NP-Completeness and Public Key Cryptosystem
Antibes Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
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
Bergen Theme

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

Berkeley Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
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

Berlin Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
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

Boadilla Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
Why NPC cannot be a building block for PKC.

Even though P ≠ 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
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
Darmstadt Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
Why NPC cannot be a building block for PKC.

Even though $P \neq NP$, NP-Completeness is \textit{not} well suited to Public Key Cryptosystem.

- NP-Completeness only guarantee \textit{worst-case} complexity.
- NP-Completeness deals with a \textit{single isolated instance} of a problem.
- \textbf{Not} every NP-Complete problem \textit{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
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.

Why NPC cannot be a building block for PKC.

Even though $P \neq NP$, NP-Completeness is \textit{not} well suited to Public Key Cryptosystem.

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

NP-Completeness and Public Key Cryptosystem

Goettingen Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
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
Hannover Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
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
Ilmenau Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
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
JuanLesPins Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
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

Luebeck Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
Introduction (Luebeck theme)

NPC vs PKC

Why NPC cannot be a building block for PKC.

Even though \( P \neq NP \), NP-Completeness is \textit{not} well suited to Public Key Cryptosystem.

- NP-Completeness only guarantees \textit{worst-case} complexity.
- NP-Completeness deals with a \textit{single isolated instance} of a problem.
- \textbf{Not} every NP-Complete problem \textit{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
Why NPC cannot be a building block for PKC.

Even though $P \neq NP$, NP-Completeness is \textit{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
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
Marburg Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
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
Montpellier Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
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

PaloAlto Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
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
Pittsburgh Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
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
Rochester Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
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
Singapore Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
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

Szeged Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
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
Warsaw Theme

Kilgore Trout

Tralfamadorian Institute of Technology (TIT)

January 31, 2006
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.