Identity-based encryption and Generic group model (work in progress)

Peeter Laud

Arvutiteaduse teooriaseminar

Tallinn, 05.01.2012

Identity-based encryption

- Public-key encryption, where "public key" = "name"
  - no PKI necessary
- Formally, 4-tuple of algorithms:
  - Master public key **G**eneration
  - Secret **K**ey construction
  - **E**ncryption
  - **D**ecryption

IBE algorithms

- $\mathbf{G}(msk)$ outputs mpk.
  - Master secret key $\rightarrow$ master public key
- $\mathbf{K}(msk, \mathsf{ID})$ outputs sk_{ID}.
- $\mathbf{E}(m, mpk, \mathsf{ID}; r)$ outputs c.
  - We always take $m \in \{0, 1\}$.
- $\mathbf{D}(mpk, sk_{\mathsf{ID}}, c)$ outputs m.

Functionality: For all msk, ID, m, r:

$$\mathbf{D}(\mathbf{G}(msk), \mathbf{K}(msk, \mathsf{ID}), \mathbf{E}(m, \mathbf{G}(msk), \mathsf{ID}; r)) = m$$

Weak IND-CPA security for IBE

- The environment randomly generates $msk \in \{0,1\}^{\ell(\eta)}$. Computes $mpk = \mathbf{G}(msk)$ and sends it to the adversary.
  - η — the security parameter, determining the lengths and runtime bounds of everything.
- The adversary picks the identities $ID_1, \ldots, ID_{q_\eta}, ID^\star$ as bit-strings of length $\ell(\eta)$ and gives them to the environment.
- The environment generates $m \in \{0,1\}$ and the randomness r, computes $sk_{\mathsf{ID}_i} = \mathbf{K}(msk, \mathsf{ID}_i)$.
- Gives $sk_{\mathsf{ID}_1}, \ldots, sk_{\mathsf{ID}_q}, \mathbf{E}(m, mpk, \mathsf{ID}^\star; r)$ to the adversary.

The adversary must guess m. The scheme is weakly IND-CPA-secure if the guess is correct only with probability $1/2 + 1/negl(\eta)$.

Generic group model

- A cyclic group where “all details of representation are hidden / unusable”.
- One can only
  - generate a random element of the group;
  - perform algebraic operations with the constructed elements.
- Group size may also be known.
- Can be used to analyse group-theory-related hardness assumptions in a generic manner.
- Introduced by Nechayev, Shoup, Schnorr in late 1990s.

Generic group model (GGM)

- A machine $\mathcal{M}$, accessible to all parties of a protocol.
  - Similar to random oracles in this sense.
- Internally keeps a partial map $\mu : \{0, \ldots, p_\eta - 1\} \to \{0, 1\}^{\ell(\eta)}$.
  - p_η — size of the group for security parameter η.
- Accepts queries of the form $(\mathrm{op}, h_1, \ldots, h_k)$.
  - Returns $\mu(\mathrm{op}(\mu^{-1}(h_1), \ldots, \mu^{-1}(h_k)))$
  - Undefined points of μ will be randomly defined.
- op — one of "addition", "inverse", "unit".

Example: CDH is hard in generic group model

- **CDH:** Environment generates g, a, b. Defines $g_a = \mathcal{M}((a\cdot), g)$ and $g_b = \mathcal{M}((b\cdot), g)$. Gives g, g_a, g_b to adversary which returns h. Environment checks $h \stackrel{?}{=} \mathcal{M}((ab\cdot), g)$.
- Adversary can only create group elements of the form $g_a^x g_b^y g^z = g^{ax+by+z}$ for x, y, z chosen by him.
- For randomly chosen a, b: $g^{ax+by+z} = g^{ax'+by'+z'}$ implies $x = x', y = y', z = z'$ with high probability.
- For randomly chosen a, b: $g^{ax+by+z} \neq g^{ab}$ with high probability.
  - Schwartz-Zippel lemma

DDH is similarly hard.

Things to notice

- The attacker's computational power was not constrained.
  - The attacker only had to pay for the access to $\mathcal{M}$.
- The proof was all about polynomials in the exponents of g.
  - Indeed, we could change $\mathcal{M}$: let the domain of μ be polynomials, not $\{0, \ldots, p-1\}$.
  - This change would be indistinguishable.
- All other hardness assumptions for cyclic groups are also true in GGM.
  - Otherwise the cryptographic community wouldn't accept them.

Example: public-key encryption in GGM

- Generate $a \in \{0, \ldots, p-1\}$, $g \in \{0,1\}^\ell$. Let $h = \mathcal{M}((a\cdot), g)$. (g, h) is public key. a is secret key.
- Encryption:
  - Generate $r \in \{0, \ldots, p-1\}$. Let
    - $c_1 = \mathcal{M}((r\cdot), g)$;
    - $c_2 = \mathcal{M}(+, \mathcal{M}((m\cdot), g), \mathcal{M}((r\cdot), h))$.
  - Send (c_1, c_2).
- Decryption: Compare $\mathcal{M}(+, \mathcal{M}((-a\cdot), c_1), c_2)$ with $\mathcal{M}(0)$.

That's El-Gamal.

No IBE in GGM

Theorem. There are no weakly IND-CPA-secure identity-based encryption schemes in the generic group model.

- I.e. a computationally unconstrained adversary will break any IBE scheme.
  - Only constraint — must pay for the access to $\mathcal{M}$.
- What does this mean?
- Must use other hardness assumptions for IBE
  - Bilinear pairings and associated hardness assumptions
  - Factorization-related hardness assumptions
  - ...

A possible setup for IBE in GGM

Master public key generation:

- input — msk — a bit-string.
- $\mathbf{G}$ is given by functions
  - $P_1, \ldots, P_t : \{0,1\}^* \to \{0, \ldots, p-1\}$;
  - $P_0 : \{0,1\}^* \to \{0,1\}^*$.
- MPK is $\langle g^{P_1(msk)}, \ldots, g^{P_t(msk)}, P_0(msk) \rangle$

(that's almost completely generic)

A possible setup for IBE in GGM

Secret key generation:

- input — msk and ID — bit-strings.
- $\mathbf{K}$ is given by functions
  - $Q_1, \ldots, Q_u : (\{0,1\}^*)^2 \to \{0, \ldots, p-1\}$;
  - $Q_0 : (\{0,1\}^*)^2 \to \{0,1\}^*$.
- sk_{ID} is $\langle g^{Q_1(msk,\mathsf{ID})}, \ldots, g^{Q_u(msk,\mathsf{ID})}, Q_0(msk, \mathsf{ID})\rangle$

(that's also almost completely generic)

A possible setup for IBE in GGM

Encryption:

- input: $\langle g_1, \ldots, g_t, G_0 \rangle$, $m \in \{0,1\}$, ID, $r \in \{0,1\}^*$.
- $\mathbf{E}$ is given by functions $e_{ij}(\text{ID}, G_0, m, r)$.
- The encryption of m is a tuple of group elements

$$\left\langle \prod_{j=1}^{t} g_j^{e_{ij}(\text{ID}, G_0, m, r)} \right\rangle_{i=1}^{v} .$$

(now we're losing genericity, but still resemble existing schemes of various kinds)

A possible setup for IBE in GGM

Decryption:

- input: $\langle g_1, \ldots, g_t, G_0 \rangle$, $\langle \bar{g}_1, \ldots, \bar{g}_u, \bar{G}_0 \rangle$, $\langle h_1, \ldots, h_v \rangle$, ID.
- $\mathbf{D}$ is given by functions $d_i, d'_i, d''_i : (\{0,1\}^*)^3 \to \{0, \ldots, p-1\}$.
- Decryption computes

$$\prod_{i=1}^{t} g_i^{d_i(G_0, \bar{G}_0, \mathsf{ID}))} \cdot \prod_{i=1}^{u} \bar{g}_i^{d'_i(G_0, \bar{G}_0, \mathsf{ID})} \cdot \prod_{i=1}^{v} h_i^{d''_i(G_0, \bar{G}_0, \mathsf{ID})}$$

  if the result is the unit element in $\mathcal{M}$ then the plaintext was 0, otherwise it was 1.

Substitute, expand, collect similar terms. . .

- $\mathbf{K}(msk, \mathsf{ID})$ may return
  - coefficients $D_{\mathsf{ID},1}, \ldots, D_{\mathsf{ID},v}$;
  - a group element H_{ID}.
- Decryption checks whether

$$\prod_{i=1}^{v} h_i^{D_{\mathsf{ID},i}} = H_{\mathsf{ID}} \quad .$$

Attack

- $sk_{\mathsf{ID}} = \langle D_{\mathsf{ID},1}, \ldots, D_{\mathsf{ID},v}, H_{\mathsf{ID}} \rangle$.
  - Let $\widetilde{sk}_{\mathsf{ID}} = \langle D_{\mathsf{ID},1}, \ldots, D_{\mathsf{ID},v} \rangle$.
- Attacker has $sk_{\mathsf{ID}_1}, \ldots, sk_{\mathsf{ID}_q}$.
- Randomly sample msk' that agrees with all $D_{\mathsf{ID}_i,j}$ and the master public key.
- Compute $\langle D_{\mathsf{ID}^\star,1}, \ldots, D_{\mathsf{ID}^\star,v}, \cdot \rangle = \mathbf{K}(msk', \mathsf{ID}^\star)$.
- Encrypt 0 for $\mathsf{ID}^\star$. Decrypt it in order to find $H_{\mathsf{ID}^\star}$.
  - Maybe do it several times.

Why does the attack work?

- $\mathcal{X}$ — set of all msk.
- Let $\rho_i \in \mathbf{Eqv}(\mathcal{X})$ be the kernel of $\widetilde{\mathbf{K}}(\cdot, \mathsf{ID}_i)$.
- If msk and msk' are randomly chosen, such that $msk \; \rho_i \; msk'$ for each $i \in \{1, \ldots, q\}$, what is the probability that $msk \; \rho^\star \; msk'$?
  - Probability taken over choices of msk, msk' and $\mathsf{ID}_1, \ldots, \mathsf{ID}_q, \mathsf{ID}^\star$.
- For $\rho \in \mathbf{Eqv}(\mathcal{X})$ define $|\rho| = \sum_{i=1}^{k} |\mathcal{X}_i|^2$, where $\mathcal{X}_1, \ldots, \mathcal{X}_k \subseteq \mathcal{X}$ are the equivalence classes of ρ.
- For fixed $\mathsf{ID}_1, \ldots, \mathsf{ID}_q, \mathsf{ID}^\star$, the interesting probability is $\dfrac{|\rho_1 \wedge \cdots \wedge \rho_q \wedge \rho^\star|}{|\rho_1 \wedge \cdots \wedge \rho_q|}$.

Averaging over $\mathsf{ID}_1, \ldots, \mathsf{ID}_q, \mathsf{ID}^\star$

- Let $w \in \mathbb{N}$. Let $\rho_1, \ldots, \rho_w \in \mathbf{Eqv}(\mathcal{X})$. Let $W \subseteq \{1, \ldots, w\}$.
  - Let $\rho^W = \bigwedge_{i \in W} \rho_i$.
- Let $P^W = \dfrac{1}{|W|} \displaystyle\sum_{i \in W} \dfrac{|\rho^W|}{|\rho^{W \setminus \{i\}}|}$.
- **Theorem.** If $P^W \leq 1/c$ for some constant c and each W, then $w = O(\log |\mathcal{X}|, \frac{1}{\log c})$.
- The attacker can choose W, such that P^W is large.

Random oracle

- A machine accessible to all parties in the protocol.
- Implements a random function $\rho : \{0,1\}^{\ell(\eta)} \to \{0,1\}^{\ell(\eta)}$.
- On input x, returns $\rho(x)$.
- If $\rho(x)$ does not exist yet, it is randomly generated.

Public key encryption

- Algorithms:
  - $pk = \mathbf{K}(sk)$,
  - $c = \mathbf{E}(pk, m; r)$, $\qquad (m \in \{0, 1\})$
  - $m = \mathbf{D}(sk, c)$.
- IND-CPA security:
  - The adversary is given pk and c.
  - The adversary must guess m.

No PKE in ROM

- **Theorem.** There is no public key encryption scheme in the random oracle model that is secure against a computationally unbounded adversary.
  - The adversary only pays for oracle access.
- A consequence of *Russell Impagliazzo, Steven Rudich*. Limits on the Provable Consequences of One-way Permutations. STOC '89.

Proof idea

- Alice generates pk and sends it to Bob. Bob encrypts m and sends c to Alice. Alice decrypts.
- Computationally unbounded Eve sees pk and c.
- Everybody can access the RO.
- Let R_A, R_B and ρ be the randomness used by Alice, Bob, and RO.
- Eve samples runs of Alice and Bob consistent with pk and c.
- Eve probably finds all RO queries that Alice and Bob both made.
- RO query made only by Alice or only by Bob does not help in transmitting m.

Also relevant

- *Dan Boneh, Periklis A. Papakonstantinou, Charles Rackoff, Yevgeniy Vahlis, Brent Waters.* On The Impossibility of Basing Identity Based Encryption on Trapdoor Permutations. FOCS '08.
- No black-box construction of IBE from trapdoor permutations.
- Shows the existence of an oracle relative to which trapdoor permutations exist but IBE does not.
  - Considering computationally unbounded adversary.
- *Steven Rudich*. The Use of Interaction in Public Cryptosystems. CRYPTO '91.
- Considers the helpfulness of queries made by Alice and Bob.

Future work

- Get the details right in here.
- Consider other primitives.
- Consider the generic bilinear group.