Hindawi Publishing Corporation
Mobile Information Systems
Volume 2015, Article ID 430797, 10 pages
http://dx.doi.org/10.1155/2015/430797

Research Article

New Construction of PVPKE Scheme and Its Application in Information Systems and Mobile Communication

Minqing Zhang,[1,2] Xu An Wang,[2] Xiaoyuan Yang,[2] and Weihua Li[1]

[1]*School of Computer Science, Northwestern Polytechnical University, Xi'an 710072, China*
[2]*Key Laboratory of Information and Network Security, Engineering University of Chinese Armed Police Force, Xi'an 710086, China*

Correspondence should be addressed to Xu An Wang; wangxazjd@163.com

Received 29 August 2014; Accepted 1 September 2014

Academic Editor: David Taniar

In SCN12, Nieto et al. discussed an interesting property of public key encryption with chosen ciphertext security, that is, ciphertexts with public verifiability. Independently, we introduced a new cryptographic primitive, CCA-secure publicly verifiable public key encryption without pairings in the standard model (PVPKE), and discussed its application in proxy reencryption (PRE) and threshold public key encryption (TPKE). In Crypto'09, Hofheiz and Kiltz introduced the group of signed quadratic residues and discussed its application; the most interesting feature of this group is its "gap" property, while the computational problem is as hard as factoring, and the corresponding decisional problem is easy. In this paper, we give new constructions of PVPKE scheme based on signed quadratic residues and analyze their security. We also discuss PVPKE's important application in modern information systems, such as achieving ciphertext checkable in the cloud setting for the mobile laptop, reducing workload by the gateway between the open internet and the trusted private network, and dropping invalid ciphertext by the routers for helping the network to preserve its communication bandwidth.

1. Introduction

In modern information systems such as mobile wireless network, social network, open internet, and cloud computation, security is an important issue [1, 2]. Public key encryption [3] is among the most important basic tools to strengthen the whole system's security. Along with the development of information system, the security notion for public key encryption has been strengthened. The first proposal on public key encryption, RSA, though a great breakthrough in cryptography, only achieves the security notion of one-way security [4]. In 1984, Goldwasser and Micali [5] proposed the notion of semantic security (also known as indistinguishable security (IND-CPA)). This security notion states that the challenge ciphertext needs to contain no more information than a randomly chosen ciphertext. Although it is a reasonable security notion, many applications using public key encryption as a basic tool need stronger security notion, that is, chosen ciphertext security (IND-CCA). Compared with the semantic security notion, this security notion considers that the adversary can get help from the decryption oracle (the adversary can query the decryption oracle with his chosen ciphertexts, except the challenge ciphertext which cannot be queried). Until now, many CCA-secure PKE schemes have been proposed [6–11].

Active attackers play more and more important role in breaking the security of modern information systems [1, 2]; thus chosen ciphertext security of the encryption scheme is essential for these systems. However, if the validity can only be checked by the decrypter privately with his secret key, the whole system can easily suffer from ciphertext-malleable attack. The active attackers can easily modify the right ciphertext transferred in the network to get numerous malicious ciphertexts and thus cost the precious bandwidth greatly. Although these ciphertexts can be rejected by the decrypter at the last moment, they have already caused great problem in the systems. These problems can affect the users' feeling on using the system. Even more seriously, they cause shutting down the whole system and bring damage to the service providing corporations. If the validity of these ciphertexts can be checked publicly, the problems can be easily solved, the routers or the access infrastructure can drop

these maliciously created ciphertexts, and the bandwidth has been effectively preserved [12]. As a concrete example, can you imagine, when using mobile phone for secure instant-message talking like MSN, you always have to deal with nonsense invalid ciphertexts maliciously created by active attackers? But if the access infrastructure equipped with PVPKE can help you to filter these invalid ciphertexts, you certainly will feel better. In one word, PVPKE is an important tool for smoothly running modern information systems if these systems have employed public key encryption as a basic way to achieve security.

However, researchers give little care to the property of public verifiability of the chosen ciphertext-secure ciphertexts. In bilinear map setting or by using the random oracle, public verifiability of ciphertexts coming from an IND-CCA-secure public key encryption can be easily achieved. Thus, in this paper, we care about how to construct publicly verifiable public key encryption without pairing in the standard model. Recently, in [13], we introduced an interesting cryptographic primitive: PVPKE, defined as publicly verifiable chosen ciphertext-secure public key encryption in the standard model without pairing. PVPKE is a very powerful building block to construct some other interesting cryptographic protocols and cloud computation [14, 15]. For example, it can be used to construct chosen ciphertext-(CCA-) secure threshold public key encryption (TPKE) [16–20]. In TPKE, chosen ciphertext security always requires that the distributed decryption server can check the ciphertext's validity before decryption; otherwise some valuable information about decryption will be returned to the adversary and this will help the adversary to break the chosen ciphertext security. For another example, PVPKE can be a core block to construct chosen ciphertext-secure proxy reencryption (PRE) [21–26]. Chosen ciphertext attackers can query the delegator and delegatee's decryption oracle arbitrarily; if invalid ciphertexts forwarded by the proxy to the delegatee have been decrypted by the delegatee, the attackers can get useful information to break CCA security. Since the proxy without secret keys needs to check the validity of the ciphertext for the delegatee before reencryption, thus public verifiability of the ciphertext seems to be an essential requirement for achieving CCA security for proxy reencryption.

In SCN12, Nieto et al. [27] discussed an interesting property of public key encryption with chosen ciphertext security, that is, ciphertexts with public verifiability. They also demonstrated an important application of this new primitive, that is, "nontrivial filtering" of an incoming IND-CCA-secure ciphertext to be an IND-CPA-secure ciphertext with reduced workload by a gateway. They formally defined (nontrivial) public variability of ciphertexts for general encryption schemes, key encapsulation mechanisms, and hybrid encryption schemes, encompassing public key, identity-based, and tag-based encryption and also gave several concrete constructions. But we also note that their constructions cannot simultaneously satisfy the four requirements on "PVPKE": (1) chosen ciphertext-secure; (2) publicly verifiable; (3) in the standard model; (4) without pairing. Thus their work further explores PVPKE's application but does not give concrete construction of PVPKE.

In Crypto'09, Hofheinz and Kiltz [28] introduced the group of signed quadratic residues and discussed its application; the most interesting feature of this group is its "gap" property, while the computational problem is as hard as factoring, and the corresponding decisional problem is easy. Membership in QR_N^+ can be publicly and efficiently verified while it inherits some nice intractability properties of the quadratic residues. For example, computing square roots in QR_N^+ is also equivalent to factoring the modulus N. We therefore have a gap group, in which the corresponding decisional problem (i.e., deciding if an element is a signed square) is easy, whereas the computational problem (i.e., computing a square root) is as hard as factoring. We also can show that, in the group of signed quadratic residues, the Strong Diffie-Hellman problem is implied by the factoring assumption.

1.1. Our Contribution. In [13], based on the core idea of changing the prime modular field to the composite modular field and masking the verifying secret key with secret order of the composite group and making the resulting "pseudosecret key" public, we find it is relatively easy to construct PVPKE scheme based on the Cramer-Shoup encryption and the Hanaoka-Kurosawa CCA-secure public key encryption.

In this paper, we show that, in case of basing some of Nieto et al.'s schemes on signed quadratic residues, the resulting schemes can meet the requirements of PVPKE. The core idea about this construction is that the DDH oracle can be publicly instantiated by bilinear pairing, while DDH oracle cannot be instantiated by discrete logarithm group or RSA group. But, in signed quadratic residues, the DDH oracle can be efficiently publicly instantiated. Based on this observation, we give new constructions of PVPKE scheme based on signed quadratic residues and discuss their security.

Furthermore, we discuss PVPKE's important application in modern information system, such as achieving ciphertext checkable in the cloud setting for the mobile laptop, reducing the workload by the gateway between the open internet and the trusted private network, and dropping the invalid ciphertext by the routers for helping the network to preserve its communication bandwidth effectively.

1.2. Related Works

1.2.1. Chosen Ciphertext Security in the Standard Model. Naor and Yung [29] introduced the notion of CCA security for public key encryption, and this notion was further extended by Rackoff and Simon [30], Dolev et al. [31], and Sahai [32]. *Noninteractive zero-knowledge (NIZK) proofs* are core blocks of these constructions, which is a relatively inefficient paradigm and its efficient realization always relies on bilinear pairing or random orale. In 1993, Bellare and Rogaway [33] introduced a so-called *random oracle* which idealizes the hash function as a perfect random function to devise efficient CCA-secure public key encryption with provable security. However, random oracle model has seen criticism by cryptographers for its unrealistic assumption [34]. More and more cryptographers show interest in constructing efficient

CCA-secure PKE in the standard model. Till now, there are at least four ways to construct efficient CCA-secure PKE in the standard model. The first way is proposed by Cramer and Shoup [8], which was further extended by themselves and other cryptographers [35–37]. The second way to construct CCA-secure PKE is the paradigm of IBE *transformation*, which allows transforming selective-ID CPA-secure identity-based encryption (IBE) into a CCA-secure PKE [38–41]. The third way is based on *verifiable broadcast encryption*, which is proposed by Hanaoka and Kurosawa [9]. The fourth way is by relying on lossy trapdoor function introduced by Peikert and Waters [42] and further extended by Rosen and Segev [43] and many other works. Among the CCA-secure PKE schemes from these four ways, only the ones from the IBE transformation are publicly verifiable. However, most of existing practical IBE are based on the time-consuming pairings.

1.2.2. Without Pairings. The bilinear pairings enable the construction of first practical identity-based encryption by Boneh and Franklin [44]. Since then, many wonderful results can be achieved by using the bilinear pairings, such as fully collusion resistant broadcast encryption [45], efficient practical zero-knowledge proof [46], searchable public key encryption [47, 48], attribute based encryption [49], and predicate encryption [50].

But we note that, on the one hand, bilinear pairing is a very powerful cryptographic tool; on the other hand, the implementation speed of bilinear pairing is still relatively slower. So recently many researchers show interest in construction of schemes without pairings, because, on the one hand, it can clarify to us which cryptographic task inherits the bilinear property of pairings and which does not; on the other hand, it gives us a new view on old cryptographic problems. For example, Baek et al. constructed the first certificateless public key encryption without pairing [51], while the concept of certificateless public key cryptography was first raised by using bilinear pairings [52]. Other examples include Deng et al. and Shao and Cao's CCA-secure proxy reencryption without pairing [53, 54].

1.2.3. Verifiable Public Key Encryption. Another related research area is (private) verifiable public key encryption, such as Camenisch and Shoup's work [55]. However, their work was concerned with only the decryptor's verifiability of the ciphertext instead of *public* verifiability. Kiayias et al. extended their work by introducing some new concepts for constructing group encryption [56]. Owing to bilinear property of pairings, CCA-secure public key encryption with public verifiability can be easily achieved in the bilinear pairing setting. However, the situation is completely different in the "without pairing" setting; constructing PVPKE scheme remains as an open problem left for almost decades.

1.3. Organization. We organize our paper as follows: In Section 2, we give some preliminaries. In Section 3, we give our PVPKE's construction based on signed quadratic residues and analyse its security. In Section 4, we discuss PVPKE's applications. In the last section, we give our conclusion.

2. Preliminaries

2.1. Publicly Verifiable Public Key Encryption. A publicly verifiable public key encryption system consists of the following algorithms.

(i) The randomized key generation algorithm Gen takes as input a security parameter 1^k and outputs a public key (PK) and a secret key (SK). We write $(\mathrm{PK}, \mathrm{SK}) \leftarrow \mathrm{Gen}(1^k)$.

(ii) The randomized encryption algorithm $\mathscr{E}$ takes as input a public key (PK) and a message $m \in \{0,1\}^*$ and outputs a ciphertext C. We write $C \leftarrow \mathscr{E}_{\mathrm{PK}}(m)$.

(iii) The verification algorithm $\mathscr{V}$ takes as input a ciphertext C and a public key (PK). It returns valid or invalid to indicate whether the ciphertext is valid or not. Note that the validity of C can be verified publicly.

(iv) The decryption algorithm $\mathscr{D}$ takes as input a ciphertext C and a secret key (SK). It returns a message $m \in \{0.1\}^*$ or the distinguished symbol $\perp$. We write $m \leftarrow \mathscr{D}_{\mathrm{SK}}(C)$.

We require that, for all (PK, SK) output by Gen, all $m \in \{0,1\}^*$, and all C output by $\mathscr{E}_{\mathrm{PK}}(m)$, we have $\mathscr{D}_{\mathrm{SK}} = m$.

2.2. Chosen Ciphertext Security. We recall the standard definition of security against adaptive chosen ciphertext attack. A publicly verifiable public key encryption (PKE scheme is secure against adaptive chosen ciphertext attacks (i.e., "CCA-secure") if the advantage of any PPT adversary A in the following game is negligible in the security parameter k.

(1) $\mathsf{Gen}(1^k)$ outputs (PK, SK). Adversary A is given 1^k and PK.

(2) The adversary may make many polynomial-many queries to a decryption oracle $\mathscr{D}_{\mathrm{SK}}(\cdot)$.

(3) The adversary may make many polynomial-many queries to a verification oracle $\mathscr{V}_{\mathrm{PK}}(\cdot)$.

(4) At some point, A outputs two messages m_0, m_1 with $|m_0| = |m_1|$. A bit b is randomly chosen and the adversary is given a "challenge ciphertext" $C^* \leftarrow \mathscr{E}_{\mathrm{PK}}(m_b)$.

(5) A may continue to query its decryption oracle $\mathscr{D}_{\mathrm{SK}}(\cdot)$ except that it may not request the decryption of C^*.

(6) A may continue to make polynomial-many queries to a verification oracle $\mathscr{V}_{\mathrm{PK}}(\cdot)$.

(7) Finally, A outputs a guess b'.

We say that A succeeds if $b' = b$ and denote the probability of this event by $\Pr_{A,\mathrm{PKE}}[\mathrm{Succ}]$. The adversary's advantage is defined as $|\Pr_{A,\mathrm{PKE}}[\mathrm{Succ}] - 1/2|$.

2.3. The Group of Signed Quadratic Residues

2.3.1. RSA Instance Generator. Let $0 \le \delta \le 1/2$ be a constant and let $n(k)$ be a function. Let RSAgen be an algorithm that generates elements (N, P, Q), such that $N = PQ$ is an n-bit Blum integer ($N = PQ$ (where $P = 3 \bmod 4$ and $Q = 3 \bmod 4$)) and all prime factors of $\phi(N)/4$ are pairwise distinct and at least δn-bit integers.

2.3.2. Factoring Assumption. The factoring assumption is that computing P, Q from N (generated by RSAgen) is hard. We write

$$\mathrm{Adv}^{\mathrm{fac}}_{\mathscr{A},\mathrm{RSAGen}} = \Pr\left[\{P,Q\} \longleftarrow_R \mathscr{A}(N) : (N,P,Q) \longleftarrow_R \mathrm{RSAGen}\left(1^k\right)\right]. \tag{1}$$

The factoring assumption for RSAgen holds if $\mathrm{Adv}^{\mathrm{fac}}_{\mathscr{A},\mathrm{RSAGen}}$ is negligible for all efficient $\mathscr{A}$.

2.3.3. The Group of Signed Quadratic Residues. Let N be an integer. For $x \in \mathbb{Z}_N$ we define $|x|$ as the absolute value of x, where x is represented as a signed integer in the set $\{-(N-1)/2, \ldots, (N-1)/2\}$. For a subgroup $\mathbb{G}$ of $\mathbb{Z}^*_N$, we define the signed group, $\mathbb{G}^+$, as the group

$$\mathbb{G}^+ = \{|x| : x \in \mathbb{G}\} \tag{2}$$

with the following group operation. Namely, for $g, h \in \mathbb{G}^+$ and an integer x, we define

$$g \circ h = \left|g \cdot h \bmod N\right|, \quad \underline{g^x} = g \circ g \circ \cdots \circ g = \left|g^x \bmod N\right|. \tag{3}$$

More complicated expressions in the exponents are computed modulo the group order; for example, $\underline{g^{1/2}} = \underline{g^{2^{-1} \bmod \mathrm{ord}(G^+)}}$. Note that taking the absolute value is a surjective homomorphism from $\mathbb{G}$ to $\mathbb{G}^+$ with trivial kernel if -1 does not belong to $\mathbb{G}$ and with kernel $\{-1, 1\}$ if $-1 \in \mathbb{G}$.

Let N be a Blum integer such that -1 does not belong to QR_N. We will mainly be interested in QR^+_N, which we call signed quadratic residues (modulo N). QR^+_N is a subgroup of $Z^*_N/\pm 1$, with absolute values as a convenient computational representation. The following basic facts hold.

Theorem 1. *Let N be a Blum integer; then we have the following.*

(1) $(QR^+_N, \circ)$ *is a group of order* $\phi(N)/4$.

(2) $QR^+_N = J^+_N$. *In particular, QR^+_N is efficiently recognizable (given only N).*

(3) *If QR_N is cyclic, so is QR^+_N.*

2.3.4. Strong DH Assumption Reduced to Factoring Assumption. Hofheinz and Kiltz [28] also proved that the strong DH assumption can be reduced to factoring assumption. Here we review the theorem and its proof.

Theorem 2. *If the factoring assumption holds then the strong DH assumption holds relative to* RSAgen. *In particular, for every strong DH adversary $\mathscr{A}$, there exists a factoring adversary $\mathscr{B}$ (with roughly the same complexity as $\mathscr{A}$) such that*

$$Adv^{SDH}_{\mathscr{A},RSAgen}(k) \le Adv^{fac}_{\mathscr{B},RSAgen}(k) + O\left(2^{-\delta n(k)}\right). \tag{4}$$

Proof. We construct $\mathscr{B}$ from given $\mathscr{A}$. Concretely, $\mathscr{B}$ receives a challenge $N = PQ$, chooses uniformly $u \leftarrow_R (Z^*_N)^+ \setminus QR^+_N$, and sets $h = \underline{u^2}$. Note that, by definition of N, we have $\langle h \rangle = QR^+_N$ except with probability $O(2^{-\delta n(k)})$. Then $\mathscr{B}$ chooses $a, b \in [N/4]$ and sets

$$g := \underline{h^2}, \quad := h \circ \underline{g^a}, \quad := h \circ \underline{g^b} \tag{5}$$

(here we omit mod$N$ operation, and hereafter we continue to omit mod$N$ for typical exponential modular operation). This implicitly defines

$$d\log^X_g = a + \frac{1}{2} \bmod \mathrm{ord}\left(QR^+_N\right), \quad d\log^Y_g = b + \frac{1}{2} \bmod \mathrm{ord}\left(QR^+_N\right), \tag{6}$$

where the discrete logarithms are of course considered in $(QR^+_N, \circ)$. Again, by definition of N, the statistical distance between these (g, X, Y) and the input of $\mathscr{A}$ in the strong DH experiment is bounded by $O(2^{-\delta n(k)})$. So $\mathscr{B}$ runs $\mathscr{A}$ on input (g, X, Y) and answers $\mathscr{A}$'s oracle queries $(\widehat{Y}, \widehat{Z})$ as follows. First, we may assume that $(\widehat{Y}, \widehat{Z}) \in QR^+_N$ since $QR^+_N = J^+_N$ is efficiently recognizable. Next, since N is a Blum integer, the group order $\mathrm{ord}(QR^+_N) = (P-1)(Q-1)/4$ is odd, and hence

$$\begin{aligned} &\widehat{Y}^{\underline{d\log^X_g}} = \widehat{Z} \\ &\Longleftrightarrow \widehat{Y}^{\underline{2d\log^X_g}} = \widehat{Z}^{\underline{2}} \\ &\Longleftrightarrow \widehat{Y}^{2a+1} = \widehat{Z}^{\underline{2}}. \end{aligned} \tag{7}$$

Thus, $\mathscr{B}$ can implement the strong DH oracle by checking whether $\widehat{Y}^{2a+1} = \widehat{Z}^{\underline{2}}$ hold.

Consequently, with probability $\mathrm{Adv}^{\mathrm{SDH}}_{\mathscr{A},\mathrm{RSAgen}}(k) - O(2^{-\delta n(k)})$, $\mathscr{A}$ will finally output

$$Z = \underline{g^{(d\log^X_g)(d\log^Y_g)}} = \underline{g^{(a+1/2)(b+1/2)}} = \underline{h^{2ab+a+b+1/2}} \in QR^+_N \tag{8}$$

from which $\mathscr{B}$ can extract $v := \underline{h^{1/2}} \in QR^+_N$ (using its knowledge about a and b). Since u is not in QR^+_N and $v \in QR^+_N$ are two nontrivially different square roots of h, $\mathscr{B}$ can factor N by computing $gcd(u - v, N)$. □

3. CCA-Secure Publicly Verifiable Public Key Encryption in the Standard Model Based on Signed Quadratic Residues

3.1. Review of Nieto et al.'s Publicly Verifiable PKE Scheme. Their construction is inspired by the IND-CCA public key

KEM of Kiltz [57]; the $\mathsf{PG}(\mathsf{ParamGen})$ algorithm is similar to [57] except that it uses gap groups: $\mathsf{PG}(1^k)$ outputs public parameters $\text{par} = (\mathbb{G}, p, g, \text{DDH}, H)$, where $\mathbb{G} = g$ is a multiplicative cyclic group of prime order p, $2^k \le p \le 2^{k+1}$, DDH is an efficient algorithm such that $\text{DDH}(g^a, g^b, g^c) = 1 \leftrightarrow c = ab(p)$, and $H : \mathbb{G} \to \{0,1\}^{l_1(k)}$ is a cryptographic hash function such that $l_1(k)$ is a polynomial in k. We also use a strong one-time signature scheme $\mathsf{OTS} = (\mathsf{KG}, \mathsf{Sign}, \mathsf{Vrfy})$ with verification key space $\{0,1\}^{l_2(k)}$ such that $l_2(k)$ is a polynomial in k and a target collision resistant hash function $\text{TCR} : \mathbb{G} \times \{0,1\}^{l_2(k)} \to Z_p$. The message space is $\text{MsgSp} = \{0,1\}^{l_1(k)}$. The scheme works as follows.

(i) $\mathsf{PKE.KG}(\mathsf{par})$

$$\begin{aligned} &x \longleftarrow Z_p^* \\ &u \longleftarrow g^x, \quad v \longleftarrow \mathbb{G} \\ &ek \longleftarrow (u, v), \quad dk \longleftarrow x \\ &\text{Return } (ek, dk) \end{aligned} \tag{9}$$

(ii) $\mathsf{PKE.Enc}(\mathsf{par}, \mathsf{ek}, \mathsf{M})$

$$\begin{aligned} &(u, v) \longleftarrow ek \\ &(vk, \text{sig}\,k) \longleftarrow \text{OTS.KG}\left(1^k\right) \\ &r \longleftarrow_R Z_p^*, \quad c_1 \longleftarrow g^r \\ &t \longleftarrow \text{TCR}\left(c_1, vk\right), \quad \pi \longleftarrow \left(u^t v\right)^r \\ &K \longleftarrow H\left(u^r\right), \quad c_2 \longleftarrow M \oplus K \\ &c \longleftarrow \left(c_1, c_2, \pi\right) \\ &\delta \longleftarrow \text{OTS.Sign}\left(\text{sig}\,k, c\right) \\ &\text{Return } C = (c, \delta, vk) \end{aligned} \tag{10}$$

(iii) $\mathsf{PKE.Ver}(\mathsf{par}, \mathsf{ek}, \mathsf{C})$

$$\begin{aligned} &(u, v) \longleftarrow ek \\ &(c, \delta, vk) \longleftarrow C \\ &\left(c_1, c_2, \phi\right) \longleftarrow c \\ &t \longleftarrow \text{TCR}\left(c_1, vk\right) \\ &\text{If DDH}\left(c_1, u^t v, \pi\right) \neq \quad \text{Or} \\ &\text{OTS.Vrfy}\left(c, \delta, vk\right) = \perp, \text{ return } \perp \\ &\text{Return } C' = \left(c_1, c_2\right) \end{aligned} \tag{11}$$

(iv) $\mathsf{PKE.Dec}'(\mathsf{par}, \mathsf{ek}, \mathsf{dk}, \mathsf{C}')$

$$\begin{aligned} &\left(c_1, c_2\right) \longleftarrow C' \\ &x \longleftarrow dk \\ &K \longleftarrow H\left(c_1^x\right), \quad M \longleftarrow c_2 \oplus K \\ &\text{Return } M. \end{aligned} \tag{12}$$

3.2. Our Proposed PVPKE Scheme Based on Signed Quadratic Residues. First we give the core idea behind our construction. We observe that Nieto et al.'s PKE scheme actually is a PVPKE scheme, but the only issue is that they use an abstract DDH oracle. They instantiate this oracle by bilinear pairings, but we require that PVPKE scheme cannot rely on bilinear pairings. We also observe that signed quadratic residues can also instantiate the abstract DDH oracle, so we modify Nieto et al.'s scheme to be based on signed quadratic residues group, which now give a natural new PVPKE scheme. Notation: we omit the mod$N$ operation and every modular exponentiation in signed quadratic residues such as the fact that $h = u^2$ is represented as $h = u^2$, which implies all the modular exponentiation and other operations obey the rules defined in [28] instead of obeying the normal group rules. The following is the concrete scheme.

(i) $\mathsf{PVPKE.PG}(1^k)$ is as follows.

(a) Here we focus on QR_N^+ group; we first generate an RSA modulus $N = PQ$ with $\mathsf{RSAgen}(1^k)$ [28], then choose uniformly $u \longleftarrow_R (Z_N^*)^+ \setminus QR_N^+$, and set $h = u^2$. Note that, by definition of N, we have $G = \langle h \rangle = QR_N^+$ except with probability $O(2^{-\delta n(k)})$.

(b) $H : \mathbb{G} \to \{0,1\}^{l_1(k)}$ is a cryptographic hash function such that $l_1(k)$ is a polynomial in k.

(c) We also use a strong one-time signature scheme $\mathsf{OTS} = (\mathsf{KG}, \mathsf{Sign}, \mathsf{Vrfy})$ with verification key space $\{0,1\}^{l_2(k)}$ such that $l_2(k)$ is a polynomial in k and a target collision resistant hash function $\text{TCR} : \mathbb{G} \times \{0,1\}^{l_2(k)} \to Z_p$. The message space is $\text{MsgSp} = \{0,1\}^{l_1(k)}$.

(d) DDH is an efficient algorithm such that $\text{DDH}(g^a, g^b, g^c) = 1 \leftrightarrow c = ab \bmod p$. For the scheme relying on QR_N^+ group, we can easily decide the DDH tuple; concretely, we do the following.

(1) Choose $a, b \in [N/4]$ and $m, n \in \text{ord}(QR_N^+)$ satisfying $2^m(a + 1/2) > n \times \text{ord}(QR_N^+)$, $2^m(b + 1/2) > n \times \text{ord}(QR_N^+)$, and m is not very little. Then set

$$g := h^2, \quad X := h \circ g^a, \quad Y := h \circ g^b. \tag{13}$$

(2) Publish $a' = 2^m(a + 1/2) \bmod n \times \text{ord}(QR_N^+)$, $b' = 2^m(b + 1/2) \bmod n \times \text{ord}(QR_N^+)$ as the parameters for public verifying.

(3) The $\mathsf{DDHParams} = (g, X, Y, a', b', 2^m)$.

(e) $\mathsf{PG}(1^k)$ outputs public parameters $\mathrm{par} = (\mathbb{G}, N, \mathrm{DDHParams}, H, \mathrm{OTS}) = (\mathbb{G}, N, g, X, Y, a', b', 2^m, H, \mathrm{OTS})$.

(ii) $\mathsf{PVPKE.KG}(\mathsf{par})$

$$\begin{aligned} &x \longleftarrow Z_N^* \\ &u \longleftarrow g^x, \quad X = h \circ g^a, \quad Y = h \circ g^b \\ &ek \longleftarrow (u, X, Y), \quad dk \longleftarrow x \\ &\text{Return } (ek, dk) \end{aligned} \tag{14}$$

(iii) $\mathsf{PVPKE.Enc}(\mathsf{par}, \mathsf{ek}, \mathsf{M})$

$$\begin{aligned} &(u, X, Y) \longleftarrow ek \\ &(vk, \mathrm{sig}k) \longleftarrow \mathrm{OTS.KG}\left(1^k\right) \\ &r \longleftarrow_R Z_N^*, \quad c_1 \longleftarrow g^r \\ &t \longleftarrow \mathrm{TCR}(c_1, vk), \quad \pi \longleftarrow \left(X^t Y\right)^r \\ &K \longleftarrow H\left(u^r\right), \quad c_2 \longleftarrow M \oplus K \\ &c \longleftarrow (c_1, c_2, \pi) \\ &\delta \longleftarrow \mathrm{OTS.Sign}(\mathrm{sig}k, c) \\ &\text{Return } C = (c, \delta, vk) \end{aligned} \tag{15}$$

(iv) $\mathsf{PVPKE.Ver}(\mathsf{par}, \mathsf{ek}, \mathsf{C})$

$$\begin{aligned} &(u, X, Y) \longleftarrow ek \\ &(c, \delta, vk) \longleftarrow C \\ &(c_1, c_2, \pi) \longleftarrow c \\ &t \longleftarrow \mathrm{TCR}(c_1, vk) \\ &\text{If } c_1^{a't+b'} \neq (\pi)^{2^m} \quad \text{Or} \\ &\mathrm{OTS.Vrfy}(c, \delta, vk) = \perp, \text{ return } \perp \\ &\text{Return } C' = (c_1, c_2) \end{aligned} \tag{16}$$

(v) $\mathsf{PVPKE.Dec}'(\mathsf{par}, \mathsf{ek}, \mathsf{dk}, \mathsf{C}')$

$$\begin{aligned} &(c_1, c_2) \longleftarrow C' \\ &x \longleftarrow dk \\ &K \longleftarrow H\left(c_1^x\right), \quad M \longleftarrow c_2 \oplus K \\ &\text{Return } M. \end{aligned} \tag{17}$$

3.3. Security Analysis. Based on Nieto et al.'s security result and the property of signed quadratic residues, we can give the following theorem.

Theorem 3. *Assume that* TCR *is a target collision resistant hash function and* OTS *is a strongly unforgeable one-time signature scheme. Under a variant of hashed Diffie-Hellman assumption for* $\mathbb{G}$ *(signed quadratic residues group) and* H*, the factoring assumption of* RSAGen *(which implies the strong Diffie-Hellman assumption in signed quadratic residues group proved in [28]), our PVPKE scheme based on signed quadratic residues is IND-CCA-secure.*

Proof. In the following we give our scheme's security proof roughly.

(1) We observe that, in Nieto et al.'s PKE scheme, u plays two roles: one used to be deriving the DEM message mask key and the other used to be as part of the DDH test. But many research results show that it is secure to split these two roles separately [8]; thus we introduce X as the role of part of the DDH test, while maintaining u as the source of deriving DEM message mask key, which is the reason why we use $(X^t Y)$ instead of $(u^t v)$ in our scheme.

(2) In our scheme, we adopt Hofheinz and Kiltz's technique of reducing SDH assumption to the factoring assumption; concretely, we set X, Y, g, h, a, and b the same as theirs, but we make $a' = 2^m(a + 1/2) \bmod n \times \mathrm{ord}(QR_N^+)$ and $b' = 2^m(b+1/2) \bmod n \times \mathrm{ord}(QR_N^+)$ public, which is used for public verifying. The verifying equation $(g^r)^{a't+b'} = ((X^t Y)^r)^{2^m}$ can also be used for deciding the DDH relationship of $(g, X^t Y, g^r, (X^t Y)^r)$, but an attacker cannot figure out $\pi = (X^t Y)^r$ through finding $1/2^m$ root of $(g^r)^{a't+b'}$, for we know finding square root in QR_N is as hard as factoring and this also holds in QR_N^+.

(3) We require $2^m(a+1/2) > n \times \mathrm{ord}(QR_N^+)$, $2^m(b+1/2) > n \times \mathrm{ord}(QR_N^+)$ for avoiding the trivial attack of computing $a + 1/2 = a'/2^m$ and $b + 1/2 = b'/2^m$ without any modular operation, and thus trivial computing $\pi = (X^t Y)^r = (g^r)^{(a+1/2)t+(b+1/2)}$. Obviously this attack can easily forge a valid π and thus a valid ciphertext and break the IND-CCA property. We also require that m is not too little to resist the brute force attack on finding a from a'.

(4) Generally speaking, our scheme is almost identical to Nieto et al.'s scheme; thus the security proof is almost the same as theirs. Below are the details.

Let (c^*, δ^*, vk^*) be the challenge ciphertext. The proposed PKE without the CHK transform can be seen as a KEM/DEM combination, which is at least IND-CPA-secure due to Herranz et al. [58]. As for the KEM, a variant of the hashed Diffie-Hellman (HDH) assumption [48] can be used to prove the IND-CPA security of the resulting PKE. Note that the message does not depend on vk^* and is just the signature on c^*. Therefore c^* being an output of the IND-CPA-secure scheme hides the value of the chosen b from the adversary.

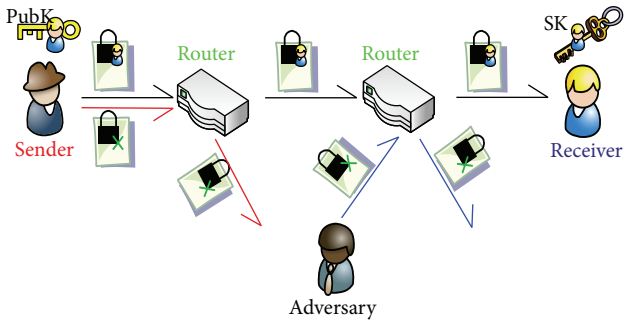

Figure 1: Routers drop the invalid ciphertexts via PVPKE.

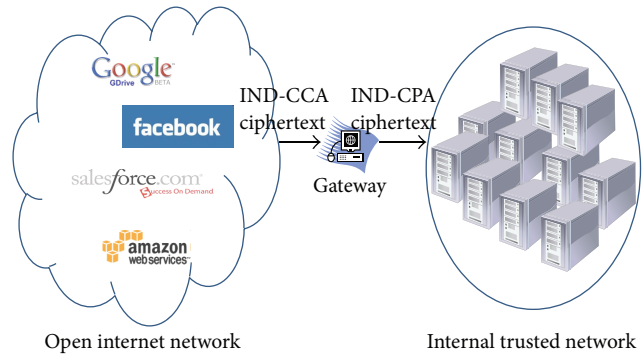

Figure 2: Gateways reduce the workload via PVPKE.

Below we prove that the IND-CCA adversary $\mathcal{A}$ may access decryption oracle and will gain no help in guessing the value of b. Suppose the adversary submits a ciphertext $(c', \delta', vk') \neq (c^*, \delta^*, vk^*)$ to the decryption oracle. Now there are two cases.

(i) When $vk' = vk^*$, the decryption oracle will output $\perp$ as the adversary fails to break the underlying strongly unforgeable one-time signature scheme with respect to vk'.

(ii) When $vk' \neq vk$, the attacker $\mathcal{B}$ against the variant of HDH problem can set the public keys as seen in the IND-CCA security proof for the KEM by Kiltz [57] such that (1) $\mathcal{B}$ can answer except for the challenge ciphertext all decryption queries from $\mathcal{A}$ even without the knowledge of the secret key and (2) $\mathcal{B}$ solves HDH if $\mathcal{A}$ wins. Note in Nieto et al.'s scheme u, v is the public key while in our scheme u, X, Y is the public key, but we observe v is randomly chosen from G, while in our scheme X, Y are set as $h \circ g^a, h \circ g^b$ which are also random because a, b are random. Thus our scheme roughly shares the same security proof outline as in [57] except that our scheme is in signed quadratic residues. □

4. Applications

4.1. Application 1: The Routers Drop the Invalid Ciphertexts via PVPKE. As shown in Figure 1, PVPKE can be used in the open internet network to help the routers to filter the invalid ciphertexts, while traditional IND-CCA-secure public key encryption does not have this function. First a sender (encrypter) wants to encrypt his message to a receiver (decrypter) by using public key encryption, and the ciphertexts in many cases have to be sent through open networks, which are not equipped with security guards to resist malicious attack; thus the sender should better choose an IND-CCA-secure public key encryption to encrypt his message. When an error or a data loss occurs in the ciphertexts through the transferring, the PVPKE can help the routers drop invalid ciphertexts by using the algorithm of public verifying. Note here the routers need not any secret, which will greatly reduce the cost of resetup of the old system. Also, if there exists malicious attacker modifying the ciphertexts, the invalid ciphertexts will also be dropped. This will greatly help the network to preserve its communication band only to effective data blocks and help the routers and the receiver to reduce the workload for they now only need to do the necessary computation. However, PVPKE cannot resist the following case: an attacker generates a ciphertext following the right encryption algorithm and this ciphertext will certainly pass through the algorithm of public verifying. We think this time the attacker is indeed an encrypter, which will be a trivial case, and any verifying algorithm cannot avoid it.

4.2. Application 2: The Gateways Reduce the Workload via PVPKE. The following scenarios are always existing: ciphertexts need to be transferred from a public open network like internet to an internal network like the government's network. As shown in Figure 2, PVPKE can be used to help the gateways reduce the workload: transforming an IND-CCA ciphertext to be an IND-CPA ciphertext. When an IND-CCA ciphertext was captured by the gateway, the gateway first verifies its validity by using the publicly verifying algorithm. If it has passed, then the gateway can drop one part of the ciphertext: the part which is used to authenticate the ciphertext, like (δ, vk) in our PVPKE and Nieto et al.'s PKE scheme (here we do not claim that any PVPKE scheme has this separate authentication part, for there exist PVPKE schemes in which the authentication part has been integrated in the other parts of the ciphertext as a whole). Thus the remaining ciphertext will be IND-CPA-secure and will be shorter compared with the original ciphertext. Because the government's network usually will be protected well with many security mechanisms, IND-CPA security is enough to assure the security of the ciphertext. This will also reduce the workload of the employees who work on the internal network of the government.

4.3. Application 3: Achieving Ciphertext Checkable in the Clouds via PVPKE. Today more and more people prefer to upload their personal data contents to the clouds, but they do not want the cloud to know what the data contents

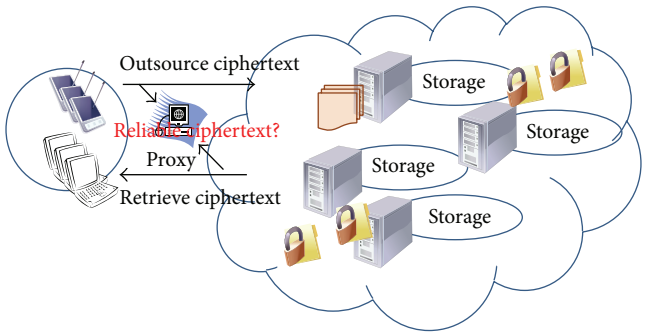

Figure 3: Achieving ciphertext checkable in the clouds via PVPKE.

are. Thus they need to encrypt the personal data contents before uploading them to the clouds. PVPKE can be used to achieve ciphertext checkable in this case, which can be seen in Figure 3. When the data owner uploads the ciphertexts to the cloud, there may exist incident things, like data loss or malicious attacker modifying the ciphertexts; in these cases, a proxy can be used to check the ciphertext's validity by using PVPKE. When the data owner or data user needs to retrieve the content, the clouds return the corresponding ciphertext to them. Also this time the proxy can be used to check the ciphertext's validity by using PVPKE. Note here that the proxy needs only to be semitrusted; it can perform the check without any secret; this will greatly benefit reducing the system management. For example, the proxy can be the access infrastructure in the wireless network setting. Note here that we do not claim that every ciphertext needs to be checked, which will be too heavy. This check must be run probabilistically with randomly chosen ciphertext.

5. Conclusions

PVPKE is a very powerful block to construct other cryptographic primitives or protocols, and its construction remains open for almost decades. In [13], we give several constructions and analyze their security. In this paper, by using the fact that the DDH oracle can be instantiated in signed quadratic residues, we give new PVPKE construction and roughly prove its security. The future work will be further exploring our idea and prove our proposal's security strictly.

Disclosure

This paper is a revised and expanded version of a paper titled "New Construction of PVPKE Scheme Based on Signed Quadratic Residues" presented at the Incos 2013 Conference [59]. The second author is the corresponding author.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The authors would like to express their gratitude to the editors for many helpful comments. This work is supported by the National Natural Science Foundation of China under Contracts nos. 61103230, 61272492, 61103231, and 61202492.

References

[1] A. J. Jara, S. Varakliotis, A. F. Skarmeta, and P. Kirstein, "Extending the Internet of things to the future internet through IPv6 support," *Mobile Information Systems*, vol. 10, no. 1, pp. 3–17, 2014.

[2] A. J. Jara, D. Fernandez, P. Lopez, M. A. Zamora, and A. F. Skarmeta, "Lightweight MIPv6 with IPSec support," *Mobile Information Systems*, vol. 10, no. 1, pp. 37–77, 2014.

[3] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[4] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the Association for Computing Machinery*, vol. 21, no. 2, pp. 120–126, 1978.

[5] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270–299, 1984.

[6] M. Abe, E. Kiltz, and T. Okamoto, "Chosen ciphertext security with optimal ciphertext overhead," in *Advances in Cryptology—ASIACRYP*, vol. 5350 of *Lecture Notes in Computer Science*, pp. 355–371, Springer, Berlin, Germany, 2008.

[7] M. Bellare and P. Rogaway, "Optimal asymmetric encryption: how to encrypt with RSA," in *Advances in Cryptology—EUROCRYPT'94*, vol. 950 of *Lecture Notes in Computer Science*, pp. 92–111, 1994.

[8] R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," in *Advances in Cryptology—CRYPTO '98*, vol. 1462 of *Lecture Notes in Computer Science*, pp. 13–25, Springer, Berlin, Germany, 1998.

[9] G. Hanaoka and K. Kurosawa, "Efficient chosen ciphertext secure public key encryption under the computational Diffie-Hellman assumption," in *Advances in Cryptology—ASIACRYPT 2008*, vol. 5350 of *Lecture Notes in Computer Science*, pp. 308–325, Springer, Berlin, Germany, 2008.

[10] D. Hofheinz, E. Kiltz, and V. Shoup, "Practical chosen ciphertext secure encryption from factoring," *Journal of Cryptology*, vol. 26, no. 1, pp. 102–118, 2013.

[11] Y. Lindell, "A simpler construction of cca2-secure public-key encryption under general assumptions," in *Advances in Cryptology—EUROCRYPT 2003*, vol. 2656 of *Lecture Notes in Computer Science*, pp. 241–254, Springer, Berlin, Germany, 2003.

[12] K. Goto, Y. Sasaki, T. Hara, and S. Nishio, "Data gathering using mobile agents for reducing traffic in dense mobile wireless sensor networks," *Mobile Information Systems*, vol. 9, no. 4, pp. 295–314, 2013.

[13] M. Zhang, X. A. Wang, W. Li, and X. Yang, "CCA secure publicly verifiable public key encryption without pairings nor random oracle and its applications," *Journal of Computers*, vol. 8, no. 8, pp. 1987–1994, 2013.

[14] X. Chen, J. Li, and W. Susilo, "Efficient fair conditional payments for outsourcing computations," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1687–1694, 2012.

[15] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," in *Computer Security—ESORICS 2012*, vol. 7459 of *Lecture Notes in Computer Science*, pp. 541–556, Springer, Berlin, Germany, 2012.

[16] R. Canetti and S. Goldwasser, "An efficient *threshold* public key cryptosystem secure against adaptive chosen ciphertext attack," in *Advances in Cryptology—EUROCRYPT'99*, vol. 1592 of *Lecture Notes in Computer Science*, pp. 90–106, Springer, Berlin, Germany, 1999.

[17] J. Baek and Y. Zheng, "Identity-based threshold decryption," in *Public Key Cryptography—PKC 2004*, vol. 2947 of *Lecture Notes in Computer Science*, pp. 262–276, Springer, Berlin, Germany, 2004.

[18] D. Boneh, X. Boyen, and S. Halevi, "Chosen ciphertext secure public key threshold encryption without random oracles," in *Topics in Cryptology—CT-RSA 2006*, vol. 3860 of *Lecture Notes in Computer Science*, pp. 226–243, 2006.

[19] V. Shoup and R. Gennaro, "Securing threshold cryptosystems against chosen ciphertext attack," *Journal of Cryptology*, vol. 15, no. 2, pp. 75–96, 2002.

[20] C. Delerablée and D. Pointcheval, "Dynamic threshold public-key encryption," in *Advances in Cryptology—CRYPTO*, vol. 5157 of *Lecture Notes in Computer Science*, pp. 317–334, Springer, Berlin, Germany, 2008.

[21] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in *Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS '05)*, pp. 29–43, San Diego, Calif, USA, 2005.

[22] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security*, vol. 9, no. 1, pp. 1–30, 2006.

[23] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," in *Public Key Cryptography—PKC 2008*, vol. 4939 of *Lecture Notes in Computer Science*, pp. 360–379, Springer, Berlin, Germany, 2008.

[24] R. Canetti and S. Hohenberger, "Chosen ciphertext secure proxy re-encryption," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 185–194, ACM, 2007.

[25] J. Zhang and X. A. Wang, "On the security of a multi-use CCA-secure proxy re-encryption scheme," in *Proceedings of the 4th International Conference on Intelligent Networking and Collaborative Systems (INCoS '12)*, pp. 571–576, Bucharest, Romania, September 2012.

[26] J. Zhang and X. Wang, "Security analysis of a multi-use identity based CCA-secure proxy reencryption scheme," in *Proceedings of the 4th International Conference on Intelligent Networking and Collaborative Systems (INCoS '12)*, pp. 581–586, September 2012.

[27] J. Nieto, M. Manulis, B. Poettering, J. Rangasamy, and D. Stebila, "Publicly verifiable ciphertexts," in *Proceedings of the 8th International Conference on Security and Cryptography for Networks (SCN '12)*, vol. 7485 of *Lecture Notes in Computer Science*, pp. 393–410, Amalfi, Italy, 2012.

[28] D. Hofheinz and E. Kiltz, "The group of signed quadratic residues and applications," in *Advances in Cryptology—CRYPTO 2009*, vol. 5677 of *Lecture Notes in Computer Science*, pp. 637–653, Springer, Berlin, Germany, 2009.

[29] M. Naor and M. Yung, "Public-key cryptosystems provably secure against chosen ciphertext attacks," in *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (STOC '90)*, pp. 427–437, May 1990.

[30] C. Rackoff and D. R. Simon, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack," in *Advances in Cryptology—CRYPTO '91*, vol. 576 of *Lecture Notes in Computer Science*, pp. 433–444, Springer, Berlin, Germany, 1992.

[31] D. Dolev, C. Dwork, and M. Naor, "Non-malleable cryptography," in *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing (STOC '91)*, pp. 542–552, May 1991.

[32] A. Sahai, "Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security," in *Proceedings of the 40th Annual Symposium on Foundations of Computer Science (IEEE FOCS '99)*, pp. 543–553, New York, NY, USA, October 1999.

[33] M. Bellare and P. Rogaway, "Random oracles are practical: a paradigm for designing efficient protocols," in *Proceedings of the 1st ACM Conference on Computer and Communications Security (CCS '93)*, pp. 62–73, November 1993.

[34] R. Canetti, O. Goldreich, and S. Halevi, "Random oracle methodology, revisited," in *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC '98)*, pp. 209–218, May 1998.

[35] R. Cramer and V. Shoup, "Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack," *SIAM Journal on Computing*, vol. 33, no. 1, pp. 167–226, 2003.

[36] K. Kurosawa and Y. Desmedt, "A new paradigm of hybrid encryption scheme," in *Advances in Cryptology—CRYPTO 2004*, vol. 3152 of *Lecture Notes in Computer Science*, pp. 426–442, 2004.

[37] M. Abe, R. Gennaro, K. Kurosawa, and V. Shoup, "Tag-kem/dem: a new framework for hybrid encryption and a new analysis of kurosawa-desmedt kem," in *Advances in Cryptology—EUROCRYPT 2005*, vol. 3494 of *Lecture Notes in Computer Science*, pp. 128–146, Springer, Berlin, Germany, 2005.

[38] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in *Advances in Cryptology—EUROCRYPT 2004*, vol. 3027 of *Lecture Notes in Computer Science*, pp. 207–222, Springer, Berlin, Germany, 2004.

[39] D. Boneh and J. Katz, "Improved efficiency for CCA-secure cryptosystems built using identity-based encryption," in *Topics in Cryptology—CT-RSA 2005*, vol. 3376 of *Lecture Notes in Computer Science*, pp. 87–103, Springer, Berlin, Germany, 2005.

[40] X. Boyen, Q. Mei, and B. Waters, "Direct chosen ciphertext security from identity-based techniques," in *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS '05)*, pp. 320–329, November 2005.

[41] E. Kiltz, "Chosen-ciphertext security from tag-based encryption," in *Theory of Cryptography*, vol. 3876 of *Lecture Notes in Computer Science*, pp. 581–600, Springer, Berlin, Germany, 2006.

[42] C. Peikert and B. Waters, "Lossy trapdoor functions and their applications," in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC '08)*, pp. 187–196, 2008.

[43] A. Rosen and G. Segev, "Chosen-ciphertext security via correlated products," in *Theory of Cryptography*, vol. 5444, pp. 419–436, Springer, Berlin, Germany, 2009.

[44] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology—CRYPTO 2001: Proceedings of the 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19–23, 2001*, vol. 2139 of

Lecture Notes in Computer Science, pp. 213–229, Springer, Berlin, Germany, 2001.

[45] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in *Proceedings of the 25th Annual International Cryptology Conference (CRYPTO '05)*, vol. 3621 of *Lecture Notes in Computer Science*, pp. 258–275, Santa Barbara, Calif, USA, 2005.

[46] J. Groth and A. Sahai, "Efficient non-interactive proof systems for bilinear groups," in *Advances in Cryptology—EUROCRYPT 2008*, vol. 4965 of *Lecture Notes in Computer Science*, pp. 415–432, Springer, Berlin, Germany, 2008.

[47] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Computational Science and Its Applications—ICCSA 2008*, vol. 3089 of *Lecture Notes in Computer Science*, pp. 31–45, Springer, Berlin, Germany, 2004.

[48] M. Abdalla, M. Bellare, D. Catalano et al., "Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions," in *Advances in Cryptology—CRYPTO 2005*, vol. 3621 of *Lecture Notes in Computer Science*, pp. 205–222, Springer, Berlin, Germany, 2005.

[49] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 89–98, November 2006.

[50] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in *Advances in Cryptology—EUROCRYPT 2008*, vol. 4965 of *Lecture Notes in Computer Science*, pp. 146–162, Springer, Berlin, Germany, 2008.

[51] J. Baek, R. Safavi-Naini, and W. Susilo, "Certificateless public key encryption without pairing," in *Information Security*, vol. 3650 of *Lecture Notes in Computer Science*, pp. 134–148, Springer, Berlin, Germany, 2005.

[52] S. Al Riyami and K. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology—ASIACRYPT 2003*, vol. 2894 of *Lecture Notes in Computer Science*, pp. 452–473, Springer, 2003.

[53] R. Deng, J. Weng, S. Liu, and K. Chen, "Chosen ciphertext secure proxy re-encryption without pairings," in *Cryptology and Network Security*, vol. 5339 of *Lecture Notes in Computer Science*, pp. 1–17, Springer, Berlin, Germany, 2008, http://eprint.iacr.org/2008/509.

[54] J. Shao and Z. Cao, "CCA-secure proxy re-encryption without pairings," in *Public Key Cryptography—PKC 2009*, vol. 5443 of *Lecture Notes in Computer Science*, pp. 357–376, Springer, Berlin, Germany, 2009.

[55] J. Camenisch and V. Shoup, "Practical verifiable encryption and decryption of discrete logarithms," in *Advances in Cryptology—CRYPTO 2003*, vol. 2729 of *Lecture Notes in Computer Science*, pp. 126–144, Springer, Berlin, Germany, 2003.

[56] A. Kiayias, Y. Tsiounis, and M. Yung, *Group Encryption*, Cryptology ePrint Archive, 2007, http://eprint.iacr.org/2007/015.pdf.

[57] E. Kiltz, "Chosen-ciphertext secure key-encapsulation based on gap hashed Diffie-Hellman," in *Public Key Cryptography—PKC*, vol. 4450 of *Lecture Notes in Computer Science*, pp. 282–297, Springer, Berlin, Germany, 2007.

[58] J. Herranz, D. Hofheinz, and E. Kiltz, "KEM/DEM: necessary and sucffcient conditions for secure hybrid encryption," in *IACR Cryptology ePrint Archive*, Report 2006/256, IACR, 2006.

[59] J. Zhang and X. Wang, "New construction of PVPKE scheme based on signed quadratic residues," in *Proceedings of the 5th International Conference on Intelligent Networking and Collaborative Systems (INCoS '13)*, pp. 434–437, September 2013.