Identity-Based Encryption: A 30-Minute Tour

Palash Sarkar

Applied Statistics Unit
Indian Statistical Institute, Kolkata
India
palash@isical.ac.in

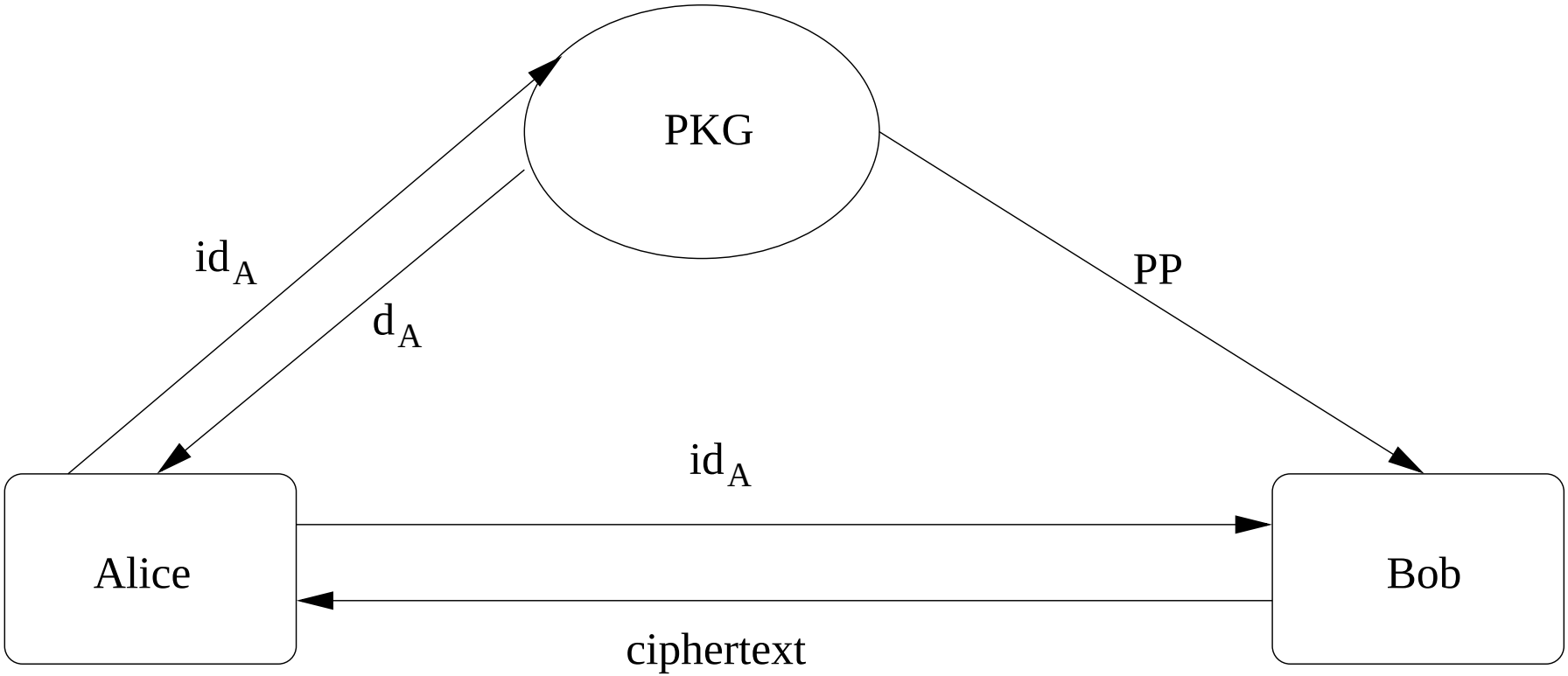


Structure of the Presentation

- A brief overview of IBE.
- Some constructions.
- Some issues.



Identity-Based Encryption



Bob sends a message to Alice.

Identity-Based Encryption

Proposed by Shamir in 1984.



Identity-Based Encryption

Proposed by Shamir in 1984.

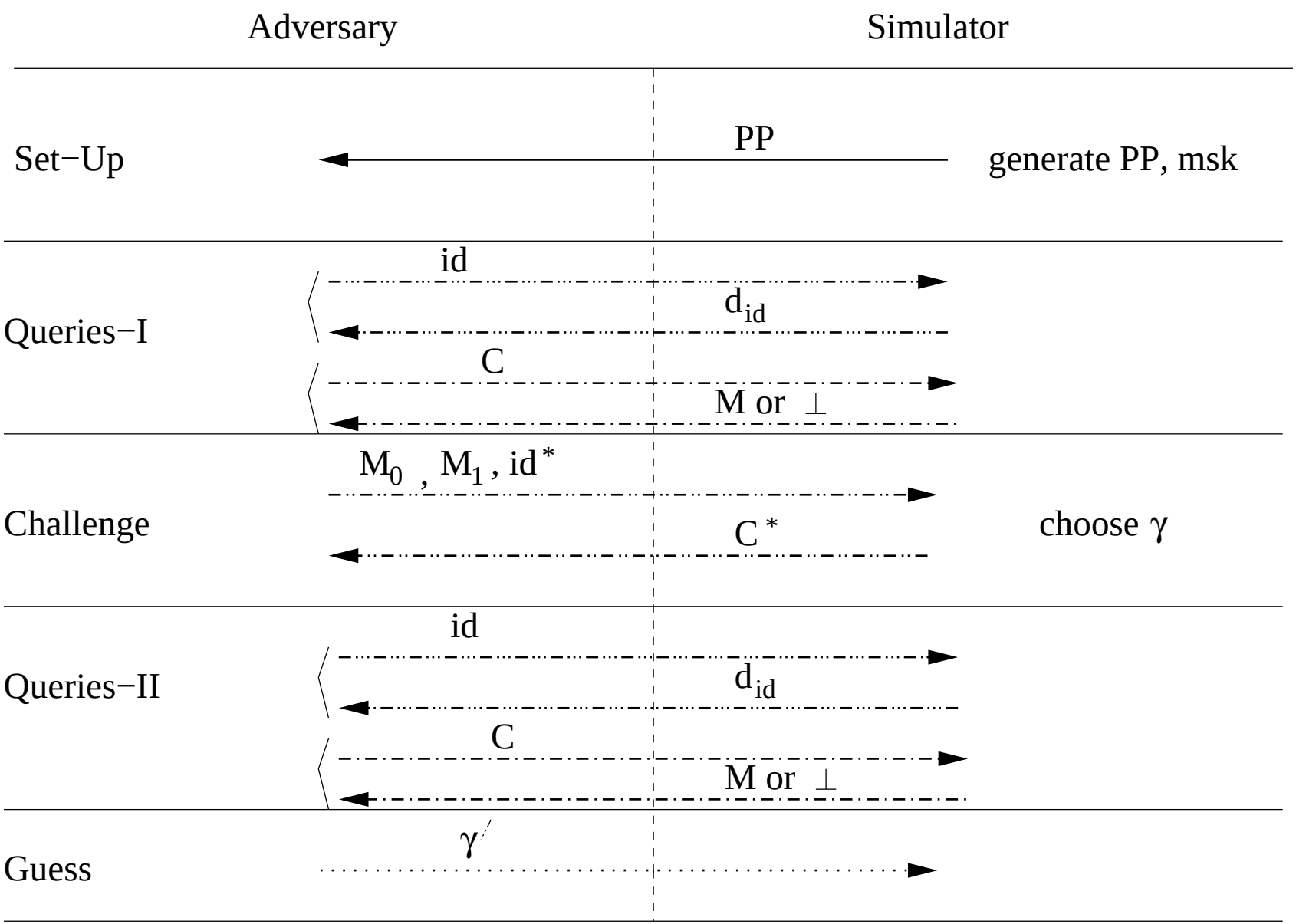
Solutions:

- Cocks: 2001.
- Sakai, Ohgishi and Kasahara: 2000.
  - Described an identity-based key agreement scheme.
- Boneh and Franklin: 2001.

- Cocks' solution was based on quadratic residues.
- SOK and BF were based on bilinear maps.
- BF provided an appropriate security model.
- The BF work spurred a great deal of later research.



Identity-Based Encryption: Security Model



Identity-Based Encryption: Security Model

“Full” model: supports adaptive-identity and adaptive-ciphertext queries in an interleaved fashion.



Identity-Based Encryption: Security Model

"Full" model: supports adaptive-identity and adaptive-ciphertext queries in an interleaved fashion.

Restricted Models:

- CPA-secure: Ciphertext queries not allowed.
- Selective-identity: The challenge identity id^* is to be provided by the adversary even before receiving the PP.



Construction Approaches

- Based on quadratic residues.
- Based on lattices.
- Based on bilinear pairings of elliptic curve groups.



Cocks' IBE

Setting: $N = pq$;
$J(N)$: set of elements with Jacobi symbol 1 modulo N;
$QR(N)$: set of quadratic residues modulo N.



Cocks' IBE

Setting: $N = pq$;
$J(N)$: set of elements with Jacobi symbol 1 modulo N;
$QR(N)$: set of quadratic residues modulo N.

Public Parameters.
N; $u \xleftarrow{\$} J(N) \setminus QR(N)$;
(u is a random pseudo-square;)
hash function $H()$ which maps identities into $J(N)$.
Master Secret Key: p and q.



Cocks' IBE

Setting: $N = pq$;
$J(N)$: set of elements with Jacobi symbol 1 modulo N;
$QR(N)$: set of quadratic residues modulo N.

Public Parameters.
N; $u \xleftarrow{\$} J(N) \setminus QR(N)$;
(u is a random pseudo-square;)
hash function $H()$ which maps identities into $J(N)$.
Master Secret Key: p and q.

Key Gen: identity id.
$R = H(\text{id})$; $r = \sqrt{R}$ or $\sqrt{uR}$ according as R is square or not;
$d_{\text{id}} = r$.



Cocks' IBE (contd.)

Encryption: bit m, identity id.

- $R = H(\text{id})$; $t_0, t_1 \xleftarrow{\$} \mathbb{Z}_N$;
- compute $d_a = (t_a^2 + u^a R)/t_a$ and $c_a = (-1)^m \cdot (\frac{t_a}{N})$;
- ciphertext: $((d_0, c_0), (d_1, c_1))$.

Decryption: ciphertext $((d_0, c_0), (d_1, c_1))$, identity id; $d_{\text{id}} = r$:

- $R = H(\text{id})$; set $a \in \{0, 1\}$ such that $r^2 = u^a R$;
- set $g = d_a + 2r$; (note $g = \left(\frac{(t_a + r)^2}{t_a}\right)$ and so, $(\frac{g}{N}) = (\frac{t_a}{N})$;)
- compute $(-1)^m$ to be $c_a \cdot (\frac{g}{N})$.



Cocks' IBE: Discussion

- Ciphertext expansion is large; efficiency not good.
- Boneh, Gentry and Hamburg (2007) obtained improved space efficiency by reusing randomness; but, encryption and decryption efficiencies are worse.
- Jhanwar and Barua (2008) consider the problem of improving efficiency.



Cocks' IBE: Discussion

- Ciphertext expansion is large; efficiency not good.
- Boneh, Gentry and Hamburg (2007) obtained improved space efficiency by reusing randomness; but, encryption and decryption efficiencies are worse.
- Jhanwar and Barua (2008) consider the problem of improving efficiency.

This approach currently does not lead to practical schemes.



Lattice-Based Approach

Gentry, Peikert and Vaikuntanathan (2008).

- Based on a technique called efficient Pre-Image Sampling.
  - This technique naturally leads to a signature scheme.
  - By considering the decryption key corresponding to an identity to be the PKG's signature on the identity (cf. Naor) suggests an IBE scheme.
- Security is based on the hardness of the Learning With Errors (LWE) problem.
- Later work have improved efficiency and provided constructions of hierarchical IBE (HIBE) schemes.



Lattice-Based Approach: Pros and Cons

Motivation:

- Multi-precision arithmetic not required;
- Security based on the hardness of worst-case instance;
- No known quantum algorithm for solving lattice problems.



Lattice-Based Approach: Pros and Cons

Motivation:

- Multi-precision arithmetic not required;
- Security based on the hardness of worst-case instance;
- No known quantum algorithm for solving lattice problems.
- These apply to all lattice problems and are not specific to lattice-based IBE.



Lattice-Based Approach: Pros and Cons

Motivation:

- Multi-precision arithmetic not required;
- Security based on the hardness of worst-case instance;
- No known quantum algorithm for solving lattice problems.
- These apply to all lattice problems and are not specific to lattice-based IBE.

Cons:

- The sizes of keys and ciphertexts are far too large compared to pairing-based schemes.



Pairing

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T.$$

- $\mathbb{G}_1$ and $\mathbb{G}_2$ are sub-groups of points on an elliptic curve; $\mathbb{G}_T$ is a sub-group of the multiplicative group of a finite field.
- Types of pairings:
  - **Type-1:** $\mathbb{G}_1 = \mathbb{G}_2$ (symmetric pairing).
  - **Type-2:** An efficiently computable isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$ is known.
  - **Type-3:** There is no known efficiently computable isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$ (or vice versa).
- **Type-3** pairings are the fastest to compute and provide the most compact parameter sizes.



Boneh-Franklin IBE

- **Setup:** $\mathbb{G}_1 = \langle P \rangle$, $s \xleftarrow{\$} \mathbb{Z}_p$, $Q = sP$;
  $\mathsf{PP} = (P, Q, H_1(), H_2())$, $\mathsf{msk} = s$.
- **Key-Gen:** Given id, compute $Q_{\mathsf{id}} = H_1(\mathsf{id})$; $d_{\mathsf{id}} = sQ_{\mathsf{id}}$.
- **Encrypt:** Choose $r \xleftarrow{\$} \mathbb{Z}_p$; $C = (rP, M \oplus H_2(\underbrace{e(Q, Q_{\mathsf{id}})^r}))$
- **Decrypt:** Given $C = (U, V)\rangle$ and d_{id} compute
  $V \oplus H_2(\underbrace{e(U, d_{\mathsf{id}})}) = M$.



Boneh-Franklin IBE

- **Setup:** $\mathbb{G}_1 = \langle P \rangle$, $s \xleftarrow{\$} \mathbb{Z}_p$, $Q = sP$;
  $\mathsf{PP} = (P, Q, H_1(), H_2())$, $\mathsf{msk} = s$.
- **Key-Gen:** Given id, compute $Q_{\mathsf{id}} = H_1(\mathsf{id})$; $d_{\mathsf{id}} = sQ_{\mathsf{id}}$.
- **Encrypt:** Choose $r \xleftarrow{\$} \mathbb{Z}_p$; $C = (rP, M \oplus H_2(\underbrace{e(Q, Q_{\mathsf{id}})^r}))$
- **Decrypt:** Given $C = (U, V)\rangle$ and d_{id} compute
  $V \oplus H_2(\underbrace{e(U, d_{\mathsf{id}})}) = M$.

Correctness:

$$e(U, d_{ID}) = e(rP, sQ_{ID}) = e(sP, Q_{ID})^r = e(Q, Q_{ID})^r.$$



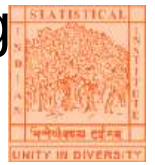
Boneh-Franklin IBE

- **Setup:** $\mathbb{G}_1 = \langle P \rangle$, $s \xleftarrow{\$} \mathbb{Z}_p$, $Q = sP$;
  $\mathsf{PP} = (P, Q, H_1(), H_2())$, $\mathsf{msk} = s$.
- **Key-Gen:** Given id, compute $Q_{\mathsf{id}} = H_1(\mathsf{id})$; $d_{\mathsf{id}} = sQ_{\mathsf{id}}$.
- **Encrypt:** Choose $r \xleftarrow{\$} \mathbb{Z}_p$; $C = (rP, M \oplus H_2(\underbrace{e(Q, Q_{\mathsf{id}})^r}))$
- **Decrypt:** Given $C = (U, V)\rangle$ and d_{id} compute
  $V \oplus H_2(\underbrace{e(U, d_{\mathsf{id}})}) = M$.

Correctness:

$$e(U, d_{ID}) = e(rP, sQ_{ID}) = e(sP, Q_{ID})^r = e(Q, Q_{ID})^r.$$

The scheme is CPA-secure; can be converted to CCA-secure using standard techniques such as the Fujisaki-Okamoto conversion.



BF-IBE: Discussion

Pros:

- Simple, elegant, efficient, compact, ...
- Leads naturally to signature scheme, HIBE and other primitives.
- Best known practical attack: Solve DL in $\mathbb{G}_1$ or $\mathbb{G}_2$.



BF-IBE: Discussion

Pros:

- Simple, elegant, efficient, compact, ...
- Leads naturally to signature scheme, HIBE and other primitives.
- Best known practical attack: Solve DL in $\mathbb{G}_1$ or $\mathbb{G}_2$.

Cons:

- Security argument is based on random oracles.
- Security reduction to the Decisional Bilinear Diffie-Hellman (DBDH) problem is not tight.



Some Important Pairing-Based IBE Schemes

Boneh-Boyen (2004): BB-IBE1 (also BB-IBE2).

- Selective-id secure.
- Introduced the so-called “commutative blinding” framework and algebraic techniques to handle key-extraction queries.
- Described using Type-1 pairings; can be easily modified to Type-3 pairings.
- Extends easily to HIBE.
- Later used by Boyen-Mei-Waters to convert CPA-secure pairing-based schemes to CCA-secure schemes.



Some Important Pairing-Based IBE Schemes

Waters (2005):

- Adaptive-id secure without random oracles.
- Builds on BB-IBE1 and another work by Boneh and Boyen.
- Public parameter size rather large ($\approx$ 160 EC points for 80-bit security).
  - Independent follow up work by Naccache (2005) and Chatterjee-Sarkar (2005) showed how to reduce the PP size; trade-off is a looser security reduction.
- Original description in the Type-1 setting.
  - Converted to Type-2 setting by Bellare and Ristenpart (2009).
  - Converted to Type-3 setting by Chatterjee and Sarkar (2010).
- Security analysis introduced a technique called artificial abort.
  - Later analysis by Bellare-Ristenpart showed how to avoid artificial abort, but, at the cost of loosing tightness.



Some Important Pairing-Based IBE Schemes

Gentry (2006):

- Adaptive-id secure, no random oracles, tight reduction, efficient.
- But, based on the hardness of a non-static assumption, i.e., the number of elements in the instance depends on the number of queries made by the adversary.



Some Important Pairing-Based IBE Schemes

Waters (2009):

- Introduces a new technique called dual-system encryption.
- Adaptive-id secure, no random oracles, standard (static) assumption.
- Constant size public parameters.
  - For Waters (2005) and its variants the size of the PP asymptotically grows with the security parameter.
- Extends to HIBE and BE schemes.
- Uses the Type-1 setting.
  - Simplification and conversion to Type-3 setting by Ramanna-Chatterjee-Sarkar (2011).



Some Important Pairing-Based IBE Schemes

Waters (2009):

- Introduces a new technique called dual-system encryption.
- Adaptive-id secure, no random oracles, standard (static) assumption.
- Constant size public parameters.
  - For Waters (2005) and its variants the size of the PP asymptotically grows with the security parameter.
- Extends to HIBE and BE schemes.
- Uses the Type-1 setting.
  - Simplification and conversion to Type-3 setting by Ramanna-Chatterjee-Sarkar (2011).

Lewko-Waters (2010):

- Dual-system based IBE; extends to constant-size ciphertext HIBE.
- Using pairing over composite order groups and also Type-3 setting.
  - An improved variant in the Type-3 setting (coming).



An Open Problem

Obtain an IBE scheme with the following properties.

- Adaptive-id secure.
- No random oracles.
- Standard hardness assumptions.
- (Efficient – constant size parameters; constant number of scalar multiplications, pairings; ...)
- *Tight security reduction.*



An Open Problem

Obtain an IBE scheme with the following properties.

- Adaptive-id secure.
- No random oracles.
- Standard hardness assumptions.
- (Efficient – constant size parameters; constant number of scalar multiplications, pairings; ...)
- *Tight security reduction.*

Or show that this cannot be done.



Secure and Efficient IBE: A Practical Issue

Which IBE scheme should I use?



Secure and Efficient IBE: A Practical Issue

Which IBE scheme should I use?

- QR, lattice-based or pairing-based?



Secure and Efficient IBE: A Practical Issue

Which IBE scheme should I use?

- QR, lattice-based or pairing-based?
- For pairing-based schemes, the best known attack on all proposed schemes is to solve DL. So, do I use BF?



Secure and Efficient IBE: A Practical Issue

Which IBE scheme should I use?

- QR, lattice-based or pairing-based?
- For pairing-based schemes, the best known attack on all proposed schemes is to solve DL. So, do I use BF?
- For pairing-based schemes, should I care about using Type-1 versus Type-3 pairings.
  - From a security point of view, is the use of Type-3 pairing weaker because of the *assumption* that isomorphisms between $\mathbb{G}_1$ and $\mathbb{G}_2$ cannot be computed?



Secure and Efficient IBE: A Practical Issue

Which IBE scheme should I use?

- QR, lattice-based or pairing-based?
- For pairing-based schemes, the best known attack on all proposed schemes is to solve DL. So, do I use BF?
- For pairing-based schemes, should I care about using Type-1 versus Type-3 pairings.
  - From a security point of view, is the use of Type-3 pairing weaker because of the *assumption* that isomorphisms between $\mathbb{G}_1$ and $\mathbb{G}_2$ cannot be computed?
- Should I care about security reductions? If so, then
  - Should I care about selective-id versus adaptive-id models?
  - Should I care about the underlying assumptions? Should I care about static versus non-static assumptions? Among static assumptions, should I care about standard versus non-standard assumptions?
  - Should I care about the tightness of reduction?



Thank you for your attention!

