6.897 Special Topics in Cryptography Instructors: Ran Canetti and Ron Rivest

Lecture 25: Pairing-Based Cryptography

May 5, 2004 *Scribe: Ben Adida*

1 Introduction

The field of Pairing-Based Cryptography has exploded over the past 3 years [cry, DBS04]. The central idea is the construction of a mapping between two useful cryptographic groups which allows for new cryptographic schemes based on the reduction of one problem in one group to a different, usually easier problem in the other group.

In many research papers, the first of these two groups is referred to as a *Gap Group*, where the Decisional Diffie-Helman problem [Bon98] is easy (because it reduces to an easy problem in the second group), but the Computational Diffie-Helman problem remains hard.

The known implementations of these pairings – the Weil and Tate pairings – involve fairly complex mathematics. Fortunately, they can be dealt with abstractly, using only the group structure and mapping properties. Many interesting schemes have been built based purely on abstract bilinear maps.

2 Bilinear Maps

The major pairing-based construct is the bilinear map. Consider two groups G_1 and G_2 of prime order q. For clarity, we denote G_1 using additive notation and G_2 using multiplicative notation, even though the group operations in G_1 and G_2 may well be very different from the well-known arithmetic addition and multiplication. (Sometimes G_1 is also written multiplicatively in the literature.)

We consider P and Q two generators of G_1, and we write

$$aP = \overbrace{P + P + \ldots + P}^{a \text{ times}}$$

We now consider the mapping e as follows:

$$e : G_1 \times G_1 \rightarrow G_2$$

(Note that we do not know how to build a self-bilinear map, $G_1 \times G_1 \rightarrow G_1$. This would be quite powerful.)

Useful bilinear maps have three properties:

Bilinearity

$$\forall P, Q \in G_1, \forall a, b \in \mathbb{Z}_q^*,$$
$$e(aP, bQ) = e(P, Q)^{ab}$$

Non-Degeneracy If everything maps to the identity, that's obviously not interesting:

$$\forall P \in G_1, P \neq 0 \Rightarrow \langle e(P,P) \rangle = G_2 \ (e(P,P) \text{ generates } G_2)$$

In other words:

$$P \neq 0 \Rightarrow e(P,P) \neq 1$$

Computability e is efficiently computable.

We can find G_1 and G_2 where these properties hold: the Weil and Tate pairings prove the existence of such constructions. Typically, G_1 is an elliptic-curve group and G_2 is a finite field.

3 Complexity Implications

The construction of a bilinear map comes with a number of complexity implications.

Theorem 1 *The Discrete Log Problem in G_1 is no harder than the Discrete Log Problem in G_2.*

Proof 1 *Consider $Q = aP$ (still using additive notation), though a is unknown. Solving the Discrete Log Problem involves discovering a for a given P and a random Q.*

We note:

$$\begin{aligned} e(P,Q) &= e(P,aP) \\ &= e(P,P)^a \end{aligned}$$

Thus, we can reduce the Discrete Log Problem in G_1 to the Discrete Log Problem in G_2. Given $P \in G_1$ and a random $Q \in G_1$, and noting that the mapping e is easily computable, we can compute $\log_P(Q)$ as follows:

1. *determine $P' = e(P,P)$*
2. *determine $Q' = e(P,Q)$*
3. *determine $a = \log_{P'}(Q')$ in G_2.*
4. *a is also $\log_P(Q)$.*

Theorem 2 *The Decisional Diffie-Helman [Bon98] is easy in G_1.*

Proof 2 *Solving the DDH problem involves distinguishing:*

$$\langle P, aP, bP, cP \rangle \text{ with } a,b,c \in_R \mathbb{Z}_q^*, \text{ and}$$

$$\langle P, aP, bP, abP \rangle \text{ with } a,b \in_R \mathbb{Z}_q^*$$

If we define P, A, B, C as the four values given to the distinguisher, the distinguisher functions as follows:

1. *Determine* $v_1 = e(A, B)$ *and* $v_2 = e(P, C)$

2. *If* $v_1 = v_2$*, then the tuple is of the type* $\langle P, aP, bP, abP \rangle$*.*

Indeed, assume $C = abP$*, then:*

$$\begin{aligned} e(A, B) &= e(aP, bP) \\ &= e(P, P)^{ab} \\ &= e(P, abP) \\ &= e(P, C) \end{aligned}$$

Since we know the mapping e *is non-degenerate, the equality* $e(A, B) = e(P, C)$ *is equivalent to* $c = ab$*. The distinguisher can gain a significant advantage in deciding DDH given the mapping* e*.*

4 Cryptographic Schemes

The application of bilinear maps leads to numerous interesting cryptographic schemes.

4.1 One-Round, 3-party Key Agreement Scheme

In 2000, Joux introduced a scheme for one-round, 3-party key agreement based on bilinear maps [Jou00]. Key agreement schemes based on Diffie-Helman [DH76] are well known, but all require more than one round of exchanged data.

In the Joux scheme, assume the above notation and existence of a bilinear map between groups G_1 and G_2 with P a generator of G_1. Three parties A, B, C respectively have secrets $a, b, c \in \mathbb{Z}_q^*$. The protocol functions as follows:

1. $A \longrightarrow B, C$: aP
2. $B \longrightarrow A, C$: bP
3. $C \longrightarrow A, B$: cP
4. Note that steps 1, 2, 3 are done in one round of parallel message exchanges.
5. A computes $e(bP, cP)^a = e(P, P)^{abc}$.
6. B computes $e(aP, cP)^b = e(P, P)^{abc}$.
7. C computes $e(aP, bP)^c = e(P, P)^{abc}$.
8. Note that steps 5, 6, 7 are done in parallel.
9. All parties have the same shared key $K = e(P, P)^{abc} \in G_2$.

This protocol is contingent on the *BDH assumption.*

Definition The Bilinear Diffie-Helman (BDH) Assumption considers the computation of $e(P, P)^{abc}$ given $\langle P, aP, bP, cP \rangle$ to be hard.

4.2 Identity-Based Encryption

In 1984, Shamir imagined a public-key encryption scheme where any publicy-known string (e.g. someone's email address) could be used as a public key [Sha85]. In this scheme,

the corresponding private key is delivered to the proper owner of this string (e.g. the recipient of the email address) by a trusted private key generator. This key generator must verify the user's identity before delivering a private key, of course, though this verification is essentially the same as that required for issuing a certificate in a typical Public Key Infrastructure (PKI). Thus, an *Identity-Based Encryption Scheme* enables the deployment of a public-key cryptosystem without the prior setup of a PKI: a user proves his identity in a lazy way, only once he needs his private key to decrypt a message sent to him.

In 2001, Boneh and Franklin devised the first practical implementation of such an Identity-Based Encryption scheme [BF01]. Their approach uses bilinear maps and relies on the BDH Assumption and the Random Oracle model.

Setup

- the usual G_1 and G_2 with a bilinear mapping $e : G_1 \times G_1 \longrightarrow G_2$ and P a generator
- a system-wide secret key $s \in_R \mathbb{Z}_q^*$.
- a corresponding system-wide public key $P_{pub} = sP$.

Encrypt We want to encrypt a message m to public key A using the system-wide settings from above. The encryption function is:

$$\begin{aligned} Enc(P_{pub}, A, m) = \langle rP, M \oplus H_2(g_A^r)\rangle, r \in_R \mathbb{Z}_q^* \\ g_A = e(Q_A, P_{pub}) \\ Q_A = H_1(A) \\ H_1 : \{0,1\}^* \longrightarrow G_1, \text{ a random oracle} \\ H_2 : G_2 \longrightarrow \{0,1\}^*, \text{ a random oracle} \end{aligned}$$

Decrypt We want to decrypt a ciphertext $c = (u, v)$ encrypted with public-key string A. The secret key is delivered to the owner of A as $d_A = sQ_A$, with Q_A defined as above: $Q_A = H_1(A)$. We define:

$$\begin{aligned} Dec(u, v, d_A) &= v \oplus H_2(e(d_A, u)) \\ &= v \oplus H_2(e(sH_1(A), rP)) \\ &= v \oplus H_2(e(H_1(A), P)^{rs}) \\ &= v \oplus H_2(e(Q_A, sP)^r) \\ &= v \oplus H_2(e(Q_A, P_{pub})^r) \\ &= v \oplus H_2(g_A^r) \\ &= (m \oplus H_2(g_A^r)) \oplus H_2(g_A^r) \\ &= m \end{aligned}$$

This scheme is not CCA2-secure, but can be made so with the Fujisaki-Okamoto construction [FO99], which assumes the Random Oracle model — nothing further than what we already assume.

References

[BF01] Dan Boneh and Matt Franklin. Identity-based encryption from the Weil pairing. *Lecture Notes in Computer Science*, 2139:213–??, 2001.

[Bon98] Dan Boneh. The decisional diffie-hellman problem. In *Third Algorithmic Number Theory Symposium*, pages 48–63. Springer-Verlag, 1998.

[cry] Pairing-based crypto lounge. available at `http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html`.

[DBS04] Ratna Dutta, Rana Barua, and Palash Sarkar. Pairing-based cryptography : A survey. Cryptology ePrint Archive, Report 2004/064, 2004. `http://eprint.iacr.org/`.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. *Lecture Notes in Computer Science*, 1666:537–554, 1999.

[Jou00] Antoine Joux. A one round protocol for tripartite diffie-hellman. In *Proceedings of the 4th International Symposium on Algorithmic Number Theory*, pages 385–394. Springer-Verlag, 2000.

[Sha85] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Crypto '84, LNCS Vol. 196*, pages 47–53. Springer, 1985.