Potential applications of pairings

Laszlo CSIK

Laboratory of Cryptography and System Security (CrySyS)

Budapest University of Technology and Economics

`laszlo.csik@crysys.hu`

Outline

- Definition of Pairing
- Identity Based Encryption
- Group Signatures
- Searchable Encryption
- Advantages / Disadvantages
- Summary

Bilinear pairing – Mathematical definition

Let G_1, G_2 be two groups of the same prime order q. We view G_1 as an additive group and G_2 as a multiplicative group. Let P be an arbitrary generator of G_1. A mapping $\hat{e}: G_1 \times G_1 \rightarrow G_2$ satisfying the following properties is called a bilinear map:

$-Bilinearity: \hat{e}(aP, bQ) = \hat{e}(P,Q)^{ab}$ for all $P, Q \in G_1$ and $a, b \in \text{¢}_q^*$

$-Non\text{-}degeneracy:$ If P is a generator of G_1, then $\hat{e}(P,P)$ is a generator of G_2. In other words, $\hat{e}(P,P) \neq 1$.

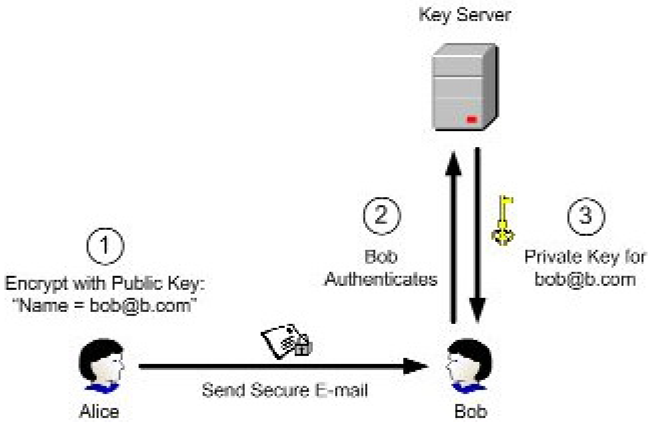
$-Computable:$ There exists an efficient algorithm to compute $\hat{e}(P,Q)$ for all $P, Q \in G_1$.

Bilinear pairing - Overview

- Today there are only two known bilinear pairings
  - Weil pairing
  - Tate pairing
- Both of them are defined over modular elliptic curves
- Their first application in cryptography was for attacking cryptosystems
- They were first used in cryptography for ‘good’ in 2001 by Boneh in the ID-based cryptography
- Since then the number of pairing based solution grows exponentially
- The operation is relatively slow, but can be optimalized
  - Nowadays comparable to RSA signature generation

ID based cryptography (IDBC)

- 1984, Shamir:
  - Public key encryption scheme
  - Public key can be an arbitrary string



- IDBC Advantages:
  - Does not require a PKI

  → ID is a well known property of the subject

  User credentials can be managed easily

  Easy to revoke public keys

IDBC - Advantages

- Revoking public keys:
  - Alice encrypts an e-mail by using the public key:

    bob@company.com || current-year
  - unlike the existing PKI, Alice does not need to obtain a new certificate from Bob every time Bob refreshes his private key

- Delegation to duties (Roles)
  - Alice encrypts mail to Bob using the subject line as the IBE encryption key

  → Corresponding decryption keys can be given to assistants

  bob@company.com || current-year || role=sales

A Manet Communication Model

- Requirements
  - Every message should be authenticated
  - Anyone should be able to explicitly verify the authenticity
  - This should not require a third party
  - An authority must be able to distinguish between signatures
  - Signatures should be short (smaller than 200 bytes)

- In case of one Global signature:
  - Revocation can be hard
  - Incorrect behavior cannot be filtered

- In case of Unique signatures:
  - Anonymity should be assured (Privacy Problems)

- In case of a mixed solution, both problems should be handled

A possible solution - Group Signature

- The specification implies that a Ring or Group signature should be applied.

- These are authentic signature which provides **signer anonymity**
  - Anyone can verify if a message is signed by a group member
  - No one, except the central authority can decode the ID of the signer of a signature

  → Current PKI unable to provide these properties

  - A ring signature can be considered as a simplified group signature with no manager, no group setup procedure, and no revocation mechanism against signer’s anonymity

Group Signatures – Additional Properties

- Revocability (Important)
  - Group membership can be selectively disabled without affecting the signing ability of unrevoked members
- Exculpability (Useful)
  - No member of the group and not even the group manager—the entity that is given the tracing key—can produce signatures on behalf of other users
- Security proof depth
  - Random Oracle
  - Real world computational model

Group Signatures - History

- Idea was first introduced by Chaum and van Heyst in Eurecrypt, 1991.
- Until 2003, the best revocable mechanisms were based on the Strong RSA assumption
  - Most of them are only provably secure in the Random Oracle Model
- In our case the signature length is very important – The ideal limit is about 250 bytes
  - None of the RSA assumption based models are able to meet this requirement
- After 2003, with bilinear pairings efficient solutions were introduced

Example Group signatures with Pairings

- Short Group Signatures
  - *Dan Boneh, Xavier Boyen, Hovav Shacham*
  - Eurecrypt 2004
  - Message length is smaller than 200 bytes
  - The solution has the exculpability property

- Practical Group Signatures without Random Oracles
  - *Giuseppe Ateniese, Jan Camenisch, Susan Hohenberger, Breno de Medeiros*
  - February 26, 2006
  - Provably secure in the Real world model, 35% additional length, size independent from the number of signers

- Compact Group Signatures Without Random Oracles
  - *Xavier Boyen, Brent Waters*
  - March 7, 2006
  - Short, provably secure in the real model, size increases logarithmically

PEKS – Public Key Encryption with Keyword Search

- The goal is to decide whether an encrypted data contains a specific keyword
- The search is performed in an untrusted environment

  → no one should learn nothing about the data itself

- Example: secure LOG
- Different authorities might be able search in the log file for different keywords

  → Police: User=Bob

Solution with paring based trapdoor functions! A test function which returns YES or NO if a specific keyword exist in the subject line

Summary

- The mentioned schemes are computationally secure
  - Constants are still questions
- It is hard to efficiently implement pairings
  - The HP Labs created an ID-based solution which is comparable to RSA signature speed
- Industry does not use them yet
- They can solve several open problems

Than you for your Intension

- Questions?