Efficient File Sharing in Electronic Health Records

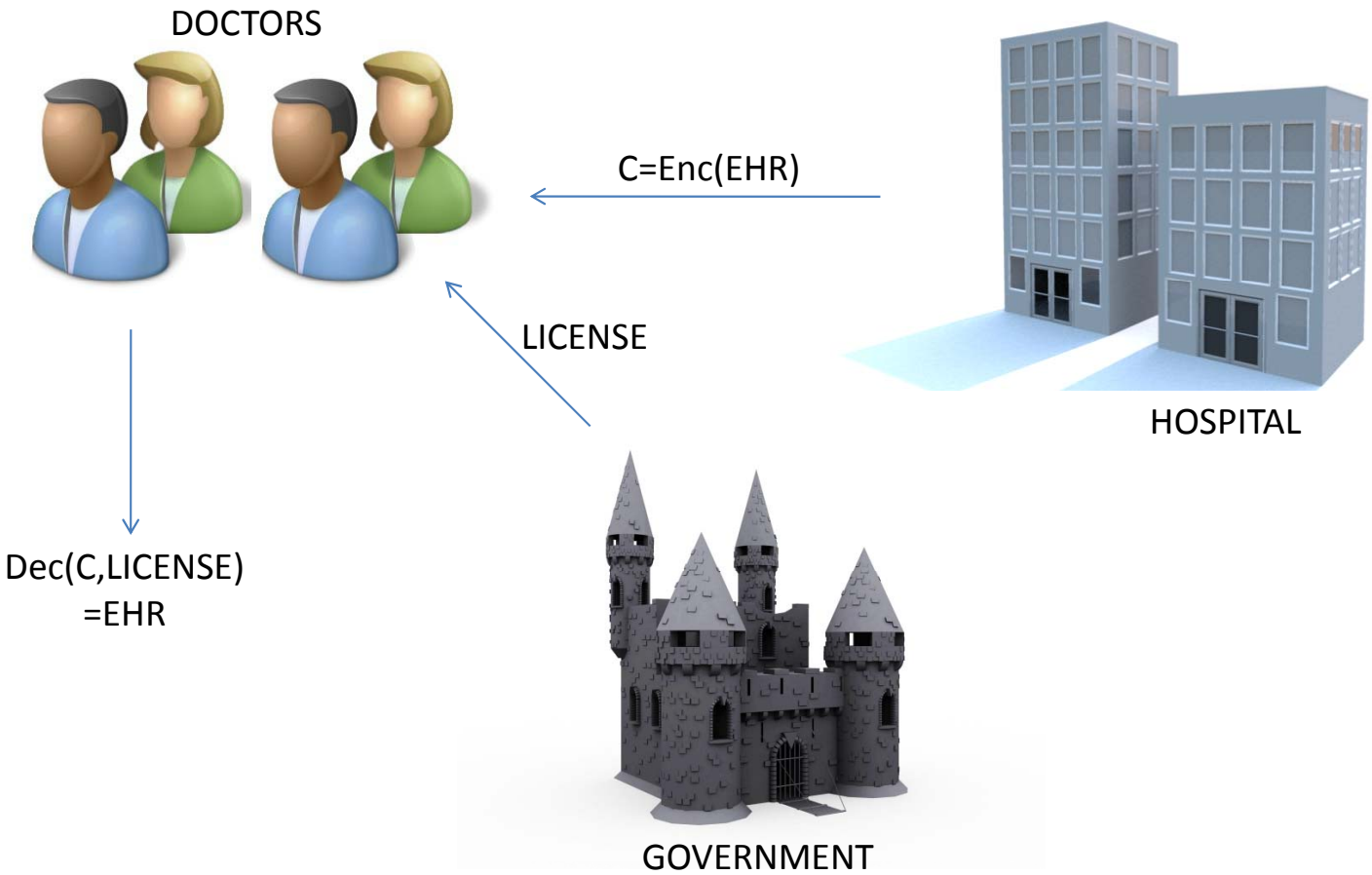
Clémentine Gritti, Willy Susilo and Thomas Plantard

University of Wollongong, Australia

27/02/2015

Outline for Section 1

Scenario


DOCTORS
C=Enc(EHR)
LICENSE
HOSPITAL
Dec(C,LICENSE)
=EHR
GOVERNMENT

Entities and Roles

1. Hospital forwarding important information (EHR) to Doctors
   - Hospital = Broadcaster
   - Forwarding = Broadcasting
2. Government and other legislators granting the license for Doctors
   - Legislators = Certifiers
   - License = Certificate
3. Doctors working in that Hospital
   - Doctors = Users

Previous Results

- Multi-Receiver Certificate-Based Encryption (MR-CBE)
- **However not suitable results:** size of public parameters and ciphertexts linear in the number of users n + only 1 certifier + selective CPA security in ROM


C.-I. Fan, P.-J. Tsai, J.-J. Huang and W.-T. Chen, *Anonymous Multi-receiver Certificate-Based Encryption*. In CyberC 2013.


C. Sur, C. D. Jung and K.-H. Rhee, *Multi-receiver Certificate-Based Encryption and Application to Public Key Broadcast Encryption*. In BLISS 2007.

Outline for Section 2

Broadcast Encryption (BE)

Broadcaster

PK and SK

C=Enc(PK,K,S')

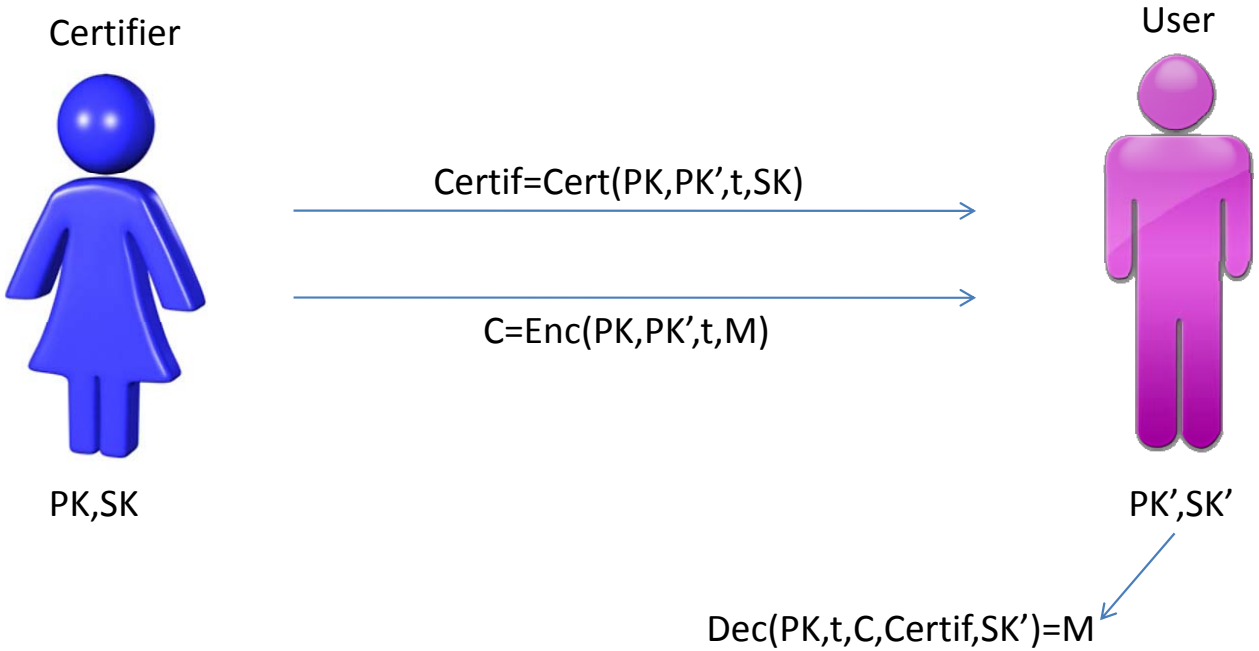
Group of users

S

S'

Dec(PK,C,S',SK)=K
if user belongs to S'

Certificate-Based Encryption (CBE)



Suitable Results

- BE: constant size for secret key and ciphertext + selective CPA security in SM
- CBE: constant size for certificate and ciphertext + adaptive CCA security in ROM


D. Boneh, C. Gentry, and B. Waters, *Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys*. In CRYPTO 2005.


C. Gentry, *Certificate-Based Encryption and the Certificate Revocation Problem*. In EUROCRYPT 2003.

Simple Combination

- BE: communication between 1 sender and n receivers
- CBE: communication between 1 sender and 1 receiver
- **However not so appropriate results:** simple combination BE + CBE gives size for ciphertext linear in number of users and number of certifiers

Efficient Combination

- File Sharing in Electronic Health Records (FSEHR)
  - Constant size for secret key, certificate and ciphertext
  - Selective CCA security in ROM
  - Size for public parameters linear in number of users and number of certifiers

Outline for Section 3

Our Scheme - Setup

- On input security parameter λ, total number n of users and total number k of certifiers
- Run $(p, \mathbb{G}, \mathbb{G}_T, e) \leftarrow$ **GroupGen**(λ, n, k)
- For $i = 1, \cdots, n, n+2, \cdots, 2n$, for $g \in_R \mathbb{G}$, $\alpha \in_R \mathbb{Z}_p$ and $\gamma \in_R \mathbb{Z}_p$, compute $g_i = g^{(\alpha^i)}$ and $v = g^{\gamma}$
- Hash functions $H_1 : \mathbb{G} \times \{0,1\}^* \rightarrow \mathbb{G}$, $H_2 : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}$ and $H_3 : \mathbb{G}_T \times \mathbb{G} \times \mathbb{G} \times \mathbb{G} \times \mathbb{G} \rightarrow \{0,1\}^{\lambda}$
- For $i \in \{1, \cdots, n\}$, compute user i's secret key $d_i = g_i^{\gamma} (= v^{(\alpha^i)})$
- For $j \in \{1, \cdots, k\}$, for $\sigma_j \in_R \mathbb{Z}_p$, compute certifier j's public key $w_j = g^{\sigma_j}$ and secret key $d_{c_j} = \sigma_j$
- Set public parameters $PK = (p, \mathbb{G}, \mathbb{G}_T, g, g_1, \cdots, g_n, g_{n+2}, \cdots, g_{2n}, v, w_1, \cdots, w_k, H_1, H_2, H_3)$

Our Scheme - Certif

- On input public parameters PK, certifier j's secret key d_{c_j}, user i and time period l represented as a string in $\{0,1\}^*$
- For $r_{i,j,l} \in_R \mathbb{Z}_p$, compute user i's certificate $e_{i,j,l}$
  - $e_{i,j,l,1} = g_i^{\sigma_j} \cdot H_1(w_j, l)^{\sigma_j \cdot r_{i,j,l}} = w_j^{(\alpha^i)} \cdot H_1(w_j, l)^{\sigma_j \cdot r_{i,j,l}}$
  - $e_{i,j,l,2} = g^{\sigma_j \cdot r_{i,j,l}} = w_j^{r_{i,j,l}}$

Our Scheme - Encrypt

- On input public parameters PK, set $S_u \subseteq \{1, \cdots, n\}$ of users, set $S_c \subseteq \{1, \cdots, k\}$ of certifiers and time period l
- For $t \in_R \mathbb{Z}_p$, compute session key $K = e(g_{n+1}, g)^t$ and ciphertext C
  - $C_1 = g^t$
  - $C_2 = \prod_{j \in S_c} H_1(w_j, l)^t$
  - $C_3 = (v \cdot \prod_{j \in S_c} w_j \cdot \prod_{i' \in S_u} g_{n+1-i'})^t$
  - $C_4 = H_2(C_1, C_3)^t$
  - $C_5 = H_3(K, C_1, C_2, C_3, C_4)$

Our Scheme - Decrypt

- On input public parameters PK, set $S_u \subseteq \{1, \cdots, n\}$ of users, set $S_c \subseteq \{1, \cdots, k\}$ of certifiers, time period l, user $i \in S_u$ with its secret key d_i and its certificates $e_{i,j,l}$ for $j \in S_c$ and l, and ciphertext C
- Check whether $e(C_1, H_2(C_1, C_3)) \stackrel{?}{=} e(g, C_4)$
- Compute $K = \frac{e(g_i, C_3) \cdot e(\prod_{j \in S_c} e_{i,j,l,2}, C_2)}{e(d_i \cdot \prod_{j \in S_c} e_{i,j,l,1} \cdot \prod_{i' \in S_u \setminus \{i\}} g_{n+1-i'+i}, C_1)} = e(g_{n+1}, g)^t$
- Compute $C_5' = H_3(K, C_1, C_2, C_3, C_4)$
- If $C_5' = C_5$, then return K; otherwise return $\perp$

Outline for Section 4

Assumption

Definition (Decisional n-Bilinear Diffie-Hellman Exponent assumption)

For any t-time adversary $\mathcal{B}$ that is given $(g, h, g^a, g^{a^2}, \cdots, g^{a^n}, g^{a^{n+2}}, \cdots, g^{a^{2n}}) \in \mathbb{G}^{2n+1}$, and a candidate to the Decisional n-BDHE problem that is either $e(g,h)^{a^{n+1}} \in \mathbb{G}_T$ or a random value T, cannot distinguish the two cases with advantage greater than ε:

$$
\begin{aligned}
&AdvBDHE_{\mathcal{B},n} \\
&= |Pr[\mathcal{B}(g, h, g^a, g^{a^2}, \cdots, g^{a^n}, g^{a^{n+2}}, \cdots, g^{a^{2n}}, e(g,h)^{a^{n+1}}) = 1] \\
&- Pr[\mathcal{B}(g, h, g^a, g^{a^2}, \cdots, g^{a^n}, g^{a^{n+2}}, \cdots, g^{a^{2n}}, T) = 1]| \\
&\leq \varepsilon.
\end{aligned}
$$

Security Proofs

Theorem (Selective CCA Security)

The File Sharing scheme in Electronic Health Records FSEHR *achieves Selective CCA Security under the Decisional* n*-BDHE assumption, in the random oracle model.*

Theorem (Collusion Resistance)

The File Sharing scheme in Electronic Health Records FSEHR *is fully secure against any number of colluders, in the random oracle model.*

Thank you for your attention

Any Questions?