

Cryptography from Pairings

Kenny Paterson

Information Security Group

Royal Holloway, University of London

`kenny.paterson@rhul.ac.uk`

May 31st 2007

The Pairings Explosion

- Pairings originally used “destructively” in MOV/Frey-Rück attack.
 - Translate discrete log problem on supersingular elliptic curve to a (relatively) easy discrete log problem in a related finite field.
- 2000/2001: Key papers by Sakai-Ohgish-Kasahara, Joux and Boneh-Franklin.
- 2007: Boneh-Franklin now has over 1000 citations on google scholar.
- We provide a “taster” of this work, with the benefit of hindsight guiding our selection of topics.

Overview

- Pairings in the abstract
- Sakai-Ohgishi-Kasahara identity-based non-interactive key distribution
- Joux's three-party key exchange protocol
- Boneh-Franklin identity-based encryption
- Boneh-Lynn-Shacham short signatures
- Hierarchical IBE
- Waters' IBE and its applications

1 Pairings in the Abstract

Basic properties:

- Triple of groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$, all of prime order r .
- A mapping $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ such that:
 - $e(P + Q, R) = e(P, R) \cdot e(Q, R)$
 - $e(P, R + S) = e(P, R) \cdot e(P, S)$
 - Hence

$$e(aP, bR) = e(P, R)^{ab} = e(bP, aR) = \dots$$

- Non-degeneracy: $e(P, R) \neq 1$ for some $P \in \mathbb{G}_1, R \in \mathbb{G}_2$.
- Computability: $e(P, R)$ can be efficiently computed.

Pairings in the Abstract

- Typically, $\mathbb{G}_1, \mathbb{G}_2$ are subgroups of the group of r -torsion points on an elliptic curve E defined over a field \mathbb{F}_q .
- Hence additive notation for $\mathbb{G}_1, \mathbb{G}_2$.
- Then \mathbb{G}_T is a subgroup of $\mathbb{F}_{q^k}^*$ where k is the least integer with $r | q^k - 1$.
- Hence multiplicative notation for \mathbb{G}_T .
- k is called the *embedding degree*.

Pairings in the Abstract

- A curve E for which a suitable collection $\langle e, r, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T \rangle$ exists is said to be *pairing-friendly*.
- If E is supersingular, then we can arrange $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$.
- Simplifies presentation of schemes and security analyses.
- Allows “small” representations of group elements in both \mathbb{G}_1 and \mathbb{G}_2 .
- But then we are limited to $k \leq 6$ with consequences for efficiency at higher security levels.
- Even generation of parameters may become difficult.

Pairings in the Abstract

- If E is ordinary, then a variety of constructions for pairing-friendly curves are known.
- Typically $\mathbb{G}_1 \subset E(\mathbb{F}_q)[r]$ and $\mathbb{G}_2 \subset E(\mathbb{F}_{q^k})[r]$.
- But then certain trade-offs are involved:
 - Only elements of \mathbb{G}_1 may have short representations.
 - It may be difficult to hash onto \mathbb{G}_2 .
 - $\log_2 q / \log_2 r$ may be large, so we don't get full security of the curve E defined over \mathbb{F}_q .
- Further details beyond scope of this talk – see “Pairings for Cryptographers” by Galbraith, Paterson, Smart at <http://eprint.iacr.org/2006/165> for further discussion.

2 Sakai-Ohgishi-Kasahara

At SCIS2000, Sakai, Ohgishi and Kasahara used pairings to construct:

- An identity-based signature scheme (IBS); and
- An identity-based non-interactive key distribution scheme (NIKDS).

The latter has proven to be very influential ...

(At SCIS2001, Sakai, Ohgishi and Kasahara also used pairings to construct the first efficient and secure IBE scheme.)

SOK ID-based NIKDS

- Assume we have a pairing $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ and a hash function $H : \{0, 1\}^* \rightarrow \mathbb{G}$.
- The Trusted Authority (TA) selects as its master secret a value $s \in \mathbb{Z}_r$.
- Entity A 's public key is defined to be $H(\text{ID}_A)$; similarly for B .
 - So public keys can be obtained using knowledge only of system parameters and identities.
 - Hence an *identity-based* scheme.

SOK ID-based NIKDS (ctd.)

- Now entity A with identity ID_A receives private key $sH(ID_A)$ from the TA; likewise for B .

- A and B can non-interactively compute a shared key via:

$$e(sH(ID_A), H(ID_B)) = e(H(ID_A), H(ID_B))^s = e(H(ID_A), sH(ID_B)).$$

- A version exists in the more general setting $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.

Security of SOK ID-based NIKDS

Security (in an appropriate model, and modelling H as a random oracle) depends on the hardness of the **Bilinear Diffie-Hellman Problem (BDHP)**:

Given $\langle P, aP, bP, cP \rangle$ for $a, b, c \leftarrow_R \mathbb{Z}_r$, compute $e(P, P)^{abc}$.

The *BDH assumption* is that there is no efficient algorithm to solve the BDH problem with non-negligible probability (as a function of some security parameter k that controls the instance size).

Applications of SOK ID-based NIKDS

- Identity-based key exchange:
 - use SOK as a key to a MAC to authenticate a Diffie-Hellman exchange (Boyd-Mao-Paterson,...)
 - use a SOK-variant in an interactive key-exchange (Smart, Chen-Kudla, many others)
- Secret handshake protocols (Balfanz *et al.*,...).
- Strong designated verifier signatures (Huang *et al.*,...).
- etc.

More on the Bilinear Diffie-Hellman Problem

Given $\langle P, aP, bP, cP \rangle$ for $a, b, c \leftarrow_R \mathbb{Z}_r$, compute $e(P, P)^{abc}$.

- BDHP is not harder than CDH problem in \mathbb{G}, \mathbb{G}_T .
- The pairing makes DDH easy in \mathbb{G} :
 - P, aP, bP, cP is a Diffie-Hellman quadruple iff

$$e(aP, bP) = e(P, cP).$$

- A variant of BDHP exists for the setting $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.
- A zoo of other computational and decisional problems have been defined for the purposes of proving secure certain pairing-based schemes.

3 Joux's Three-Party Key Exchange Protocol (2000)

- Fix generator $P \in \mathbb{G}$, with $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$.
- Parties A , B and C respectively choose random $a, b, c \in \mathbb{Z}_r$.
- A broadcasts aP .
- B broadcasts bP .
- C broadcasts cP .
- All three parties can now compute shared secret:

$$e(P, P)^{abc} = e(aP, bP)^c = e(aP, cP)^b = e(cP, bP)^a$$

Joux's Protocol

- Since all messages can be sent simultaneously this protocol can be completed in one round.
- This is in contrast to all previous key exchange protocols for 3 parties.
- Security against passive adversary based on hardness of BDHP.
- Not secure against active adversaries.
- To make an authenticated 3-party protocol, add signatures or adapt MQV/MTI protocols.
- Basis for several proposals for efficient multi-party protocols.

4 Boneh-Franklin IBE

- Boneh and Franklin (Crypto 2001) gave first efficient ID-based encryption scheme with security model and proof.
 - Shamir (Crypto'84) proposed IBE concept but no IBE scheme.
 - SOK scheme (SCIS 2001) is roughly the same scheme, but without security model or proof.
 - Cocks' scheme (IMA C&C 2001) has long ciphertexts.
 - Maurer-Yacobi scheme (Eurocrypt'91) is inefficient.
- Basic version provides CPA security, enhanced version gives CCA security.
- Boneh-Franklin paper was the main trigger for the flood of research in pairing-based cryptography.

Boneh-Franklin IBE

Setup:

1. On input a security parameter k , generate parameters $\langle \mathbb{G}, \mathbb{G}_T, e, r \rangle$ where $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a pairing on groups of prime order r .
2. Select two hash functions $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}$, $H_2 : \mathbb{G}_T \rightarrow \{0, 1\}^n$, where n is the length of plaintexts.
3. Choose an arbitrary generator $P \in \mathbb{G}$.
4. Select a master-key s uniformly at random from \mathbb{Z}_r^* and set $P_0 = sP$.
5. Return the public system parameters $\text{params} = \langle \mathbb{G}, \mathbb{G}_T, e, r, P, P_0, H_1, H_2 \rangle$ and the master-key s .

Boneh-Franklin IBE

Extract: Given an identity $ID \in \{0, 1\}^*$, set $d_{ID} = sH_1(ID)$ as the private key – identical to private key extraction of SOK.

Encrypt: Inputs are message M and an identity ID .

1. Choose random $t \in \mathbb{Z}_r$.
2. Compute the ciphertext $C = \langle tP, M \oplus H_2(e(H_1(ID), P_0)^t) \rangle$.

Decrypt: Given a ciphertext $\langle U, V \rangle$ and a private key d_{ID} , compute:

$$M = V \oplus H_2(e(d_{ID}, U)).$$

Boneh-Franklin IBE – What Makes it Tick?

- Both sender (who has t) and receiver (who has d_{ID}) can compute $e(H_1(\text{ID}), P)^{st}$:

$$e(H_1(\text{ID}), P)^{st} = e(H_1(\text{ID}), sP)^t = e(H_1(\text{ID}), P_0)^t$$

$$e(H_1(\text{ID}), P)^{st} = e(sH_1(\text{ID}), tP) = e(d_{\text{ID}}, U)$$

Boneh-Franklin IBE – What Makes it Tick? (ctd.)

Alternatively: the scheme encrypts with a mask obtained by hashing the SOK key shared between identities with public keys $H_1(\text{ID})$ and tP .

- Here, the sender uses the “reference key-pair” P, P_0 to create a fresh key-pair tP, tP_0 for each message.
- SOK key is then $e(H_1(\text{ID}), tP)^s$.
- So Boneh-Franklin IBE can be obtained by making a simple modification to the SOK ID-based NIKDS.

Security of Boneh-Franklin IBE

Informally:

- Adversary sees message XORed with hash of $e(H_1(\text{ID}), P_0)^t$.
- Adversary also sees $P_0 = sP$ and $U = tP$.
- Write $H_1(\text{ID}) = zP$ for some (unknown) z .
- Then $e(H_1(\text{ID}), P_0)^t = e(P, P)^{stz}$.
- Because H_2 is modeled as a random oracle, adversary needs to compute $e(P, P)^{stz}$ when given as inputs sP, tP, zP .
- This is an instance of the BDH problem.

Security Model for IBE

Similar game to standard security game for PKE:

- Challenger \mathcal{C} runs Setup and adversary \mathcal{A} is given the public parameters.
- \mathcal{A} accesses Extract and Decrypt oracles.
- \mathcal{A} outputs two messages m_0, m_1 and a challenge identity ID^* .
- \mathcal{C} selects random bit b and gives \mathcal{A} an encryption of m_b under identity ID^* , denoted c^* .
- \mathcal{A} makes further oracle access and finally outputs a guess b' for b .

\mathcal{A} wins the game if $b' = b$. Define

$$\text{Adv}(\mathcal{A}) = 2|\Pr [b' = b] - 1/2|.$$

Security Model for IBE

Natural limitations on oracle access and selection of ID^* :

- No Extract query on ID^* .
- No Decrypt query on c^*, ID^* .

An IBE scheme is said to be IND-ID-CCA secure if there is no poly-time adversary \mathcal{A} which wins the above game with non-negligible advantage.

An IBE scheme is said to be IND-ID-CPA secure if there is no poly-time adversary \mathcal{A} having access only to the Extract oracle which wins the above game with non-negligible advantage.

Security of Boneh-Franklin IBE

- Boneh and Franklin prove that their encryption scheme is IND-ID-CPA secure, provided the BDH assumption holds.
- The proof is in the random oracle model.
- “Standard” techniques can be used to transform Boneh-Franklin IBE into an IND-ID-CCA secure scheme.
- These generally add complexity, require random oracles, and result in inefficient security reductions.

ID-based Signatures from Boneh-Franklin IBE

Several authors quickly showed how to derive ID-based signature schemes using the SOK/BF keying infrastructure (already in SOK, Paterson, Hess, Cha-Cheon, Yi, etc).

But ID-based signatures can be constructed generically from ordinary signatures (folklore?).

And non-pairing-based constructions were also already known (from Shamir84 onwards).

Aim was to build a suite of identity-based crypto-primitives re-using same computational primitives.

Non ID-based Signatures from IBE

An observation of Naor: any IND-ID-CPA secure IBE scheme can be transformed into a (normal) signature scheme that is secure in the sense of EUF-CMA.

Setup: Run Setup algorithm of IBE scheme, set:

public key = public parameters, private key = master secret.

Sign: To sign a message m , treat m as an identity string and output $\sigma = d_m$, the private key corresponding to m .

Verify: Encrypt a random message with identity m and try to decrypt using $\sigma = d_m$.

5 Boneh-Lynn-Shacham Short Sigs

Apply Naor's idea to the Boneh-Franklin IBE and optimise the verification algorithm.

Setup: Generate public key $\langle \mathbb{G}, \mathbb{G}_T, e, r, P, P_0 = sP, H_1 \rangle$ and private key s .

Sign: To sign a message m , output $\sigma = sH_1(m) \in \mathbb{G}$.

Verify: Check

$$e(H_1(m), P_0) \stackrel{?}{=} e(\sigma, P).$$

Note that $P, P_0, H_1(m), \sigma$ is a DH quadruple when σ is a valid signature. Verification checks this relationship.

Security of BLS signatures based on hardness of CDH in \mathbb{G} , a group in which DDH is easy.

Boneh-Lynn-Shacham Short Signatures

- Aim to minimise signature size: one element of \mathbb{G} .
- For \mathbb{G} a subgroup of $E(\mathbb{F}_q)$, this is about $\log_2 q$ bits.
- CDH in \mathbb{G} only as hard as DLP in \mathbb{G}_T , a subgroup of \mathbb{F}_{q^k} . So try to maximise k .
- But $k \leq 6$ in the supersingular setting. And for $k = 6$, \mathbb{F}_q must have characteristic 3.
- For $q \approx 2^{170}$, $|\mathbb{F}_{q^6}| \approx 2^{1024}$.
- But special low characteristic algorithms for DLP apply, substantially reducing security compared to 1024-bit RSA (for 80 bits of security).
- Need to compensate with larger q .
- So short signatures are not as short as we'd like them to be.

Boneh-Lynn-Shacham Short Signatures

- An example where working in the simplified setting with $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is limiting.
- Solution is to work with pairings $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$.
- Enables use of ordinary curves with $k = 6$ and q a prime field.
- Or even larger k at higher security levels (e.g. $k = 12$ with $q \approx 2^{256}$ at 128-bit security level).
- Arrange $\sigma \in \mathbb{G}_1$ and $sP \in \mathbb{G}_2$.
- Allows short signatures but large public keys.
- Generating suitable curves is non-trivial.

Extensions of BLS Signatures

The algebraic simplicity of BLS signatures allows easy construction of signatures with additional properties.

Example: BGLS aggregate signatures

- n BLS signatures $\sigma_i \in \mathbb{G}_1$ on n distinct messages m_i for parties with public keys $s_i P \in \mathbb{G}_2$.
- Aggregation *by any party* to form a single signature $\sigma = \sum_i \sigma_i \in \mathbb{G}_1$.
- Verification via:

$$e(\sigma, P) \stackrel{?}{=} \prod_{i=1}^n e(H_1(m_i), s_i P).$$

Further Extensions of BLS Signatures

- Ring signatures, Verifiably encrypted signatures (Boneh-Gentry-Lynn-Shacham, Eurocrypt'03)
- Multisignatures, Blind signatures, Threshold signatures (Boldyreva, PKC'03)
- Universal designated verifier signatures (Steinfeld-Bull-Pieprzyk-Wang, Asiacrypt'03)
- ...

6 Hierarchical IBE

- Extension of IBE to provide hierarchy of TAs, each generating private keys for TAs in level below.
- Encryption needs only root TA's parameters and list of identities.
- First secure, multi-level scheme due to Gentry and Silverberg.
- Also an important theoretical tool:
 - Forward secure encryption.
 - Generation of IND-ID-CCA secure (H)IBE from IND-ID-CPA secure HIBE.
 - Intrusion-resilient cryptography.

7 IBE in the Standard Model

- Prior to circa 2004, most applications of pairings to construct cryptographic schemes involved use of the Random Oracle Model (ROM).
- ROM provides a powerful and convenient tool for modeling hash functions in security proofs.
- Question marks over extent to which ROM accurately models the behavior of hash functions.
- Several examples in the literature of schemes secure in the ROM but insecure for every family of hash functions.
- General move towards “proofs in the standard model” in cryptography.

CHK, BB, and Waters

IBE in the standard model:

- Eurocrypt 2003: Canetti-Halevi-Katz provide Selective-ID secure IBE scheme.
 - fairly inefficient and with limitations on adversarial capabilities.
- Eurocrypt 2004: Boneh-Boyen present efficient Selective-ID secure (H)IBE scheme.
- Crypto 2004: Boneh-Boyen present inefficient, but IND-ID-CPA secure IBE scheme.
- Eurocrypt 2005: Waters presents efficient, IND-ID-CPA secure IBE by “tweaking” Boneh-Boyen construction from Eurocrypt 2004.

A Notational Switch

Boneh-Boyen initiated a switch of notation which has remained popular in recent papers.

Henceforth in this talk all groups are written multiplicatively and g denotes a generator of \mathbb{G} .

And we have $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$ etc.

Waters' IBE

Setup:

1. On input a security parameter k , generate parameters $\langle \mathbb{G}, \mathbb{G}_T, e, r \rangle$ where $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a pairing on groups of prime order r .
2. Select $u', u_0, \dots, u_{n-1} \leftarrow_R \mathbb{G}^{n+1}$. Here n is the length of (hashed) identities.
3. Choose an arbitrary generator $g \in \mathbb{G}$ and $s \leftarrow_R \mathbb{Z}_r$. Set $g_1 = g^s, g_2 \leftarrow_R \mathbb{G}$.
4. The master-key is g_2^s .
5. Output $\text{params} = \langle \mathbb{G}, \mathbb{G}_T, e, r, g, g_1, g_2, u', u_0, \dots, u_{n-1} \rangle$.

Waters' IBE

The Waters Hash: Given an n -bit string $b = b_0b_1 \dots b_{n-1}$, define

$$H_W(b) = u' u_0^{b_0} \dots u_{n-1}^{b_{n-1}} = u' \prod_{b_i=1} u_i.$$

Extract: Given an identity $ID \in \{0, 1\}^*$, select $t \leftarrow_R \mathbb{Z}_r$ and set

$$d_{ID} = \langle g_2^s H_W(ID)^t, g^t \rangle \in \mathbb{G}^2$$

– randomised private key extraction.

Waters' IBE

Encrypt: Inputs are a message $m \in \mathbb{G}_T$ and an identity ID.

1. Choose random $z \in \mathbb{Z}_r$.
2. Compute the ciphertext

$$c = \langle m \cdot e(g_1, g_2)^z, g^z, H_W(\text{ID})^z \rangle \in \mathbb{G}_T \times \mathbb{G}^2.$$

Decrypt: Given a ciphertext $c = \langle c_1, c_2, c_3 \rangle$ and a private key $d_{\text{ID}} = \langle d_1, d_2 \rangle$, compute:

$$m = c_1 \cdot \frac{e(d_2, c_3)}{e(d_1, c_2)}.$$

Correctness of Waters' IBE

The Waters scheme is correct:

$$e(d_2, c_3) = e(g^t, H_W(\text{ID})^z) = e(g, H_W(\text{ID}))^{tz}$$

and

$$\begin{aligned} e(d_1, c_2) &= e(g_2^s H_W(\text{ID})^t, g^z) \\ &= e(g_2^s, g^z) \cdot e(H_W(\text{ID})^t, g^z) \\ &= e(g_2, g)^{sz} \cdot e(g, H_W(\text{ID}))^{tz}. \end{aligned}$$

Hence

$$\frac{e(d_2, c_3)}{e(d_1, c_2)} = e(g_2, g)^{-sz} = e(g_1, g_2)^{-z}$$

so

$$c_1 \cdot \frac{e(d_2, c_3)}{e(d_1, c_2)} = m \cdot e(g_1, g_2)^z \cdot e(g_1, g_2)^{-z} = m.$$

Efficiency of Waters' IBE

- Large public parameters: dominated by $n + 1$ random group elements.
 - Could generate these pseudo-randomly.
- Small private keys (2 group elements) and ciphertexts (3 group elements).
- Encryption: on average $n/2 + 1$ group operations in \mathbb{G} , two exponentiations in \mathbb{G} , one exponentiation in \mathbb{G}_1 (assuming $e(g_1, g_2)$ is pre-computed).
- Decryption: dominated by cost of two pairing computations.
- Size of public parameters can be reduced at the cost of a looser security reduction using ideas of Chatterjee-Sarker and Naccache.

Security for Waters' IBE

Waters showed that his scheme is **IND-ID-CPA** secure assuming the hardness of the *decisional* BDHP:

Given $\langle g, g^a, g^b, g^c, Z \rangle$ for $a, b, c \leftarrow_R \mathbb{Z}_r$, and $Z \in \mathbb{G}_T$,
decide if $Z = e(g, g)^{abc}$.

c.f. Proof of security for Boneh-Franklin IBE based on hardness of BDHP *in the Random Oracle Model*.

8 Applications of Standard Model IBE

- Canetti-Halevi-Katz (Eurocrypt 2004) showed how to build an IND-CCA secure PKE scheme from *any* IND-ID-CPA secure IBE scheme.
- Selective-ID security sufficient for this application.
- Techniques later improved by Boneh-Katz (RSA-CT 2005).
- Can be applied to selective-ID secure IBE scheme of Boneh-Boyen scheme (don't need full security of Waters' IBE).
- Provides a new method for constructing IND-CCA secure PKE in the standard model.

The CHK construction: PKE from IBE

Setup: Public key of PKE set to params of IBE; private key is set to master-key.

Encrypt:

- Generate a key-pair $\langle vk, sk \rangle$ for a strong one-time signature scheme;
- IBE-encrypt m using as the identity the verification key vk to obtain c ;
- Sign c using signature key sk to obtain σ ;
- Output $\langle vk, c, \sigma \rangle$ as the encryption of m .

The CHK construction: PKE from IBE

Decrypt:

- Check that σ is a valid signature on c given vk ;
- Use the master-key to generate the IBE private key for identity vk ;
- Use this key to IBE-decrypt c to obtain m .

Informally: a decryption oracle is of no use to an attacker faced with $\langle vk^*, c^*, \sigma^* \rangle$:

- If oracle queried on $\langle vk, c, \sigma \rangle$ with $vk = vk^*$, then σ will be incorrect (unforgeability).
- If query with $vk \neq vk^*$, then IBE decryption will be done with a different “identity” so result won’t help (IBE security).

A Hierarchical Version of Waters' IBE

- A simple generalisation of Waters' IBE yields a HIBE scheme that is IND-ID-CPA secure assuming DBDHP is hard.
- IND-ID-CCA security for ℓ -level HIBE can be attained by applying CHK/BK/BMW ideas to the $(\ell + 1)$ -level IND-ID-CPA secure scheme.
- $\ell = 2$ case gives IND-ID-CCA secure IBE.
- Size of public parameters grows linearly with ℓ .
- Quality of the security reduction declines exponentially with ℓ .
 - Recent alternative approaches due to Kiltz-Galindo/Kiltz has a tighter reduction.
 - Recent scheme of Gentry (Eurocrypt 2006) also has tighter reduction, but a less natural hardness assumption.

Signatures from Waters' IBE

Using Naor's observation, we can create a signature scheme from Waters' IBE:

Setup: Generate public key $\langle \mathbb{G}, \mathbb{G}_T, e, r, g, g_1, g_2, u', u_0, \dots, u_{n-1} \rangle$ and private key g_2^s as in Waters' IBE.

Sign: To sign a message m , select $t \leftarrow_R \mathbb{Z}_r$ and output $\sigma = \langle g_2^s H_W(\text{ID})^t, g^t \rangle \in \mathbb{G}^2$.

Verify: Given $\sigma = \langle \sigma_1, \sigma_2 \rangle$, check

$$e(\sigma_1, g) / e(\sigma_2, H_W(m)) \stackrel{?}{=} e(g_1, g_2).$$

Signatures from Waters' IBE

- Signature scheme is secure in the standard model, assuming only the hardness of CDH in \mathbb{G} .
- Signature consists of 2 elements of \mathbb{G} , so is relatively compact (but similar length issues as to BLS signatures).
- Signature generation is pairing-free (two exponentiations).
- Verification requires two pairings (assuming $Z = e(g_1, g_2)$ is placed in public key).
- Scheme is attractive in comparison to other standard model secure signature schemes.

Further extensions of Waters signatures

- Sequential aggregate signatures, multisignatures and verifiably encrypted signatures (Lu *et al.*, Eurocrypt'06)
- Strongly unforgeable signature (Boneh-Shen-Waters, PKC'06)
- Ring signatures (Shacham-Waters, PKC'07)
- Blind signatures (Okamoto, TCC'06)
- Group signatures (Boyen-Waters, Eurocrypt'06 and PKC'07)
- Identity-based signatures (Paterson-Schuldt, ACISP'06)
- Universal designated verifier signatures (Laguillaumie-Libert-Quisquater, SCN'06)
- Forward-secure (Boyen-Shacham-Shen-Waters, ACM-CCS'06) and intrusion-resilient (Libert-Quisquater-Yung, Inscrypt'06) signatures
-

9 Conclusions

- Pairing-based cryptography has seen very rapid development.
- Theoretical applications far beyond IBE.
- We have touched on some early important contributions.
- Recent focus on removing reliance on random oracle model – sometimes at the expense of reliance on less natural hardness assumptions.