Broadcast Encryption and Attribute Based Encryption

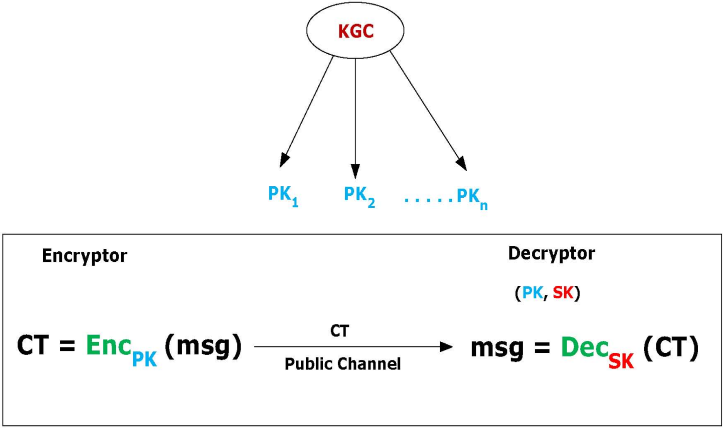
Ratna Dutta

Associate Professor
Department of Mathematics
Indian Institute of Technology Kharagpur
Kharagpur-721302, India

Email: ratna@maths.iitkgp.ernet.in

Public Key Encryption (PKE)

- 1-to-1

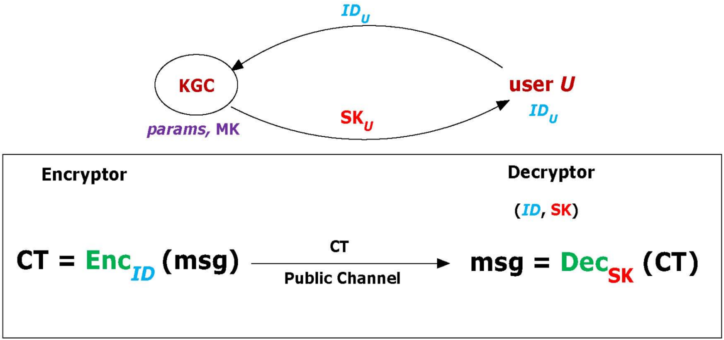


Example

- Encryption - Rabin, RSA, Merkle-Hellman, Paillier, Goldwasher-Micali, ElGamal, Generalised ElGamal
- Signature - RSA, ElGamal, DSA
- Key agreement - Diffie-Hellman

Identity Based Encryption (IBE)

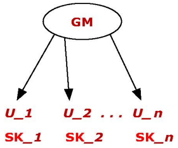
- 1-to-1
- no need to maintain public directory
- ID_U is the public key of user U (email id, biometric, etc.)

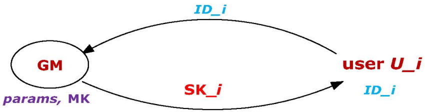


Example

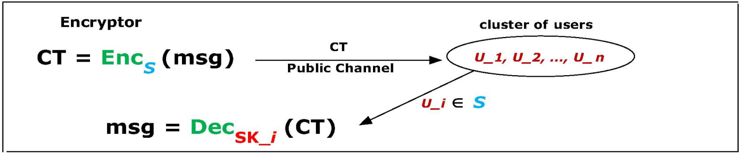
- Boneh-Franklin's Identity-Based Encryption, Crypto 2001
- Boneh- Boyen's Secure identity based encryption without random oracles, Crypto 2004
- Sahai-Waters' Fuzzy Identity Based Encryption Eurocrypt 2005.

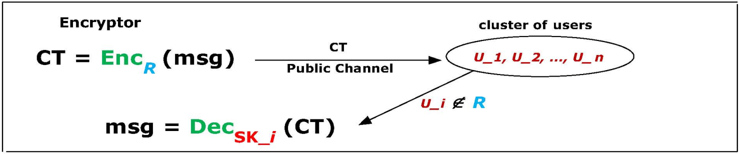
Broadcast Encryption (BE)





U = {U_1, U_2, ..., U_n} is universe of users
S is active users, *R* is revocation list





Bilinear Map

Let $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ be multiplicative cyclic groups of prime order p. A map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ satisfying the following properties is called a *bilinear map* or *bilinear pairing*.

- $e(u^a, v^b) = e(u, v)^{ab}, \forall\, u \in \mathbb{G}_1, v \in \mathbb{G}_2, a, b \in \mathbb{Z}_p$,
- if $g_1 \neq 1_{\mathbb{G}_1}$ and $g_2 \neq 1_{\mathbb{G}_2}$, then $e(g_1, g_2) \neq 1_{\mathbb{G}_T}$,
- $e(u, v)$ is efficiently computable for all $u \in \mathbb{G}_1, v \in \mathbb{G}_2$.

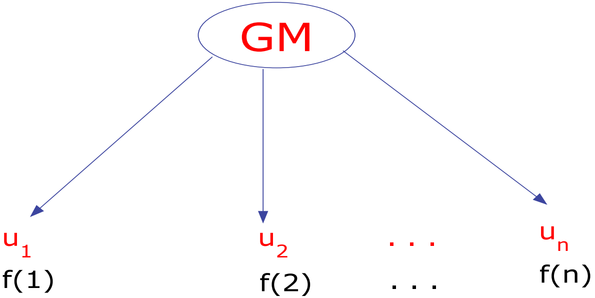
Example: Weil pairing, Tate pairing, Ate pairing, Eta pairing.

Types

Some researchers classify pairing instantiations into three types:

- Type 1: $G_1 = G_2$;
- Type 2: $G_1 \neq G_2$ but there is an efficiently computable homomorphism $\phi : G_2 \rightarrow G_1$
- Type 3: $G_1 \neq G_2$ and there are no efficiently computable homomorphisms between G_1 and G_2

BE with t-revocation



Setup(t)

- Sets a polynomial $f(x)$ of degree t-1.
- Sends secret key $f(i)$ to user i securely.

BE with t-revocation

Encrypt$(R, f(x))$

- Sets a polynomial $r(x) = (x - r_1)(x - r_2)\ldots(x - i_l)$ for a group of revoked users $R = \{u_{r_1}, \ldots, u_{r_l}\}$.
- Selects session key K and sets $h(x) = r(x)K + f(x)$.
- Broadcasts $(R, h(x))$.

BE with t-revocation

Decrypt$(u_i, f(i))$

- If user $u_i \notin R$, then recovers $K = \frac{h(i) - f(i)}{r(i)}$.
- If user $u_i \in R$, then $r(i) = 0$ and unable to recover K.

BE with t-revocation

Security

- Secure as long as less than t user colludes.
- If more than t user collides then $f(x)$ can be recovered using Lagrange's interpolation formulae. As a result K will be revealed.

BE using access polynomial

Setup(t)

- Sets a polynomial $f(x)$ of degree t-1.
- Sends secret key $f(i)$ to user i securely.

BE using access polynomial

Encrypt$(S, f(x))$

- Selects a group of users $S = \{u_{i_1}, \ldots, u_{i_l}\}$ and sets a polynomial $a(x) = 1 + (x - \theta)(x - i_1)(x - i_2)\ldots(x - i_l)$.
- Selects session key K and sets $h(x) = a(x)K + f(x)$.
- Broadcasts $(S, h(x))$.

BE using access polynomial

Decrypt$(u_i, f(i))$

- If user $u_i \in S$, then recovers $K = h(i) - f(i)$.
- If user $u_i \notin S$, then $a(i) \neq 0$ and recovers a random key as $K = \frac{h(i)-f(i)}{a(i)}$.

BE using access polynomial

Security

- Secure as long as less than t user collides.
- If more than t user collides then $f(x)$ can be recovered using Lagrange's interpolation formulae. As a result K will be revealed.

BE (Boneh, Gentry, Waters [3])

$(\mathsf{PP}, \mathsf{MK}) \leftarrow \mathsf{BE.Setup}(N, \lambda)$:

- Chooses a prime order bilinear group system $\mathbb{S} = (p, \mathbb{G}, \mathbb{G}_1, e)$, where $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ is a bilinear mapping.
- Selects $\alpha, \gamma \in_R \mathbb{Z}_p$ and sets $\mathsf{MK} = (\alpha, \gamma)$, $\mathsf{PP} = (\mathbb{S}, g, g_1, \ldots, g_N, g_{N+2}, \ldots, g_{2N}, v = g^{\gamma})$, where $g_i = g^{\alpha^i}$ for $i \in [1, N] \cup [N+2, 2N]$.
- Keeps MK secret to itself and makes PP public.

BE (Boneh, Gentry, Waters [3])

$(sk_u) \leftarrow$ BE.KeyGen(PP, MK, u):

- For each user $u \in [N]$, PKGC generates a secret key as $sk_u = (g_u)^\gamma$.

BE (Boneh, Gentry, Waters [3])

$(\mathsf{Hdr}, K) \leftarrow$ BE.Encrypt(G, PP):

- Extracts g_N from PP, chooses an integer $s \in_R \mathbb{Z}_p$ and computes a header Hdr as

$$\mathsf{Hdr} = (C_1, C_2) = \left(\left(v \prod_{j \in G} g_{N+1-j} \right)^s, (g)^s \right).$$

- Sets a session key K as

$$K = e(g_N, g_1)^s = e(g_{N+1}, g)^s,$$

- Finally, publishes Hdr and keeps K secret to itself.

BE (Boneh, Gentry, Waters [3])

$(K) \leftarrow$ BE.Decrypt(PP, sk_u, Hdr, G, u): A subscribed user u recovers the session key K as

$$K = \frac{e(g_u, C_1)}{e(sk_u \cdot \prod_{j \in G, j \neq u} g_{N+1-j+u}, C_2)}.$$

BE (Boneh, Gentry, Waters [3])

Correctness: The correctness of BE.Decrypt algorithm is as follows:

$$
\begin{aligned}
K &= \frac{e(g_u, C_1)}{e\left(sk_u \cdot \prod_{j \in G, j \neq u} g_{N+1-j+u}, C_2\right)} \\
&= \frac{e\left(g, g\right)^{s\alpha^u(\gamma + \sum_{j \in G} \alpha^{N+1-j})}}{e\left(g, g\right)^{s\alpha^u(\gamma + \sum_{j \in G, j \neq u} \alpha^{N+1-j})}} \\
&= e(g, g)^{s\alpha^{N+1}} = e(g_{N+1}, g)^s.
\end{aligned}
$$

Security

Theorem

The broadcast encryption scheme achieves selective semantic security as per the key indistinguishability security model under N-DBDHE assumption.

Security

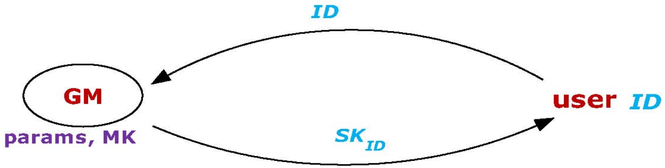
l-Decisional Bilinear Diffie-Hellman Exponent (l-DBDHE) Problem:

Input: $\langle Z = (\mathbb{S}, h, g, g^{\alpha}, \ldots, g^{\alpha^l}, g^{\alpha^{l+2}}, \ldots, g^{\alpha^{2l}}), K \rangle$, where $h \in_R \mathbb{G}, \alpha \in_R \mathbb{Z}_p, K$ is either $e(g,h)^{\alpha^{l+1}}$ or a random element $X \in \mathbb{G}_1$.
Output: 0 if $K = e(g,h)^{\alpha^{l+1}}$; 1 otherwise.

BE with Revocation (Lewko, Sahai, Waters [4])

Setup(λ)

- $(p, \mathbb{G}, g, \mathbb{G}_T, e)$.
- params $= [p, e, g, Y = e(g,g)^{\alpha}, T_1 = g^b, T_2 = g^{b^2}, T = h^b]$, where $\alpha, b \xleftarrow{R} \mathbb{Z}_p, h \xleftarrow{R} \mathbb{G}$
- MK $= [\alpha, b]$.



$$\text{SK}_{ID} = [ID, d_0 = g^{\alpha} T_2^t, d_1 = (T_1^{ID} h)^t, d_2 = g^{-t}],$$
$$ID \in \mathbb{Z}_p, t \xleftarrow{R} \mathbb{Z}_p$$

BE with Revocation (Lewko, Sahai, Waters [4])

Encrypt(params $= [p, e, g, Y, T_1, T_2, T]$, msg $\in \mathbb{G}_T, R = \{ID_1, \ldots, ID_r\}$)

- $\mathsf{CT}_R = [R, C, C_0, \{C_{i,1}, C_{i,2}\}_{i=1}^r]$, where $C = \mathsf{msg} \cdot Y^s, C_0 = g^s, C_{i,1} = T_1^{s_i}, C_{i,2} = (T_2^{ID_i} T)^{s_i}$, $s, s_1, \ldots, s_r \xleftarrow{R} \mathbb{Z}_p$ such that $s = s_1 + \cdots + s_r$.

Decrypt(params, $\mathsf{SK}_{ID} = [ID, d_0, d_1, d_2], \mathsf{CT}_R$)

- If $ID \in R$, then decryption will fail.
- If $ID \notin R$ (i.e., $ID \neq ID_i, \forall i = 1, \ldots, r$), then
$$Y^s = \frac{e(C_0, d_0)}{e\left(d_1, \prod_{i=1}^r C_{i,1}^{1/(ID-ID_i)}\right) \cdot e\left(d_2, \prod_{i=1}^r C_{i,2}^{1/(ID-ID_i)}\right)}$$
$\mathsf{msg} = C/Y^s$.

Correctness

$$
\begin{aligned}
RHS &= \frac{e(C_0, d_0)}{e\left(d_1, \prod_{i=1}^{r} C_{i,1}^{1/(ID-ID_i)}\right) \cdot e\left(d_2, \prod_{i=1}^{r} C_{i,2}^{1/(ID-ID_i)}\right)} \\
&= \frac{e(C_0, d_0)}{\prod_{i=1}^{r} \left\{e(d_1, C_{i,1}) \cdot e(d_2, C_{i,2})\right\}^{1/(ID-ID_i)}}
\end{aligned}
$$

Now,

$$
\begin{aligned}
e(d_1, C_{i,1}) \cdot e(d_2, C_{i,2}) &= e(g^{btID}h^t, g^{bs_i}) \cdot e(g^{-t}, g^{b^2 s_i ID_i} h^{bs_i}) \\
&= e(g,g)^{b^2 ts_i ID} \cdot e(h,g)^{tbs_i} \\
&\quad \cdot e(g,g)^{-b^2 ts_i ID_i} \cdot e(g,h)^{-tbs_i} \\
&= e(g,g)^{b^2 ts_i (ID-ID_i)}.
\end{aligned}
$$

BE with Revocation

$$
\begin{aligned}
& \prod_{i=1}^{r} \left\{ e(d_1, C_{i,1}) \cdot e(d_2, C_{i,2}) \right\}^{1/(ID-ID_i)} \\
= & \prod_{i=1}^{r} \left\{ e(g,g)^{b^2 t s_i (ID-ID_i)} \right\}^{1/(ID-ID_i)} \\
= & \; e(g,g)^{b^2 t \sum_{i=1}^{r} s_i} = e(g,g)^{b^2 ts}.
\end{aligned}
$$

$$
\begin{aligned}
RHS & = \frac{e(g^s, g^{\alpha} g^{b^2 t})}{e(g,g)^{b^2 ts}} \\
& = \frac{e(g,g)^{\alpha s} \cdot (g,g)^{b^2 ts}}{e(g,g)^{b^2 ts}} = e(g,g)^{\alpha s}.
\end{aligned}
$$

BE with Revocation

Therefore,

$$\frac{C}{e(g,g)^{\alpha s}} = \frac{\mathsf{msg} \cdot e(g,g)^{\alpha s}}{e(g,g)^{\alpha s}} = \mathsf{msg}.$$

Key Encapsulation Mechanism (KEM)

Encapsulation(params $= [p, e, g, Y, T_1, T_2, T], R = \{ID_1, \ldots, ID_r\}$)

- $\mathsf{EP}_R = [R, C_0, \{C_{i,1}, C_{i,2}\}_{i=1}^{r}]$, where $C_0 = g^s$, $C_{i,1} = T_1^{s_i}$, $C_{i,2} = (T_2^{ID_i} T)^{s_i}$, $s, s_1, \ldots, s_r \xleftarrow{R} \mathbb{Z}_p$ such that $s = s_1 + \cdots + s_r$.
- Encapsulation of the key $\mathsf{Key} = Y^s$ is EP_R

Decapsulation(params, $\mathsf{SK}_{ID} = [ID, d_0, d_1, d_2], \mathsf{EP}_R$)

- If $ID \in R$, then decapsulation fails.
- If $ID \notin R$ (i.e., $ID \neq ID_i, \forall i = 1, \ldots, r$), then

$$\mathsf{Key} = \frac{e(C_0, d_0)}{e\left(d_1, \prod_{i=1}^{r} C_{i,1}^{1/(ID-ID_i)}\right) \cdot e\left(d_2, \prod_{i=1}^{r} C_{i,2}^{1/(ID-ID_i)}\right)}$$

Security

Theorem

The BE scheme with revocation is semantically secure in selective set model assuming q-Decisional Multi-Exponent Bilinear Diffie-Hellman (q-DMEDH) problem is hard in $(\mathbb{G}, \mathbb{G}_T)$, where the challenge ciphertext is encrypted to $r \leq q$ revoked users.

Security

q-Decisional Multi-Exponent Bilinear Diffie-Hellman (q-DMEDH) Problem

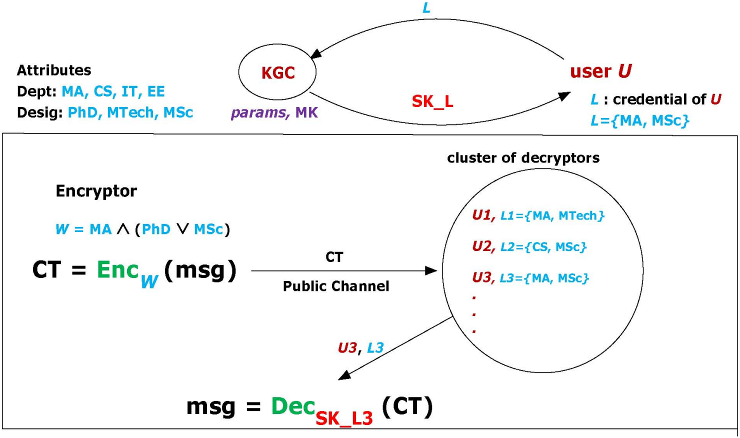
Given

$$\begin{array}{rl} & g, g^s, e(g,g)^\alpha, \\ \forall 1 \leq i,j \leq q & g^{a_i}, g^{a_i s}, g^{a_i a_j}, g^{\alpha/a_i^2}, \\ \forall \leq i,j,k \leq q, i \neq j & g^{a_i a_j s}, g^{\alpha a_j/a_i^2}, g^{\alpha a_i a_j/a_k^2}, g^{\alpha a_i^2/a_j^2}, \\ & Z \in \mathbb{G}_T, \end{array}$$

for some $s, \alpha, a_1, \ldots, a_q \in \mathbb{Z}_p$,
to decide whether $Z = e(g,g)^{\alpha s}$ or a random element in $\mathbb{G}_T$.

Attribute Based Encryption (ABE)

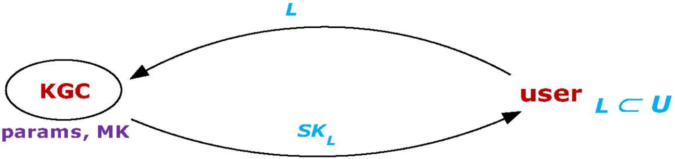
- 1-to-many
- fine grained access control



ABE (Sahai and Waters [5])

Setup(n, λ)

- $(p, \mathbb{G}, g, \mathbb{G}_T, e)$.
- $U = \{att_1, att_2, \ldots, att_n\} = \{1, 2, \ldots, n\}$.
- params $= [p, g, e, g_2, h, Y = e(g, g_2)^\alpha, T_1, T_2, \ldots, T_n]$, where $\alpha \xleftarrow{R} \mathbb{Z}_p, g_2, h, T_i \xleftarrow{R} \mathbb{G}$.
- MK $= \alpha$



SK$_L = [L, d_1 = g^r, d_2 = g_2^\alpha h^r, d_i = T_i^r, \forall i \in L]$, where $r \xleftarrow{R} \mathbb{Z}_p$

ABE (Sahai and Waters [5])

Encrypt(params$[p, g, e, g_2, h, Y = e(g, g_2)^{\alpha}, T_1, T_2, \ldots, T_n]$, $W = i_1 \wedge i_2 \wedge \ldots \wedge i_k$, msg $\in \mathbb{G}_T$)

- CT $= [W, C_1, C_2, C_3]$,
  where $C_1 =$ msg $\cdot Y^s$, $C_2 = g^s$, $C_3 = (h \prod_{j=1}^{k} T_{i_j})^s$, $s \xleftarrow{R} \mathbb{Z}_p$

Decrypt(params,SK$_L = [L, d_1, d_2, d_i, \forall i \in L]$, CT $=$ $[W, C_1, C_2, C_3]$)

- If $\{i_1, i_2, \ldots, i_k\} \not\subset L$, decryption fails
- If $\{i_1, i_2, \ldots, i_k\} \subset L$, then $d = d_2 \prod_{j=1}^{k} d_{i_j}$ and

$$\text{msg} = \frac{C_1 \cdot e(d_1, C_3)}{e(d, C_2)}$$

ABE (Sahai and Waters [5])

Correctness

- $\mathsf{SK}_L = [L, d_1 = g^r, d_2 = g_2^\alpha h^r, d_i = T_i^r, \forall i \in L]$
- $\mathsf{CT} = [W, C_1 = \mathsf{msg} \cdot Y^s, C_2 = g^s, C_3 = (h \prod_{j=1}^k T_{i_j})^s]$,

  where $Y = e(g, g_2)^\alpha$ and $d = d_2 \prod_{j=1}^k d_{i_j}$

$$
\begin{aligned}
\frac{C_1 \cdot e(d_1, C_3)}{e(d, C_2)} &= \frac{\mathsf{msg} \cdot e(g, g_2)^{\alpha s} \cdot e(g^r, (h \prod_{j=1}^k T_{i_j})^s)}{e(g_2^\alpha h^r \prod_{j=1}^k T_{i_j}^r, g^s)} \\
&= \frac{\mathsf{msg} \cdot e(g, g_2)^{\alpha s} \cdot e(g, h \prod_{j=1}^k T_{i_j})^{rs}}{e(g_2^\alpha, g^s) \cdot e(h \prod_{j=1}^k T_{i_j}, g)^{rs}} \\
&= \mathsf{msg}
\end{aligned}
$$

Security

Theorem

The ABE is semantically secure in selective attribute model, assuming DBDH problem is hard in $(\mathbb{G}, \mathbb{G}_T)$.

Decisional Bilinear Diffie-Hellman (DBDH) Problem

Given $(p, e, g, g^x, g^y, g^z, e(g,g)^\theta)$ for some $x, y, z \in \mathbb{Z}_p$, decide whether $\theta = xyz$ or a random element in $\mathbb{Z}_p$.

Conclusion

- IBE is the poster child for PBC
- Pairings a piece of nice mathematics looking for some good uses
- More flexible, more exploitable structure, than methods based on Integer factorization and discrete log

References I

[1] D. Boneh and X. Boyen. Secure identity based encryption without random oracles. In Proceedings of the Advances in Cryptology (CRYPTO 04), 2004.

[2] D. Boneh, M. Franklin. Identity Based Encryption from the Weil Pairing. SIAM J. of Computing, Vol. 32, No. 3, pp. 586−615, 2003, Extended Abstract in Crypto 2001.

[3] D. Boneh, C. Gentry, B. Waters: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 258275. Springer 2005.

[4] A. Lewko, A. Sahai, B. Waters, Revocation systems with very small private keys, in: IEEE Symposium on Security and Privacy, S&P, pages 273−285, 2010.

[5] A. Sahai and B.Waters.: Fuzzy Identity Based Encryption. In: *Advances in Cryptology - Eurocrypt,* volume 3494 of *LNCS,* pages 457-473. Springer, 2005.

Thank You