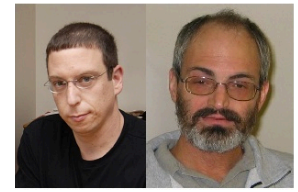
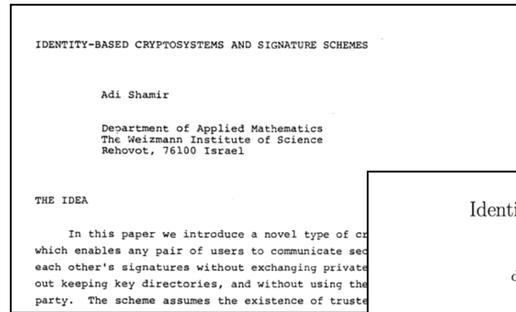
Identity-Based Encryption and Pairings

The People



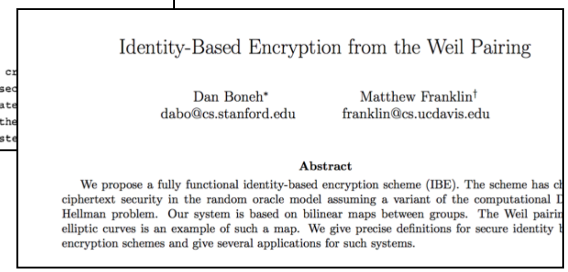

IDENTITY-BASED CRYPTOSYSTEMS AND SIGNATURE SCHEMES

Adi Shamir

Department of Applied Mathematics
The Weizmann Institute of Science
Rehovot, 76100 Israel

THE IDEA

In this paper we introduce a novel type of cr
which enables any pair of users to communicate sec
each other's signatures without exchanging private
out keeping key directories, and without using the
party. The scheme assumes the existence of truste


Identity-Based Encryption from the Weil Pairing

Dan Boneh* dabo@cs.stanford.edu
Matthew Franklin† franklin@cs.ucdavis.edu

Abstract

We propose a fully functional identity-based encryption scheme (IBE). The scheme has c
ciphertext security in the random oracle model assuming a variant of the computational D
Hellman problem. Our system is based on bilinear maps between groups. The Weil pairi
elliptic curves is an example of such a map. We give precise definitions for secure identity b
encryption schemes and give several applications for such systems.

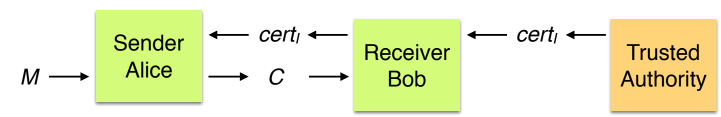
The Awards

Dan Boneh receives 2014 ACM-Infosys Foundation Award in the Computing Sciences

Dan Boneh's work was central to establishing the field of pairing-based cryptography where pairings are used to construct new cryptographic capabilities and improve the performance of existing ones. Boneh, in joint work with Matt Franklin, constructed a novel pairing-based method for identity-based encryption (IBE), whereby a user's public identity, such as an email address, can function as the user's public key. Since then, Boneh's contributions, together with those of others, have shown the power and versatility of pairings, which are now used as a mainstream tool in cryptography. The transfer of pairings from theory to practice has been rapid. Organizations now using pairings include healthcare, financial, and insurance institutions. Over a billion IBE-encrypted emails are sent each year.

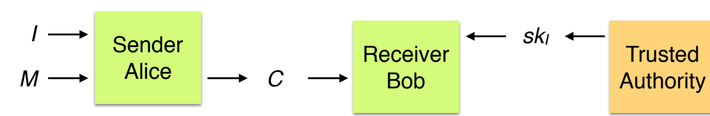
Receiver has identity I
Example: I = bob@example.com

PKE



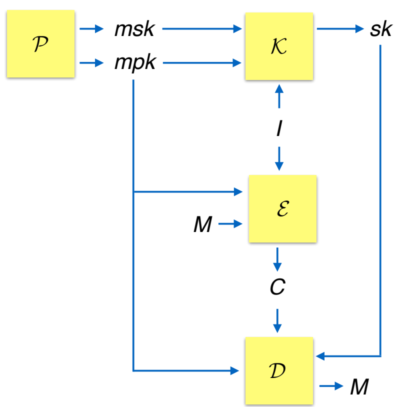
Receiver generates her own key pair (pk,sk)
Trusted authority (CA), given pk, provides receiver with a certificate $cert_I$
Sender needs Receiver's certificate before she can encrypt

IBE



Receiver generates nothing a priori
Sender only needs receiver's identity I before she can encrypt
Trusted authority (CA), given I, provides receiver with a decryption key

Syntax of an IBE scheme



$\mathcal{IBE} = (\mathcal{P}, \mathcal{K}, \mathcal{E}, \mathcal{D})$

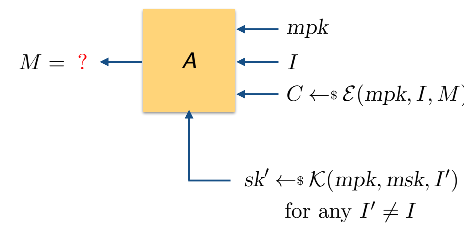
	algorithm
$\mathcal{P}$	parameter generation
$\mathcal{K}$	key generation
$\mathcal{E}$	encryption
$\mathcal{D}$	decryption

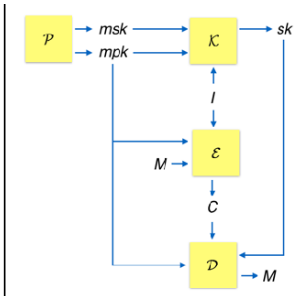
mpk	master public key
msk	master secret key
I	identity
sk	secret (decryption) key for *I*
M	message
C	ciphertext

The correct decryption requirement for identity I and message M asks that

$$\Pr[\mathcal{D}(mpk, \mathcal{K}(mpk, msk, I), \mathcal{E}(mpk, I, M)) = M] = 1$$

Security of an IBE scheme





$\mathcal{IBE} = (\mathcal{P}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is an IBE scheme.

Adversary A should be unable to figure out a message M encrypted to identity I, even given

- The master public key mpk
- The identity I
- The ciphertext C
- AND: Secret key sk' for any identity $I' \neq I$

Security of an IBE scheme

$\mathcal{IBE} = (\mathcal{P}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is an IBE scheme.
Let A be an adversary.

Game IND-CPA$_{\mathcal{IBE}}$

Initialize
$(mpk, msk) \leftarrow\$ \mathcal{P}$; $b \leftarrow\$ \{0,1\}$
$\mathrm{ExI} \leftarrow \emptyset$; $\mathrm{ChI} \leftarrow \emptyset$
Return mpk

Expose(I)
If $(I \in \mathrm{ChI})$ then return $\perp$
$\mathrm{ExI} \leftarrow \mathrm{ExI} \cup \{I\}$
$sk \leftarrow\$ \mathcal{K}(mpk, msk, I)$
Return sk

LR(I, M_0, M_1)
If $(I \in \mathrm{ExI})$ then return $\perp$
$\mathrm{ChI} \leftarrow \mathrm{ChI} \cup \{I\}$
$C \leftarrow\$ \mathcal{E}(mpk, I, M_b)$
Return C

Finalize(b')
Return $(b = b')$

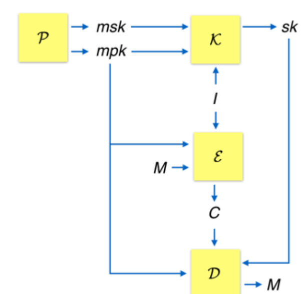
$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{IBE}}(A) = 2\Pr[\text{IND-CPA}^{A}_{\mathcal{IBE}} \Rightarrow \text{true}] - 1$$

b	Challenge bit
ExI	Set of exposed identities
ChI	Set of challenge identities
b'	A's output, guess of b

Security requires that adversary can't figure out whether left (*b*=0) or right (*b*=1) messages are encrypted for challenge identities.

Even when it is allowed to obtain the secret keys of non-challenge identities.

Building an IBE scheme



$\mathcal{IBE} = (\mathcal{P}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is an IBE scheme.

It is hard to find a way to build an IND-CPA-secure IBE scheme based on conventional number theory.

With RSA, let

- *mpk = (N,e)*
- *msk = (N,d)*
- *sk = ?*
- *C = ?*

Pairings

Let $\mathbf{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be a function, where $\mathbb{G}, \mathbb{G}_T$ are groups whose order p is a prime. Let g be a generator of $\mathbb{G}$.

We say that $\mathbf{e}$ is a pairing if the following are true:

- Bi-linearity: $\mathbf{e}(g^x, g^y) = \mathbf{e}(g, g)^{xy}$ for all $x, y \in \mathbb{Z}_p$
- Non-degeneracy: $\mathbf{e}(g, g)$ is a generator of $\mathbb{G}_T$.

Game $\mathrm{BDH}_{\mathbf{e},g}$

Initialize

$a, b, c \leftarrow\$ \mathbb{Z}_p$

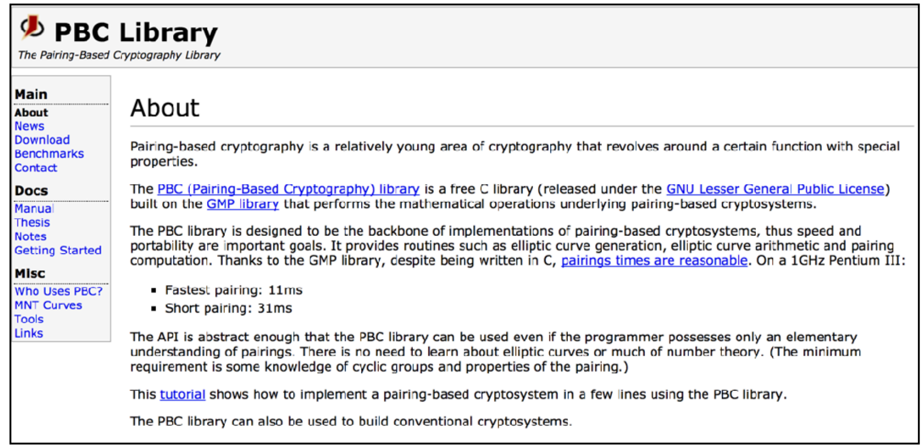
Return g^a, g^b, g^c

Finalize(Z)

Return $(Z = \mathbf{e}(g, g)^{abc})$

$$\mathbf{Adv}^{\mathrm{bdh}}_{\mathbf{e},g}(A) = \Pr[\mathrm{BDH}^A_{\mathbf{e},g} \Rightarrow \mathsf{true}]$$

Pairings that appear to be BDH-secure can be built from the Weil and Tate pairings over elliptic curves.



PBC Library

The Pairing-Based Cryptography Library

Main: About, News, Download, Benchmarks, Contact

Docs: Manual, Thesis, Notes, Getting Started

Misc: Who Uses PBC?, MNT Curves, Tools, Links

About

Pairing-based cryptography is a relatively young area of cryptography that revolves around a certain function with special properties.

The PBC (Pairing-Based Cryptography) library is a free C library (released under the GNU Lesser General Public License) built on the GMP library that performs the mathematical operations underlying pairing-based cryptosystems.

The PBC library is designed to be the backbone of implementations of pairing-based cryptosystems, thus speed and portability are important goals. It provides routines such as elliptic curve generation, elliptic curve arithmetic and pairing computation. Thanks to the GMP library, despite being written in C, pairings times are reasonable. On a 1GHz Pentium III:

- Fastest pairing: 11ms
- Short pairing: 31ms

The API is abstract enough that the PBC library can be used even if the programmer possesses only an elementary understanding of pairings. There is no need to learn about elliptic curves or much of number theory. (The minimum requirement is some knowledge of cyclic groups and properties of the pairing.)

This tutorial shows how to implement a pairing-based cryptosystem in a few lines using the PBC library.

The PBC library can also be used to build conventional cryptosystems.

Boneh-Franklin IBE scheme

$\mathbf{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ a BDH-secure pairing
g a generator of $\mathbb{G}$
p the order of $\mathbb{G}, \mathbb{G}_T$
Identity $I \in \{0,1\}^*$
Message $M \in \{0,1\}^m$
Function $H : \{0,1\}^* \to \mathbb{G}$
Function $G : \mathbb{G}_T \to \{0,1\}^m$

Algorithm $\mathcal{P}$
$msk \leftarrow\$ \mathbb{Z}_p$; $mpk \leftarrow g^{msk}$
Return (mpk, msk)

Algorithm $\mathcal{K}(mpk, msk, I)$
$sk \leftarrow H(I)^{msk}$; Return sk

Algorithm $\mathcal{E}(mpk, I, M)$
$r \leftarrow\$ \mathbb{Z}_p$; $R \leftarrow g^r$; $K \leftarrow \mathbf{e}(mpk, H(I)^r)$
$W \leftarrow G(K) \oplus M$; Return (R, W)

Algorithm $\mathcal{D}(mpk, sk, (R, W))$
$L \leftarrow \mathbf{e}(R, sk)$; $M \leftarrow G(L) \oplus W$; Return M

Proof of correct decryption requirement:

Let $I \in \{0,1\}^*$ be an identity.
Let $M \in \{0,1\}^m$ be a message
Let $sk = \mathcal{K}(mpk, msk, I) = H(I)^{msk}$
Let $(R, W) \leftarrow\$ \mathcal{E}(mpk, I, M)$
We show that $\mathcal{D}(mpk, sk, (R, W)) = M$

Let i be such that $H(I) = g^i$

$$\begin{aligned}
L &= \mathbf{e}(R, sk) && \leftarrow \text{from decryption algorithm}\\
&= \mathbf{e}(g^r, H(I)^{msk}) && \leftarrow \text{from encryption algorithm}\\
&= \mathbf{e}(g^r, g^{i \cdot msk}) && \leftarrow \text{because } H(I) = g^i\\
&= \mathbf{e}(g, g)^{ri \cdot msk} && \leftarrow \text{bi-linearity}\\
&= \mathbf{e}(g^{msk}, g^{ir}) && \leftarrow \text{bi-linearity}\\
&= \mathbf{e}(mpk, H(I)^r) && \leftarrow\\
&= K && \leftarrow \text{from encryption algorithm}
\end{aligned}$$

IBE features

Sender only needs receiver's identity *I* before she can encrypt

``Trusted'' authority can decrypt all ciphertexts for all identities

Revocation is a pain

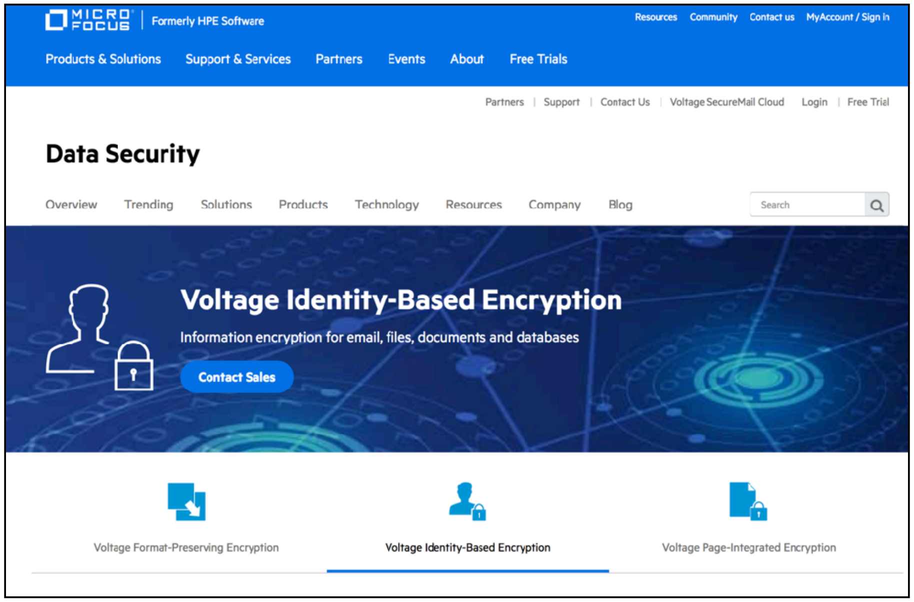
IBE issues

``Trusted'' authority can decrypt all ciphertexts for all identities

Compromise of server storing *msk* can result in adversary decrypting all ciphertexts for all identities

A secure channel is needed to communicate *sk* from trusted authority to receiver

Revocation is a pain


MICRO FOCUS
Formerly HPE Software
Resources Community Contact us MyAccount / Sign in
Products & Solutions Support & Services Partners Events About Free Trials
Partners | Support | Contact Us | Voltage SecureMail Cloud Login | Free Trial
Data Security
Overview Trending Solutions Products Technology Resources Company Blog
Search
Voltage Identity-Based Encryption
Information encryption for email, files, documents and databases
Contact Sales
Voltage Format-Preserving Encryption
Voltage Identity-Based Encryption
Voltage Page-Integrated Encryption