Provable Security for Public-Key Schemes

II – Encryption

Provable Security

One can prove that:
- if an adversary is able to break the cryptographic scheme
  then one can break the underlying problem
  (integer factoring, discrete logarithm, 3-SAT, etc)

Outline

1. Game-based Proofs
   - Provable Security
   - Game-based Approach
   - Transition Hops

2. Advanced Security for Encryption
   - Advanced Security Notions
   - Cramer-Shoup Encryption Scheme

3. Conclusion
Direct Reduction

Unfortunately

- Security may rely on several assumptions
- Proving that the view of the adversary, generated by the simulator, in the reduction is the same as in the real attack game is not easy to do in such a one big step

Sequence of Games

Real Attack Game
The adversary plays a game, against a challenger (security notion)

Simulation
The adversary plays a game, against a sequence of simulators
Output

- The output of the simulator in Game 1 is related to the output of the challenger in Game 0 (adversary's winning probability).
- The output of the simulator in Game 3 is easy to evaluate (e.g., always zero, always 1, probability of one-half).
- The gaps (Game 1 ↔ Game 2, Game 2 ↔ Game 3, etc.) are clearly identified with specific events.

Outline

1. Game-based Proofs
   - Provable Security
   - Game-based Approach
   - Transition Hops

2. Advanced Security for Encryption

3. Conclusion
Two Simulations

- Identical behaviors: \( \Pr[\text{Game}_A] - \Pr[\text{Game}_B] = 0 \)
- The behaviors differ only if \( \text{Ev} \) happens:
  - \( \text{Ev} \) is negligible, one can ignore it
  - Shoup's Lemma: \( \Pr[\text{Game}_A] - \Pr[\text{Game}_B] \leq \Pr[\text{Ev}] \)

\[
|\Pr[\text{Game}_A] - \Pr[\text{Game}_B]| \\
= |\Pr[\text{Game}_A|\text{Ev}] \Pr[\text{Ev}] + \Pr[\text{Game}_A|\neg\text{Ev}] \Pr[\neg\text{Ev}] - \Pr[\text{Game}_B|\text{Ev}] \Pr[\text{Ev}] - \Pr[\text{Game}_B|\neg\text{Ev}] \Pr[\neg\text{Ev}]| \\
= (\Pr[\text{Game}_A|\text{Ev}] - \Pr[\text{Game}_B|\text{Ev}]) \times \Pr[\text{Ev}] + (\Pr[\text{Game}_A|\neg\text{Ev}] - \Pr[\text{Game}_B|\neg\text{Ev}]) \times \Pr[\neg\text{Ev}] \\
\leq |1 \times \Pr[\text{Ev}] + 0 \times \Pr[\neg\text{Ev}]| \leq \Pr[\text{Ev}] \\
\]

- \( \text{Ev} \) is non-negligible and independent of the output in \( \text{Game}_A \), Simulator B terminates in case of event \( \text{Ev} \)

Two Distributions

- Identical behaviors: \( \Pr[\text{Game}_A] - \Pr[\text{Game}_B] = 0 \)
- The behaviors differ only if \( \text{Ev} \) happens:
  - \( \text{Ev} \) is negligible, one can ignore it
  - \( \text{Ev} \) is non-negligible and independent of the output in \( \text{Game}_A \), Simulator B terminates and outputs 0, in case of event \( \text{Ev} \):

\[
\Pr[\text{Game}_B] = \Pr[\text{Game}_B|\text{Ev}] \Pr[\text{Ev}] + \Pr[\text{Game}_B|\neg\text{Ev}] \Pr[\neg\text{Ev}] \\
= 0 \times \Pr[\text{Ev}] + \Pr[\text{Game}_A|\neg\text{Ev}] \times \Pr[\neg\text{Ev}] \\
= \Pr[\text{Game}_A] \times \Pr[\neg\text{Ev}] \\
\]

Simulator B terminates and flips a coin, in case of event \( \text{Ev} \):

\[
\Pr[\text{Game}_B] = \Pr[\text{Game}_B|\text{Ev}] \Pr[\text{Ev}] + \Pr[\text{Game}_B|\neg\text{Ev}] \Pr[\neg\text{Ev}] \\
= \frac{1}{2} \times \Pr[\text{Ev}] + \Pr[\text{Game}_A|\neg\text{Ev}] \times \Pr[\neg\text{Ev}] \\
= \frac{1}{2} + (\Pr[\text{Game}_A|\neg\text{Ev}] \times \frac{1}{2}) \times \Pr[\neg\text{Ev}] \\
\]
Two Simulations

- Identical behaviors: $\Pr[\text{Game}_A] - \Pr[\text{Game}_B] = 0$
- The behaviors differ only if $\text{Ev}$ happens:
  - $\text{Ev}$ is negligible, one can ignore it
  - $\text{Ev}$ is non-negligible and independent of the output in $\text{Game}_A$,
    Simulator $B$ terminates in case of event $\text{Ev}$

**Event $\text{Ev}$**

- Either $\text{Ev}$ is negligible, or the output is independent of $\text{Ev}$
- For being able to terminate simulation $B$ in case of event $\text{Ev}$,
  this event must be *efficiently* detectable
- For evaluating $\Pr[\text{Ev}]$, one re-iterates the above process,
  with an initial game that outputs 1 when event $\text{Ev}$ happens

Two Distributions

$$\Pr[\text{Game}_A] - \Pr[\text{Game}_B] \leq \text{Adv}(\text{Doracles})$$

- For identical/statistically close distributions, for any oracle:
  $$\Pr[\text{Game}_A] - \Pr[\text{Game}_B] = \text{Dist}(\text{Distrib}_A, \text{Distrib}_B) = \text{negl}()$$
- For computationally close distributions, in general, we need to
  exclude additional oracle access:
  $$\Pr[\text{Game}_A] - \Pr[\text{Game}_B] \leq \text{Adv}^{\text{Distrib}}(t)$$
  where $t$ is the computational time of the distinguisher

Outline

1. Game-based Proofs
2. Advanced Security for Encryption
   - Advanced Security Notions
   - Cramer-Shoup Encryption Scheme
3. Conclusion
Public-Key Encryption

**IND – CPA Security Game**

The adversary cannot get any information about a plaintext of a specific ciphertext (validity, partial value, etc).

**Malleability**

Semantic security (ciphertext indistinguishability) guarantees that no information is leaked from $c$ about the plaintext $m$. But it may be possible to derive a ciphertext $c'$ such that the plaintext $m'$ is related to $m$ in a meaningful way:

- ElGamal ciphertext: $c_1 = g^r$ and $c_2 = m \times y^r$
- Malleability: $c_1' = c_1 = g^r$ and $c_2' = 2 \times c_2 = (2m) \times y^r$

From an encryption of $m$, one can build an encryption of $2m$, or a random ciphertext of $m$, etc.

A formal security game for NM – CPA has been defined, but we ignore it for the moment.

**Additional Information**

More information modeled by oracle access:

- reaction attacks: oracle which answers, on $c$, whether the ciphertext $c$ is valid or not
- plaintext-checking attacks: oracle which answers, on a pair $(m, c)$, whether the plaintext $m$ is really encrypted in $c$ or not (whether $m = D_{sk}(c)$)
- chosen-ciphertext attacks (CCA): decryption oracle (with the restriction not to use it on the challenge ciphertext) ⇒ the adversary can obtain the plaintext of any ciphertext of its choice (excepted the challenge)
  - non-adaptive (CCA – 1) only before receiving the challenge
  - adaptive (CCA – 2) unlimited oracle access

[Naor-Yung – STOC ’90]
[Rackoff-Simon – Crypto ’91]
The adversary can ask any decryption of its choice: Chosen-Ciphertext Attacks (oracle access)

\[(sk, pk) \leftarrow \mathcal{K}(); (m_0, m_1, \text{state}) \leftarrow \mathcal{A}^D(pk);
\]
\[b \overset{\$}{\leftarrow} \{0, 1\}; \quad c = \varepsilon_{pk}(m_b); \quad b' \leftarrow \mathcal{A}^D(\text{state}, c)\]

\[\text{Adv}^{\text{ind-cca}}_S(\mathcal{A}) = \Pr[b' = 1 | b = 1] - \Pr[b' = 1 | b = 0] = 2 \times \Pr[b' = b] - 1\]

**Cramer-Shoup Encryption Scheme**

**Key Generation**

- \(G = (\langle g \rangle, \times)\) group of order \(q\)
- \(sk = (x_1, x_2, y_1, y_2, z)\), where \(x_1, x_2, y_1, y_2, z \overset{\$}{\leftarrow} \mathbb{Z}_q\)
- \(pk = (g_1, g_2, \mathcal{H}, c, d, h)\), where
  - \(g_1, g_2\) are independent elements in \(G\)
  - \(\mathcal{H}\) a hash function (second-preimage resistant)
  - \(c = g_1^{x_1} g_2^{x_2}, \quad d = g_1^{y_1} g_2^{y_2}\), and \(h = g_1^z\)

**Encryption**

\[u_1 = g_1^r, \quad u_2 = g_2^r, \quad e = m \times h^r, \quad v = c^r d^\alpha \text{ where } \alpha = \mathcal{H}(u_1, u_2, e)\]
Cramer-Shoup Encryption Scheme vs. ElGamal

\[ u_1 = g_1^e, \quad u_2 = g_2^e, \quad e = m \times h^f, \quad v = c^f d^r \alpha \quad \text{where} \quad \alpha = \mathcal{H}(u_1, u_2, e) \]

\((u_1, e)\) is an ElGamal ciphertext, with public key \( h = g_1^x \)

**Decryption**

- Since \( h = g_1^x, h^f = u_1^x, \) thus \( m = e / u_1^x \)
- Since \( c = g_1^{x_1} g_2^{x_2} \) and \( d = g_1^{y_1} g_2^{y_2} \)

\[ c' = g_1^{r x_1} g_2^{r x_2} = u_1^{x_1} u_2^{x_2}, \quad d' = u_1^{y_1} u_2^{y_2} \]

One thus first checks whether

\[ v = u_1^{x_1 + \alpha y_1} u_2^{x_2 + \alpha y_2} \quad \text{where} \quad \alpha = \mathcal{H}(u_1, u_2, e) \]

---

**Security of the Cramer-Shoup Encryption Scheme**

**Theorem**

The Cramer-Shoup encryption scheme achieves IND−CCA security, under the DDH assumption, and the second-preimage resistance of \( \mathcal{H} \):

\[
\text{Adv}_{\mathcal{C}S}^{\text{IND−CCA}}(t) \leq 2 \times \text{Adv}_{\mathcal{C}S}^{\text{ddh}}(t) + \text{Succ}^{\mathcal{H}}(t) + 3q_D / q
\]

Let us prove this theorem, with a sequence of games, in which \( A \) is an IND−CCA adversary against the Cramer-Shoup encryption scheme.

**Real Attack Game**

**Proof: Invalid ciphertexts**

- **Game_0**: use of the oracles \( \mathcal{K}, \mathcal{D} \)
- **Game_1**: we abort (with a random output \( b' \))

  in case of bad (invalid) accepted ciphertext,

  where invalid ciphertext means \( \log_{g_1} u_1 \neq \log_{g_2} u_2 \)

**Event F**

\( A \) submits a bad accepted ciphertext

(note: this is not computationally detectable)

The advantage in \( \text{Game}_1 \) is:

\[
\Pr_{\text{Game}_1}[b' = b | F] = 1/2
\]

\[
\Pr_{\text{Game}_0}[F] = \Pr_{\text{Game}_1}[F]
\]

\[
\Pr_{\text{Game}_1}[b' = b | \neg F] = \Pr_{\text{Game}_0}[b' = b | \neg F]
\]

\( \implies \text{Hop-S-Negl}: \text{Adv}_{\text{Game}_1} \geq \text{Adv}_{\text{Game}_0} - \text{Pr}[F] \)
### Proof: Simulations

**Game 2**: we use the simulations

**Key Generation Simulation**

$$x_1, x_2, y_1, y_2, z_1, z_2 \overset{R}{\leftarrow} \mathbb{Z}_q, g_1, g_2 \overset{R}{\leftarrow} \mathbb{G}: sk = (x_1, x_2, y_1, y_2, z_1, z_2)$$

$$c = g_1^{x_1} g_2^{x_2}, d = g_1^{y_1} g_2^{y_2}, \text{ and } h = g_1^{z_1} g_2^{z_2}: pk = (g_1, g_2, \mathcal{H}, c, d, h)$$

**Decryption Simulation**

If $$v = u_1^{x_1 + \alpha y_1} u_2^{x_2 + \alpha y_2}$$ where $$\alpha = \mathcal{H}(u_1, u_2, e): m = e/u_1^{z_1} u_2^{z_2}$$

Under the assumption of $$\neg F$$, perfect simulation

$$\Rightarrow \text{Hop-S-Perfect: } \text{Adv}_{\text{Game}_2} = \text{Adv}_{\text{Game}_1}$$

### Details: Shoup’s Lemma

Let us move to the exponents, in basis $$g_1$$, with $$g_2 = g_1^s$$:

$$\log c = x_1 + sx_2$$

$$\log d = y_1 + sy_2$$

$$\log v = r_1(x_1 + \alpha y_1) + sr_2(x_2 + \alpha y_2)$$

The system is under-defined: for any $$v$$, there are $$(x_1, x_2, y_1, y_2)$$ that satisfy the system $$\Rightarrow v$$ is unpredictable

$$\Rightarrow \Pr[F] \leq q_d/q \quad \Rightarrow \text{Adv}_{\text{Game}_1} \geq \text{Adv}_{\text{Game}_0} - q_d/q$$

### Details: Bad Accept

In order to evaluate $$\Pr[F]$$, we study the probability that

- $$r_1 = \log_{g_1} u_1 \neq \log_{g_2} u_2 = r_2$$,
- whereas $$v = u_1^{x_1 + \alpha y_1} u_2^{x_2 + \alpha y_2}$$

The adversary just knows the public key:

$$c = g_1^{x_1} g_2^{x_2}, d = g_1^{y_1} g_2^{y_2}$$

Let us move to the exponents, in basis $$g_1$$, with $$g_2 = g_1^s$$:

$$\log c = x_1 + sx_2$$

$$\log d = y_1 + sy_2$$

$$\log v = r_1(x_1 + \alpha y_1) + sr_2(x_2 + \alpha y_2)$$

The system is under-defined: for any $$v$$, there are $$(x_1, x_2, y_1, y_2)$$ that satisfy the system $$\Rightarrow v$$ is unpredictable

$$\Rightarrow \Pr[F] \leq q_d/q \quad \Rightarrow \text{Adv}_{\text{Game}_1} \geq \text{Adv}_{\text{Game}_0} - q_d/q$$

### Proof: Computable Adversary

- **Game 3**: we do no longer exclude bad accepted ciphertexts

  $$\Rightarrow \text{Hop-S-Negl!}$$

- **Game 3**: we do no longer exclude bad accepted ciphertexts

  $$\Rightarrow \text{Hop-S-Perfect: } \text{Adv}_{\text{Game}_3} \geq \text{Adv}_{\text{Game}_2} - \Pr[F] \geq \text{Adv}_{\text{Game}_2} - q_d/q$$

  This is technical: to make the simulator/adversary computable
Proof: DDH Assumption

- **Game**₄: we modify the generation of the challenge ciphertext:

  **Original Challenge**
  
  Random choice: \( b \overset{R}{\leftarrow} \{0, 1\} \), \( r \overset{R}{\leftarrow} \mathbb{Z}_q \) \[\alpha = \mathcal{H}(u_1, u_2, e)\]
  
  \( u_1 = g_{1}^{r}, \ u_2 = g_{2}^{r}, \ e = m_b \times h^r, \ v = c^d f^\alpha \)

  **New Challenge 1**
  
  Given \((U = g_{1}^{r}, V = g_{2}^{r})\) from outside, and random choice \( b \overset{R}{\leftarrow} \{0, 1\} \)
  
  \( u_1 = U, \ u_2 = V, \ e = m_b \times U^{z_1} V^{z_2}, \ v = U^{x_1 + \alpha y_1} V^{x_2 + \alpha y_2} \)

  With \((U = g_{1}^{r}, V = g_{2}^{r})\): \( U^{z_1} V^{z_2} = h^r \) and \( U^{x_1 + \alpha y_1} V^{x_2 + \alpha y_2} = c^d f^\alpha \)
  
  \(\implies\) **Hop-S-Perfect**: \( \text{Adv}_{\text{Game}_4} = \text{Adv}_{\text{Game}_3} \)

Proof: DDH Assumption

- **Game**₅: we modify the generation of the challenge ciphertext:

  **Previous Challenge 1**
  
  Given \((U = g_{1}^{r}, V = g_{2}^{r})\) from outside, and random choice \( b \overset{R}{\leftarrow} \{0, 1\} \)
  
  \( u_1 = U, \ u_2 = V, \ e = m_b \times U^{z_1} V^{z_2}, \ v = U^{x_1 + \alpha y_1} V^{x_2 + \alpha y_2} \)

The input from outside changes from \((U = g_{1}^{r}, V = g_{2}^{r})\) (a CDH tuple) to \((U = g_{1}^{r}, V = g_{2}^{r})\) (a random tuple):

\[
\Pr_{\text{Game}_4}[b' = b] - \Pr_{\text{Game}_5}[b' = b] \leq \text{Adv}^{ddh}_{G}(t)
\]

\(\implies\) **Hop-D-Comp**: \( \text{Adv}_{\text{Game}_5} \geq \text{Adv}_{\text{Game}_4} - 2 \times \text{Adv}^{ddh}_{G}(t) \)

(Since \( \text{Adv} = 2 \times \Pr[b' = b] - 1 \))

Proof: Collision

- **Game**₆: we abort (with a random output \( b' \)) in case of second pre-image with a decryption query

  \( \mathcal{A} \) submits a ciphertext with the same \( \alpha \) as the challenge ciphertext, but a different initial triple: \((u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)\), but \( \alpha = \alpha^* \), were \( ^* \) are for all the elements related to the challenge ciphertext

**Event \( F_H \)**

Second pre-image of \( \mathcal{H} \):

\[
\implies \Pr[F_H] \leq \text{Succ}^H(t)
\]

The advantage in **Game**₆ is:

\[
\Pr_{\text{Game}_6}[b' = b | F_H] = 1/2
\]

\[
\Pr_{\text{Game}_6}[b' = b | \neg F_H] = \Pr_{\text{Game}_6}[b' = b | \neg F_H]
\]

\(\implies\) **Hop-S-Negl**: \( \text{Adv}_{\text{Game}_6} \geq \text{Adv}_{\text{Game}_5} - \Pr[F_H] \)

\[
\text{Adv}_{\text{Game}_6} \geq \text{Adv}_{\text{Game}_5} - \text{Succ}^H(t)
\]
Proof: Invalid ciphertexts

- **Game**\(_7\): we abort (with a random output \(b'\)) in case of bad accepted ciphertext, we do as in **Game**\(_1\)

Details: Bad Accept

- **Event** \(F'\)

\\(\mathcal{A}\) submits a bad accepted ciphertext (note: this is not computationally detectable)

The advantage in **Game**\(_7\) is: \(\Pr_{\text{Game}_7}[b' = b|F'] = 1/2\)

\[
\Pr_{\text{Game}_6}[F'] = \Pr_{\text{Game}_7}[F'] - \Pr_{\text{Game}_6}[b' = b|\neg F'] \Rightarrow \text{Hop-S-Negl: } Adv_{\text{Game}_7} \geq Adv_{\text{Game}_6} - \Pr[F']
\]

Details: Bad Accept (Case 3)

The adversary knows the public key, and the (invalid) challenge ciphertext:

\[
c = g_1^{x_1} g_2^{x_2} \quad d = g_1^{y_1} g_2^{y_2}
\]

\[
v^* = U^{x_1 + y_1} v^{x_2 + y_2} = g_1^{r_1^*(x_1 + y_1)} g_2^{r_2^*(x_2 + y_2)}
\]

Let us move to the exponents, in basis \(g_1\), with \(g_2 = g_1^s\):

\[
\log c = x_1 + sx_2
\]

\[
\log d = y_1 + sy_2
\]

\[
\log v^* = r_1^*(x_1 + y_1) + sr_2^*(x_2 + y_2)
\]

\[
\log v = r_1(x_1 + y_1) + sr_2(x_2 + y_2)
\]

Details: Bad Accept (Case 3)

In order to evaluate \(\Pr[F']\), we study the probability that

- \(r_1 = \log g_1, u_1 \neq \log g_2, u_2 = r_2,\)
- whereas \(v = u_1^{x_1 + y_1} u_2^{x_2 + y_2}\)

Let us use \(**\) for all the elements related to the challenge ciphertext:

Three cases may appear:

- **Case 1**: \((u_1, u_2, e) = (u_1^*, u_2^*, e^*), \) then necessarily

\[
v^* = U^{x_1 + y_1} v^{x_2 + y_2} = u_1^{x_1 + y_1} u_2^{x_2 + y_2}
\]

Then, the ciphertext is rejected

\[
\Rightarrow \Pr[F'_1] = 0
\]

- **Case 2**: \((u_1, u_2, e) \neq (u_1^*, u_2^*, e^*)\), but \(\alpha = \alpha^*\): From the previous game, Aborts

\[
\Rightarrow \Pr[F'_2] = 0
\]

- **Case 3**: \((u_1, u_2, e) \neq (u_1^*, u_2^*, e^*), \) and \(\alpha \neq \alpha^*\)

The determinant of the system is

\[
\Delta = \begin{vmatrix}
1 & s & 0 & 0 \\
0 & 0 & 1 & s \\
r_1^* & sr_2^* & r_1^* \alpha^* & sr_2^* \alpha^* \\
r_1 & sr_2 & r_1 \alpha & sr_2 \alpha \\
\end{vmatrix}
\]

\[
= s^2 \times ((r_2 - r_1) \times (r_2^* - r_1^*) \times \alpha^* - (r_2^* - r_1^*) \times (r_2 - r_1) \times \alpha)
\]

\[
= s^2 \times (r_2 - r_1) \times (r_2^* - r_1^*) \times (\alpha^* - \alpha)
\]

\[
\neq 0
\]

The system is under-defined: for any \(v\), there are \((x_1, x_2, y_1, y_2)\) that satisfy the system

\[
\Rightarrow \nu \text{ is unpredictable} \quad \Rightarrow \Pr[F'_3] \leq q_D/q
\]

\[
\Rightarrow Adv_{\text{Game}_7} \geq Adv_{\text{Game}_6} - q_D/q
\]
Proof: Analysis of the Final Game

In the final Game$_7$:
- only valid ciphertexts are decrypted
- the challenge ciphertext contains
  \[ e = m_b \times U^{z_1} V^{z_2} \]
- the public key contains
  \[ h = g_1^{z_1} g_2^{z_2} \]

Again, the system is under-defined:
for any $m_b$, there are $(z_1, z_2)$ that satisfy the system
\[ \implies m_b \text{ is unpredictable} \quad \implies b \text{ is unpredictable} \]
\[ \implies \text{Adv}_{\text{Game}_7} = 0 \]

\[
\begin{align*}
\text{Adv}_{\text{Game}_7} &= 0 \\
\text{Adv}_{\text{Game}_7} &\geq \text{Adv}_{\text{Game}_6} - \frac{q_D}{q} \\
\text{Adv}_{\text{Game}_6} &\geq \text{Adv}_{\text{Game}_5} - \text{Succ}^H(t) \\
\text{Adv}_{\text{Game}_5} &\geq \text{Adv}_{\text{Game}_4} - 2 \times \text{Adv}_{\text{ddh}}^G(t) \\
\text{Adv}_{\text{Game}_4} &= \text{Adv}_{\text{Game}_3} \\
\text{Adv}_{\text{Game}_3} &\geq \text{Adv}_{\text{Game}_2} - \frac{q_D}{q} \\
\text{Adv}_{\text{Game}_2} &= \text{Adv}_{\text{Game}_1} \\
\text{Adv}_{\text{Game}_1} &\geq \text{Adv}_{\text{Game}_0} - \frac{q_D}{q} \\
\text{Adv}_{\text{Game}_0} &= \text{Adv}_{\text{ind–cca}}^G (\mathcal{A}) \\
\text{Adv}_{\text{ind–cca}}^G (\mathcal{A}) &\leq 2 \times \text{Adv}_{\text{ddh}}^G(t) + \text{Succ}^H(t) + 3\frac{q_D}{q}
\end{align*}
\]

Conclusion

Game-based Methodology: the story of OAEP

[Bellare-Rogaway EC ’94]

- Reduction proven indistinguishable for an IND-CCA adversary
  (actually IND-CCA1, and not IND-CCA2) but widely believed for
  IND-CCA2, without any further analysis of the reduction
  The direct-reduction methodology

[Shoup - Crypto ’01]

Shoup showed the gap for IND-CCA2, under the OWP
Granted his new game-based methodology

[Fujisaki-Okamoto-Pointcheval-Stern – Crypto ’01]

FOPS proved the security for IND-CCA2, under the PD-OWP
Using the game-based methodology

Outline

1. Game-based Proofs
   - Provable Security
   - Game-based Approach
   - Transition Hops

2. Advanced Security for Encryption
   - Advanced Security Notions
   - Cramer-Shoup Encryption Scheme

3. Conclusion