Converting Cryptographic Schemes from Composite Order to Prime Order Pairing

R. Kabaleeshwaran, M. Prem Laxman Das* & Sanjit Chatterjee

Dept. of CSA, Indian Institute of Science, *SETS, Chennai.

kabaleeshwaran.r@csa.iisc.ernet.in

Computer Science and Automation

Introduction

- Bilinear pairing - used to design many cryptographic schemes,
  - One round 3-party key agreement protocol,
  - Identity-based encryption (IBE),
  - Aggregate signatures, etc.,
- Composite order pairing - used to design cryptographic schemes with additional properties
  - Boneh-Goh-Nissim partial homomorphic encryption scheme (BGN) [BGN05],
  - Predicate encryption (KSW08, SSW09)
  - Signatures with additional properties [BW07, SW07, MSF10], etc.,

Motivation

- Composite order bilinear group has special properties like projecting, cancelling.
  - useful to construct new cryptographic primitives
- But composite order bilinear group is more expensive than the prime order version
  - Guillevic showed that composite order pairing is 254 times slower than prime order pairing on particular choice of underlying elliptic curve.
- Transformation is not a block box, it is protocol specific.

Definition

Bilinear group generator An algorithm $\mathcal{G}(\lambda) \rightarrow (G, H, G_T, e, G_1, H_1, G'_T)$, where G, H and G_T are abelian groups and subgroups $G_1 \subset G$ and $H_1 \subset H$ and $e : G \times H \longrightarrow G_T$ is a bilinear map. The properties of the efficiently computable map e are as follows:

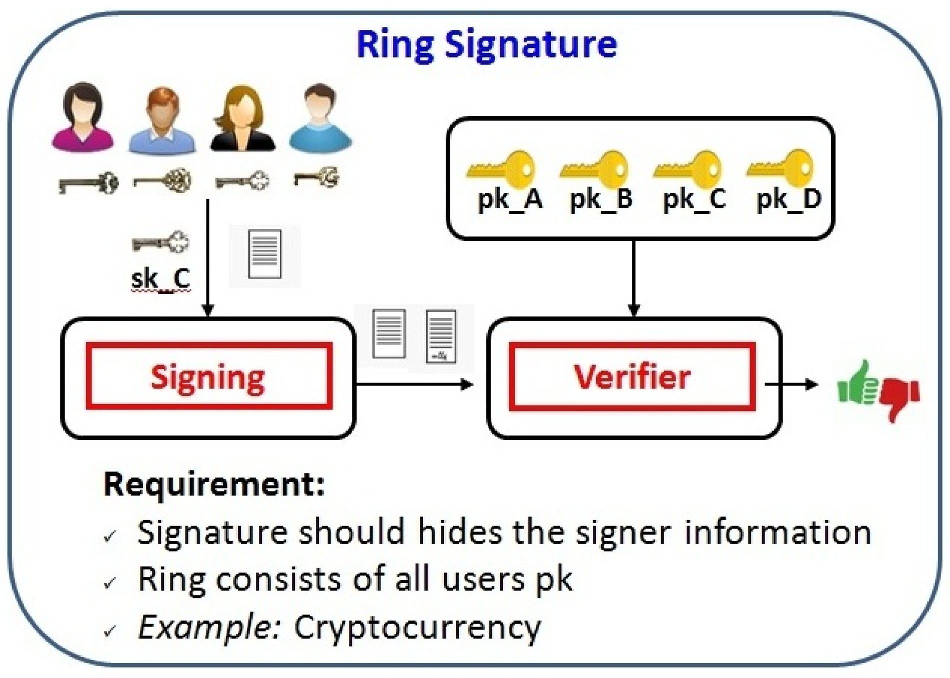
- *Bilinearity*: For all $g, g' \in G$ and $h, h' \in H$, one has
$$e(g \cdot g', h \cdot h') = e(g, h) \cdot e(g, h') \cdot e(g', h) \cdot e(g', h'),$$
- *Non degeneracy* If a fixed $g \in G$ satisfies $e(g, h) = 1$ for all $h \in H$, then $g = 1$ and similarly for elements of H

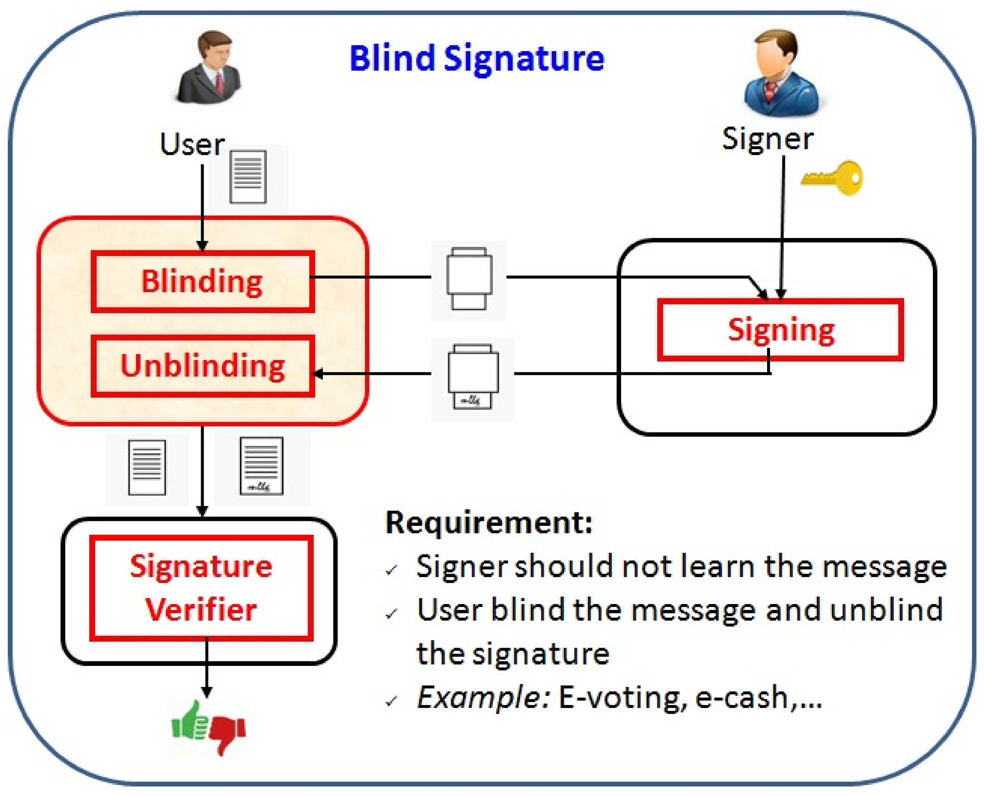
Projecting property $\mathcal{G}$ is said to be projecting if it outputs homomorphisms π_G, π_H and π_T defined on G, H and G_T to themselves, such that

- $G_1 \subseteq$ Ker (π_G), $H_1 \subseteq$ Ker (π_H) and $G'_T \subseteq$ Ker (π_T) and
- $e(\pi_G(g), \pi_H(h)) = \pi_T(e(g, h))$, for all $g \in G$ and $h \in H$.

Cancelling property $\mathcal{G}$ is said to satisfy the r-cancelling property if, in addition, outputs groups G_i, H_i, $i = 1, \ldots, r$, such that

- $G \cong G_1 \times \cdots \times G_r$ and $H \cong H_1 \times \cdots \times H_r$ and
- $e(g_i, h_j) = 1$, whenever $g_i \in G_i$, $h_j \in H_j$ and $i \neq j$.





Major conversion steps [Fre10]

1. Write the scheme in the abstract group framework with the appropriate pairing,
   - Translate BGN scheme from symmetric to asymmetric groups,
2. Translate the corresponding security assumption to general framework,
   - Translate SDP in G_{pq} to (2,1)-SDP in $\mathbb{G}_1^2$ and $\mathbb{G}_2^2$,
3. Instantiate scheme and assumption using the abstract groups,
   - DDH in $\mathbb{G}_1$ and $\mathbb{G}_2$ implies (2,1)-SDP in $\mathbb{G}_1^2$ and $\mathbb{G}_2^2$.

Seo-Cheon's projecting cum cancelling framework [SC12]

- Here $G = G_1 \oplus G_2 \cong \mathbb{G}_1^4$, $H = H_1 \oplus H_2 \cong \mathbb{G}_2^4$, $G_T = \mathbb{G}_T^2$, $e : G \times H \rightarrow G_T$ is defined as
$e(\mathfrak{g}^{(\alpha_{11},\alpha_{12},\alpha_{21},\alpha_{22})}, \mathfrak{h}^{(\beta_{11},\beta_{12},\beta_{21},\beta_{22})}) := \left(\hat{e}(\mathfrak{g}^{\alpha_{11}}, \mathfrak{h}^{\beta_{11}})\, \hat{e}(\mathfrak{g}^{\alpha_{12}}, \mathfrak{h}^{\beta_{12}}),\ \hat{e}(\mathfrak{g}^{\alpha_{21}}, \mathfrak{h}^{\beta_{21}})\, \hat{e}(\mathfrak{g}^{\alpha_{22}}, \mathfrak{h}^{\beta_{22}})\right)$
- We proved security under SXDH instead of non-standard assumption.

Our unbalanced projecting framework

We formulate Freeman projecting framework in unbalanced pairing setting.

- Using Chatterjee et al. techniques on Ghadafi et al. NIWI proof system, we obtain Type-3 variant of proof system, from this we extracted unbalanced projecting framework,
- $G = G_1 \oplus G_2 \cong \mathbb{G}_1^2$, $H = H_1 \oplus H_2 \oplus H_3 \cong \mathbb{G}_2^3$, $G_T = \mathbb{G}_T^6$, pairing map $e : G \times H \rightarrow G_T$ is defined as $e(\mathfrak{g}^{\vec{x}}, \mathfrak{h}^{\vec{y}}) := \hat{e}(\mathfrak{g}, \mathfrak{h})^{\vec{x} \otimes \vec{y}}$, for any $\mathfrak{g}^{\vec{x}} \in G$ and $\mathfrak{h}^{\vec{y}} \in H$.
- Security: DDH$_{\mathbb{G}_1} \Rightarrow (2,1)$-SDP$_G$ and DLin$_{\mathbb{H}} \Rightarrow (3,2)$-SDP$_{\mathbb{H}^3}$, where $\mathbb{H} = \langle(\mathfrak{g}, \mathfrak{h})\rangle$.

Results

Round Optimal Blind Signature instantiations

- Convert ROBS using Freeman's unbalanced projecting framework.
  - Blindness under SDP in G and $\mathbb{H}^3$
  - OMU under co-DHP* in $\mathbb{G}_1$ and $\mathbb{G}_2$
    - We use Seo-Cheon proof strategy,
    - Avoid Translating property [SC12], as simulator knows the subgroup generators exponent,
  - Both scheme construction and blindness proof uses neither projecting nor cancelling. But OMU uses only projecting, not cancelling as opposed to [MSF10]
- Convert ROBS using Seo-Cheon's projecting cum cancelling framework
  - Blindness under SDP in G and H
  - OMU under security of Waters signature defined in $G_2 \subseteq G$ and $H_2 \subseteq H$.
    - We use [MSF10] proof strategy
  - OMU proof uses both projecting and cancelling as similar to [MSF10].
- Comparison: Communication cost - Unbalanced; Computation cost - Seo-Cheon.

Table 1: Comparing ROBS instantiation using unbalanced projecting framework and Seo-Cheon's framework

	Unbalanced Framework	Seo-Cheon Framework
$\|CRS\|$	$1792\|\mathbb{G}_1\| + 1077\|\mathbb{G}_2\|$ ✓	$1436\|\mathbb{G}_1\| + 1432\|\mathbb{G}_2\|$
$\|Key\|$	$2\|\mathbb{G}_1\| + 6\|\mathbb{G}_T\|$	$4\|\mathbb{G}_1\| + 2\|\mathbb{G}_T\|$ ✓
$\|req\|$	$4096\|\mathbb{G}_1\| + 2304\|\mathbb{G}_2\|$ ✓	$3072(\|\mathbb{G}_1\| + \|\mathbb{G}_2\|)$
$\|BSig\|$	$6\|\mathbb{G}_1\| + 3\|\mathbb{G}_2\|$ ✓	$12\|\mathbb{G}_1\| + 4\|\mathbb{G}_2\|$
$\|Sig\|$	$4\|\mathbb{G}_1\| + 3\|\mathbb{G}_2\|$ ✓	$8\|\mathbb{G}_1\| + 4\|\mathbb{G}_2\|$
Setup	$1790E_{\mathbb{G}_1} + 1075E_{\mathbb{G}_2}$ ✓	$1436E_{\mathbb{G}_1} + 1432E_{\mathbb{G}_2}$
KeyGen	$6\mathbb{P} + 2E_{\mathbb{G}_1}$	$4\mathbb{P} + 2M_{\mathbb{G}_T} + 4E_{\mathbb{G}_1}$ ✓
User	$48\mathbb{P} + 6M_{\mathbb{G}_T} + 8708E_{\mathbb{G}_1} + 7572M_{\mathbb{G}_1} + 4611(E_{\mathbb{G}_2} + M_{\mathbb{G}_2})$	$32\mathbb{P} + 18M_{\mathbb{G}_T} + 3592E_{\mathbb{G}_1} + 5416M_{\mathbb{G}_1} + 2564E_{\mathbb{G}_2} + 1540M_{\mathbb{G}_2}$ ✓
Signer	$13312\mathbb{P} + 6144M_{\mathbb{G}_T} + 6E_{\mathbb{G}_1} + 1226M_{\mathbb{G}_1} + 3E_{\mathbb{G}_2} + 768M_{\mathbb{G}_2} + 512I_{\mathbb{G}_1} + 768I_{\mathbb{G}_2}$	$6144\mathbb{P} + 4096M_{\mathbb{G}_T} + 12E_{\mathbb{G}_1} + 2452M_{\mathbb{G}_1} + 4E_{\mathbb{G}_2} + 1024M_{\mathbb{G}_2} + 1024(I_{\mathbb{G}_1} + I_{\mathbb{G}_2})$ ✓
Verify	$24\mathbb{P} + 6M_{\mathbb{G}_T} + 712M_{\mathbb{G}_1}$	$16\mathbb{P} + 10M_{\mathbb{G}_T} + 1424M_{\mathbb{G}_1}$ ✓

For any group $X \in \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T\}$, we denote E_X, M_X, I_X and $|X|$ as the exponentiation, multiplication and inversion in X and bit size of X and $\mathbb{P}$ denotes atomic asymmetric pairing.

Ring Signature instantiation

- Convert using Freeman projecting framework with full decomposition
  - $G = G_1 \oplus G_2 \cong \mathbb{G}_1^2$, $H = H_1 \oplus H_2 \cong \mathbb{G}_2^2$ and $G_T = \mathbb{G}_T^4$, e - tensor product
- Both scheme construction and anonymity proof uses neither projecting nor cancelling. But UF proof uses only projecting, not cancelling as opposed to [SW07]
  - Anonymity under SDP in G and H,
  - UF under co-CDH+ in $\mathbb{G}_1$ and $\mathbb{G}_2$,
- Convert using Seo-Cheon's framework
  - Similar to the previous instantiation, except bilinear group construction as described in Seo-Cheon framework
  - Inefficient instantiation

Table 2: Comparing Freeman framework versus Seo-Cheon's projection cum cancelling framework

Framework	Freeman	Seo-Cheon
$1\|G\|, 1\|H\|, 1\|G_T\|$	$2\|\mathbb{G}_1\|, 2\|\mathbb{G}_2\|, 4\|\mathbb{G}_T\|$	$4\|\mathbb{G}_1\|, 4\|\mathbb{G}_2\|, 2\|\mathbb{G}_T\|$
O_G, O_H, O_{G_T}	$2O_G, 2O_H, 4O_{G_T}$	$4O_G, 4O_H, 2O_{G_T}$
$1P$	$4\mathbb{P}$	$4\mathbb{P} + 2M_{\mathbb{G}_T}$

The operation O can be either exponentiation or multiplication or inversion.

Conclusion

- Efficient instantiation of ROBS as compared to previous instantiation
- Converted Shacham-Waters Ring Signatures and Boyen-Waters Group Signatures.
- Framework for projecting cum cancelling is not essential for converting any existing scheme, but gives efficient instantiation of round optimal blind signature scheme.

References

[BGN05] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-DNF formulas on ciphertexts. In *TCC*, pages 325–341, 2005.

[BW07] Xavier Boyen and Brent Waters. Full-domain subgroup hiding and constant-size group signatures. In *PKC 2007*, pages 1–15, 2007.

[Fre10] David Mandell Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In *EUROCRYPT*, pages 44–61, 2010.

[MSF10] Sarah Meiklejohn, Hovav Shacham, and David Mandell Freeman. Limitations on transformations from composite-order to prime-order groups: The case of round-optimal blind signatures. In *ASIACRYPT*, pages 519–538, 2010.

[SC12] Jae Hong Seo and Jung Hee Cheon. Beyond the limitation of prime-order bilinear groups, and round optimal blind signatures. In *TCC*, pages 133–150, 2012.

[SW07] Hovav Shacham and Brent Waters. Efficient ring signatures without random oracles. In *PKC 2007*, pages 166–180, 2007.

Converting cryptographic schemes from composite-order to prime-order pairing

R. Kabaleeshwaran

Dept of CSA,
Indian Institute of Science, Bangalore

April 8th, EECS SYMPOSIUM 2017, Bangalore

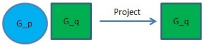
Joint work with Sanjit Chatterjee and M. Prem Laxman Das

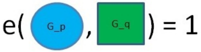
Motivation

- In 2005, Boneh-Goh-Nissim (BGN) proposed partial homomorphic encryption scheme
- BGN setting: $G = \langle g \rangle$, $|G| = p \cdot q$, $g_1 \in G_p \subset G$, $e : G \times G \to G_T$
- Ciphertext $c = g^m g_1^r$ with $m \in \{0,1\}^n$, for small n
  - Additive homomorphism: $c_1 \cdot c_2 = g^{m_1+m_2} g_1^{r_1+r_2}$
  - One-time multiplicative homomorphism: $e(c_1, c_2) = e(g,g)^{m_1 m_2} e(g, g_1)^r$
  - Evaluate quadratic polynomial on ciphertexts
- secure under subgroup decision problem (SDP) in G
- Application: E-voting scheme
- Inefficient: defined over composite-order group
  - Approx. 254 times slower than prime order pairing

Background

Freeman defined two properties for converting to prime-order pairing

- Projecting: 

- Cancelling: 

Major conversion steps

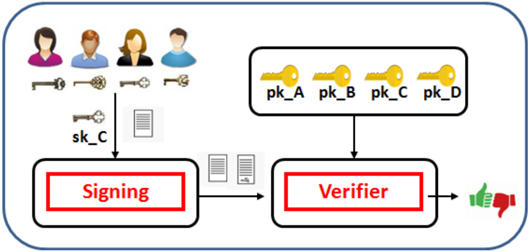
1. Express the scheme in the abstract group framework
    - Translate BGN scheme from symmetric to asymmetric groups,
2. Translate the corresponding security assumption to general framework,
    - Translate SDP in G to (2,1)-SDP in $\mathbb{G}_1^2$ and $\mathbb{G}_2^2$, which is reduced from DDH in $\mathbb{G}_1$ and $\mathbb{G}_2$
3. Instantiate scheme and argue the security in the abstract groups,
    - Prove the security of BGN under DDH in $\mathbb{G}_1$ and $\mathbb{G}_2$

- Partial list of composite-order schemes:
  - Katz-Sahai-Waters predicate encryption
  - Shen-Shi-Waters predicate encryption in private-key setting
  - Lewko-Waters identity based encryption
  - Shacham-Waters ring signature scheme
  - Meiklejohn et al.'s round optimal blind signature scheme
  - Boyen-Waters group signature scheme, etc.,
- Frameworks available
  - Projection frameworks: Groth-Sahai, Freeman, Seo's optimal symmetric and Herold et al's polynomial
  - Cancelling frameworks: Freeman, Okamoto-Takashima (Dual pairing vector spaces - DPVS)
  - Projecting cum cancelling framework: Seo-Cheon, Lewko-Meiklejohn
  - Projecting and Translating: Seo-Cheon

Cryptosystems - converting frameworks

- Protocol-centric approach - comparative analysis of different frameworks
- This talk:
  - Shacham-Waters ring signature scheme - Not yet converted
  - More efficient instantiation of round optimal blind signature scheme

Ring Signature Scheme



- Ring hides the actual signer in a ring of public keys
- Security attributes:
  - Anonymous - signature should hide the signer information
  - Unforgeable - one of the member should sign the message

Application: Govt. officials exposing the corruption without revealing their identity

Shacham-Waters Ring Signature

- Defined in symmetric composite order group G, $|G| = p \cdot q$
- Cryptographic tools - GOS NIWI proof (hides signers pk) + Waters signatures (generates the signature)
- Anonymity under SDP in G
- Unforgeability (UF) under security of Waters signature in G_q
- UF proof requires
  - Cancelling - well-formedness of the public parameter and ring signature
  - Projecting - obtain CDH solution from forgery

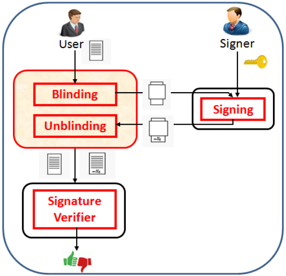
Our instantiation

- Extended Freeman projection definition to projection with full decomposition
  - $G = G_1 \oplus G_2 \cong \mathbb{G}_1^2$, $H = H_1 \oplus H_2 \cong \mathbb{G}_2^2$ and $G_T = \mathbb{G}_T^4$, $e : G \times H \to G_T$ is defined using tensor product
- Anonymity under SDP; UF under co-DHP+ in $\mathbb{G}_1$ and $\mathbb{G}_2$,
- UF proof uses only projecting,
  - We avoid cancelling by using full decomposition setting
  - Simulator constructs the subgroup, can compute $g_1^a \to g_2^a$
- More efficient instantiation as compared to Seo-Cheon's projecting cum cancelling framework

Framework	Freeman	Seo-Cheon
$1G, 1H, 1G_T$	$2\mathbb{G}_1$, $2\mathbb{G}_2$, $4\mathbb{G}_T$	$4\mathbb{G}_1$, $4\mathbb{G}_2$, $2\mathbb{G}_T$
O_G, O_H, O_{G_T}	$2O_G, 2O_H$, $4O_{G_T}$	$4O_G, 4O_H, 2O_{G_T}$
$1P$	$4\mathbb{P}$	$4\mathbb{P} + 2M_{\mathbb{G}_T}$

The operation O can be either exponentiation or multiplication or inversion.

Blind signature



- User blind the message and unblind the signature
- Security attributes:
  - Blindness: Signer should not learn any information about message
  - Unforgeability: Conservation of signature, user cannot produce forgery

Application: E-Cash, E-Voting

Blind Signature

Meiklejohn-Shacham-Freeman's construction

- Defined in composite-order group G, $|G| = p \cdot q$
- Cryptographic tools - GOS NIWI proof (hides the message from signer) + Waters signatures
- Blindness under SDP in G
- Unforgeability (UF) proof requires
  - Cancelling - well-formedness of blinded signature
  - Projecting - obtain CDH solution from forgery

Seo-Cheon's prime order instantiation

- Converted using projecting framework in symmetric pairing
- Used additional property called "translating property"
- Used projecting property and avoided cancelling property

Our approach

Defined unbalanced unbalanced projecting framework

- Formulate variant of Freeman projecting framework in unbalanced pairing setting, $G = \mathbb{G}_1^2$, $\mathbb{H}^3 \subset \mathbb{G}_1^3 \times \mathbb{G}_2^3$, $G_T = \mathbb{G}_T^6$, e - tensor product.
- UF proof uses Seo-Cheon proof strategy,
  - secure under co-DHP* in $\mathbb{G}_1$ and $\mathbb{G}_2$
  - uses only projecting, neither cancelling nor translating
  - Proof strategy: simulator construct the subgroups generator exponent and uses the knowledge of these exponents
- Blindness under NIWI proof system defined in G and $\mathbb{H}^3$
  - used random self reducibility for tighter reduction

Efficient Analysis

- Convert ROBS using Seo-Cheon framework
- Signature size is better in unbalanced framework
- Time computation of Sign() and Verify() is better in Seo-Cheon framework

Conclusion

- Framework for projecting cum cancelling is not essential for converting any existing scheme, but gives efficient instantiation of ROBS
- Instantiated
  - Shacham-Waters ring signatures
  - Meiklejohn et al.'s round optimal blind signatures
  - Boyen-Waters group signatures.

Further Reading I

[CDK-2017] Sanjit Chatterjee, M. Prem Laxman Das and R. Kabaleeshwaran, “Converting pairing-based cryptosystems from composite to prime order setting – A comparative analysis”, (*In submission*)