NP-Completeness and Public Key Cryptosystem Antibes Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.

< ロ > < 同 > < E > < E > < E > の Q @

• Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

NP-Completeness and Public Key Cryptosystem Bergen Theme

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

Who? Kilgore TroutFrom? Tralfamadorian Institute of Technology (TIT)When? January 31, 2006

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.

 Not every NP-Complete problem can be efficiently transformed into a cryptosystem.
Adi Shamir, On the Cryptocomplexity of Knapsack Systems, STOC, 1979.

NPC vs PKC
(Berkeley)

Kilgore Trout

Introduction (Berkeley theme) NPC vs PKC

NP-Completeness and Public Key Cryptosystem Berkeley Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

NPC vs PKC (Berkeley)

Kilgore Trout

Introduction (Berkeley theme) NPC vs PKC Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.

▲ロト ▲帰 ト ▲ヨト ▲ヨト 三三 - のへぐ

• Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

NP-Completeness and Public Key Cryptosystem Berlin Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

Kilgore Trout NPC vs PKC (Berlin) TIT

-2

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.
- Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

Adi Shamir, On the Cryptocomplexity of Knapsack Systems, STOC, 1979.

3

・ロン ・回 と ・ ヨ と ・ ヨ と …

NP-Completeness and Public Key Cryptosystem Boadilla Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

Kilgore Trout (TIT)

NPC vs PKC (Boadilla)

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.
- Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

NP-Completeness and Public Key Cryptosystem Copenhagen Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

Kilgore Trout NPC vs PKC (Copenhagen)

< ∃ >

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.
- Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

NP-Completeness and Public Key Cryptosystem Darmstadt Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

NPC vs PKC

Why NPC cannot be a building block for PKC.

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

• Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

NP-Completeness and Public Key Cryptosystem Dresden Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

Kilgore Trout NPC vs PKC (Dresden) TIT

-2

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.
- Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

Adi Shamir, On the Cryptocomplexity of Knapsack Systems, STOC, 1979.

3

・ロン ・回 と ・ ヨ と ・ ヨ と …

NP-Completeness and Public Key Cryptosystem Frankfurt Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

< ロ > < 同 > < E > < E > < E > の Q @

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

• Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

NPC vs PKC (Goettingen)

Kilgore Trout

Introduction (Goettingen theme) NPC vs PKC

NP-Completeness and Public Key Cryptosystem Goettingen Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

・ロト ・ 日 ・ ・ 日 ・ ・ 日 ・ ・ つ へ つ ・

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.
- Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

Adi Shamir, On the Cryptocomplexity of Knapsack Systems, STOC, 1979.

NPC vs PKC (Goettingen)

Kilgore Trout

Introduction (Goettingen theme) NPC vs PKC NPC vs PKC (Hannover)

Kilgore Trout

Introduction (Hannover theme) NPC vs PKC

NP-Completeness and Public Key Cryptosystem Hannover Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

NPC vs PKC (Hannover)

Kilgore Trout

Introduction (Hannover theme) NPC vs PKC

Why NPC cannot be a building block for PKC.

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.

▲ロト ▲帰 ト ▲ヨト ▲ヨト 三三 - のへぐ

• Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

NP-Completeness and Public Key Cryptosystem Ilmenau Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

Kilgore Trout NPC vs PKC (Ilmenau) TIT

-2

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.
- Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

Adi Shamir, On the Cryptocomplexity of Knapsack Systems, STOC, 1979.

3

・ロン ・回 と ・ ヨ と ・ ヨ と …

NP-Completeness and Public Key Cryptosystem JuanLesPins Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

NPC vs PKC (JuanLesPins) Introduction (JuanLesPins theme) NPC vs PKC

Why NPC cannot be a building block for PKC.

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.

< ロ > < 同 > < E > < E > < E > の Q @

• Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

NP-Completeness and Public Key Cryptosystem Luebeck Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

Kilgore Trout NPC vs PKC (Luebeck)

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.
- Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

NP-Completeness and Public Key Cryptosystem Madrid Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

Kilgore Trout (TIT)

NPC vs PKC (Madrid)

January 31, 2006 1 / 2

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.
- Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

NP-Completeness and Public Key Cryptosystem Malmoe Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.
- Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

NPC vs PKC (Marburg)

Kilgore Trout

ntroduction [Marburg theme] NPC vs PKC

NP-Completeness and Public Key Cryptosystem Marburg Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

ション ふゆ アメリア オリア しょうくしゃ

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.
- Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

Adi Shamir, On the Cryptocomplexity of Knapsack Systems, STOC, 1979.

NPC vs PKC (Marburg)

Kilgore Trout

Introduction (Marburg theme) NPC vs PKC

NP-Completeness and Public Key Cryptosystem Montpellier Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

▲□▶▲□▶▲□▶▲□▶ □ のQ@

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

• Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

NPC vs PKC (PaloAlto)

Kilgore Trout

Introduction (PaloAlto theme) NPC vs PKC

NP-Completeness and Public Key Cryptosystem PaloAlto Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

NPC vs PKC (PaloAlto)

Kilgore Trout

Introduction (PaloAlto theme) NPC vs PKC Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.

▲ロト ▲帰 ト ▲ヨト ▲ヨト 三三 - のへぐ

• Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

NP-Completeness and Public Key Cryptosystem Pittsburgh Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

▲□▶▲□▶▲□▶▲□▶ □ のQ@

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.

< □ > < 同 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

• Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

NP-Completeness and Public Key Cryptosystem Rochester Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

• Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

NP-Completeness and Public Key Cryptosystem Singapore Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

< □ > < 同 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.
- Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

Adi Shamir, On the Cryptocomplexity of Knapsack Systems, STOC, 1979.

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

NP-Completeness and Public Key Cryptosystem Szeged Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

NPC vs PKC (Szeged)

-

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.
- Not every NP-Complete problem can be efficiently transformed into a cryptosystem.

Adi Shamir, On the Cryptocomplexity of Knapsack Systems, STOC, 1979.

伺 と く ヨ と く ヨ と

NP-Completeness and Public Key Cryptosystem Warsaw Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006

Kilgore Trout NPC vs PKC (Warsaw)

Even though P \neq NP, NP-Completeness is *not* well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee worst-case complexity.
- NP-Completeness deals with a single isolated instance of a problem.
- Not every NP-Complete problem can be efficiently transformed into a cryptosystem.