

An Identity Based Key Encapsulation Mechanism

Liqun Chen ¹, Michael Cheng ², John Malone-Lee³, Nigel Smart³

¹HP Labs Bristol, UK

²University of Middlesex, UK

³University of Bristol, UK

IEEE P1363

19 August 2005

Background (1)

- Shamir 1984: IBE concept
- Boneh & Franklin, Sakai et al. and Cocks 1999-2001: Solutions
- Boneh & Franklin 2000: Security model
- Bentahar et al. 2005: KEM/DEM framework for IBE
- Today's presentation: An efficient ID-based KEM

Background (2)

- Shoup 2000: KEM/DEM idea: encrypt a random key using public key techniques; encrypt any data using that key; send the encrypted key along with the encrypted data
- Cramer & Shoup 2003: Security definitions for KEM and DEM to build IND-CCA2 scheme
- Forthcoming standard ISO 18033-2 for public key encryption has adopted KEM/DEM approach
- Bentahar et al. 2005: KEM/DEM analogue for IBE

The Scheme: Parameters and Key Generation

- Parameters: groups \mathbb{G}_1 , \mathbb{G}_2 and \mathbb{G}_T of order p , pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, generators u_1 of \mathbb{G}_1 and u_2 of \mathbb{G}_2 with $u_1 = \psi(u_2)$, $u_T = \hat{e}(u_1, u_2)$, hash functions

$$H_1 : \{0, 1\} \rightarrow \mathbb{Z}_p, H_2 : \mathbb{G}_T \rightarrow \{0, 1\}^n$$

$$H_3 : \{0, 1\}^n \rightarrow \mathbb{Z}_p \text{ and } H_4 : \{0, 1\}^n \rightarrow \{0, 1\}^\kappa$$

- $\mathbb{G}_{\text{ID-KEM}}$:
 $s \leftarrow \mathbb{Z}_p^*$, $R \leftarrow u_1^s$.
 M_{pk} is R and other parameters.
 M_{sk} is s .

- $\mathbb{X}_{\text{ID-KEM}}(M_{pk}, \text{ID}, s)$:
 $D_{\text{ID}} \leftarrow u_2^{1/(s+H_1(\text{ID}))}$

The Scheme: Encapsulation and Decapsulation

$\mathbb{E}_{\text{ID-KEM}}(M_{\text{pt}}, \text{ID})$

- $m \leftarrow \{0, 1\}^n$
- $r \leftarrow H_3(m)$
- $Q \leftarrow R \cdot u_1^{H_1(\text{ID})}$
- $U \leftarrow Q^r$
- $V \leftarrow m \oplus H_2(u_T^r)$
- $k \leftarrow H_4(m)$
- $c \leftarrow (U, V)$
- Return (k, c)

$\mathbb{D}_{\text{ID-KEM}}(M_{\text{pt}}, \text{ID}, D_{\text{ID}}, c)$

- Parse c as (U, V)
- $\alpha \leftarrow \hat{e}(U, D_{\text{ID}})$
- $m \leftarrow H_2(\alpha) \oplus V$
- $r \leftarrow H_3(m)$
- $Q \leftarrow R \cdot u_1^{H_1(\text{ID})}$
- If $U \neq Q^r$, return \perp
- $k \leftarrow H_4(m)$
- Return k

Where does this scheme come from?

- Sakai et al. 2003: A method of deriving keys from identities.
- Bentahar et al. 2005: How to build a fully secure KEM from a weakly secure IBE scheme.
- We constructed a weakly secure encryption scheme from Sakai et al.'s primitive and applied the Bentahar et al. technique.

- Security proof in ROM relative to q -Bilinear Diffie-Hellman Inverse problem (Boneh and Boyen 2004): Given group elements $(g_1, g_2, g_2^x, g_2^{x^2}, \dots, g_2^{x^q})$ with $x \in_R \mathbb{Z}_p^*$, compute $\hat{e}(g_1, g_2)^{1/x}$.

Scheme	pairings		exponentiations		hashes	
	\mathbb{E}_{ID}	\mathbb{D}_{ID}	\mathbb{E}_{ID}	\mathbb{D}_{ID}	\mathbb{E}_{ID}	\mathbb{D}_{ID}
BF	1	1	2	1	4	3
SK-KEM	0	1	3	1	4	3