Cryptography

Security Proof of Boneh-Franklin IBE

Jean-Sébastien Coron

Université du Luxembourg

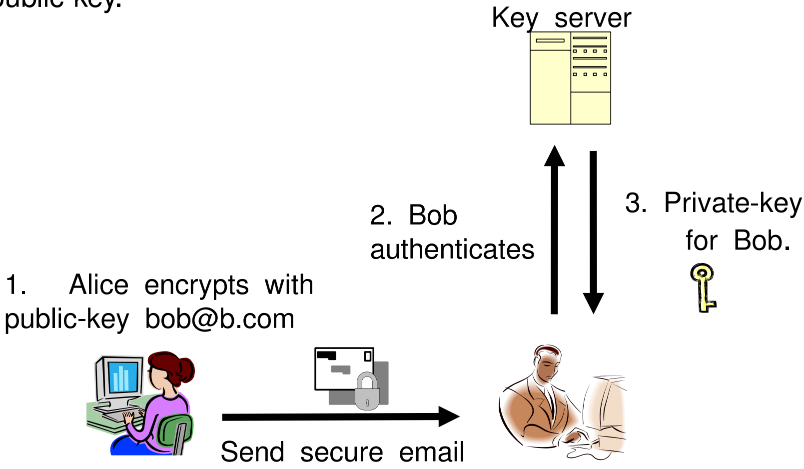
June 6, 2014

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.



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 $h_1, h_2 \in \mathbb{G}$.

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 $H_1 : \{0,1\}^* \to \mathbb{G}$ 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 $r \in \mathbb{Z}_p$.

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

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

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

- 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:
  - $\mathrm{Adv}^{\mathcal{A}} = \left|\Pr[b' = b] - \frac{1}{2}\right|$
- 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

Adversary		Challenger
	$\xleftarrow{params}$	$(Params, Master\text{-}key)$
Private-key queries	$\xrightarrow{v}$	Using *Master-key*
	$\xleftarrow{d_v}$	
Challenge phase	$\xrightarrow{v^*, m_0, m_1}$	$c^* = \text{Encrypt}(m_b, v^*)$
	$\xleftarrow{c^*}$	for random b
Private-key queries	$\xrightarrow{v \neq v^*}$	Using *Master-key*
	$\xleftarrow{d_v}$	
Guess phase	$\xrightarrow{b'}$	$b' \stackrel{?}{=} b$

$$\text{Adv}^{\mathcal{A}} = \left|\Pr[b' = b] - \frac{1}{2}\right|$$

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.

Security of Boneh-Franklin

- 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.

BasicIdent'

- We prove the security of a variant BasicIdent'
  - The message m belongs to $\mathbb{G}_1$, where

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

  - Encryption is done as:

$$C = (g^r,\ m \cdot e(H(v), h)^r)$$

  instead of

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

- Proving the security of the original BasicIdent is then easy.

BasicIdent'

- Setup
  - Let $h = g^a$ for $a \leftarrow \mathbb{Z}_p$
  - Public: (g, h). Secret: a.
- Keygen for identity v
  - Private-key $d_v = H(v)^a$
- Encryption
  - $C = (g^r,\ m \cdot e(H(v), h)^r) = (c_1, c_2)$
- Decryption
  - $m = c_2 / e(H(v)^a, c_1)$
  - $e(H(v), h)^r = e(H(v), g^a)^r = e(H(v)^a, g^r)$

Security intuition/statement

$$\begin{array}{llcl} \textbf{Sender} & g^a, g^b, c & \rightarrow & e(g,g)^{abc} = e(g^a, g^b)^c \\ \textbf{Receiver} & g^{ab}, g^c & \rightarrow & e(g,g)^{abc} = e(g^{ab}, g^c) \\ \textbf{Adversary} & g^a, g^b, g^c & \nrightarrow & e(g,g)^{abc} \end{array}$$

Theorem Let $\mathcal{A}$ an IND-ID-CCA adversary running in time t and with advantage ε against BF-IBE making at most q_E, q_D, q_H queries. Then there exists $\mathcal{B}$ running in time roughly t with advantage at least $\frac{\varepsilon}{q_H^2 q_D}$ against BDH problem in $\mathbb{G}$.

The DBDH problem

- Bilinear DH problem (BDH)
  - Given (g, g^a, g^b, g^c), compute $e(g, g)^{abc}$
- Decisional Bilinear DH problem (DBDH)
  - Let β be a random bit.
  - Given (g, g^a, g^b, g^c, z) where $z = e(g, g)^{abc}$ if $\beta = 1$ and $z \leftarrow \mathbb{G}_1$ otherwise, determine β.
  - $\mathsf{Adv}^{\mathcal{A}} = \left|\Pr[\beta' = \beta] - \frac{1}{2}\right|$
- If BDH is easy, then DBDH is easy.
  - Conversely, if DBDH is hard, then BDH is hard.
  - The converse is not necessarily true.

Proof of security

- Proof for the basic construction
  - From an adversary $\mathcal{A}$ that breaks the BasicIdent', we construct an algorithm $\mathcal{R}$ that solves the DBDH problem.
- Setup
  - $\mathcal{R}$ receives the DBDH challenge $(g, A = g^a, B = g^b, C = g^c, z)$ where $z = e(g, g)^{abc}$ if $\beta = 1$ and $z \leftarrow \mathbb{G}_1$ otherwise.
  - We must output a guess β' of β
  - Public-key: $(g, h = A = g^a)$.
    - Master-key a unknown.
  - Generate a random index $j \in [1, q_h + q_e + 1]$
    - q_h: number of hash queries.
    - q_e: number of private-key queries.

Proof of security

- i-th hash queries for $H_1(v)$:
  - If $i = j$, answer $H_1(v) = B = g^b$.
  - Otherwise generate a random $x \in \mathbb{Z}_q$, and answer $H_1(v) = g^x$
- Private-key query for v :
  - If no hash-query for $H_1(v)$, simulate one.
  - If $H_1(v) = B$, abort and return a random β'.
  - Otherwise $H_1(v) = g^x$ for some known x.
  - Then return $d_v = H_1(v)^a = g^{ax} = A^x$

Challenge and guess

- Challenge phase for identity v^* with m_0, m_1.
  - If $H_1(v^*) = B = g^b$, then let

$$\mathcal{C} = \left(C = g^c,\ m_\gamma \cdot z\right)$$

    for random bit γ. If $z = e(g,g)^{abc}$, then with $h = A = g^a$:

$$\mathcal{C} = \left(g^c,\ m_\gamma \cdot e(H(v^*), h)^c\right)$$

    which is a regular BasicIdent' ciphertext for identity v^*.
  - Otherwise abort and return a random β'.
- Guess phase: $\mathcal{A}$ answers γ'
  - If $\gamma' = \gamma$, output $\beta' = 1$ (meaning $z = e(g,g)^{abc}$)
  - otherwise output $\beta' = 0$ ($z \neq e(g,g)^{abc}$)

Analysis (1)

- We first consider the case $z = e(g,g)^{abc}$ ($\beta = 1$)
  - If $i = j$ then

$$\begin{aligned} \mathcal{C} &= \left(g^c,\ m_\gamma \cdot e(g,g)^{abc}\right) = \left(g^c,\ m_\gamma \cdot e(g^b, g^a)^c\right) \\ &= \left(g^c,\ m_\gamma \cdot e(H_1(v^*), h)^c\right) \end{aligned}$$

  - The ciphertext is distributed correctly, so

$$\Pr[\gamma' = \gamma | \beta = 1 \wedge i = j] = 1/2 + \varepsilon_A$$

which gives:

$$\Pr[\beta' = \beta | \beta = 1 \wedge i = j] = 1/2 + \varepsilon_A$$

  - When $i \neq j$ we return a random β', therefore

$$\Pr[\gamma' = \gamma | \beta = 1 \wedge i \neq j] = 1/2$$

Analysis (2)

- This gives

$$
\begin{aligned}
\Pr[\gamma' = \gamma | \beta = 1] &= \Pr[\gamma' = \gamma | \beta = 1 \wedge i = j] \cdot \Pr[i = j] \\
&+ \Pr[\gamma' = \gamma | \beta = 1 \wedge i = j] \cdot \Pr[i \neq j] \\
&= \left(\frac{1}{2} + \varepsilon_A\right) \cdot \frac{1}{q_h + q_e + 1} \\
&+ \frac{1}{2} \cdot \left(1 - \frac{1}{q_h + q_e + 1}\right) \\
&= \frac{1}{2} + \varepsilon_A \cdot \frac{1}{q_h + q_e + 1}
\end{aligned}
$$

- Therefore

$$\Pr[\beta' = \beta | \beta = 1] = \frac{1}{2} + \varepsilon_A \cdot \frac{1}{q_h + q_e + 1}$$

Analysis (3)

- If z is randomly distributed in $\mathbb{G}_1$ ($\beta = 0$)
  - Then the adversary gets no information about γ
  - $\Pr[\gamma' = \gamma | \beta = 0] = 1/2$
  - $\Pr[\beta' = \beta | \beta = 1] = 1/2$
- One obtains

$$\begin{aligned} \Pr[\beta' = \beta] &= \Pr[\beta' = \beta | \beta = 1] \cdot \Pr[\beta = 1] \\ &\quad + \Pr[\beta' = \beta | \beta = 0] \cdot \Pr[\beta = 0] \\ &= \left(\frac{1}{2} + \varepsilon_A \cdot \frac{1}{q_h + q_e + 1} \right) \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} \\ &= \frac{1}{2} + \frac{\varepsilon_A}{2(q_h + q_e + 1)} \end{aligned}$$

- The advantage ε of $\mathcal{R}$ in solving DBDH is then:

$$\varepsilon = |\Pr[\beta' = \beta] - 1/2| = \frac{\varepsilon_A}{2(q_h + q_e + 1)}$$

Security result

- Theorem
  - If the DBDH problem cannot be solved with advantage better than ε in time t, then the BasicIdent' scheme cannot be IND-ID-CPA broken with probability better than ε_A in time t_A
  - where $\varepsilon_A = 2 \cdot (q_h + q_e + 1) \cdot \varepsilon$
  - and $t_A = \mathcal{O}(t)$