Pairing-Based Cryptography – An Introduction

Kenny Paterson

Information Security Group

Royal Holloway, University of London

kenny.paterson@rhul.ac.uk

May 4th 2007

The Pairings Explosion

- Pairings originally used destructively in MOV/Frey-Rück attack.
- 2000/2001: Papers by Sakai-Ohgish-Kasahara, Joux and Boneh-Franklin.
- 2007: Boneh-Franklin now has over 900 citations on Google Scholar.
- We provide a "taster" of this work, with the benefit of hindsight guiding our selection of topics.
  - We focus on Identity-Based Encryption (IBE) in this talk.
  - Next talk will look at other applications.

Overview

- Pairings in the abstract
- Sakai-Ohgishi-Kasahara non-interactive key distribution
- Joux's three-party key exchange protocol
- Boneh-Franklin Identity-Based Encryption (IBE)
- Gentry-Silverberg hierarchical IBE
- IBE in the standard model
- Applications of standard-model-secure IBE

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 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ 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 $\mathbb{F}_q$.
- See e-print paper by Galbraith, Paterson, Smart for more info.

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 $H(\mathsf{ID}_A)$; similarly for B.
- Entity A with identity ID_A receives private key $sH(\mathsf{ID}_A)$ from the TA; likewise for B.
- A and B can non-interactively compute a shared key via:

  $$e(sH(\mathsf{ID}_A), H(\mathsf{ID}_B)) = e(H(\mathsf{ID}_A), H(\mathsf{ID}_B))^s = e(H(\mathsf{ID}_A), sH(\mathsf{ID}_B)).$$

- 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 DH quadruple iff
$$e(aP, bP) = e(P, cP).$$
- A variant of BDHP exists for the setting $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$.
- 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 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 $\mathsf{ID} \in \{0,1\}^*$, set $d_{\mathsf{ID}} = sH_1(\mathsf{ID})$ 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 $C = \langle tP, M \oplus H_2(e(H_1(\mathsf{ID}), P_0)^t)\rangle$.

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

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

Boneh-Franklin IBE – What Makes it Tick?

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

$$\begin{aligned} e(H_1(\mathsf{ID}), P)^{st} &= e(H_1(\mathsf{ID}), sP)^t = e(H_1(\mathsf{ID}), P_0)^t \\ e(H_1(\mathsf{ID}), P)^{st} &= e(sH_1(\mathsf{ID}), tP) = e(d_{\mathsf{ID}}, U) \end{aligned}$$

- Alternatively: the scheme encrypts with a mask obtained by hashing the SOK key shared between identities with public keys $H_1(\mathsf{ID})$ 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 $e(H_1(\mathsf{ID}), tP)^s$.
  - 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 $e(H_1(\mathsf{ID}), P_0)^t$.
- Adversary also sees $P_0 = sP$ and $U = tP$.
- Write $H_1(\mathsf{ID}) = zP$ for some (unknown) z.
- Then $e(H_1(\mathsf{ID}), P_0)^t = e(P, P)^{stz}$.
- 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 $\mathsf{Extract}$ and $\mathsf{Decrypt}$ 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

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

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.

5 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.

6 IBE in the Standard Model

- Prior to ca. 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 $u', u_0, \ldots, u_{n-1} \leftarrow_R \mathbb{G}^{n+1}$. 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 params $= \langle \mathbb{G}, \mathbb{G}_T, e, r, g, g_1, g_2, u', u_0, \ldots, u_{n-1} \rangle$.

Waters' IBE

The Waters Hash: Given an n-bit string $b = b_0 b_1 \ldots b_{n-1}$, define

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

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

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

– 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

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

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

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

and

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

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.*

7 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).

The BMW construction: PKE from Waters' IBE

Boneh-Mei-Waters (ACM-CCS 2005) used a direct approach to produce an efficient PKE scheme from Waters' IBE (and from Boneh-Boyen).

Key generation:

- Public key:

  $$\langle \mathbb{G}, \mathbb{G}_T, e, r, g, g_1, g_2, s', u' = g^{y'}, u_0 = g^{y_0}, \ldots, u_{n-1} = g^{y_{n-1}} \rangle$$

  with s' a key for a collision-resistant hash family $H_{s'} : \mathbb{G}_T \times \mathbb{G} \to \{0,1\}^n$ and $y', y_0, \ldots, y_{n-1} \leftarrow_R \mathbb{Z}_r$.

- Private key:

  $$\langle g_2^s, y', y_0, \ldots, y_{n-1} \rangle$$

The BMW construction: PKE from Waters' IBE

Encrypt: Given a message $m \in \mathbb{G}_T$,

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

$$c = \langle c_1, c_2, c_3 \rangle = \langle m \cdot e(g_1, g_2)^z, g^z, H_W(w)^z \rangle \in \mathbb{G}_T \times \mathbb{G}^2$$

where

$$w = H_{s'}(c_1, c_2).$$

The BMW construction: PKE from Waters' IBE

Decrypt: Given a ciphertext $c = \langle c_1, c_2, c_3 \rangle$ and the private key:

1. Compute $w = H_{s'}(c_1, c_2)$;
2. Test if $\langle g, c_2, H_W(w), c_3 \rangle$ is a DH quadruple by using the pairing (or more efficiently using knowledge of the values y', y_i).
3. Calculate

$$m = c_1 / e(c_2, g_2^s).$$

The BMW construction: PKE from Waters' IBE

- Scheme is similar to Waters' IBE, but with "identity" in c_3 being computed from components c_1, c_2.
- Scheme is more efficient than CHK/BK approach – no external one-time signature/MAC involved.
- Security can be related to security of Waters' IBE, so rests on hardness of DBDHP.
- Security proof needs full security model for IBE (selective-ID security not enough).
- A specific rather than a generic transform from IBE to PKE (c.f. CHK approach).

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.
  - A recent alternative approach due to Kiltz and Galindo has a tighter reduction.
  - Recent scheme of Gentry (Eurocrypt 2006) also has tighter reduction, but a less natural hardness assumption.

Conclusions

- Pairing-based cryptography has seen very rapid development.
- Theoretical applications far beyond IBE.
- We have touched on just a few of the important contributions.
- More to come in the next talk.
- Recent focus on removing reliance on random oracle model – sometimes at the expense of relying on less natural hardness assumptions.