PROPERTY PRESERVING SYMMETRIC ENCRYPTION REVISITED

SANJIT CHATTERJEE AND M. PREM LAXMAN DAS

Abstract. At Eurocrypt'12, Pandey and Rouselakis [PR12a] proposed the notion of property preserving symmetric encryption (PPEnc). They defined several security notions for PPEnc and studied their relationship. They also proposed a concrete scheme which preserves the orthogonality of encrypted vectors. The proposed construction is claimed to achieve the strongest security notion of property preserving encryption, called LoR security. In this work, we take a critical look at the three security theorems in the context of PPEnc from [PR12a]. In particular, we show that the Pandey-Rouselakis scheme for orthogonality property does not even satisfy the weakest notion of security for PPEnc. We also note that the paper fails to demonstrate that the separation results pertaining to different security notions of PPEnc are non-vacuous. We fill up this gap in the separation results of [PR12a] by suggesting an example construction of PPEnc for the concrete property under consideration.

1. Introduction

The notion of *property preserving symmetric encryption* was introduced by Pandey and Rouselakis in [PR12a]. This kind of scheme may be used to check for a property satisfied by plaintexts by running a public test on the corresponding ciphertexts. It is claimed [PR12a] that such schemes will be of interest to develop private algorithms for data classification such as clustering streaming data based on some property.

Pandey and Rouselakis also discussed several notions of security for PPEnc such as Find-then-Guess (FtG) and Left-or-Right (LoR) security. Informally speaking, the former corresponds to a single challenge and the latter to multiple challenges. While LoR naturally implies FtG security, [PR12a] claims that the other way is not true. They also define a hierarchy of FtG security notions based on the number of challenge queries the adversary is allowed to make. They claim that this hierarchy does not collapse.

While arguing the separation between FtG and LoR, [PR12a] start by assuming the existence of a FtG secure scheme Π for some property (called P_{qr}) based on quadratic residuosity. They convert Π, using one-time pad, to a scheme Π' which is FtG secure, but not LoR secure. The authors also comment that the separation result for the FtG hierarchy can be proven using the same property.

Finally, the authors describe a scheme for testing orthogonality property. Their scheme is instantiated on a bilinear group of composite order ($N = pq$). They claim that their scheme is LoR secure in the generic group model.

Our Contribution: In this work we take a critical look at the security theorems stated in [PR12a]. Our study reveals some interesting facts as summarised below.

Date: December 31, 2013.

- We show that the PPEnc scheme given in [PR12a, Sec.5] for testing orthogonality property is not even selective FtG secure. We show a simple attack with just a single valid query. Our observation contradicts the claim of [PR12a, Theorem 5.1] that their proposed construction is LoR secure.
- We observe that the authors fail to show that their separation result between FtG and LoR security is non-vacuous. This is because the paper does not provide any evidence that a concrete FtG secure scheme exists for the quadratic residuocity property for which the separation result holds. We exhibit the existence of such a scheme and thereby fill the gap in the separation result. The same observation holds for the second separation result for the hierarchy of FtG security and we extend our previous result to fill that gap.

Organization. In §2, we recall the definition of property preserving encryption scheme from [PR12a] and provide an informal description of the security notions. In §3 we describe the Pandey-Rouselakis scheme for testing orthogonality and then demonstrate our attack. In §4 we comment on the limitation of their separation results and fill in the gaps. Finally we make some concluding remarks in §5.

2. Property Preserving Encryption

The notion of property preserving symmetric encryption (PPEnc) was introduced recently by Pandey and Rouselakis [PR12a]. A PPEnc scheme allows computation on encrypted data – a topic that has gained a lot of attention in the context of cloud/outsourced computation. Suppose given the encryption of two vectors $(\overrightarrow{x}, \overrightarrow{y})$, an *untrusted* server wants to check whether $\overrightarrow{x} \cdot \overrightarrow{y} = 0$ and then cluster the data accordingly. A PPEnc scheme comes with a public Test algorithm that allows anybody to check whether a set of ciphertexts satisfy a certain property or not without revealing any other meaningful information about the underlying plaintext. A symmetric PPEnc scheme is defined [PR12a] as follows.

Definition 1. *A property preserving encryption scheme for the k-ary property P is a collection of four probabilistic polynomial time (PPT) algorithms, which are defined as follows:*

1. *Setup(λ): This takes as input the security parameter λ and outputs the message space ($\mathcal{M}$), public parameters (PP) and the secret key (SK).*
2. *Encrypt(PP, SK, m): This algorithm outputs the ciphertext CT corresponding to the message m, using the secret key SK and public parameter PP.*
3. *Decrypt(PP, SK, CT): This algorithm outputs the plaintext message m.*
4. *Test($CT_1, \ldots, CT_k, PP$): This is a public algorithm that takes as inputs ciphertexts corresponding to messages $m_1, \ldots, m_k$ and outputs a bit.*

These set of four algorithms must satisfy the standard correctness requirement. In addition, if the Test *algorithm outputs 1 then, except with negligible probability, one has $P(m_1, \ldots, m_k) = 1$.*

Remark 1. *When it comes to the actual construction, Pandey-Rouselakis* [PR12a]*, actually proposed a "slightly weaker" variant called* PPTag *scheme. The* PPTag *construction does not have a decryption algorithm. The authors claim that correct decryption can be obtained by appropriate use of any IND-CPA secure symmetric encryption scheme.*

2.1. **Security Notions.** Pandey and Rouselakis [PR12a] proposed several notions of security for property-preserving encryption. These security definitions are derived from the corresponding notion of security for symmetric key encryption after taking into account the specific nature of PPEnc. Here we (informally) describe two different models of security for property preserving encryption schemes from [PR12a]. For these definitions, one first needs the following notion of *equality pattern*:

Definition 2. *For a k-ary property P, two sequences $X = (x_1, \ldots, x_n)$ and $Y = (y_1, \ldots, y_n)$ are said to have the same equality pattern if for all $(i_1, \ldots, i_k) \in [n]^k$, the following holds:*

$$P(x_{i_1}, \ldots, x_{i_k}) = P(y_{i_1}, \ldots, y_{i_k}).$$

Find-then-Guess Security (FtG). In this game the adversary, after getting the public parameters, first adaptively queries the encryption oracle for messages $(m_1, \ldots, m_t)$. Then the adversary outputs the challenge messages (m_0^*, m_1^*). The challenger returns the ciphertext c_b^* where $b \in_R \{0, 1\}$. The adversary again adaptively queries $(m_{t+1}, \ldots, m_l)$. The adversary wins the game if s/he can correctly predict the bit b. In order to ensure that the adversary cannot trivially win the game, the adversarial queries must satisfy the *extra* condition that the equality patterns of $(m_1, \ldots, m_t, m_0^*, m_{t+1}, \ldots, m_l)$ and $(m_1, \ldots, m_t, m_1^*, m_{t+1}, \ldots, m_l)$ are the same.

Left-or-Right Security (LoR). In this game the adversary makes q encryption queries, where each query is of the form $(m_0^{(i)}, m_1^{(i)})$. The queries are such that $(m_0^{(1)}, \ldots, m_0^{(q)})$ and $(m_1^{(1)}, \ldots, m_1^{(q)})$ have the same equality pattern. The challenger returns the encryption of $m_b^{(i)}$ for each i where $b \in_R \{0, 1\}$ is chosen at the beginning of the game and kept hidden from the adversary. At the end, the adversary has to output a guess b' of b and wins if $b' = b$.

Remark 2. *Maintaining the same equality patterns for the two sequences of adversarial queries is crucial for the security of* PPEnc *scheme. For example, consider the binary property of testing the orthogonality of two vectors mentioned earlier. If two vectors $(x_{i_1}, x_{i_2}) \in X$ are orthogonal where as the vectors having the same index i_1, i_2 in Y, i.e., (y_{i_1}, y_{i_2}) are* not *orthogonal, then the public Test algorithm can be used to trivially break the* LoR *security of a* PPEnc *scheme.*

It is easy to see that LoR implies FtG. Pandey-Rouselakis claimed that LoR security is, in fact, a strictly stronger notion than FtG security (see Theorem 4.1 of [PR12a]). They also claim (as one of their main results – see Theorem 4.4 of [PR12a]) that there is a hierarchy of FtG notions for PPEnc, indexed by integers $\eta \in \mathbb{N}$, that do not collapse.[1]

3. Pandey-Rouselakis Construction and its Insecurity

Pandey-Rouselakis proposed a PPTag scheme for testing the orthogonality property of two vectors. The construction is in the composite order bilinear group setting and claimed to achieve LoR security in the generic group model. The security claim is established in Theorem 5.1 of [PR12a] with a precise bound on the adversarial advantage while the proof is left for the full version.

[1]The FtG notion described above is for $\eta = 1$. FtG$^\eta$ for $\eta \in \mathbb{N}$ allows the adversary to make η many challenge queries interleaved between encryption oracle queries.

Here, we first reproduce the PPTag scheme described in [PR12a] and then discuss about its (in)security.

- **Setup**(λ, n). Pick two different primes p and q uniformly in the range $(2^{\lambda-1}, 2^{\lambda})$ where λ is the security parameter. Let $\mathbb{G}$ and $\mathbb{G}_T$ be two groups of order $N = pq$ such that there is an efficiently computable bilinear map $e : \mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_T$. Select a vector $(\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}_q$ such that $\sum_{i=1}^{n} \gamma_i^2 = \delta^2 \pmod q$. Let g_0 (resp. g_1) be a generator of a subgroup of order p (resp. q) of $\mathbb{G}$. Set the message space as $\mathcal{M} = (\mathbb{Z}_N^* \bigcup \{0\})^n$. Then set
$$PP = \langle n, N, G, G_T, e \rangle,\ SK = \langle g_0, g_1, \{\gamma_i\}, \delta \rangle,$$
- **Encrypt**(PP, SK, M). On input a message $M = (m_1, \ldots, m_n)$, select two random elements ϕ and ψ from $\mathbb{Z}_N$. The ciphertext is computed as
$$CT = (ct_0, \{ct_i\}_{i=1}^n) = \left(g_1^{\psi\delta}, \{g_0^{\phi m_i} \cdot g_1^{\psi\gamma_i}\}_{i=1}^n \right).$$
- **Test**$(PP, CT^{(1)}, CT^{(2)})$. On input two ciphertexts $CT^{(1)} = (ct_0^{(1)}, \{ct_i^{(1)}\}_{i=1}^n)$ and $CT^{(2)} = (ct_0^{(2)}, \{ct_i^{(2)}\}_{i=1}^n)$, the algorithm outputs 1 if and only if:
$$\prod_{i=1}^{n} e(ct_i^{(1)}, ct_i^{(2)}) = e(ct_0^{(1)}, ct_0^{(2)}).$$

3.1. **Attack on Pandey and Rouselakis Scheme.** We show that the construction of Pandey and Rouselakis is not even FtG secure, and hence, by implication, cannot be LoR secure. This contradicts the claim of Theorem 5.1 of [PR12a]. In fact, the PPTag scheme of [PR12a] does not even satisfy the weaker *selective* notion of FtG security.

We first illustrate our attack with a simple example for the case of $n = 2$. Next, we show that our attack works in the weaker *selective* model of security and can be trivially extended to the case of any $n > 2$.

Intuition: Recall that in Setup, the user chooses secret key components $\gamma_1, \gamma_2, \delta \in \mathbb{Z}_q$ such that $\delta^2 = \gamma_1^2 + \gamma_2^2 \bmod q$. Now observe that for such values, we have

$$\delta^2 = \gamma_1(\gamma_1 + \gamma_2) + \gamma_2(\gamma_2 - \gamma_1) \bmod q. \tag{1}$$

The above relation (Eqn. 1) immediately suggests the following attack. The adversary sets vectors $(0, 1)$ and $(1, 0)$ as the challenge messages. Next, the adversary queries vector $(1, 1)$ and obtains a corresponding ciphertext. It processes the ciphertext to obtain a *pseudo-ciphertext* for $(2, 0)$ by taking product and ratio of the second and third components of the given ciphertext and retaining the first component of the ciphertext. Note that $(0, 1)$ is orthogonal to $(2, 0)$, while the other challenge vector $(1, 0)$ is not. Now the adversary uses the pseudo-ciphertext in the Test algorithm to distinguish the challenge messages as shown below.

(i) In the FtG game $\mathcal{A}$ receives the public parameter PP from its challenger $\mathcal{S}$.
(ii) $\mathcal{A}$ asks for the encryption of $\vec{v}_1 = (1, 1)$ and obtains,
$$(C_0, C_1, C_2) = (g_1^{\psi\delta}, g_0^{\phi} g_1^{\psi\gamma_1}, g_0^{\phi} g_1^{\psi\gamma_2}),$$
where $\phi, \psi \in_R \mathbb{Z}_N$ are chosen by the challenger (unknown to $\mathcal{A}$).

(iii) From the obtained ciphertext (C_0, C_1, C_2), $\mathcal{A}$ computes the following:

$$\xi = (\xi_0, \xi_1, \xi_2) = (C_0, C_1 \cdot C_2, C_2/C_1) = (g_1^{\psi\delta}, g_0^{2\phi} g_1^{\psi(\gamma_1+\gamma_2)}, g_1^{\psi(\gamma_2-\gamma_1)}). \tag{2}$$

(iv) $\mathcal{A}$ outputs the challenge vectors $\vec{w}_0^* = (0,1)$ and $\vec{w}_1^* = (1,0)$.

(v) The challenger returns the encryption $C_{\vec{w}_b}$, for a bit $b \in_R \{0,1\}$. We shall denote the ciphertext of $\vec{w}_b = (m_1, m_2)$ by $C_{\vec{w}_b}$ where

$$C_{\vec{w}_b} = (\zeta_0, \zeta_1, \zeta_2) = (g_1^{\psi_1\delta}, g_0^{\phi_1 m_1} g_1^{\psi_1\gamma_1}, g_0^{\phi_1 m_2} g_1^{\psi_1\gamma_2}). \tag{3}$$

(vi) $\mathcal{A}$ runs the Test algorithm with inputs $(\xi, C_{\vec{w}_b})$ and returns $b' = 0$ if $Test(\xi, C_{\vec{w}_b})$ returns 1. Otherwise $\mathcal{A}$ returns $b' = 1$.

The following claim establishes that $\mathcal{A}$ wins the FtG security game with overwhelming probability of success. In particular, the "pseudo-ciphertext" ξ of the vector $(2,0)$ can be used to distinguish vectors orthogonal to it from those which are not.

Claim 1. *The vector $\vec{w}_b = (m_1, m_2)$ is orthogonal to $(2,0)$ (except with negligible probability) if Test$(C_{\vec{w}_b}, \xi) = 1$, where the algorithm Test outputs 1 if and only if*

$$e(\zeta_0, \xi_0) = e(\zeta_1, \xi_1) \cdot e(\zeta_2, \xi_2). \tag{4}$$

Proof. We show that if the algorithm Test$(\xi, C_{\vec{w}_b})$ outputs 1 then $m_1 = 0$, except with negligible probability. We verify the following regarding the left hand side of Eqn. 4:

$$e(\zeta_0, \xi_0) = e(g_1, g_1)^{\psi_1\psi\delta^2}.$$

Similarly, using Eqn. 2 and Eqn. 3 the right hand side of Eqn. 4 equals (where the last but one equality is obtained by using Eqn. 1):

$$\begin{aligned} e(\zeta_1, \xi_1) \cdot e(\zeta_2, \xi_2) &= e(g_0, g_0)^{2m_1\phi_1\phi} \cdot e(g_1, g_1)^{\psi_1\psi\gamma_1(\gamma_1+\gamma_2)} \cdot e(g_1, g_1)^{\psi_1\psi\gamma_2(\gamma_2-\gamma_1)} \\ &= e(g_0, g_0)^{2m_1\phi_1\phi} \cdot e(g_1, g_1)^{\psi_1\psi(\gamma_1^2+\gamma_2^2)} \\ &= e(g_0, g_0)^{2m_1\phi_1\phi} \cdot e(g_1, g_1)^{\psi_1\psi\delta^2}. \end{aligned} \tag{5}$$

Hence, except with a negligible probability, Test outputs 1 only when $m_1 = 0$. □

The above attack can be easily extended to prove the following more general claim.

Proposition 2. *The* PPTag *scheme proposed in* [PR12a] *for testing orthogonality is not even* ***selective FtG*** *secure.*

Proof. We establish the claim in terms of the following attack game between the adversary and the challenger.

(i) $\mathcal{A}$ outputs two n-dimensional vectors $\overrightarrow{m}_0^*, \overrightarrow{m}_1^*$ as the challenge messages where $n \ll N$. The challenges are of the form $\overrightarrow{m}_0^* = (m_1, m_0, 1, \ldots, 1)$ and $\overrightarrow{m}_1^* = (m_1, m_1, 1, \ldots, 1)$, where $m_1 \neq m_0$ are from $\mathbb{Z}_N^*$.

(ii) $\mathcal{A}$ receives the public parameter PP from challenger.

(iii) $\mathcal{A}$ queries $Q = ((m_1 + m_0)/2, (m_0 - m_1)/2, 1, \ldots, 1, -(n-3))$. Observe that Q is not orthogonal to either of the challenge messages $(\overrightarrow{m}_0^*, \overrightarrow{m}_1^*)$ and hence, is a valid query.

(iv) $\mathcal{S}$ responds with

$$CT_Q = \left(g_1^{\psi\delta}, g_0^{\phi(m_1+m_0)/2} g_1^{\psi\gamma_1}, g_0^{\phi(m_0-m_1)/2} g_1^{\psi\gamma_2}, g_0^{\phi} g_1^{\psi\gamma_3}, \ldots, g_0^{\phi} g_1^{\psi\gamma_{n-1}}, g_0^{-(n-3)\phi} g_1^{\psi\gamma_n}\right)$$

for some $\psi, \phi \in_R \mathbb{Z}_N$.

(v) Given CT_Q, $\mathcal{A}$ takes the product and ratio of the second and third components of the ciphertext to obtain $g_0^{m_0\phi} g_1^{\psi(\gamma_1+\gamma_2)}, g_0^{-m_1\phi} g_1^{\psi(\gamma_2-\gamma_1)}$. $\mathcal{A}$ now computes the *pseudo-ciphertext* for $\overrightarrow{m}' = (m_0, -m_1, 1, \ldots, 1, -(n-3))$ as

$$CT'_Q = (g_1^{\psi\delta}, g_0^{m_0\phi} g_1^{\psi(\gamma_1+\gamma_2)}, g_0^{-m_1\phi} g_1^{\psi(\gamma_2-\gamma_1)}, g_0^{\phi} g_1^{\psi\gamma_3}, \ldots, g_0^{\phi} g_1^{\psi\gamma_{n-1}}, g_0^{-(n-3)\phi} g_1^{\psi\gamma_n}).$$

Note that the message vector $\overrightarrow{m}'$ is orthogonal to $\overrightarrow{m}_0^*$ but not to $\overrightarrow{m}_1^*$. As in our previous attack, the pseudo-ciphertext for $\overrightarrow{m}'$ can be used to distinguish the challenge messages $(\overrightarrow{m}_0^*, \overrightarrow{m}_1^*)$.

(vi) $\mathcal{A}$ now asks for the challenge ciphertext. Suppose that the challenger responds with

$$CT_b = \left(g_1^{\tilde{\psi}\delta}, g_0^{m_1\tilde{\phi}} g_1^{\gamma_1\tilde{\psi}}, g_0^{m_b\tilde{\phi}} g_1^{\gamma_2\tilde{\psi}}, g_0^{\tilde{\phi}} g_1^{\gamma_3\tilde{\psi}}, \cdots, g_0^{\tilde{\phi}} g_1^{\gamma_n\tilde{\psi}}\right),$$

where $b \in_R \{0,1\}$ is chosen by $\mathcal{S}$ and $\tilde{\phi}, \tilde{\psi} \in_R \mathbb{Z}_N$.

(vii) $\mathcal{A}$ runs the Test algorithm on CT'_Q and CT_b. This amounts to computing:

$$\begin{aligned} A &= e(g_1^{\psi\delta}, g_1^{\tilde{\psi}\delta}) \text{ and} \\ B &= e(g_0^{m_0\phi} g_1^{\psi(\gamma_1+\gamma_2)}, g_0^{m_1\tilde{\phi}} g_1^{\gamma_1\tilde{\psi}}) \cdot e(g_0^{-m_1\phi} g_1^{\psi(\gamma_2-\gamma_1)}, g_0^{m_b\tilde{\phi}} g_1^{\gamma_2\tilde{\psi}}) \\ &\quad \prod_{i=3}^{n-1} e(g_0^{\phi} g_1^{\psi\gamma_i}, g_0^{\tilde{\phi}} g_1^{\gamma_i\tilde{\psi}}) \cdot e(g_0^{-(n-3)\phi} g_1^{\psi\gamma_n}, g_0^{\tilde{\phi}} g_1^{\gamma_n\tilde{\psi}}). \end{aligned}$$

(viii) If $A = B$ then $\mathcal{A}$ outputs $b' = 0$, otherwise $\mathcal{A}$ outputs $b' = 1$.

Using the fact that

$$\delta^2 = \gamma_1(\gamma_1 + \gamma_2) + \gamma_2(\gamma_2 - \gamma_1) + \gamma_3^2 + \ldots + \gamma_n^2 \bmod q,$$

we observe that, except with negligible probability, $A = B$ implies $m_b = m_0$. Hence, the adversary wins the selective FtG game with overwhelming probability of success. □

4. On the Separation of Security Notions

The other two contributions of Pandey and Rouselakis are to establish that (i) $\mathsf{FtG} \nrightarrow \mathsf{LoR}$ and (ii) $\mathsf{FtG}^{\eta} \nrightarrow \mathsf{FtG}^{\eta+1}$. The former is established through Theorem 4.1 and the latter through Theorem 4.4. We now briefly comment on these two contributions of [PR12a].

Both the above theorems are claimed to have been established for a property based on quadratic residuosity. Let $\mathcal{QR}_p$ (resp. $\mathcal{QNR}_p$) be the set of quadratic residues (resp. quadratic non-residues) in $\mathbb{Z}_p^*$ for some prime p. For any two messages $(m_1, m_2) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ a binary property is defined as follows:

$$P_{qr}(m_1, m_2) = \begin{cases} 1 & \text{if} \quad m_1 \cdot m_2 \in \mathcal{QR}_p \\ 0 & \text{if} \quad m_1 \cdot m_2 \in \mathcal{QNR}_p \end{cases} \tag{6}$$

Given a PPEnc scheme Π for P_{qr} that is FtG secure, Pandey-Rouselakis shows how to construct another scheme Π' which is FtG secure but not LoR secure and thereby prove their Theorem 4.1. However, the paper does not provide any concrete construction of a PPEnc scheme for P_{qr}. Nor is there any evidence at all to assume that such a scheme actually exists. In the absence of any concrete scheme satisfying the P_{qr} property that is FtG secure, the authors leave open the possibility that Theorem 4.1 can, in fact, be *vacuous*.[2]

In Theorem 4.4, Pandey-Rouselakis claims that for the same property P_{qr} they can show that $\mathsf{FtG}^{\eta} \nrightarrow \mathsf{FtG}^{\eta+1}$. However, the paper does not suggest any concrete scheme that satisfies the FtG^{η} security property. Our observation in the context of Theorem 4.1 discussed above is applicable for Theorem 4.4 as well.

4.1. **A Concrete FtG Secure Scheme for P_{qr}.** We now complete the gap in the separation result for the FtG and LoR security notions. In particular, we show the existence of an FtG secure scheme for the property P_{qr} as defined in Eqn. 6. The existence of such a scheme together with Lemma 4.2 and Lemma 4.3 of [PR12a], will complete the argument that, in general, $\mathsf{FtG} \nrightarrow \mathsf{LoR}$ for property preserving encryption.

The basic strategy is as follows. Note that LoR secure schemes exist only for the inner product property [KT13, AAB$^+$13]. However, one needs a concrete FtG secure scheme for the property P_{qr} based on quadratic residuosity for the separation result to go through. So we realize the property P_{qr} using the test for orthogonality for two-dimensional vectors. Using the scheme described in [AAB$^+$13, Sec. 8] one can obtain FtG secure property preserving encryption scheme for the property P_{qr} as outlined below. Alternatively, one can construct a PPEnc scheme for P_{qr} from the symmetric inner product preserving encryption (SIPE) scheme of [KT13, Sec. 2.4].

We first observe that the P_{qr} property of an integer α modulo a prime p is captured by the following encoding:

$$v(\alpha) = \begin{cases} (1,1), \text{ if } \alpha \text{ is a QR modulo } p, \\ (1,-1), \text{ otherwise.} \end{cases} \tag{7}$$

It is easy to see that $x \cdot y \bmod p$ is a non-residue if and only if $v(x) \cdot v(y) = 0$. We now use, for example, the PPEnc scheme for inner product [AAB$^+$13, Sec. 8] for two-dimensional vectors and the message space restricted to $\mathcal{M} = \{(1,1),(1,-1)\}$. By [AAB$^+$13, Cor. 8.4], the above scheme is LoR secure (see [AAB$^+$13] for details) and, hence, FtG secure. We highlight this security result in the following statement.

Claim 3. *The* PPTag *scheme outlined above for the P_{qr} property is* LoR *secure.*

We use this modified scheme from [AAB$^+$13] as the scheme Π for the property P_{qr}. Now the argument given in [PR12a, Thorem 4.1] can be used to construct another scheme Π' which is FtG secure but not LoR secure.

[2]The conditional theorem of [PR12a] cannot be treated at par with a conditional theorem that assumes, for example, the existence of one-way function. It is now a standard assumption in cryptography that one-way functions exist and certain well-known functions are one-way. However, that is not the case with a completely new assumption such as the existence of an FtG-secure scheme for P_{qr}, where some evidence is warranted in order to convince the readers that the conditional theorem is non-vacuous.

4.2. **On the hierarchy result: $\mathsf{FtG}^{\eta} \nrightarrow \mathsf{FtG}^{\eta+1}$.** We now briefly comment on the result from [PR12a] concerning the hierarchy in FtG security. Note that no proof for Theorem 4.4 was provided in [PR12a]. However, the presentation given by Rouselakis at Eurocrypt'12 [PR12b] provides some intuition why this will hold for the property P_{qr}.

Note that, the construction of Π for the property P_{qr} given in the previous section is LoR secure and hence, FtG^{η} secure for any η which is polynomial in the security parameter. We can use this fact and the strategy outlined in [PR12b] to construct a scheme which is FtG^{η} secure but not $\mathsf{FtG}^{\eta+1}$ secure. This will complete the argument of Theorem 4.4 of [PR12a].

5. Concluding Remarks

In their Eurocrypt 2012 paper [PR12a], Pandey-Rouselakis stated three theorems: one pertaining to the security of their proposed construction of property preserving encryption for testing orthogonality, one concerning the separation between FtG and LoR security and the other pertaining to the existence of a strict hierarchy in the FtG notion of security. In this work we have shown an easy attack on their proposed construction and thereby established that the corresponding theorem statement does not hold. We also note that there is no evidence in the paper to claim that the other two theorems are non-vacuous. We then filled-up the gap in the proof of their first separation result by providing a concrete FtG secure scheme for the quadratic residuosity property. Finally, we outline how the same scheme can be used to complete the proof for their result regarding FtG hierarchy.

Acknowledgements

We thank Chethan Kamath, Neal Koblitz, Alfred Menezes, Omkant Pandey, Yannis Rouselakis and Palash Sarkar for their comments on earlier versions of the draft.

References

[AAB+13] Shashank Agrawal, Shweta Agrawal, Saikrishna Badrinarayanan, Abishek Kumarasubramanian, Manoj Prabhakaran, and Amit Sahai. Function private functional encryption and property preserving encryption : New definitions and positive results. Cryptology ePrint Archive, Report 2013/744, 2013. http://eprint.iacr.org/.

[KT13] Yutaka Kawai and Katsuyuki Takashima. Predicate- and attribute-hiding inner product encryption in a public key setting. Cryptology ePrint Archive, Report 2013/763, 2013. http://eprint.iacr.org/.

[PR12a] Omkant Pandey and Yannis Rouselakis. Property preserving symmetric encryption. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT*, volume 7237 of *Lecture Notes in Computer Science*, pages 375–391. Springer, 2012.

[PR12b] Omkant Pandey and Yannis Rouselakis. Property preserving symmetric encryption. Slides of the Talk Given at Eurocrypt 2012, 2012. http://www.cs.bris.ac.uk/eurocrypt2012/Program/Tues/Rouselakis.pdf.

Department of Computer Science and Automation, Indian Institute of Science
E-mail address: sanjit@csa.iisc.ernet.in

Society for Electronic Transactions and Security, Chennai
E-mail address: prem@setsindia.net