Recent Advances in Identity-based Encryption – Pairing-free Constructions

Kenny Paterson

Information Security Group

Royal Holloway, University of London

kenny.paterson@rhul.ac.uk

June 25th 2008

Overview of this Talk

The main focus in this talk is on pairing-free IBE:

- Motivation
- Cocks' IBE scheme: IBE in the RSA setting
- Boneh-Gentry-Hamburg IBE scheme
- IBE from trapdoor discrete logarithm groups
- IBE from lattice problems

1 Motivation for Pairing-free IBE

- Pairing-based IBE has seen rapid development.
- But security is based on relatively untested computational problems.
- And implementation can be complex – many choices of parameters, families of curves, implementation tricks.
- Efficiency considerations.
- Also of great theoretical interest to find alternative constructions.

2 Cocks' IBE Scheme

- Cocks's IBE scheme was proposed shortly after Boneh-Franklin IBE.
- 4 page paper published at IMA Coding and Cryptography Conference, December 2001.
- In fact, scheme was devised in late 1990's.
- Publication of Boneh-Franklin scheme allowed it to be released into the public domain.

Cocks' IBE Scheme

Setup:

1. On input a security parameter k, select $N = pq$ where p, q are large primes congruent to 3 mod 4.
2. Select $H : \{0,1\}^* \rightarrow \mathcal{J}_N$ where $\mathcal{J}_N$ denotes elements of $\mathbb{Z}_N$ with Jacobi symbol equal to $+1$.
   – This may involve iterated hashing onto $\mathbb{Z}_N$.
3. Return the public system parameters

$$\mathsf{params} = \langle N, H \rangle$$

   and master secret $\mathsf{msk} = \langle p, q \rangle$.

Cocks' IBE Scheme

Extract: Given an identity $\mathsf{ID} \in \{0,1\}^*$, set

$$d_{\mathsf{ID}} = H(\mathsf{ID})^{(N+5-(p+q))/8} \bmod N$$

as the private key.

Notice that

$$(d_{\mathsf{ID}})^2 = \pm H(\mathsf{ID}) \bmod N.$$

Cocks' IBE Scheme: Encryption

Encrypt: Inputs are a single bit message M and an identity ID.

1. Set $x = (-1)^M \in \{+1, -1\}$.
2. Choose random $t \in \mathbb{Z}_N$ such that $\left(\frac{t}{N}\right) = x$.
3. Compute the ciphertext

$$C = \left(t + \frac{H(\mathsf{ID})}{t}\right) \bmod N.$$

Cocks' IBE Scheme: Decryption

Inputs to decryption are a ciphertext C and a private key d_{ID}.
Assume (for now) that $(d_{\mathsf{ID}})^2 = +H(\mathsf{ID}) \bmod N$.

Notice that

$$\begin{aligned} C + 2d_{\mathsf{ID}} &= t + 2d_{\mathsf{ID}} + \frac{H(\mathsf{ID})}{t} \\ &= t(1 + d_{\mathsf{ID}}/t)^2 \bmod N \end{aligned}$$

so that

$$\left(\frac{C + 2d_{\mathsf{ID}}}{N}\right) = \left(\frac{t}{N}\right) = x.$$

Cocks' IBE Scheme: Decryption

Hence the following decryption procedure is correct:

Decrypt:

1. Compute
$$x = \left(\frac{C + 2d_{\mathsf{ID}}}{N}\right).$$
2. If $x = 1$, output $M = 0$, otherwise output $M = 1$.

Cocks' IBE Scheme: Decryption

- If $(d_{\mathsf{ID}})^2 = -H(\mathsf{ID}) \bmod N$, then sender should compute the ciphertext
$$C = (t - \frac{H(\mathsf{ID})}{t}) \bmod N$$
and recipient can decrypt as before.

- Problem is that sender does not (in general) know which equation recipient's private key satisfies:
$$(d_{\mathsf{ID}})^2 = +H(\mathsf{ID}) \quad \text{or} \quad (d_{\mathsf{ID}})^2 = -H(\mathsf{ID}).$$

- Solution is for sender to "hedge" and send as the ciphertext:
$$C = \langle (t + \frac{H(\mathsf{ID})}{t}) \bmod N, (t' - \frac{H(\mathsf{ID})}{t'}) \bmod N \rangle.$$

Cocks' IBE Scheme: Security

- IND-ID-CPA security (in ROM) is based on hardness of the *quadratic residuosity problem* in $\mathbb{Z}_N$:
  - Given $a \in_R \mathbb{Z}_N$ with $\left(\frac{a}{N}\right) = 1$, decide whether a is a square or a non-square modulo N.
- This problem is known to be not harder than integer factorisation
  - i.e. an efficient algorithm to factorise N leads to an efficient algorithm to solve the quadratic residuosity problem in $\mathbb{Z}_N$.
  - But equivalence with integer factorisation not known.
- Same hard problem as basis for security of Goldwasser-Micali probablistic encryption scheme.

Cocks' IBE Scheme: Security

- Original Cocks paper includes only a sketch proof of the IND-ID-CPA security proof.
- A good exercise to write down a formal proof in the ROM.
- IND-ID-CCA security using Fujisaki-Okamoto conversion.

Cocks' IBE Scheme: Efficiency

- Scheme is computationally efficient: to encrypt a single bit of message, only simple Jacobi symbol calculations and inversions modulo N are needed.
- But scheme is very wasteful in terms of bandwidth: to transmit a single bit requires $2\log_2 N$ bits of ciphertext.
- Can expect $\log_2 N \approx 1024$ for 80-bit security level.
- Hence to transport an 80-bit symmetric key, we'd need $80 \cdot 2 \cdot 1024 = 160$ kbits of ciphertext.

Cocks' IBE Scheme: Open Problems

- It has been a major open problem to find a bandwidth-efficient scheme using the same number-theoretic setting as Cocks' scheme.
- Cocks' approach does not seem to lend itself to further applications in the same way that Boneh-Franklin IBE does.
- Quiz question: What is the (Naor-style) signature scheme corresponding to Cocks' IBE scheme?
- Is there an ID-NIKD scheme related to Cocks' IBE scheme?

3 Boneh-Gentry-Hamburg IBE

- Paper published at FOCS'2007 and as IACR eprint 2007/177.
- Solves the major open problem from Cocks: bandwidth-efficient IBE based on quadratic residuosity problem.
- Encryption of ℓ-bit message needs about $\ell + \log_2 N$ bits instead of $2\ell \log_N$ bits.
- But encryption time is quartic in $\log_2 N$ (instead of cubic as in, say, RSA encryption) and private keys are large.

Boneh-Gentry-Hamburg IBE – Overview

Suppose $\mathcal{Q}$ is a deterministic algorithm that, given input (N, R, S) with $R, S \in \mathbb{Z}_N$, outputs polynomials f, g satisfying:

1. If $R, S \in \mathcal{QR}_N$, then $f(r)g(s) \in \mathcal{QR}_N$ for all square roots r of R and s of S.
2. If $R \in \mathcal{QR}_N$, then $f(r)f(-r)S \in \mathcal{QR}_N$ for all square roots r of R.

Then $\mathcal{Q}$ is said to be *IBE Compatible.*

Notice that, in this case,

$$\left(\frac{f(r)}{N}\right) = \left(\frac{g(s)}{N}\right).$$

BGH IBE – Single-bit Construction

Setup:

1. On input a security parameter k, select $N = pq$ where p, q are large primes congruent to 3 mod 4.
2. Select $H : \{0,1\}^* \rightarrow \mathcal{J}_N$.
3. Select $u \in_R \mathcal{J}_N \setminus \mathcal{QR}_N$.
4. Return the public system parameters

$$\mathsf{params} = \langle N, H, u \rangle$$

and the master secret $\mathsf{msk} = \langle p, q \rangle$.

BGH IBE – Single-bit Construction

Extract: Given an identity $\mathsf{ID} \in \{0,1\}^*$, set:

- $d_{\mathsf{ID}} = H(\mathsf{ID})^{1/2}$ if $H(\mathsf{ID}) \in \mathcal{QR}_N$, or
- $d_{\mathsf{ID}} = (uH(\mathsf{ID}))^{1/2}$ if $H(\mathsf{ID}) \in \mathcal{QNR}_N$.

BGH IBE – Single-bit Construction

Encrypt: Inputs are a single bit message M and an identity ID.

1. Set $x = (-1)^M \in \{+1, -1\}$.
2. Choose random $s \in \mathbb{Z}_N$ and set $S = s^2 \bmod N$.
3. Run IBE compatible algorithm $\mathcal{Q}$ twice:

$$(f, g) \leftarrow \mathcal{Q}(N, H(\mathsf{ID}), S), \quad (f', g') \leftarrow \mathcal{Q}(N, uH(\mathsf{ID}), S).$$

4. Compute the ciphertext

$$C = \langle S, x \cdot \left(\frac{g(s)}{N}\right), x \cdot \left(\frac{g'(s)}{N}\right) \rangle$$

BGH IBE – Single-bit Construction

Inputs to decryption are a ciphertext C and a private key d_{ID}.
Assume (for now) that $H(\mathsf{ID}) \in \mathcal{QR}_N$. Then d_{ID} is a square root of $H(\mathsf{ID})$. So:

$$\left(\frac{f(d_{\mathsf{ID}})}{N}\right) = \left(\frac{g(s)}{N}\right).$$

Hence the following decryption procedure is correct:

Decrypt: Given input $C = \langle S, c, c' \rangle$:

1. Run $\mathcal{Q}$ on input $(N, H(\mathsf{ID}), S)$ to produce polynomials (f, g).
2. Compute
$$x = c \cdot \left(\frac{f(d_{\mathsf{ID}})}{N}\right).$$
3. If $x = 1$, output $M = 0$, otherwise output $M = 1$.

BGH IBE – Single-bit Construction

Assuming that $H(\mathsf{ID}) \in \mathcal{QNR}_N$, then $uH(\mathsf{ID}) \in \mathcal{QR}_N$ and $d_{\mathsf{ID}}^2 = uH(\mathsf{ID})$.

Hence the following decryption procedure is correct in this case:

Decrypt: Given input $C = \langle S, c, c' \rangle$:

1. Run $\mathcal{Q}$ on input $(N, uH(\mathsf{ID}), S)$ to produce polynomials (f', g').
2. Compute
$$x = c' \cdot \left(\frac{f'(d_{\mathsf{ID}})}{N} \right).$$
3. If $x = 1$, output $M = 0$, otherwise output $M = 1$.

BGH IBE – Multi-bit Construction

- So far, we have been encrypting one plaintext bit at a time, with little apparent benefit over Cocks' scheme.
- Main improvement comes from re-using a single S value across many bits of plaintext $M = M_1, \ldots, M_\ell$.
- Now set $R_i = H(\mathsf{ID}, i)$ for $i = 1, \ldots, \ell$.
- Use pairs (S, R_i) for encrypting message bit i, as before.
- Transmit single S value and an additional 2 bits of ciphertext c_i, c'_i per message bit.
- Size of ciphertext is now $2\ell + \log_2 N$ bits for ℓ-bit message.

BGH IBE – Multi-bit Construction

- Recipient needs a private key component $d_{\mathsf{ID},i}$ corresponding to each value $R_i = H(\mathsf{ID}, i)$.
- Hence scheme has large private keys ($\ell \log_2 N$ bits).
- Each $d_{\mathsf{ID},i}$ needs to be a square root of $H(\mathsf{ID}, i)$ or of $uH(\mathsf{ID}, i)$.
- Care is needed to generate square roots in a unpredictable but deterministic manner.

BGH IBE – Security of Simplified Construction

- IND-ID-CPA security of the multi-bit version of the simplified BGH construction can be proven based on the hardness of the quadratic residuosity problem in $\mathbb{Z}_N$.
- Proof in the random oracle model, with a tight security reduction.
- More advanced ideas can be used to obtain a scheme with:
  - Shorter ciphertexts ($\ell + \log_2 N$ bits instead of $2\ell + \log_2 N$ bits).
  - Recipient anonymity.
  - Security proof in the standard model, based on an interactive version of the quadratic residuosity assumption.

BGH IBE – An IBE Compatible Algorithm

We have yet to show an algorithm $\mathcal{Q}$ that, given input (N, R, S) with $R, S \in \mathbb{Z}_N$, outputs polynomials f, g satisfying:

1. If $R, S \in \mathcal{QR}_N$, then $f(r)g(s) \in \mathcal{QR}_N$ for all square roots r of R and s of S.
2. If $R \in \mathcal{QR}_N$, then $f(r)f(-r)S \in \mathcal{QR}_N$ for all square roots r of R.

BGH IBE – An IBE Compatible Algorithm

Algorithm $\mathcal{Q}(N, R, S)$:

- Construct a solution (x, y) to the equation:

$$Rx^2 + Sy^2 = 1 \bmod N.$$

- Output $f(r) = xr + 1$ and $g(s) = 2ys + 2$.

IBE compatibility?

BGH IBE – An IBE Compatible Algorithm

Suppose r, s are square roots of R, S (respectively, if these exist).
Then:

$$\begin{aligned} f(r)g(s) &= (xr+1)(2ys+2) \\ &= 2xrys + 2xr + 2ys + 2 + (Rx^2 + Sy^2 - 1) \\ &= (xr + ys + 1)^2 \bmod N. \end{aligned}$$

Hence $f(r)g(s) \in \mathcal{QR}_N$. Moreover,

$$f(r) \cdot f(-r) \cdot S = \ldots = (Sy)^2 \bmod N.$$

BGH IBE – Solving $Rx^2 + Sy^2 = 1 \bmod N$

- We need to solve this equation twice for each bit of the plaintext.
- BGH paper contains several algorithmic tricks for doing this.
- One idea is to use the Pollard-Schnorr algorithm that was introduced to break the Ong-Schnorr-Shamir signature scheme.
- Another is to lift to an equation over the integers to obtain a ternary quadratic form:

$$\hat{R}x^2 + \hat{S}y^2 - z^2 = 0$$

  and then use an algorithm of Cremona and Rusin (itself using lattice reduction).
- Further optimisations possible because we only need 2ℓ solutions to related problems.

4 IBE From Trapdoor Discrete Logarithm Groups

A Trapdoor Discrete Log group generator (TDL group generator) is defined by a pair of algorithms `TDLGen` and `SolveDL`:

- `TDLGen`: An algorithm that takes a security parameter 1^k as input and outputs (G, r, g, T) where G is a (description of a) cyclic group of some order r with generator g and T denotes trapdoor information.
- `SolveDL`: An algorithm which takes as input (G, r, g, T) and a group element h and outputs $a \in \mathbb{Z}_r$ such that $h = g^a$.

IBE From Trapdoor Discrete Logarithm Groups

- r, the group order, need not be prime (allows us to handle both RSA and elliptic curve settings)
- In the RSA setting, r must be kept secret by the party running the `TDLGen` algorithm.
  - We assume instead that a suitable bound R on the group order is available as part of the description of G.
- We do not insist that `SolveDL` runs in time polynomial in k.
- We will require CDH to still be hard in G without knowledge of T.

IBE From Trapdoor Discrete Logarithm Groups

Construction due to P. and Srinivasan (IACR eprint 2007/453):

`Setup:` On input 1^k, this algorithm runs `TDLGen` to obtain (G, r, g, T). It outputs $\mathsf{params} = \langle G, g, H_1, H_2, n \rangle$ where $H_1 : \{0,1\}^* \to G$ and $H_2 : G \to \{0,1\}^n$ are hash functions and n is the size of plaintexts. It also outputs $\mathsf{msk} = \langle G, g, H_1, H_2, n, r, T \rangle$.

`Extract:` On input msk and identifier $\mathsf{ID} \in \{0,1\}^*$, run `SolveDL` on input $H_1(\mathsf{ID})$ to obtain a value $d_{\mathsf{ID}} \in \mathbb{Z}_r$ such that

$$g^{d_{\mathsf{ID}}} = H_1(\mathsf{ID}).$$

The algorithm then outputs d_{ID}.

IBE From Trapdoor Discrete Logarithm Groups

`Encrypt:` On input params, identifier $\mathsf{ID} \in \{0,1\}^*$ and message M, this algorithm returns a ciphertext $C = \langle U, V \rangle$ where:

$$U = g^s, \quad V = M \oplus H_2(H_1(\mathsf{ID})^s), \quad \text{where } s \in_R \mathbb{Z}_r.$$

`Decrypt:` On input params, a private key d_{ID} and a ciphertext $C = \langle U, V \rangle$, this algorithm outputs $M = V \oplus H_2(U^{d_{\mathsf{ID}}})$.

Decryption works because:

$$U^{d_{\mathsf{ID}}} = g^{s \cdot d_{\mathsf{ID}}} = H_1(\mathsf{ID})^s$$

- Essentially, we have an ID-based version of Elgamal encryption.
- We have key pair $(d_{\mathsf{ID}}, H(\mathsf{ID}) = g^{d_{\mathsf{ID}}})$ in place of usual (x, g^x).

Security of IBE From Trapdoor Discrete Logarithm Groups

- IND-ID-CPA security can be proved based on the hardness of Computational Diffie-Hellman problem in G, a trapdoor discrete log group.
- Proof models H_1 and H_2 as random oracles.
- IND-ID-CCA security can be obtained by applying a Fujisaki-Okamoto conversion.

So: do we have any trapdoor discrete log groups G for which we can construct a function H_1 hashing onto G?

An RSA-based Instantiation

- Set $N = pq$ where $p = 3 \bmod 4$, $q = 1 \bmod 4$, and $\gcd(p-1, q-1) = 2$.
- Let $g \in \mathbb{Z}_N$ be such that $g_p = g \bmod p$ is primitive in $\mathbb{Z}_p$ and $g_q = g \bmod q$ is primitive in $\mathbb{Z}_q$.
- Then g has maximal order $(p-1)(q-1)/2$ and $\left(\frac{g}{N}\right) = 1$.
- Let $G = \langle g \rangle$. Then $G = \mathcal{J}_N$.
- Hashing onto G:
  - We have $\left(\frac{-1}{N}\right) = -1$.
  - Let $H : \{0,1\}^* \to \mathbb{Z}_N$ be a hash function.
  - Then define

$$H_1(\mathsf{ID}) = \left(\frac{H(\mathsf{ID})}{N}\right) \cdot H(\mathsf{ID}).$$

An RSA-based Instantiation

- Now we assume that, for some fixed B to be determined, both $p-1$ and $q-1$ are B-smooth.
- We can use Pollard's ρ algorithm and Pohlig-Hellman algorithm to find discrete logs in $\mathbb{Z}_p$ and $\mathbb{Z}_q$ in time $O(\ell B^{1/2})$, where ℓ is the number of prime factors of $p-1$ and $q-1$.
- So, given trapdoor $\langle p, q \rangle$, we can solve DLP in G in time $O(\ell B^{1/2})$.

An RSA-based Instantiation

- Without the trapdoor, solving DLP in $G = \mathcal{J}_N$ is known to be equivalent to factoring N.
- Best (known) algorithm is NFS (with running time $L_N(1/3, c)$) or Pollard's $p-1$ algorithm (running time $O(B \log N / \log B)$).
- By appropriate choice of N, we can achieve an asymmetry in the time needed to solve DLP in G with and without the trapdoor.
- For $B = 2^{80}$ and $N \approx 2^{1024}$, the times are (roughly) 2^{40} and 2^{80}, respectively.

An RSA-based Instantiation

- Resulting IBE scheme has efficient encryption (two exps mod N) and decryption (one exp mod N), compact ciphertexts and public parameters, and small private keys.
- It has IND-ID-CPA/CCA security in the ROM, assuming the hardness of factoring integers of the form $N = pq$ with $p - 1$ and $q - 1$ that are B-smooth.
- Only drawback is the 2^{40} effort required for each private key extraction.
- This scheme is a variant of the Maurer-Yacobi scheme from Eurocrypt 1991.
  - Maurer-Yacobi actually presented an ID-NIKDS scheme.
  - Their scheme (and later variants) omitted hashing.

An Instantiation from Elliptic Curves

- GHS (Eurocrypt 2002) and Teske (JoC, 2004) proposed the use of Weil descent to build a trapdoor discrete log for the elliptic curve setting.
- Main idea is to build a special curve $E(\mathbb{F}_{q^k})$ and an explicit homomorphism $\Phi : E(\mathbb{F}_{q^k}) \to J_C(\mathbb{F}_q)$ where C is a hyperelliptic curve of high genus.
- DLP in $J_C(\mathbb{F}_q)$ can be solved in sub-exponential time using index-calculus approach.
- $E(\mathbb{F}_{q^k})$ can be "disguised" using a random walk of isogenies to create a seemingly random curve $E'(\mathbb{F}_{q^k})$.
- So DLP in $E'(\mathbb{F}_{q^k})$ should take time $O(q^{k/2})$ using generic algorithms.

An Instantiation from Elliptic Curves

- This gives us a trapdoor for the discrete log problem in a cyclic subgroup $\langle P' \rangle$ of $E'(\mathbb{F}_{q^k})$:
    - Use inverse of random walk of isogenies to map DLP from $E'(\mathbb{F}_{q^k})$ to $E(\mathbb{F}_{q^k})$
    - Then use Φ to map DLP to $J_C(\mathbb{F}_q)$.
- Example parameters: $q = 2^{23}$, $k = 7$, giving (conjectured) 80 bits of security.

An Instantiation from Elliptic Curves

- Resulting IBE scheme requires 2 (resp. 1) scalar multiplications on $E'(\mathbb{F}_{2^{161}})$ for encryption (resp. decryption).
- Fast hashing onto subgroup of E' using standard techniques.
- Hence extremely fast encryption and decryption, with compact ciphertexts, public parameters and private keys.
- Index calculus techniques make finding many discrete logs almost as easy as finding one.
  - So amortised cost of roughly 2^{26} bit operations per private key extraction.
- Well suited to deployment in constrained environments with a computationally meaty TA.

TDL Groups: Open Problems

- Neither of our instantiations is completely satisfactory from a practical perspective.
- We have very efficient schemes (in terms of encryption and decryption), but:
  - RSA setting: relatively high cost of extracting discrete logs with trapdoor compared to without.
  - ECC setting: uncertainty over hardness of DLP on chosen curves (depends on effectiveness of using isogenies to disguise E); scalability to higher security levels.
- A truly efficient trapdoor for the DLP in some class of cryptographically interesting groups would have many applications in cryptography!

5 IBE From Lattice Problems

- Recent paper of Gentry, Peikert and Vaikuntanathan (STOC 2008 and IACR eprint 2007/432).
- IBE schemes (and much else) based on hardness of "learning with error" (LWE) problem in random modular lattices.
  - LWE problem generalises LPN problem used in RFID authentication protocols.
  - Problem is to distinguish "lattice point plus error" from a random vector in $\mathbb{Z}_q^n$.
  - Regev: as hard as solving standard worst-case lattice problems (but using a quantum algorithm!).

IBE From Lattice Problems: Overview

- Public parameters include matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, defining a modular lattice, and a hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_q^n$.
- Here, n, m and q are all moderate values.
- Master secret is a basis of short vectors for $\mathbf{A}$.
- Given this special basis, TA can solve equation:

$$H(\mathsf{ID}) = \mathbf{A} \cdot \mathbf{d}_{\mathsf{ID}} \bmod q$$

for short vector $\mathbf{d}_{\mathsf{ID}} \in \mathbb{Z}_q^m$ – giving private key extraction algorithm.

IBE From Lattice Problems: Overview

- To encrypt a bit b for identity ID, output

$$C = (\mathbf{p}, c) = (\mathbf{A}^T\mathbf{s} + \mathbf{x},\ H(\mathsf{ID})^T\mathbf{s} + \mathbf{x} + b \cdot \lfloor q/2 \rfloor) \in \mathbb{Z}_q^m \times \mathbb{Z}_q$$

- Here $\mathbf{s} \in_R \mathbb{Z}_q^n$ and $\mathbf{x}$ is an error vector selected according to some distribution.

- To decrypt $C = (\mathbf{p}, c)$, compute $b' = c - \mathbf{d}_{ID}^T \cdot \mathbf{p}$, outputting 0 if the result is closer to 0 than $\lfloor q/2 \rfloor$ mod q, and 1 otherwise.

IBE From Lattice Problems: Security and Efficiency

- Scheme can be extended to encrypt multiple bits at a time using fixed $\mathbf{s}$ and $\mathbf{p} = \mathbf{A}^T\mathbf{s} + \mathbf{x}$.
- Similar to BGH IBE scheme – requires large private keys.
- Encryption and decryption require only simple operations involving small vectors and matrices with elements from $\mathbb{Z}_q$ for moderate q.
- IND-ID-CPA security and recipient anonymity in the ROM based on hardness of LWE problem.
  - How should parameters n, m and q be selected to achieve a given security level for this scheme?

6 Conclusions

- Pairing-free IBE motivated by desire for diversification.
- Still in its infancy (relative to pairing-based approaches).
- Beautiful and sophisticated mathematical techniques.
  - Particularly in Cocks', BGH and lattice-based schemes.
- Practical evaluation of pairing-free schemes is still lacking
  - e.g. specifying secure choice of parameters for new lattice-based schemes.
  - e.g. prototyping ECC-TDL-based scheme.
- Much yet to be discovered!