A Cleaner View on IND-CCA1 Secure Homomorphic Encryption using SOAP

F. Armknecht\textsuperscript{1}  \hspace{1cm} \textbf{Andreas Peter}\textsuperscript{2}  \hspace{1cm} S. Katzenbeisser\textsuperscript{2}

\textsuperscript{1}Universität Mannheim, Germany

\textsuperscript{2}Technische Universität Darmstadt, Germany

Summer School on Applied Cryptographic Protocols, 2010
Homomorphic Encryption Scheme $\mathcal{E}$

- $\mathcal{E} = (G, E, D)$ public-key encryption scheme
- three groups: plaintexts $\mathcal{P}$, ciphertexts $\overline{\mathcal{C}}$
  
  subgroup of all encryptions $\mathcal{C} := \{ E_{pk}(m) \mid m \in \mathcal{P} \} \leq \overline{\mathcal{C}}$
- restricted decryption $D_{sk}|_\mathcal{C}$ is a group epimorphism

We can formulate an abstract subgroup membership problem (SMP) for $(\mathcal{C}, \mathcal{C}_0)$ whose hardness is equivalent to the IND-CPA security of $\mathcal{E}$ (where $\mathcal{C}_0 := \{ E_{pk}(0) \}$)

No such scheme can be secure in terms of IND-CCA2!

Therefore, IND-CCA1 is the strongest security notion for homomorphic schemes.
Homomorphic Encryption Scheme $\mathcal{E}$

- $\mathcal{E} = (G, E, D)$ public-key encryption scheme
- three groups: plaintexts $\mathcal{P}$, ciphertexts $\overline{\mathcal{C}}$
  
  subgroup of all encryptions $\mathcal{C} := \{ E_{pk}(m) \mid m \in \mathcal{P} \} \leq \overline{\mathcal{C}}$

- restricted decryption $D_{sk}|_{\mathcal{C}}$ is a group epimorphism

We can formulate an abstract subgroup membership problem (SMP) for $(\mathcal{C}, \mathcal{C}_0)$ whose hardness is equivalent to the IND-CPA security of $\mathcal{E}$ (where $\mathcal{C}_0 := \{ E_{pk}(0) \}$).

No such scheme can be secure in terms of IND-CCA2!

Therefore, IND-CCA1 is the strongest security notion for homomorphic schemes.
Homomorphic Encryption Scheme $\mathcal{E}$

- $\mathcal{E} = (G, E, D)$ public-key encryption scheme
- three groups: plaintexts $\mathcal{P}$, ciphertexts $\overline{\mathcal{C}}$
  
  subgroup of all encryptions $\mathcal{C} := \{ E_{pk}(m) \mid m \in \mathcal{P} \} \leq \overline{\mathcal{C}}$

- restricted decryption $D_{sk}|_{\mathcal{C}}$ is a group epimorphism

We can formulate an abstract \textit{subgroup membership problem} (SMP) for $(\mathcal{C}, \mathcal{C}_0)$ whose hardness is \textit{equivalent} to the IND-CPA security of $\mathcal{E}$ (where $\mathcal{C}_0 := \{ E_{pk}(0) \}$)!

\textbf{No} such scheme can be secure in terms of IND-CCA2!

Therefore, IND-CCA1 is the \textit{strongest} security notion for homomorphic schemes.
Homomorphic Encryption Scheme $\mathcal{E}$

- $\mathcal{E} = (G, E, D)$ public-key encryption scheme
- three groups: plaintexts $\mathcal{P}$, ciphertexts $\overline{\mathcal{C}}$
  
  subgroup of all encryptions $\mathcal{C} := \{ E_{pk}(m) \mid m \in \mathcal{P} \} \leq \overline{\mathcal{C}}$

- restricted decryption $D_{sk}|_{\mathcal{C}}$ is a group epimorphism

We can formulate an abstract subgroup membership problem (SMP) for $(\mathcal{C}, \mathcal{C}_0)$ whose hardness is equivalent to the IND-CPA security of $\mathcal{E}$ (where $\mathcal{C}_0 := \{ E_{pk}(0) \}$)

No such scheme can be secure in terms of IND-CCA2!

Therefore, IND-CCA1 is the strongest security notion for homomorphic schemes.
Homomorphic Encryption Scheme $\mathcal{E}$

- $\mathcal{E} = (G, E, D)$ public-key encryption scheme
- three groups: plaintexts $\mathcal{P}$, ciphertexts $\overline{\mathcal{C}}$
  - subgroup of all encryptions $\mathcal{C} := \{ E_{pk}(m) \mid m \in \mathcal{P} \} \leq \overline{\mathcal{C}}$
- restricted decryption $D_{sk}\mathcal{C}$ is a group epimorphism

We consider the following large subclass:

- $sk$ contains an efficient decision function $\delta : \overline{\mathcal{C}} \rightarrow \{0, 1\}$
  - with $\delta(c) = 1 \iff c \in \mathcal{C}$
- decryption on $\overline{\mathcal{C}} \setminus \mathcal{C}$ returns the symbol $\bot$.

Almost all currently known homomorphic schemes fall into this subclass, e.g. ElGamal, Paillier, Goldwasser-Micali, Damgård’s ElGamal ...
Homomorphic Encryption Scheme $\mathcal{E}$

- $\mathcal{E} = (G, E, D)$ public-key encryption scheme
- three groups: plaintexts $\mathcal{P}$, ciphertexts $\mathcal{C}$
  - subgroup of all encryptions $\mathcal{C} := \{ E_{pk}(m) \mid m \in \mathcal{P} \} \leq \mathcal{C}$
- restricted decryption $D_{sk}|_{\mathcal{C}}$ is a group epimorphism

We consider the following large subclass:

- $sk$ contains an efficient decision function $\delta : \mathcal{C} \to \{0, 1\}$
  - with $\delta(c) = 1 \iff c \in \mathcal{C}$
- decryption on $\mathcal{C} \setminus \mathcal{C}$ returns the symbol $\perp$.

Almost all currently known homomorphic schemes fall into this subclass, e.g. ElGamal, Paillier, Goldwasser-Micali, Damgård’s ElGamal ...
An Abstract Scheme and its Security

- We introduce an abstract homomorphic scheme that is in fact a representative of the whole subclass we’ve just defined, i.e. every scheme can be written as an instantiation of this abstract scheme.

- This abstract representative allows for defining an abstract problem that we call the *Splitting Oracle-Assisted Subgroup Membership Problem* (SOAP) whose hardness is equivalent to the IND-CCA1 security of the abstract scheme.

In total:

\[ E \text{ is IND-CPA secure } \iff \text{ SMP is hard} \]
\[ E \text{ is IND-CCA1 secure } \iff \text{ SOAP is hard} \]
The construction of new IND-CPA (resp. IND-CCA1) secure homomorphic schemes amounts to finding hard instantiations of SMP (resp. SOAP) (later).

Conversely, existing homomorphic schemes can easily be proven IND-CPA (resp. IND-CCA1) secure by analyzing the corresponding SMP (resp. SOAP). For instance, we can positively answer the open question whether Paillier is IND-CCA1 secure.
Impossibility Results

It is possible to derive impossibility results for IND-CPA secure homomorphic schemes:

- the ciphertext group is not allowed to be of prime order.
- The ciphertext group is not allowed to be a linear code. This partly answers an open question whether using linear codes as ciphertext spaces yield more efficient constructions.
New Homomorphic Scheme I

Property of $k$-linear problem in the generic group model:
If $k$-linear problem is easy, $(k + 1)$-linear problem is still hard.

We introduce a new $k$-problem, called $k$-SOAP with the same progressive property.

The new scheme is the first that is
- IND-CPA secure $\iff$ $k$-linear problem is hard
- IND-CCA1 secure $\iff$ $k$-SOAP is hard

This answers Hofheinz, Kiltz and Shacham’s open challenge for homomorphic schemes!
New Homomorphic Scheme II

- “If there exist IND-CPA secure homomorphic schemes with cyclic ciphertext group, then we can efficiently construct IND-CCA2 secure encryption schemes” [HO10]

- The existence of such homomorphic schemes is an open question!

- We construct such a scheme whose IND-CPA security is equivalent to a new problem whose hardness is equivalent to the well-analyzed SMP of the GBD-scheme [GBD01]
Future Work

Interesting future work includes

- extension to an even broader class of homomorphic schemes
- extension to the fully homomorphic case
- extension to non-standard security notions, e.g. homomorphic-CCA
- ...

...
Thank you!
Feedback is very welcome!