Public-Key Encryption

601.642/442: Modern Cryptography

Fall 2020

Trapdoor Permutations

Definition (Trapdoor OWPs)

A collection of trapdoor permutations is a family of permutations $\mathcal{F} = \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i \in \mathcal{I}}$ satisfying the following properties:

Trapdoor Permutations

Definition (Trapdoor OWPs)

A collection of trapdoor permutations is a family of permutations $\mathcal{F} = \{f_i : \mathcal{D}_i \rightarrow \mathcal{R}_i\}_{i \in \mathcal{I}}$ satisfying the following properties:

- **Sampling function:** $\exists$ a PPT Gen s.t. $\mathsf{Gen}(1^n)$ outputs $(i, t) \in \mathcal{I}$

Trapdoor Permutations

Definition (Trapdoor OWPs)

A collection of trapdoor permutations is a family of permutations $\mathcal{F} = \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i \in \mathcal{I}}$ satisfying the following properties:

- **Sampling function:** $\exists$ a PPT Gen s.t. $\mathsf{Gen}(1^n)$ outputs $(i, t) \in \mathcal{I}$
- **Sampling from domain:** $\exists$ a PPT algorithm that on input i outputs a uniformly random element of $\mathcal{D}_i$

Trapdoor Permutations

Definition (Trapdoor OWPs)

A collection of trapdoor permutations is a family of permutations $\mathcal{F} = \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i \in \mathcal{I}}$ satisfying the following properties:

- **Sampling function:** $\exists$ a PPT Gen s.t. $\mathsf{Gen}(1^n)$ outputs $(i, t) \in \mathcal{I}$
- **Sampling from domain:** $\exists$ a PPT algorithm that on input i outputs a uniformly random element of $\mathcal{D}_i$
- **Evaluation:** $\exists$ PPT that on input $i, x \in \mathcal{D}_i$ outputs $f_i(x)$

Trapdoor Permutations

Definition (Trapdoor OWPs)

A collection of trapdoor permutations is a family of permutations $\mathcal{F} = \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i \in \mathcal{I}}$ satisfying the following properties:

- **Sampling function:** $\exists$ a PPT Gen s.t. $\mathsf{Gen}(1^n)$ outputs $(i, t) \in \mathcal{I}$
- **Sampling from domain:** $\exists$ a PPT algorithm that on input i outputs a uniformly random element of $\mathcal{D}_i$
- **Evaluation:** $\exists$ PPT that on input $i, x \in \mathcal{D}_i$ outputs $f_i(x)$
- **Hard to invert::** $\forall$ n.u. PPT adversary $\mathcal{A}$, $\exists$ a negligible function $\mu(\cdot)$ s.t.:

$$\Pr\left[i \leftarrow \mathsf{Gen}\left(1^n\right), x \leftarrow \mathcal{D}_i, y \leftarrow f_i(x) : f_i\left(\mathcal{A}\left(1^n, i, y\right)\right) = y\right] \leqslant \mu(n)$$

Trapdoor Permutations

Definition (Trapdoor OWPs)

A collection of trapdoor permutations is a family of permutations $\mathcal{F} = \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i \in \mathcal{I}}$ satisfying the following properties:

- **Sampling function:** $\exists$ a PPT Gen s.t. $\mathsf{Gen}(1^n)$ outputs $(i, t) \in \mathcal{I}$
- **Sampling from domain:** $\exists$ a PPT algorithm that on input i outputs a uniformly random element of $\mathcal{D}_i$
- **Evaluation:** $\exists$ PPT that on input $i, x \in \mathcal{D}_i$ outputs $f_i(x)$
- **Hard to invert:**: $\forall$ n.u. PPT adversary $\mathcal{A}$, $\exists$ a negligible function $\mu(\cdot)$ s.t.:

$$\Pr\left[i \leftarrow \mathsf{Gen}\left(1^n\right), x \leftarrow \mathcal{D}_i, y \leftarrow f_i(x) : f_i\left(\mathcal{A}\left(1^n, i, y\right)\right) = y\right] \leqslant \mu(n)$$

- **Inversion with trapdoor:** $\exists$ a PPT algorithm that given (i, t, y) outputs $f_i^{-1}(y)$

Public-key Encryption from Trapdoor Permutations

Let $\mathcal{F} = \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i \in \mathcal{I}}$ be a family of trapdoor permutations

Public-key Encryption from Trapdoor Permutations

Let $\mathcal{F} = \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i \in \mathcal{I}}$ be a family of trapdoor permutations

- $\mathsf{Gen}(1^n)$: $(f_i, f_i^{-1}) \leftarrow \mathsf{Gen}_T(1^n)$. Output $(pk, sk) \leftarrow ((f_i, h_i), f_i^{-1})$

Public-key Encryption from Trapdoor Permutations

Let $\mathcal{F} = \{f_i : \mathcal{D}_i \rightarrow \mathcal{R}_i\}_{i \in \mathcal{I}}$ be a family of trapdoor permutations

- $\mathsf{Gen}(1^n)$: $(f_i, f_i^{-1}) \leftarrow \mathsf{Gen}_T(1^n)$. Output $(pk, sk) \leftarrow ((f_i, h_i), f_i^{-1})$
- $\mathsf{Enc}(pk, m)$: Pick $r \xleftarrow{\$} \{0,1\}^n$. Output $(f_i(r), h_i(r) \oplus m)$

Public-key Encryption from Trapdoor Permutations

Let $\mathcal{F} = \{f_i : \mathcal{D}_i \rightarrow \mathcal{R}_i\}_{i \in \mathcal{I}}$ be a family of trapdoor permutations

- $\mathsf{Gen}(1^n)$: $(f_i, f_i^{-1}) \leftarrow \mathsf{Gen}_T(1^n)$. Output $(pk, sk) \leftarrow ((f_i, h_i), f_i^{-1})$
- $\mathsf{Enc}(pk, m)$: Pick $r \xleftarrow{\$} \{0,1\}^n$. Output $(f_i(r), h_i(r) \oplus m)$
- $\mathsf{Dec}(sk, (c_1, c_2))$: $r \leftarrow f_i^{-1}(c_1)$. Output $c_2 \oplus h_i(r)$

Public-key Encryption from Trapdoor Permutations

Let $\mathcal{F} = \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i \in \mathcal{I}}$ be a family of trapdoor permutations

- $\mathsf{Gen}(1^n)$: $(f_i, f_i^{-1}) \leftarrow \mathsf{Gen}_T(1^n)$. Output $(pk, sk) \leftarrow ((f_i, h_i), f_i^{-1})$
- $\mathsf{Enc}(pk, m)$: Pick $r \xleftarrow{\$} \{0,1\}^n$. Output $(f_i(r), h_i(r) \oplus m)$
- $\mathsf{Dec}(sk, (c_1, c_2))$: $r \leftarrow f_i^{-1}(c_1)$. Output $c_2 \oplus h_i(r)$

Theorem (PKE from Trapdoor Permutations)

$(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is IND-CPA secure public-key encryption scheme*

Public-key Encryption from Trapdoor Permutations

Let $\mathcal{F} = \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i \in \mathcal{I}}$ be a family of trapdoor permutations

- $\mathsf{Gen}(1^n)$: $(f_i, f_i^{-1}) \leftarrow \mathsf{Gen}_T(1^n)$. Output $(pk, sk) \leftarrow ((f_i, h_i), f_i^{-1})$
- $\mathsf{Enc}(pk, m)$: Pick $r \xleftarrow{\$} \{0,1\}^n$. Output $(f_i(r), h_i(r) \oplus m)$
- $\mathsf{Dec}(sk, (c_1, c_2))$: $r \leftarrow f_i^{-1}(c_1)$. Output $c_2 \oplus h_i(r)$

Theorem (PKE from Trapdoor Permutations)

$(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is IND-CPA secure public-key encryption scheme*

- Think: Proof?

Public-key Encryption from Trapdoor Permutations

Let $\mathcal{F} = \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i \in \mathcal{I}}$ be a family of trapdoor permutations

- $\mathsf{Gen}(1^n)$: $(f_i, f_i^{-1}) \leftarrow \mathsf{Gen}_T(1^n)$. Output $(pk, sk) \leftarrow ((f_i, h_i), f_i^{-1})$
- $\mathsf{Enc}(pk, m)$: Pick $r \stackrel{\$}{\leftarrow} \{0,1\}^n$. Output $(f_i(r), h_i(r) \oplus m)$
- $\mathsf{Dec}(sk, (c_1, c_2))$: $r \leftarrow f_i^{-1}(c_1)$. Output $c_2 \oplus h_i(r)$

Theorem (PKE from Trapdoor Permutations)

$(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is IND-CPA secure public-key encryption scheme*

- Think: Proof?
- How to build trapdoor permutations?

Candidate Trapdoor Permutations

Definition (RSA Collection)

$\mathbf{RSA} = \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i \in \mathcal{I}}$ where:

- $\mathcal{I} = \{(N, e) \mid N = p \cdot q \text{ s.t. } p, q \in \Pi_n,\ e \in \mathbb{Z}^*_{\Phi(N)}\}$
- $\mathcal{D}_i = \{x \mid x \in \mathbb{Z}^*_N\}$
- $\mathcal{R}_i = \mathbb{Z}^*_N$
- $\mathsf{Gen}(1^n) \to ((N, e), d)$ where $(N, e) \in \mathcal{I}$ and $e \cdot d = 1 \mod \Phi(N)$
- $f_{N,e}(x) = x^e \mod N$
- $f^{-1}_{N,d}(y) = y^d \mod N$

Candidate Trapdoor Permutations

Definition (RSA Collection)

$\mathbf{RSA} = \{f_i : \mathcal{D}_i \to \mathcal{R}_i\}_{i \in \mathcal{I}}$ where:

- $\mathcal{I} = \{(N, e) \mid N = p \cdot q \text{ s.t. } p, q \in \Pi_n,\ e \in \mathbb{Z}^*_{\Phi(N)}\}$
- $\mathcal{D}_i = \{x \mid x \in \mathbb{Z}^*_N\}$
- $\mathcal{R}_i = \mathbb{Z}^*_N$
- $\mathsf{Gen}(1^n) \to ((N, e), d)$ where $(N, e) \in \mathcal{I}$ and $e \cdot d = 1 \mod \Phi(N)$
- $f_{N,e}(x) = x^e \mod N$
- $f^{-1}_{N,d}(y) = y^d \mod N$

- Think: Why is $f_{N,e}$ a permutation?

Candidate Trapdoor Permutations (contd.)

Definition (RSA Assumption)

For any n.u. PPT adversary $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ s.t.:

$$\Pr\left[\begin{array}{c} p, q \xleftarrow{\$} \Pi_n,\ N = p \cdot q,\ e \xleftarrow{\$} \mathbb{Z}^*_{\Phi(N)}, \\ y \xleftarrow{\$} \mathbb{Z}^*_N;\ x \leftarrow \mathcal{A}(N, e, y) \end{array} : x^e = y \mod N\right] \leqslant \mu(n)$$

Candidate Trapdoor Permutations (contd.)

Definition (RSA Assumption)

For any n.u. PPT adversary $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ s.t.:

$$\Pr\left[\begin{array}{c} p,q \xleftarrow{\$} \Pi_n,\ N = p\cdot q,\ e \xleftarrow{\$} \mathbb{Z}^*_{\Phi(N)}, \\ y \xleftarrow{\$} \mathbb{Z}^*_N;\ x \leftarrow \mathcal{A}(N,e,y) \end{array} : x^e = y \mod N \right] \leqslant \mu(n)$$

- Think: RSA assumption implies the factoring assumption

Candidate Trapdoor Permutations (contd.)

Definition (RSA Assumption)

For any n.u. PPT adversary $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ s.t.:

$$\Pr\left[\begin{array}{c} p, q \xleftarrow{\$} \Pi_n,\ N = p \cdot q,\ e \xleftarrow{\$} \mathbb{Z}^*_{\Phi(N)}, \\ y \xleftarrow{\$} \mathbb{Z}^*_N;\ x \leftarrow \mathcal{A}(N, e, y) \end{array} : x^e = y \mod N\right] \leqslant \mu(n)$$

- Think: RSA assumption implies the factoring assumption

Theorem

Assuming the RSA assumption, the RSA collection is a family of trapdoor permutations

Food for Thought

- Direct (more efficient) constructions of PKE (e.g., El-Gamal)
- Stronger security notions:
  - Indistinguishability under chosen-ciphertext attacks (IND-CCA) [Naor-Segev],[Dolev-Dwork-Naor],[Sahai]
  - Circular security/key-dependent message security [Boneh-Halevi-Hamburg-Ostrovsky]
  - Leakage-resilient encryption [Dziembowski-Pietrzak], [Akavia-Goldwasser-Vaikuntanathan]
- Weaker security notions:
  - Deterministic encryption [Bellare-Boldyreva-O'Neill]