M., U. B h a n j a, J. S h a o, G. Z h a n g, G. W e i. LDSCD: A Loss and DoS Resistant Secure Code Dissemination Algorithm Supporting Multiple Authorized Tenants. – Information Sciences, Vol. **420**, 2017, pp. 37-48.
62. Y a n g , P., Z. C a o, X. D o n g. Threshold Proxy Re-Signature. – Journal of Systems Science and Complexity, Vol. **24**, 2011, No 4, pp. 816-824.
63. Y a n g, X., C. W a n g. Threshold Proxy Re-Signature Schemes in the Standard Model. – Chinese Journal of Electronics, Vol. **19**, 2010, No 2E, pp. 345-350.
64. Y a n g, X., C. C h e n, T. M a, J. W a n g, C. W a n g. Revocable Identity-Based Proxy Re-Signature against Signing Key Exposure. – PloS One, Vol. **13**, 2018, No 3, p. e0194783.
65. Y a n g, X., C. L i, Y. L i, S. Z h o u, C. W a n g. Divisible On-Line/Off-Line Proxy Re-Signature. – Applied Mathematics and Information Sciences, Vol. **9**, 2015, No 2, p. 759.
66. Y a n g, X., L. X i a o, Y. L i, S. L i, J. W a n g, C. C h e n. Identity-Based Blind Proxy Re-Signature Scheme for Data Security. – In: Proc. of 3rd IEEE International Conference on Data Science in Cyberspace, 2018, pp. 28-32.
67. Y a n g, X. D., C. F. W a n g, C. H. L a n, B. W a n g. Flexible Threshold Proxy Re-Signature Schemes. – Chinese Journal of Electronics, Vol. **20**, 2011, No 4, pp. 691-696.
68. Y a n g, X. D., L. K. X i a o, C. L. C h e n, C. F. W a n g. A Strong Designated Verifier Proxy Re-Signature Scheme for IoT Environments. – Symmetry, Vol. **10**, 2018, No 11, p. 580.
69. Y u-q i a o G u M i n g-h u i, D., Y. Z. L. E. X i a o-h u a. A Blind Proxy Re-Signatures Scheme Based on Standard Model. – Journal of Electronics & Information Technology, Vol. **5**, 2010, p. 39.
70. Y u q i a o, D., S. G e. Proxy Re-Signature Scheme Based on Quadratic Residues. – Journal of Networks, Vol. **6**, 2011, No 10, p. 1459.
71. Z h a n g, J. Improvement of ID-Based Proxy Re-Signature Scheme with Pairing-Free. – Wireless Networks, Vol. **25**, 2019, No 7, pp. 4319-4329.
72. Z h a n g, J., W. B a i, Y. W a n g. Non-Interactive ID-Based Proxy Re-Signature Scheme for IoT Based on Mobile Edge Computing. – IEEE Access, Vol. **7**, 2019, pp. 37865-37875.
73. Z h i w e i, W a n g, W e i L v. Server-Aided Verification Proxy Re-Signature. College of Computer, Nanjing University of Posts and Telecommunications, Ministry of Education Jiangsu Province Nanjing, P. R. China, 2013.

Received: 24.11.2020; Second Version: 15.05.2021; Accepted: 30.06.2021