not always true. In fact, when $\mathfrak{B}$ is singular, the local-global principle makes the "compatibility" identity hold, see Chapter 1 in [17]. Furthermore, note that in the case $\mathrm{Norm}_{\mathbb{Z}[\zeta_e]}(\mathfrak{U}) = p-1$, it also holds due to the inclusion map $\iota : \dfrac{\mathbb{Z}[\zeta_e]}{\mathfrak{U}} \mapsto \dfrac{\mathbb{Z}[\zeta_f]}{\mathfrak{B}}$. Hence, we formalize the following revised theorem.

Theorem 6. *Let e, f be integers with $f \mid e$. Let $\mathfrak{p}_1$ be as Lemma 1, and let $x \in \mathbb{Z}[\zeta_e]$. Then*

$$\left(\frac{x}{\mathfrak{p}_1 \cap \mathbb{Z}[\zeta_f]}\right)_f = \left(\frac{x}{\mathfrak{p}_1}\right)_e^{\frac{e}{f}}.$$

It follows readily that $\mathfrak{p}_1 \cap \mathbb{Z}[\zeta_f] = p\mathbb{Z}[\zeta_f] + (\zeta_f - \mu^{\frac{e}{f}})\mathbb{Z}[\zeta_f]$ due to the fact that $\mu^{\frac{e}{f}}$ is a *non-degenerate* primitive f-th root of unity modulo N. Therefore, we are able to learn the value of $\left(\frac{x}{\mathfrak{a}_1}\right)_e$ by computing $\left(\frac{x}{N\mathbb{Z}[\zeta_f] + (\zeta_f - \mu^{\frac{e}{f}})\mathbb{Z}[\zeta_f]}\right)_f$ for each prime factor f of e and applying the Chinese remainder theorem.

6.2 Computing $\left(\frac{\cdot}{\mathfrak{a}_1}\right)_e$ if the Factorization $\mathfrak{a}_1 = \mathfrak{p}_1\mathfrak{q}_1$ is Known

The following simple theorem demonstrates that computing $\left(\frac{\cdot}{\mathfrak{p}_1}\right)_e$ is related to solving the discrete logarithm problem in a certain cyclic group. Recall that the *discrete logarithm problem* (DLP) is defined as: given a finite cyclic group $\mathbb{G}$ of order n with a generator α and an element $\beta \in \mathbb{G}$, find the integer $x \in \mathbb{Z}_n$ such that $\alpha^x = \beta$.

Theorem 7. $\left(\frac{y}{\mathfrak{p}_1}\right)_e = \zeta_e^x$ *if and only if* $\mu^x = y^{\frac{p-1}{e}}$ *in* $\mathbb{Z}_p^*$. *Therefore, the solution to the DLP in the finite cyclic subgroup $\langle\mu\rangle$ of order e allows the computation of* $\left(\frac{\cdot}{\mathfrak{p}_1}\right)_e$.

Proof. $\Leftarrow$ If $\mu^x = y^{\frac{p-1}{e}}$, then $y^{\frac{p-1}{e}} - \zeta_e^x = \mu^x - \zeta_e^x \in \mathfrak{p}_1$. It follows that $\left(\frac{y}{\mathfrak{p}_1}\right)_e = \zeta_e^x$.

$\Rightarrow$ If $\left(\frac{y}{\mathfrak{p}_1}\right)_e = \zeta_e^x$ for some $x \in \mathbb{Z}_e$, that is $y^{\frac{p-1}{e}} - \zeta_e^x \in \mathfrak{p}_1$. As the order of $y^{\frac{p-1}{e}}$ divides e, $y^{\frac{p-1}{e}}$ can be expressed as μ^z with an integer $z \in \mathbb{Z}_e$, which implies $\mu^x - \mu^z \in \mathfrak{p}_1$. The fact that the order of μ is e forces $x = z$. ∎

Although the DLP is considered to be intractable in general, it can be quickly solved in a few particular cases, e.g., if the order of $\mathbb{G}$ is smooth, the Pohlig-Hellman algorithm [30] turns out to be quite efficient. Taking advantage of the discovery above, Joye-Libert scheme [26] which generalizes Goldwasser-Micali cryptosystem using 2^k-th power residue symbols can be extended and rephrased as follows:

$\mathsf{KeyGen}(1^\kappa)$ Given a security parameter κ. KeyGen selects arbitrary $e = \prod_{i=1}^{\ell} e_i^{f_i}$ a product of small prime numbers, then generates an RSA modulus $N = pq$ a product of two large primes p and q such that $e \mid p-1, e \mid q-1$ and picks at random $\mu \in \mathbb{Z}_N^*$ a *non-degenerate* primitive e-th root of unity to N and $y \in \mathcal{J}_{N,e}^1 \setminus \mathcal{ER}_{N,e}$. The public and private keys are $pk = \{N, e, y\}$ and $sk = \{p, \mu\}$.

$\mathsf{Enc}(pk, m)$ To encrypt a message $m \in \mathbb{Z}_e$, Enc picks a random $x \in \mathbb{Z}_N^*$ and returns the ciphertext

$$c = y^m x^e \bmod N.$$

$\mathsf{Dec}(sk, c)$ Given the ciphertext c and the private key $sk = \{p, \mu\}$, Dec first computes $\left(\frac{c}{\mathfrak{p}_1}\right)_e = \zeta_e^z$ and then recovers the plaintext as $m = zk^{-1} \bmod e$ where $\left(\frac{y}{\mathfrak{p}_1}\right)_e = \zeta_e^k$.

The above scheme has the similar security proof as Goldwasser-Micali cryptosystem's, i.e., by the proof of Theorem 1, it is IND-CPA secure under the ER_e assumption defined as:

Definition 3 **(e-th Residue (ER_e) Assumption).** *A* PPT *algorithm* $\mathsf{RSAgen}(\lambda)$ *generates two equally sized primes* p, q *and an integer* e *such that* $p \equiv q \equiv 1 \bmod e$, *and chooses at random* $\mu \in \mathbb{Z}_N^*$ *a* non-degenerate *primitive* e*-th root of unity to* $N = pq$. *We define the following two distributions relative to* $\mathsf{RSAgen}(\kappa)$ *as:*

$$\mathbb{D}_{ER} : \left\{ (N, v, e, \mu) : (p, q, e, \mu) \leftarrow \mathsf{RSAgen}(\kappa),\ v \overset{\$}{\hookleftarrow} \mathcal{ER}_{N,e} \right\}$$
$$\mathbb{D}_{ENR} : \left\{ (N, v, e, \mu) : (p, q, e, \mu) \leftarrow \mathsf{RSAgen}(\kappa),\ v \overset{\$}{\hookleftarrow} \mathcal{J}^1_{N,e} \setminus \mathcal{ER}_{N,e} \right\}$$

The ER_e *assumption relative to* $\mathsf{RSAgen}(\kappa)$ *asserts that the advantage* $\mathsf{Adv}^{\mathsf{ER}_e}_{\mathcal{A},\mathsf{RSAgen}}(\kappa)$ *defined as*

$$\left| \Pr\left[\mathcal{A}(N, v, e) = 1 \;\middle|\; (N, v, e, \mu) \overset{\$}{\hookleftarrow} \mathbb{D}_{ER}(\kappa) \right] - \Pr\left[\mathcal{A}(N, v, e) = 1 \;\middle|\; (N, v, e, \mu) \overset{\$}{\hookleftarrow} \mathbb{D}_{ENR}(\kappa) \right] \right|$$

is negligible for any PPT *adversary* $\mathcal{A}$.

Note that when $e = 2^k$ for an integer k, ER_e assumption holds if and only if the *k-QR assumption* (Definition 2, [26]) holds since $\left(\frac{a}{p}\right) = -1$ if and only if $\left(\frac{a}{\mathfrak{p}_1}\right)_e$ is primitive (for a fixed p and arbitrary μ). Therefore, the above scheme for $e = 2^k$ (Joye-Libert scheme) is IND-CPA secure under the *k-QR assumption*.

One of the drawback of Joye-Libert scheme is that its decryption is slow. Consider decrypting a 128-bit plaintext, its algorithm [Algorithm 1, [26]] needs roughly $\binom{128}{2} = 8128$ modular multiplications. If we take $e = 10007^{10} > 2^{128}$ in our generalized scheme, the major time consuming part of decryption is performing the Pohlig-Hellman algorithm to compute $\left(\frac{\cdot}{\mathfrak{p}_1}\right)_e$. For speeding up, we also pre-evaluate the quantities $\mu^{k*10007^9} \bmod N$ for $k = 0, 1, \ldots, 10006$ in a look-up table. If we ignore the time that the Pohlig-Hellman algorithm spends on the binary search algorithm, then it only needs $\sum_{k=0}^{9} \log(10007^k) \approx 600$ modular multiplications and 10 modular inverse operations, which is approximately 10 times faster than the decryption of Joye-Libert scheme.

References

1. Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions. In *Annual International Cryptology Conference*, pages 205–222. Springer, 2005.
2. Leonard Adleman, Kenneth Manders, and Gary Miller. On taking roots in finite fields. In *18th Annual Symposium on Foundations of Computer Science (SFCS 1977)*, pages 175–178. IEEE, 1977.
3. Giuseppe Ateniese and Paolo Gasti. Universally anonymous ibe based on the quadratic residuosity assumption. In *Cryptographers' Track at the RSA Conference*, pages 32–47. Springer, 2009.
4. Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. Key-privacy in public-key encryption. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 566–582. Springer, 2001.
5. Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In *International conference on the theory and applications of cryptographic techniques*, pages 506–522. Springer, 2004.
6. Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Annual international cryptology conference*, pages 213–229. Springer, 2001.
7. Dan Boneh, Craig Gentry, and Michael Hamburg. Space-efficient identity based encryptionwithout pairings. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*, pages 647–657. IEEE, 2007.
8. Dan Boneh, Rio LaVigne, and Manuel Sabin. Identity-based encryption with e^{th} residuosity and its incompressibility. In *Autumn 2013 TRUST Conference. Washington DC (Oct 9-10, 2013), poster presentation*, 2013.
9. Eric Brier, Houda Ferradi, Marc Joye, and David Naccache. New number-theoretic cryptographic primitives. Cryptology ePrint Archive, Report 2019/484, 2019. `https://eprint.iacr.org/2019/484`.