# Cryptography

## Identity-based Encryption

Jean-Sébastien Coron and David Galindo

Université du Luxembourg

May 15, 2014

# Summary

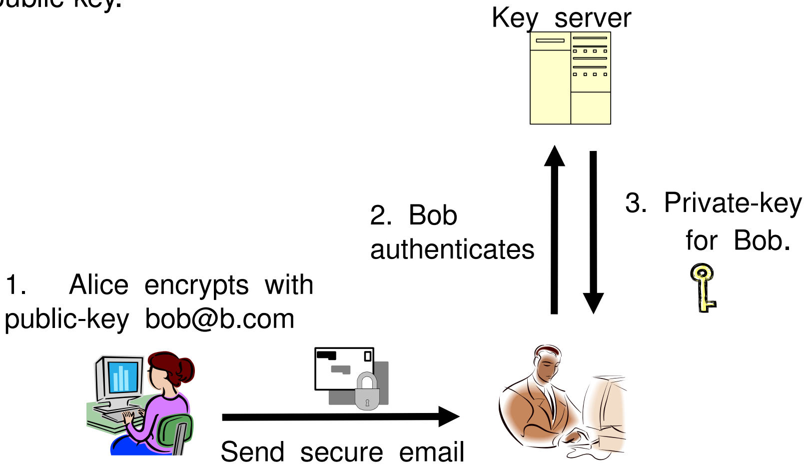
- Identity-Based Encryption (IBE)
  - What is Identity-Based Encryption ?
  - Difference with conventional PK cryptography.
  - Applications of IBE.
- Example of IBE scheme
  - Boneh-Franklin
- Security of IBE.
  - How the security of IBE is defined.
  - Security guarantee for Boneh-Franklin

# Identity-Based Encryption

- Identity-Based Encryption
  - Concept invented in 1984 by Adi Shamir.
  - First practical realization in 2001 by Boneh and Franklin.
- Principle:
  - IBE allows for a party to encrypt a message using the recipient's identity as the public-key.
  - The corresponding private-key is provided by a central authority.

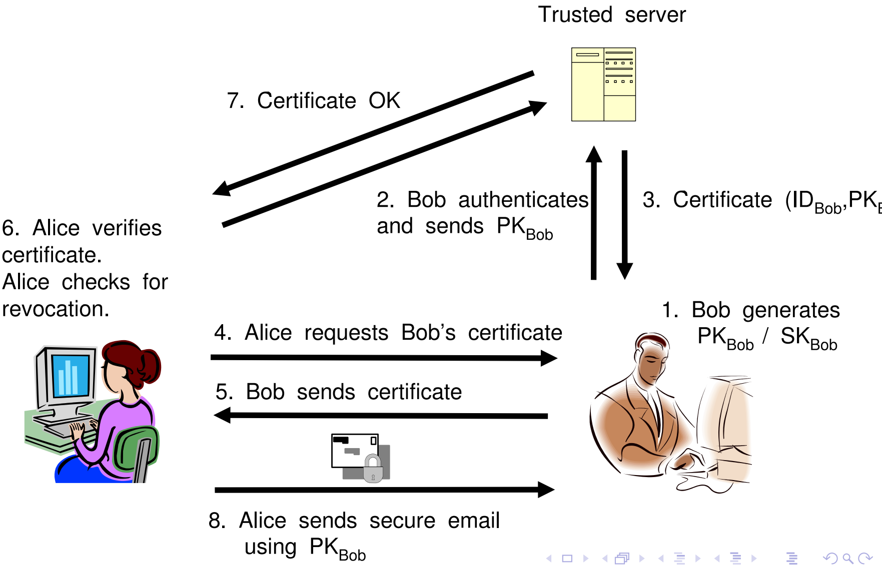
# IBE

- Alice sends an email to Bob using his identity as the public-key.



- Principle
  - Alice encrypts her email using Bob's email address `bob@b.com` as the public-key.
  - Bob receives the message. Bob contacts the key server, authenticates and obtains his private key.
  - Bob can use his private-key to decrypt the message.
  - The private-key can be used to decrypt any future message sent to Bob by Alice or any other user.

# Conventional PK



# Advantages of IBE

- Simplification of secure communications:
  - Avoids the need to distribute PK certificates.
  - Users can use their email adress as their identity
  - The recipient does not have to be online to present a PK certificate.
  - The sender does not have to be online to check that the certificate is still valid.
  - Alice can send an encrypted email to Bob even if Bob has no yet registered in the system.

# Boneh-Franklin

- Boneh-Franklin
  - First efficient IBE, proposed by Boneh and Franklin at Crypto 2001 conference.
  - Most famous IBE scheme to date.
  - Based on bilinear pairing operation over an Elliptic-Curve.
  - Proven secure, but low level of security compared to the elliptic-curve.
- Voltage Security
  - Founded in 2002 by Boneh and other people.
  - `www.voltage.com`
  - IBCS#1 standard.

# Applications of IBE

- Email encryption
  - A company hosts the Private-Key Generator (PKG) and distributes private-keys to its employees.
  - Employees can communicate securely between themselves, using their email adress as their public-key.
  - Nobody except the mail recipient (and the PKG) can decipher the communications.

# Revocation of Public-Keys

- Key-revocation in IBE is very simple
  - Alice encrypt her email sent to Bob using the public-key "**bob@company.com** ‖ **current-year**".
  - Bob can then only decrypt if he has obtained the private-key for the corresponding year.
  - With "**bob@company.com** ‖ **current-date**" instead, Bob must obtain a new private-key every day.
  - Key revocation : the PKG simply stops issuing private keys to Bob if Bob leaves the company. Then Bob can no longer read his email.
- Encrypting into the future
  - Done with "**bob@company.com** ‖ **future-date**"

# Definition of IBE

- Setup algorithm
  - Output: system public parameters *params*, and private master-key *master-key*.
- Keygen algorithm
  - Input: *params*, *master-key* and identity $v$.
  - Output: private key $d_v$ for $v$.
- Encrypt
  - Input: message $m$, identity $v$ and *params*.
  - Output: ciphertext $c$.
- Decrypt
  - Input: *params*, ciphertext $c$ and private-key $d_v$.
  - Output: plaintext $m$.

# Bilinear map

- Bilinear map :
  - Let $\mathbb{G}$ be a group of order $q$, for a large prime $q$. Let $g$ be a genarator of $\mathbb{G}$. Let $\mathbb{G}_1$ be a group of order $q$.
  - Bilinear map: function $e$ such that

$$e \ : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$$

    - Bilinear: $e(g^a, g^b) = e(g, g)^{ab}$ for all $a, b \in \mathbb{Z}$.
    - Non-degenerate: $e(g, g) \neq 1$.
    - Computable: there exists an efficient algorithm to compute $e(h_1, h_2)$ for any $h_1, h_2 \in \mathbb{G}$.

# Implementation of bilinear map

- Weil pairing or Tate pairing over an elliptic curve.
  - Let $p$ be a large prime with $p = 2 \mod 3$. Consider the Elliptic-Curve:
    $$E/\mathbb{F}_p : y^2 = x^3 + 1$$
  - The curve satisfies $\#E(\mathbb{F}_p) = p + 1$.
  - Point addition: $P = (x_1, y_1)$, $Q = (x_2, y_2)$, then $P + Q = (x_3, y_3)$ with
    $x_3 = \lambda^2 - x_1 - x_2$
    $y_3 = \lambda(x_1 - x_3) - y_1$
    with $\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{if } P \neq Q, \\ \frac{3x_1^2 + a}{2y_1}, & \text{if } P = Q. \end{cases}$

- Definition of the Weil Pairing

$$e(P, Q) = \frac{f_P(\mathcal{A}_Q)}{f_Q(\mathcal{A}_P)}$$

  - where $\mathcal{A}_P = (P + R_1) - (R_1)$ and $\mathcal{A}_Q = (Q + R_2) - (R_2)$ for random points $R_1, R_2 \in E[n]$.
  - and $n\mathcal{A}_P = (f_P)$ and $n\mathcal{A}_Q = (f_Q)$.
- Computing the Weil pairing
  - Using Miller's algorithm.
  - Algorithm in $\mathcal{O}(\log p)$ arithmetic operations mod $p$ => $\mathcal{O}(\log^3 p)$ elementary operations.

# The Boneh-Franklin IBE scheme

- Boneh-Franklin
  - First practical and secure IBE scheme.
  - Published by Boneh and Franklin at Crypto 2001 conference.
- Two versions
  - BasicIdent, which only achieves IND-ID-CPA security
  - FullIdent, that achieves IND-ID-CCA security
- Based on bilinear map
  - $e(g^a, h^b) = e(g, h)^{ab}$

# BasicIdent

- Setup
  - Let $\mathbb{G} = \langle g \rangle$ of prime order $p$. Let $H_1 : \{0,1\}^* \rightarrow \mathbb{G}$ a hash function.
  - Generate random $a \in \mathbb{Z}_p$. Let $h = g^a$.
  - Public: $(g, h)$. Secret: $a$.
- Keygen
  - Let $v$ be an identity. Private-key $d_v = H_1(v)^a$

# Boneh-Franklin

- Encryption
  - Generate a random $r \in \mathbb{Z}_p$.

$$C = \left(g^r,\ m \oplus H_2\left(e(H_1(v), h)^r\right)\right)$$

- Decryption
  - To decrypt $C = (c_1, c_2)$ using $d_v = H(v)^a$, compute:

$$m = H_2\left(e(d_v, c_1)\right) \oplus c_2$$

- Why decryption works
  - Using the bilinearity of $e$

$$e(H_1(v), h)^r = e(H_1(v), g^a)^r = e(H_1(v)^a, g^r) = e(d_v, c_1)$$

# Security of IBE

- What is security ?
  - Security is about preventing an intelligent adversary from doing certain tasks.
  - For example, recovering keys, decrypting ciphertexts, forging signatures...
- To rigorously formalize security, we must therefore:
  - 1. Specify the capabilities of the adversary (what he is allowed to do), and
  - 2. Specify in which case his attack would be successful.

# Security of IBE

- Strongest security model
  - Combine strongest capabilities with easiest adversary's goal.
- Adversary's goal
  - Could be to recover *master-key*.
    - Very ambitious goal: total break.
  - Could be to recover the private-key $d_v$ for some particular identity $v$.
  - Could be to decipher a particular ciphertext $c$.
  - Obtain only one bit of information about a plaintext $m$ given a ciphertext $c$.
    - Easiest goal

# Indistinguishability of Encryption

- The adversary should "learn nothing" about a plaintext given a ciphertext.
  - The adversary chooses messages $m_0$ and $m_1$.
  - He receives an encryption of $m_b$, for a random bit $b \in \{0, 1\}$
  - The adversary outputs a guess $b'$ of $b$.
  - Succesfull if $b' = b$.
- Adversary's advantage:
  - $\text{Adv}^{\mathcal{A}} = \left|\Pr[b' = b] - \frac{1}{2}\right|$
- Adversary's advantage must remain negligibly small.
  - Encryption must be probabilistic (or statefull).

# Adversary's capabilities

- Passive adversary
  - Can only eavesdrop communications.
- Active adversary
  - Can corrupt users, and inject and modify messages transmitted over the network.
    - Can obtain private-keys $d_v$ for identities $v$ of his choice.
    - Can obtain the decryption of ciphertexts of his choice.
  - Must still maintain "indistinguishability of encryption" for identities $v$ for which $d_v$ has not been obtained by the adversary.

# Security definition

- IND-ID-CPA
  - Indistinguishability of encryption under a chosen message attack
- IND-ID-CCA
  - Indistinguishabilty of encryption under a chosen ciphertext attack
  - The adversary may additionnally request the decryption of ciphertexts $c$ of his choice.
  - After the challenge phase, we must have $c \neq c^*$.
  - Strongest security notion.

- Theorem
  - The BasicIdent scheme achieves IND-ID-CPA security, in the random oracle model, assuming the BDH assumption.
- Random oracle model
  - The hash functions $H_1$ and $H_2$ are viewed as ideal hash-functions, returning a random output for each new input.
- BDH assumption
  - BDH problem: given $(g, g^a, g^b, g^c)$, output $e(g, g)^{abc}$.
  - BDH assumption: there is no efficient algorithm that solves the BDH problem.

# IBCS#1 standard

- Developed by Voltage Security
  - Available at `http://tools.ietf.org/html/rfc5091`
- Standard for IBE implementation
  - Algorithms for the Tate pairing over an Elliptic Curve.
  - Algorithms for Boneh-Franklin IBE
- Included at IETF (Internet Engineering Task Force) Drafts RFC 5091, RFC 5408 and RFC 5409
- IEEE P1363.3: Identity-Based Public Key Cryptography standard on-going

# Conclusion

- Identity-Based encryption
  - Enables to avoid public-key certificates.
  - Drawback: the central PKG can decrypt all communications.
- Bilinear pairings
  - Most IBE schemes are based on bilinear pairings.
  - Pairings have many other applications.
- Active research area.
  - Pairing implementations.
  - New pairing-based schemes