Pairing-Based Cryptography II - Applications

David Kubát

20. listopadu 2015

Table of contents

Identity-Based Encryption

- Proposed by Adi Shamir in 1984
- First instantiation in 2001 (Boneh-Franklin scheme)
- Another example: Cock's encryption scheme based on quadratic residues

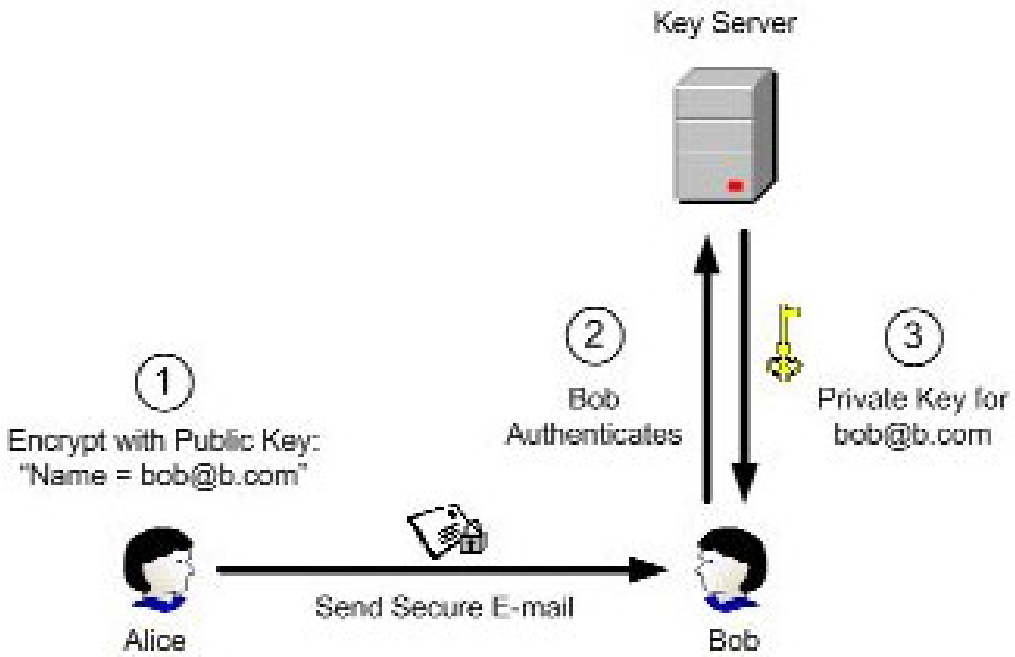
Public-Key Encryption

PKE three algorithms:

- Key Generation: $GenKey(\lambda) \Rightarrow (Pk, Sk)$
- Encryption: $Encrypt(M, Pk) \Rightarrow C$
- Decryption: $Decrypt(C, Sk) \Rightarrow M$

ID-based encryption

- IDE system: public key encryption system where the public key is an arbitrary string



ID-based encryption

IDE scheme consists of four algorithms:

- Setup algorithm: $S(\lambda) \rightarrow (MK, PP)$
  - given a security parameter λ it outputs a master key MK and public parameters PP
- Extract key: $K(MK, ID) \rightarrow sk_{ID}$
  - given a user's public key ID it outputs user's private key sk_{ID}
- Encrypt: $E(PP, ID, M) \rightarrow C$
  - encrypts a message M using public key ID (and PP)
- Decrypt: $D(sk_{ID}, C) \rightarrow M$

Correctness condition

In order for the system to work, one has to postulate that

$$D(K(ID), E(PP, ID, M)) = M$$

for every message M and $ID \in \{0,1\}^*$

Boneh-Franklin IBE

Suppose we have an algorithm *GenBilGroup*() that outputs groups G, G_T of prime order p and $P \in G$ such that there exists a bilinear map

$$e\colon G \times G \to G_T.$$

and $\langle P \rangle = G$. Furtheremore, let

$$H\colon \{0,1\}^* \to G^*$$

be a cryptographic hash function.

Boneh-Franklin IBE

- Setup algorithm:
  $(G, G_T, P, p) \leftarrow GenBilGroup(\lambda)$, $\alpha \leftarrow \mathbb{F}_p$,
  $PP := (P, y \leftarrow \alpha P)$, $MK := \alpha$
- Extract key:
  $sk_{ID} \leftarrow \alpha H(ID)$
- Encrypt:
  $s \leftarrow \mathbb{F}_p$, $C = (c_1, c_2) \leftarrow (sP, M \cdot e(\alpha P, sH(ID)))$
- Decrypt:
  $D(sk_{ID}, C) = c_2 \cdot e(c_1, sk_{ID})^{-1}$

Does it work?

To check correctness, we note that

$$e(\alpha P, sH(ID)) = e(P, H(ID))^{\alpha s} = e(sP, \alpha H(ID))$$

and hence

$$D(sk_{ID}, C) = c_2 \cdot e(c_1, sk_{ID})^{-1} = M \cdot e(\alpha P, sH(ID)) \cdot e(sP, \alpha H(ID))^{-1}$$

$$= M$$

Motivation for ABE

The goal of ABE...

- ...is to encrypt data in such a way, that those able to decrypt it are exactly the users matching a set of attributes specified while encrypting.
- we want to describe who should be able to decrypt the data in terms of an access policy over attributes.

Two kinds of ABE

We distinguish between two kinds of ABE:

- Key-Policy ABE (KP-ABE): messages are encrypted with respect to subsets of attributes and an access policy is encoded into the users secret key (in the form of monotonic boolean formulas)
- Ciphertext-Policy ABE (CP-ABE): the roles of attributes sets and formulas are flipped

But in this talk, we will only be concerned with KP-ABE

Security threat: Collusion

- An important property is collusion resistance
- It should not be possible for distinct users who wouldn't be able to decrypt a ciphertext on their own to decrypt the ciphertext by combining their secret keys
- Achieved by independently randomizing users' secret keys

Two kinds of ABE

Example of what 'Key-Policy' means:

- Define the attribute set corresponding to a certain message to be $S = \{A, B\} \subseteq \{A, B, C\}$
- Then it would be possible for a user possesing a key with acces policy $(A \wedge B) \vee C$ to decrypt such a message
- User with a key with acces policy $A \wedge C$ would not be able to decrypto such a message.

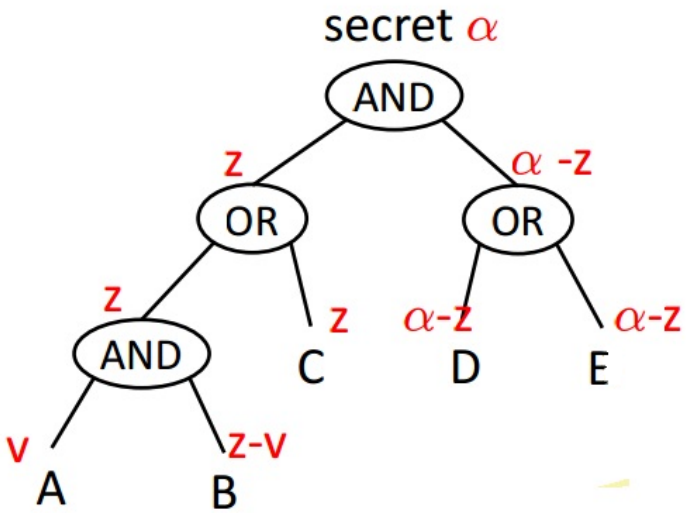
KP-ABE specification

There are four algorithms defining a KP-ABE scheme:

- $Setup(\lambda, U)$:
  Given a security parameter λ and an attribute universe U, it generates public parameters PP and a master key MK
- $KeyGen(Policy, MK)$:
  Generates a user key SK for a given policy
- $Encrypt(PP, M, S \subseteq U)$:
  Encrypts message M under attribute set S
- $Decrypt(C, SK)$:

Linear Secret Sharing

- Suppose we have a secret $\alpha \in \mathbb{F}_p$ and a set (of attributes, for example $\{A, B, C, D, E\}$)
- Define the access formula (e.g. $((A \wedge B) \vee C) \wedge (D \vee E)$)
- We want to make sure only an authorized set of shares ($\equiv$ elements of $\mathbb{F}_p$) allows reconstruction of α



Basic KP-ABE Construction

- $Setup(\alpha, U)$:
  $(G, G_T, P, p) \leftarrow GenBilGroup(\lambda)$, $\alpha \leftarrow \mathbb{F}_p$,
  $\forall i \in U : H_i \leftarrow G$
  $PP := (P, e(P,P)^{\alpha}, \{H_i\}_{i \in U})$, $MK := \alpha$
- $KeyGen(f)$ (f is a formula):
  split α into shares α_i following f
  choose random $r_i \in \mathbb{F}_p$
  $SK := \{(\alpha_i P + r_i H_i, r_i P)\}_i$
- $Encrypt(M, S \subseteq U)$:
  $s \leftarrow \mathbb{F}_p$
  $C := (M \cdot e(P,P)^{\alpha s}, sP, \{sH_i\}_{i \in S})$

Decryption

$Decrypt(C, SK)$:

- In order to decrypt, it is necessary to compute $e(P, P)^{\alpha s}$.

$$[C = (M.e(P, P)^{\alpha s}, sP, \{sH_i\}_{i \in S}), \qquad SK = \{(\alpha_i P + r_i H_i, r_i P)\}_i]$$

Decryption

$Decrypt(C, SK)$:

- In order to decrypt, it is necessary to compute $e(P, P)^{\alpha s}$.
- That's possible if S satisfies the formula associated with SK:

$$[C = (M.e(P, P)^{\alpha s}, sP, \{sH_i\}_{i \in S}), \qquad SK = \{(\alpha_i P + r_i H_i, r_i P)\}_i]$$

Decryption

$Decrypt(C, SK)$:

- In order to decrypt, it is necessary to compute $e(P,P)^{\alpha s}$.
- That's possible if S satisfies the formula associated with SK:
- we compute $e(P,P)^{\alpha_i s}$ for each i and then recover $e(P,P)^{\alpha s}$.

$$[C = (M.e(P,P)^{\alpha s}, sP, \{sH_i\}_{i \in S}), \qquad SK = \{(\alpha_i P + r_i H_i, r_i P)\}_i]$$

Decryption

$Decrypt(C, SK)$:

- In order to decrypt, it is necessary to compute $e(P,P)^{\alpha s}$.
- That's possible if S satisfies the formula associated with SK:
- we compute $e(P,P)^{\alpha_i s}$ for each i and then recover $e(P,P)^{\alpha s}$.
- We can compute $e(P,P)^{\alpha_i s}$ since

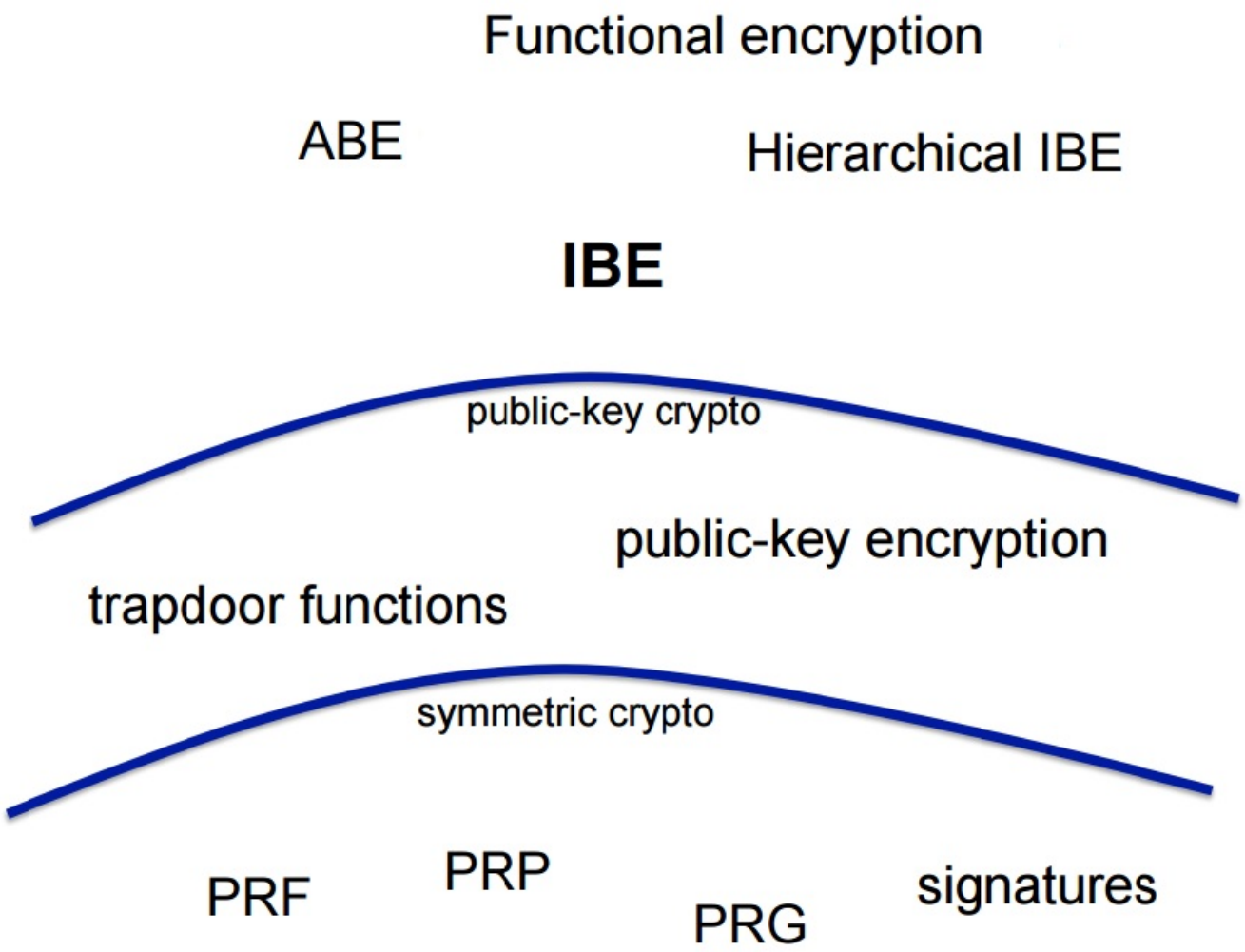
$$e(\alpha_i P + r_i H_i, sP) = e(P,P)^{\alpha_i s} e(H_i, P)^{r_i s}$$

and

$$e(sH_i, r_i P) = e(H_i, P)^{s r_i}$$

$$[C = (M.e(P,P)^{\alpha s}, sP, \{sH_i\}_{i \in S}), \qquad SK = \{(\alpha_i P + r_i H_i, r_i P)\}_i]$$

Hierarchy


Functional encryption
ABE
Hierarchical IBE
IBE
public-key crypto
public-key encryption
trapdoor functions
symmetric crypto
PRF
PRP
PRG
signatures

References


A. Menezes
An Introduction to Pairing-Based Cryptography.


D. Boneh, M. Franklin
Identity-Based Encryption from the Weil Pairing.


3rd BIU Winter School
http://crypto.biu.ac.il/3rd-biu-winter-school

Thank you for your attention!