Functional Encryption: Introduction & Recent Advances

Gil Segev
Hebrew University
What’s Functional Encryption?
Public-Key Encryption

Alice
Bob's public key $pk$

Bob
Secret key $sk$

Enc$(pk, m)$

“All-or-nothing” approach:
• Without $sk$: The ciphertext is useless
• With $sk$: Can recover the message
Filtering Encrypted Email

\[ F: \text{Emails} \rightarrow \{\text{Urgent, Later, Spam}\} \]
Filtering Encrypted Email

Can the server filter encrypted emails?

• Without $sk$: The server is useless
• With $sk$: The server can decrypt and apply $F$
Filtering Encrypted Email

Solution: Functional Encryption

• Bob issues the server a “restricted” key $s_{KF}$
• Given $\text{Enc}(pk, m)$ the server can compute $F(m)$ but nothing else!
Functional Encryption

[Sahai-Waters ’05]

Alice
Bob’s public key $pk$

Bob
Secret key $sk$

Server
Learns $F(m)$ but nothing else about $m$

Bob’s public key $pk$

Server
$F$

$sk_F$

Encrypted message $Enc(pk, m)$
This Talk

- Direct applications
- The security of functional encryption
- The road so far: From public-key to functional encryption
- The road ahead
Filtering Encrypted Email

\[ \text{Email routing server} \]

\[ \text{Alice} \]
Bob’s public key \( pk \)

\[ \text{Enc}(pk, \text{@}) \]

\[ sk_F \]

\[ F: \text{Emails} \rightarrow \{\text{Urgent, Later, Spam}\} \]

\[ \text{Bob} \]
Secret key \( sk \)

Urgent

Later

Spam
Filtering Encrypted Email

More generally: Remote access to encrypted data
- Enable user-side encryption!
- ...

Alice
Bob’s public key $pk$

Bob
Secret key $sk$

Enc($pk, @$)

Email routing server

$SK_F$

Urgent
Later
Spam

OneDrive
Dropbox
Google Drive
Who should be allowed access?

\[
\left( (\text{CEO's Office}) \lor (\text{Marketing \\& Location} = \text{CA}) \right) \land (\text{Age} \geq 24)
\]
Expressive Access Control

Any better ideas?
Expressive Access Control

\[ \phi = (\text{(CEO's Office}) \lor (\text{Marketing & Location } = \text{CA})) \land (\text{Age } \geq 24) \]
Expressive Access Control

\[ F_{\text{User}}(\phi, m) = \begin{cases} m & \text{if } \phi(\text{User}) = 1 \\ \bot & \text{otherwise} \end{cases} \]
This Talk

- Direct applications
- The security of functional encryption
- The road so far: From public-key to functional encryption
- The road ahead
What About Security?

Alice
Bob’s public key $pk$

Bob
Secret key $sk$

User
Learns $F(m)$ but nothing else about $m$

Enc$(pk, m)$
Simulation-Based Security

Variants:
- Random vs. selective vs. adaptive
- Bounded vs. unbounded collusions (number of keys)
- Poly-time vs. unbounded simulator
- ...

Bad news [BSW11, AGVW13, ...]: Generally impossible for unbounded collusions...
**Indistinguishability-Based Security**

\[ \text{Enc}(pk, m_0) \quad \text{or} \quad \text{Enc}(pk, m_1) \]

\[ F(m_0) = F(m_1) \]

**Simulation vs. Indistinguishability:**
- Equivalent for non-functional encryption [GM82]
- Indistinguishability suffices for most FE applications
This Talk

• Direct applications

• The security of functional encryption

• The road so far: From public-key to functional encryption

• The road ahead
The Road So Far

Public-Key Encryption: $F(m) = m$

PKE

[DH76]
[RSA77]
[GM82]
Public-Key Encryption

Alice
Bob’s public key $pk$

Bob
Secret key $sk$

Shamir (CRYPTO ’84):
Can Bob’s public key be an arbitrary string?

$pk = "bob@company.com"$
Identity-Based Encryption

Bob’s ID = "bob@company.com"

Secret key $sk_{ID}$

$$F_{ID}(x, m) = \begin{cases} m & \text{if } x = ID \\ \bot & \text{otherwise} \end{cases}$$
Identity-Based Encryption

Alice

Bob's $ID = \text{"bob@company.com"}$

Bob

Secret key $sk_{ID}$

Enc($ID, m$)

Current status:
- First schemes in 2001 [BF01,C01]
- By now a variety of known schemes based on standard assumptions
- Generalizations: Hierarchical IBE [HL02,GS02], fuzzy IBE [SW05],...
- Better security: Anonymity [BF01], leakage resilience [ADNSWW10], function privacy [BRS13],...
The Road So Far

Public-Key Encryption: $F(m) = m$

Identity-Based Encryption:

$F_{ID}(x, m) = \begin{cases} m & \text{if } x = ID \\ \perp & \text{otherwise} \end{cases}$
Attribute-Based Encryption

Alice
Access policy $\phi$

Enc($\phi, m$)

Bob
Attribute-specific key $sk_x$

$$F_x(\phi, m) = \begin{cases} m & \text{if } \phi(x) = 1 \\ \bot & \text{otherwise} \end{cases}$$
Expressive Access Control

\[ \phi = \left( \left( \text{CEO's} \right) \lor \left( \text{Marketing & Location} = \text{CA} \right) \right) \land (\text{Age} \geq 24) \]
Attribute-Based Encryption

Current status:

• Various schemes for specific predicates: Inner-product, subspace membership,…
• Recently: Schemes for all predicates based on lattices [GVW13,BGGHNSVV14] or multilinear maps [GGHSW13,GGHZ14]
• Extensive on-going research
Public-Key Encryption: \( F(m) = m \)

Attribute-Based Encryption:
\[
F_{\phi}(x, m) = \begin{cases} 
m & \text{if } \phi(x) = 1 \\
\bot & \text{otherwise} 
\end{cases}
\]

Identity-Based Encryption:
\[
F_{ID}(x, m) = \begin{cases} 
m & \text{if } x = ID \\
\bot & \text{otherwise} 
\end{cases}
\]

Functional Encryption:
Any function family!
Functional Encryption

Current status:
• Bounded collusions with “long” ciphertexts based on any PKE [GVW12]
• Bounded collusions with “short” ciphertexts based on lattices [GKPVZ13]
• Unbounded collusions based on breakthroughs in program obfuscation [GHRSW13,W14]
The Road So Far

PKE
[DH76]
[RSA77]
[GM82]

IBE
[S84]
[BF01]
[C01]

ABE
[SW05]
[GVW13]
...

FE
[GVW12,GKPVZ13]
[GHRSW13,W14]
...
The Road So Far

Next: The Boneh-Franklin IBE
The Boneh-Franklin IBE
(In fact, a simplified variant based on a stronger assumption)

Pairing-based cryptography:
• Let $\mathbb{G}$ and $\mathbb{G}_T$ be cyclic groups of prime order $q$
• Let $g \in \mathbb{G}$ be a generator of $\mathbb{G}$
• Let $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be a non-degenerate bilinear map:
  • $e(g, g)$ generates $\mathbb{G}_T$
  • $e(g^a, g^b) = e(g, g)^{ab}$ for all $a, b \in \mathbb{Z}_q$
Recall: ElGamal Encryption ‘84

Setup:
• Sample $sk = \alpha \leftarrow \mathbb{Z}_q$
• Let $pk = h = g^\alpha$

Encryption of $m$:
• Sample $r \leftarrow \mathbb{Z}_q$
• Output $(c_0, c_1) = (g^r, h^r \cdot m)$

Decrypting $(c_0, c_1)$ using $sk$:

$$
\frac{c_1}{(c_0)^\alpha} = \frac{h^r \cdot m}{g^{r\alpha}} = \frac{g^{\alpha r} \cdot m}{g^{r\alpha}} = m
$$

The Decisional Diffie-Hellman (DDH) Assumption:

$$(g, g^\alpha, g^r, g^{\alpha r}) \approx^c (g, g^\alpha, g^r, g^z)$$

where $\alpha, r, z \leftarrow \mathbb{Z}_q$. 
Recall: ElGamal Encryption ‘84

**Setup:**
- Sample $sk = \alpha \leftarrow \mathbb{Z}_q$
- Let $pk = h = g^\alpha$

**Encryption of $m$:**
- Sample $r \leftarrow \mathbb{Z}_q$
- Output $(c_0, c_1) = (g^r, h^r \cdot m)$

Boneh-Franklin ‘01: From ElGamal to IBE
- For each $ID$ implicitly define $pk_{ID}$ by “projecting” $pk$ onto $ID$ in $\mathbb{G}_T$
- Encrypt to $pk_{ID}$ by splitting El-Gamal between $\mathbb{G}$ and $\mathbb{G}_T$
- Security proof: Projections are “computationally independent”

$$pk = h \quad \xrightarrow{ID} \quad pk_{ID} = e(h, H(ID))$$

$$sk = \alpha \quad \xrightarrow{ID} \quad sk_{ID} = H(ID)^\alpha$$
The Boneh-Franklin IBE

Setup:
• Sample $sk = \alpha \leftarrow \mathbb{Z}_q$
• Let $pk = h = g^\alpha$

Key generation for $ID$:
• Output $sk_{ID} = H(ID)^\alpha$

Encryption of $(ID, m)$:
• Sample $r \leftarrow \mathbb{Z}_q$ and output $(c_0, c_1) = \left( g^r, e(h, H(ID))^r \cdot m \right)$

Decrypting $(c_0, c_1)$ using $sk_{ID}$:

$$\frac{c_1}{e(c_0, sk_{ID})} = \frac{e(h, H(ID))^r \cdot m}{e(g^r, H(ID)^\alpha)} = \frac{e(g^\alpha, H(ID))^r \cdot m}{e(g^r, H(ID)^\alpha)} = m$$
IBE Security

IBE security requirement:
For any efficient adversary $|\Pr[b' = b] - 1/2|$ is negligible
This Talk

• Direct applications

• The security of functional encryption

• The road so far: From public-key to functional encryption

• The road ahead
The Road Ahead

• We are current losing the **functionality vs. efficiency** battle
  • Deployment beyond identity-based encryption?
  • Better efficiency in the symmetric-key setting?
The Road Ahead

- We are current losing the **functionality vs. efficiency** battle
  - Deployment beyond identity-based encryption?
  - Better efficiency in the symmetric-key setting?
The Road Ahead

- We are currently losing the **functionality vs. efficiency** battle
  - Deployment beyond identity-based encryption?
  - Better efficiency in the symmetric-key setting?
The Road Ahead

• **We are current losing the functionality vs. efficiency battle**
  • Deployment beyond identity-based encryption?
  • Better efficiency in the symmetric-key setting?

• **More schemes based on more standard assumptions**
  • More bilinear maps & lattices
  • Less obfuscation
  • Weaker assumptions in the symmetric-key setting? [ABSV14,BS15,KSY15]

• **Better security for functional encryption**
  • Function privacy: Does $sk_F$ reveal $F$? [BRS13,...]
  • Application-specific security (e.g., deduplication [BKR13,ABMRS13,...])

• **We’re just getting started...**
Thank You