The Applications of Pairings in Cryptography

Benoît Libert

UCL Crypto Group

Belgium

benoit.libert@uclouvain.be

August 30^{th} 2007

Rio de Janeiro

The Pairings Explosion

- Pairings originally used destructively in MOV/Frey-Rück attack.
- 2000/2001: Papers by Sakai-Ohgishi-Kasahara, Joux and Boneh-Franklin show constructive applications.
- 2006: Boneh-Franklin now has over 800 citations on google scholar.
- We show a sample of results with the benefit of hindsight guiding our selection of topics.

Overview

- Pairings in the abstract
- Sakai-Ohgishi-Kasahara non-interactive key distribution
- Joux's three-party key exchange protocol
- Identity-based encryption
  - Boneh-Franklin, Sakai-Kasahara and others
  - Hierarchical IBE and applications
- Short signatures
- Groups of composite order

1 Pairings in the Abstract

Basic properties:

- Triple of groups $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$, all of prime order p.
- A mapping $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ such that:
  - $e(u \cdot v, w) = e(u, w) \cdot e(v, w)$
  - $e(u, w \cdot z) = e(u, w) \cdot e(u, z)$
  - Hence
$$e(g^a, h^b) = e(g, h)^{ab} = e(g^b, h^a) = \ldots$$
- Non-degeneracy: $e(g, h) \neq 1_{\mathbb{G}_T}$ when $g \neq 1_{\mathbb{G}_1}$ and $h \neq 1_{\mathbb{G}_2}$.
- Computability: $e(g, h)$ can be efficiently computed.

Pairings in the Abstract

- Typically, $\mathbb{G}_1$, $\mathbb{G}_2$ are subgroups of the group of p-torsion points on an elliptic curve E defined over a field $\mathbb{F}_q$.
- Precisely, $\mathbb{G}_1 \subset E(\mathbb{F}_q)[p]$ and $\mathbb{G}_2 \subset E(\mathbb{F}_{q^k})[p]$.
- Then $\mathbb{G}_T \subset \mathbb{F}^*_{q^k}$ where k is the least integer with $p|q^k - 1$.
- k is called the *embedding degree*.
- In supersingular curves, we can arrange $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$.
- In the general case $\mathbb{G}_1 \neq \mathbb{G}_2$, only elements of $\mathbb{G}_1$ may have short representations.

2 Sakai-Ohgishi-Kasahara

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

- An identity-based signature scheme
- An identity-based non-interactive key distribution scheme.

The latter has proven to be very influential ...

(At SCIS2001, Sakai and Kasahara also used pairings to construct the first efficient and secure identity-based encryption scheme.)

SOK Identity-Based NIKS

- Assume we have a pairing $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, a generator $g \in \mathbb{G}$ and a hash function $H : \{0,1\}^* \rightarrow \mathbb{G}$.
- The Trusted Authority (TA) selects as its master secret a value $s \stackrel{R}{\leftarrow} \mathbb{Z}_p$ and publishes $g_{pub} = g^s$.
- Entity A's public key is defined to be $H(\mathsf{ID}_A)$.
- Entity A with identity $\mathsf{ID_A}$ receives private key $H(\mathsf{ID}_A)^s$ from the TA.
- A and B can compute a shared key via:

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

- 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 NIKS

Dupont-Enge showed security (in an appropriate model, and viewing H as a random oracle) assuming the hardness of the **Bilinear Diffie-Hellman** (BDH) problem:

> Given $\langle g, g^a, g^b, g^c \rangle$ for $a, b, c \xleftarrow{R} \mathbb{Z}_p$, compute $e(g,g)^{abc}$.

NB: the BDH problem is *not* harder than the **Computational Diffie-Hellman** (CDH) problem:

> Given $\langle g, g^a, g^b \rangle$ for $a, b \xleftarrow{R} \mathbb{Z}_p$, compute g^{ab}.

Application of SOK-NIKS: Secret Handshakes
(Balfanz et al. - IEEE Security and Privacy'03)

- Consider a set of n group masters having public keys $g_1 = g^{s_1}$, $g_2 = g^{s_2}, \ldots, g_n = g^{s_n}$.
- User i gets credential $d_i = H(\mathsf{ID}_i)^{s_j}$ from group j.
- Suppose A and B want to know if they are members of the same group.

  - They exchange their pseudonyms $\mathsf{ID}_A, \mathsf{ID}_B$ and accept each other if they can both compute hash values of

$$e(H(\mathsf{ID}_A), d_{\mathsf{ID}_B}) = e(d_{\mathsf{ID}_A}, H(\mathsf{ID}_B))$$

  - None of them learns anything otherwise.

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

- Fix generator $g \in \mathbb{G}$, with $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$.
- Parties A, B and C respectively choose random $a, b, c \in \mathbb{Z}_p$.
- A broadcasts g^a.
- B broadcasts g^b.
- C broadcasts g^c.
- All three parties can now compute shared secret:

$$e(g,g)^{abc} = e(g^a, g^b)^c = e(g^a, g^c)^b = e(g^c, g^b)^a$$

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.
- Security against passive adversary based on hardness of BDH.
- Not secure against active adversaries.
- Basis for authenticated 3-party protocols (Al-Riaymi-Paterson, Hitchcock-Boyd-González-Nieto,...)

More on Pairings and Diffie-Hellman Assumptions

- BDH is not harder than CDH problem in $\mathbb{G}$: given $\langle g, g^a, g^b, g^c \rangle$, finding g^{ab} also yields $e(g,g)^{abc}$.
- Although the CDH problem is hard in $\mathbb{G}$, the pairing makes DDH *easy* in $\mathbb{G}$ (Joux-Nguyen, 2001): $\langle g, g^a, g^b, g^c \rangle$ is a DH tuple (i.e. $c = ab$) iff

$$e(g^a, g^b) = e(g, g^c).$$

- DDH still presumably hard in $\mathbb{G}_1$ in asymmetric configurations $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ (if $\mathbb{G}_1 \neq \mathbb{G}_2$).
- A zoo of other computational and decisional problems have been defined for the purposes of proving secure certain pairing-based schemes.

4 Identity-Based Encryption

- Allows encrypting messages using receivers' identities (e.g. email addresses) as public keys (suggested by Shamir in 1984).
- Boneh-Franklin describe the first practical IBE scheme with proof of security in 2001.
- (SK scheme at SCIS 2001 is slightly different, but no security proof, published in Japanese).
- Boneh-Franklin also give security model for IBE.
- This paper was the main trigger for the flood of research in pairing-based cryptography.

Boneh-Franklin IBE

Setup: the TA chooses a master key $s \xleftarrow{R} \mathbb{Z}_p^*$, sets $g_1 = g^s$ and also chooses a hash function $H : \{0,1\}^* \rightarrow \mathbb{G}$.

Extract: given ID, the private key is $d_{\mathsf{ID}} = H(\mathsf{ID})^s \in \mathbb{G}$.

Encrypt: to encrypt M, choose $t \xleftarrow{R} \mathbb{Z}_p^*$ and set

$$\langle U, V \rangle := \langle g^t, M \cdot e(g_1, H(\mathsf{ID}))^{\mathsf{t}} \rangle$$

Decrypt: output $M = V/e(U, d_{\mathsf{ID}})$.

Boneh-Franklin IBE

Analogous to ElGamal encryption; can also be related to Joux's protocol.

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

$$\begin{aligned} e(g, H(\mathsf{ID}))^{st} &= e(g^s, H(\mathsf{ID}))^t = e(g_1, H(\mathsf{ID}))^t \\ e(g, H(\mathsf{ID}))^{st} &= e(g^t, H(\mathsf{ID})^s) = e(U, d_{\mathsf{ID}}) \end{aligned}$$

Security of Boneh-Franklin IBE

Informally:

- Adversary sees message concealed by $e(g_1, H(\mathsf{ID}))^t$.
- Adversary also sees $g_1 = g^s$ and $U = g^t$.
- Write $H(\mathsf{ID}) = g^z$ for some (unknown) z.
- Then $e(g_1, H(\mathsf{ID}))^t = e(g, g)^{stz}$.
- Hence, adversary needs to compute $e(g, g)^{stz}$ when given as inputs g^s, g^t, g^z.
- This is an instance of the BDH problem.

The Sakai-Kasahara IBE

Setup: the TA chooses a master key $s \xleftarrow{R} \mathbb{Z}_p^*$, sets $g_1 = g^s$ and a hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$.

Extract: given ID, the private key is $d_{\mathsf{ID}} = g^{\frac{1}{s+H(\mathsf{ID})}}$.

Encrypt: to encrypt M, choose $t \xleftarrow{R} \mathbb{Z}_p^*$ and set

$$\langle U, V \rangle := \langle g_1^t \cdot g^{tH(\mathsf{ID})}, M \cdot e(g,g)^t \rangle$$

Decrypt: output $M = V/e(U, d_{\mathsf{ID}})$.

The Sakai-Kasahara IBE (cont.)

- Faster than Boneh-Franklin:
  - No pairing to compute at encryption
  - No "hash-on-curve" operation (and maybe easier to implement in asymmetric settings $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$)
- But security relies on a stronger "exponent inversion" assumption whose strength grows with the number of queries allowed to adversaries:

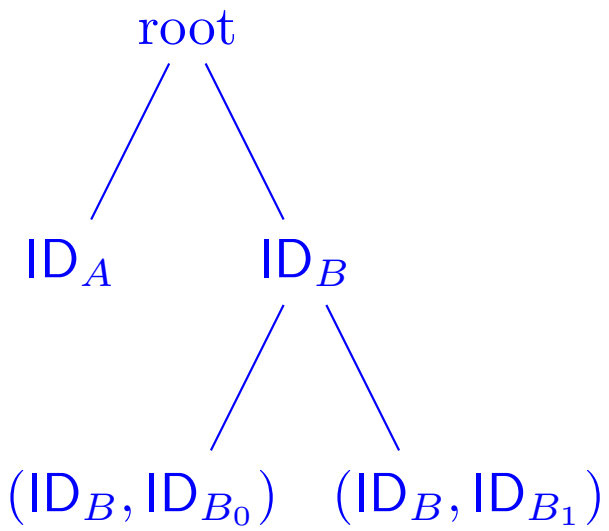
  The q-**Bilinear Diffie-Hellman Inversion Problem**: given $(g, g^a, g^{(a^2)}, \ldots, g^{(a^q)})$, find $e(g, g)^{1/a}$
- Security proof by Chen-Cheng (2005), inspired from Boneh-Boyen (2004)

Classification of IBE systems

- Full-Domain Hash IBE (Boneh-Franklin, Crypto'01)
- Exponent-Inversion IBE
  - Sakai-Kasahara
  - Boneh-Boyen II (Eurocrypt'04)
  - Gentry (Eurocrypt'06)
- Commutative Blinding IBE
  - Boneh-Boyen I (Eurocrypt'04)
  - Waters (Eurocrypt'05)
  - Boyen-Waters (Crypto'06)
- Quadratic Residuosity IBE
  - Cocks (IMA'01)
  - Boneh-Gentry-Hamburg (FOCS'07)

Hierarchical IBE

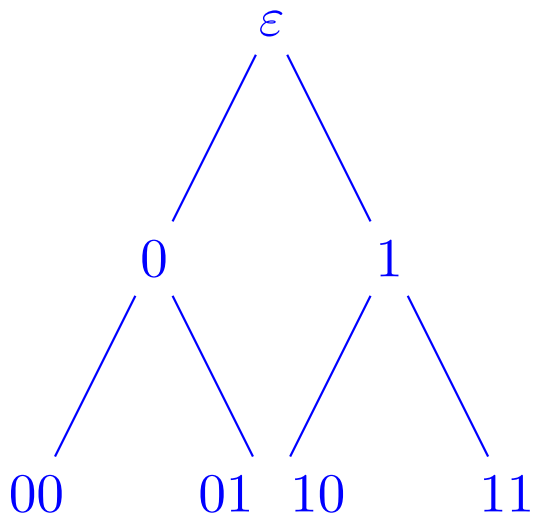
- Extension of IBE to provide hierarchy of TAs, each generating private keys for TA in level below.



- Encryption needs only root TA's parameters and list of identities.
- First secure, multi-level scheme due to Gentry and Silverberg.

Hierarchical IBE (cont.)

- Gives Forward-Secure Encryption (Canetti-Halevi-Katz, 2003):
  - Consider full binary tree, assign time periods to the leaves.



  - At period t, private key consists of node keys for right siblings of nodes on the path from the root to leaf $\langle t \rangle$.
  - Erase what is necessary at each update operation.
  - CHK obtain logarithmic complexity in all metrics (2003).

Other key-evolving schemes from IBE

Key-insulated security (Dodis-Katz-Xu-Yung 2002):

- Protect past and future time periods against break-ins by keeping long term secrets in a secure device.
- Let users perform crypto operations using short-term secrets
- Key exposure at the user during period i leaves stages $1, \ldots, i-1, i+1, \ldots, N$ totally safe.
- Close connection between key-insulated encryption (KIE) and IBE (Dodis *et al.* – 2002, Bellare-Palacio 2002).

Other key-evolving schemes from IBE (cont.)

- Generic KIE from IBE:

  Keygen: let $(pk^{\mathsf{KIE}}, msk^{\mathsf{KIE}}) = (\mathsf{mpk}^{\mathsf{IBE}}, \mathsf{msk}^{\mathsf{IBE}}) \leftarrow \mathsf{Setup}^{\mathsf{IBE}}$.

  Update(i): set $sk_i^{\mathsf{KIE}} = \mathsf{Extract}^{\mathsf{IBE}}(\mathsf{msk}^{\mathsf{IBE}}, i)$ at period i

  Encrypt(pk^{KIE}, i) : sets $C \leftarrow \mathsf{Encrypt}^{\mathsf{IBE}}(\mathsf{mpk}^{\mathsf{IBE}}, i)$

  Decrypt$(sk_i^{\mathsf{KIE}}, i, C)$: returns $M \leftarrow \mathsf{Decrypt}^{\mathsf{IBE}}(sk_i^{\mathsf{KIE}}, C)$.

- Strong key-insulation possible for specific schemes.
- Extensions with more than 1 secure devices are possible (Hanaoka-Hanaoka-Imai 2006, Libert-Quisquater-Yung 2007).

Other key-evolving schemes from IBE (cont.)

Intrusion-resilient cryptography (Itkis-Reyzin, 2002):

- IR-PKE from the CHK forward-secure encryption (Dodis-Franklin-Katz-Miyaji-Yung 2003).
- Generic IR-PKE (Dodis-Franklin-Katz-Miyaji-Yung 2004); also applies to the FS-PKE built on the Boneh-Boyen-Goh HIBE.
- Efficient IR signatures in the standard model (Libert-Quisquater-Yung, 2006).
- ...

Digital 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.

Keygen: Run Setup algorithm of IBE scheme, set:

$$\text{PK} = \text{public parameters}, \quad \text{SK} = \text{master secret}.$$

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 Short Signatures
(Boneh-Lynn-Shacham, Asiacrypt'01)

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

Keygen: Generate public key $\langle \mathbb{G}, \mathbb{G}_T, e, p, g, g_1 = g^s, H \rangle$ and private key s.

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

Verify: Check

$$e(H(m), g_1) \stackrel{?}{=} e(\sigma, g).$$

Note that $(g, g_1, H(m), \sigma)$ 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.

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 $g^{s_i} \in \mathbb{G}_2$.
- Aggregation *by any party* to form a single signature $\sigma = \prod_i \sigma_i \in \mathbb{G}_1$.
- Verification via:

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

Other Short Signatures

- With special properties:
  - Verifiably encrypted signatures (Boneh-Gentry-Lynn-Shacham, 2003)
  - Threshold signatures, blind signatures (Boldyreva, 2003)
  - ...
- In the standard model:
  - Boneh-Boyen (2004): under the q-**Strong Diffie-Hellman** assumption which posits the hardness of finding a pair $(c, g^{1/(c+a)}) \in \mathbb{Z}_p \times \mathbb{G}$ given $(g, g^a, g^{a_2}, \ldots, g^{(a^q)})$.
  - Waters (2005): under the Diffie-Hellman assumption in bilinear groups

6 Pairings in groups of composite order

Homomorphic encryption (Boneh-Goh-Nissim, TCC'05)

- Consider a group $\mathbb{G}$ of composite order $n = pq$ with $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. Let g be an element of order n an h be an element of order q.
- Encrypt $m \in \{0, 1\}$ as

$$C = g^m \cdot h^r$$

- To Decrypt, return 1 if $C^q = g^q$ and 0 otherwise.
- Semantic security under the **Subgroup Decision Assumption** (i.e. elements of order q are indistinguishable from those of order n).

Applications

- Allows computing $E(m + m')$ from $E(m)$ and $E(m')$ as well as $E(m \cdot m')$ and scalar products on encrypted boolean values.
- Yields improved private information retrieval (Boneh-Goh-Nissim).
- Also provides NIZK proof systems (Groth-Ostrovsky-Sahai, Eurocryt'06).
  - Group signatures in the standard model (Boyen-Waters, Eurocrypt'06 and PKC'07).
- Groups of composite order also yield traitor tracing with full traceability (Boneh-Sahai-Waters, Eurocrypt'06).

7 Conclusions

- Pairing-based cryptography has seen very rapid development and plagues many areas.
- Theoretical applications far beyond IBE.
- We have only outlined some famous contributions.
- Recent focus on removing reliance on random oracle model – sometimes at the expense of reliance on less natural hardness assumptions.