A New Public Key Cryptosystem with Key Escrow Capabilities

Ruxandra Olimid

University of Bucharest
ruxandra.olimid@fmi.unibuc.ro

25 september 2012
Public Key Encryption

A New PKS with KE Capabilities

25 September 2012
Motivation

- Communication monitoring
- Delegation of duties
- Backup of cryptographic keys
Communication monitoring
Delegation of duties
Backup of cryptographic keys
The authority that performs interception owns the secret keys of the users.
Trivial Approach

The authority that performs interception owns the secret keys of the users.
Our Goal

- **NOT** to find a better solution than IBE
- Find a solution based on **ASKGA (Asymmetric Group Key Agreement)**
Our Contribution

1. Define a lawful interception system based on ASGKA
2. Analyze its security and its performance
3. Extend the system to allow hierarchical structures
ASGKA

- Introduced by Wu et al. [Eurocrypt'09]
- The parties agree on a same public key
- Each party owns a different secret key
For $n = 2$ ASGKA provides lawful interception abilities...
Our Idea

We extend to $n > 2$...

![Diagram of key exchange between multiple parties]
... and make all the manager keys equal.
Definition

Let $G, G_T$ be 2 cyclic groups of prime order $p$, $G = \langle g \rangle$. An efficiently computable bilinear map is a map $e : G \times G \rightarrow G_T$ that satisfies:

1. **Bilinearity**: $e(u^a, v^b) = e(u, v)^{ab}, \forall u, v \in G$ and $\forall a, b \in \mathbb{Z}$
2. **Non-degeneracy**: $e(g, g) \neq 1$
3. **Computability**: $e(g_1, g_2)$ can be efficiently computed, $\forall g_1, g_2 \in G$
Preliminaries

Definition

Let $G$, $G_T$ be 2 cyclic groups of prime order $p$, $G = \langle g \rangle$. An efficiently computable bilinear map is a map $e : G \times G \to G_T$ that satisfies:

1. **Bilinearity**: $e(u^a, v^b) = e(u, v)^{ab}$, $\forall u, v \in G$ and $\forall a, b \in \mathbb{Z}$
2. **Non-degeneracy**: $e(g, g) \neq 1$
3. **Computability**: $e(g_1, g_2)$ can be efficiently computed, $\forall g_1, g_2 \in G$

Decisional Bilinear Diffie-Hellman (DBDH) Assumption

Given $g$, $g^a$, $g^b$, $g^c \in G$, no PPT adversary can distinguish (with a non-negligible advantage) $e(g, g)^{abc}$ from $Z = e(g, g)^z$, $z \in \mathbb{Z}_q$. 
Public parameters generation

$\text{PairGen}(1^\lambda) \rightarrow Y = (p, G, G_T, e)$
Our Proposal

1. **Public parameters generation**
   
   $\text{PairGen}(1^\lambda) \rightarrow Y = (p, G, G_T, e)$

2. **Manager keys generation**
   
   For $h_{\text{man}}, X_{\text{man}} \leftarrow R G$, $r_{\text{man}} \leftarrow R \mathbb{Z}_p$:
   - $R_{\text{man}} = g^{-r_{\text{man}}}$
   - $A_{\text{man}} = e(X_{\text{man}}, g)$
   - $\sigma_{\text{man}} = X_{\text{man}} h_{\text{man}}^{r_{\text{man}}}$
Our Proposal

1. Public parameters generation
   \[ \text{PairGen}(1^\lambda) \rightarrow Y = (p, G, G_T, e) \]

2. Manager keys generation
   For \( h_{man}, X_{man} \leftarrow^R G, r_{man} \leftarrow^R \mathbb{Z}_p^* \):
   \[
   \begin{align*}
   R_{man} &= g^{-r_{man}} \\
   A_{man} &= e(X_{man}, g) \\
   \sigma_{man} &= X_{man}h_{man}^{r_{man}}
   \end{align*}
   \]

3. Users keys generation
   For \( i = 1..n \)
   \[
   \begin{align*}
   h_i &\leftarrow^R G, r_i \leftarrow^R \mathbb{Z}_p^*: \\
   X_i &= X_{man}h_{man}^{r_{man}-r_i} \\
   R_i &= g^{-r_i} \\
   A_i &= e(X_i, g) \\
   \sigma_i &= X_ih_i^{r_i}
   \end{align*}
   \]
1. **Public parameters generation**
\[ \text{PairGen}(1^\lambda) \rightarrow Y = (p, G, G_T, e) \]

2. **Manager keys generation**
For \( h_{\text{man}}, X_{\text{man}} \leftarrow R G, r_{\text{man}} \leftarrow R \mathbb{Z}_p : \)
   \[ R_{\text{man}} = g^{-r_{\text{man}}} \]
   \[ A_{\text{man}} = e(X_{\text{man}}, g) \]
   \[ \sigma_{\text{man}} = X_{\text{man}} h_{\text{man}}^{r_{\text{man}}} \]

3. **Users keys generation**
For \( i = 1..n \)
   \[ h_i \leftarrow R G, r_i \leftarrow R \mathbb{Z}_p : \]
   \[ X_i = X_{\text{man}} h_{\text{man}}^{r_{\text{man}} - r_i} \]
   \[ R_i = g^{-r_i} \]
   \[ A_i = e(X_i, g) \]
   \[ \sigma_i = X_i h_i^{r_i} \]

4. **Keys distribution**
**Encryption:** A plaintext $m \in G_T$ is encrypted using the public key $(R_i, A_i)$ of a group member $P_i$ as $(t \rightarrow^R \mathbb{Z}_p^*)$:

$$c = (c_1, c_2, c_3) = (g^t, R_i^t, mA_i^t)$$
Our Proposal

- **Encryption**: A plaintext $m \in G_T$ is encrypted using the public key $(R_i, A_i)$ of a group member $P_i$ as $(t \rightarrow^R \mathbb{Z}_p^*)$:
  
  $$c = (c_1, c_2, c_3) = (g^t, R_i^t, mA_i^t)$$

- **Decryption**: A ciphertext $c = (c_1, c_2, c_3)$:
  
  - may be decrypted by $P_i$:
    
    $$m = \frac{c_3}{e(\sigma_i, c_1)e(h_i, c_2)}$$
  
  - may be decrypted by $P_{man}$:
    
    $$m = \frac{c_3}{e(\sigma_{man}, c_1)e(h_{man}, c_2)}$$
Our Proposal

- **Encryption**: A plaintext $m \in G_T$ is encrypted using the public key $(R_i, A_i)$ of a group member $P_i$ as ($t \rightarrow^R \mathbb{Z}_p^*$):
  $$c = (c_1, c_2, c_3) = (g^t, R_i^t, mA_i^t)$$

- **Decryption**: A ciphertext $c = (c_1, c_2, c_3)$:
  - may be decrypted by $P_i$:
    $$m = \frac{c_3}{e(\sigma_i, c_1) e(h_i, c_2)}$$
  - may be decrypted by $P_{man}$:
    $$m = \frac{c_3}{e(\sigma_{man}, c_1) e(h_{man}, c_2)}$$

**Theorem (Correctness)**

The basic system is correctly defined, in the sense that only the intended group member and the manager are allowed to decrypt a ciphertext.
The basic system is Ind-CPA secure under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.
A New Member Joins the Group

A New PKS with KE Capabilities
A Member Leaves the Group

- sk₁
- pk₁
- skman₁

- sk₂
- pk₂
- skman₂

- skₙ
- pkₙ
- skmanₙ

Ruxandra Olimid (UNIBUC)  
A New PKS with KE Capabilities

25 September 2012 22 / 31
The Manager Leaves the Group

The diagram illustrates the process of a manager leaving a group in a PKS with KE capabilities. The manager's private key, $sk_{man}$, is no longer accessible after leaving the group. The private keys of the individuals in the group, $sk_1, sk_2, \ldots, sk_n$, remain unchanged, but the manager's private key is crossed out, indicating it is no longer available.
Extension to Hierarchical Structures
Extension to Hierarchical Structures

Each secret key and each public key consists of m sub-keys.
Each secret key and each public key consists of $m$ sub-keys.
Building Blocks

- **BasicGen**: the previously proposed protocol;

![Diagram of BasicGen](image)
- **BasicGen**: the previously proposed protocol;
- **FwdGen**: BasicGen where $sk_{man} = sk_i$, $\forall i = 1..n$;
- **BasicGen**: the previously proposed protocol;
- **FwdGen**: BasicGen where $sk_{man} = sk_i$, $\forall i = 1..n$;
- **CopyGen**: BasicGen where $sk_{man} = sk_i$ and $pk_{man} = pk_i$, $\forall i = 1..n$;
for each level $l = 0..m - 1$:
  for each participant on level $l$:
    for each key component $i = 1..m$:
      - if $i < m - l$: FwdGen
      - if $i = m - l$: BasicGen
      - if $i > m - l$: CopyGen
The Extended System

- **Encryption:** A plaintext $m \in G_T$ is encrypted using the public key $((R_{i1}, A_{i1}), \ldots, (R_{im}, A_{im}))$ of a group member $P_i$ as $(t \rightarrow^R \mathbb{Z}_p^*)$:
  
  $$c = (c_1, c_{21}, \ldots, c_{2m}, c_3) = (g^t, R_{i1}^t, \ldots, R_{im}^t, m(A_{i1} \ldots A_{im})^t)$$
The Extended System

- **Encryption:** A plaintext $m \in G_T$ is encrypted using the public key $((R_{i1}, A_{i1}), \ldots, (R_{im}, A_{im}))$ of a group member $P_i$ as ($t \rightarrow^R \mathbb{Z}_p^*$):
  
  $$c = (c_1, c_{21}, \ldots, c_{2m}, c_3) = (g^t, R_{i1}^t, \ldots, R_{im}^t, m(A_{i1} \ldots A_{im})^t)$$

- **Decryption:** A ciphertext $c = (c_1, c_{21}, \ldots, c_{2m}, c_3)$:
  - may be decrypted by $P_i$:
    $$m = \frac{c_3}{e(\sigma_{i1}, c_1) \cdots e(\sigma_{im}, c_1) e(h_{i1}, c_{21}) \cdots e(h_{im}, c_{2m})}$$
  - may be decrypted by $P_{man}$, any manager of $P_i$ in the hierarchy:
    $$m = \frac{c_3}{e(\sigma_{man1}, c_1) \cdots e(\sigma_{manm}, c_1) e(h_{man1}, c_{21}) \cdots e(h_{manm}, c_{2m})}$$
The Extended System

Theorem

The extended system is correctly defined, in the sense that only the intended group member and any of his managers in the hierarchy are allowed to decrypt a ciphertext.
The Extended System

Theorem

The extended system is correctly defined, in the sense that only the intended group member and any of his managers in the hierarchy are allowed to decrypt a ciphertext.

Theorem

The extended system remains Ind-CPA secure under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.
Future Work

Possible Improvements

- Achieve Ind-CCA security
- Decrease the role of the key generation authority
Thank you!

Questions