An Adaptation of the NICE Cryptosystem to Real Quadratic Orders

Renate Scheidler

Centre for Information Security and Cryptography

UNIVERSITY OF CALGARY

joint work with:

Mike Jacobson,University of Calgary
Daniel Weimer, Charles River Development

Research supported in part by NSERC.

AfricaCrypt 2008 — June 12, 2008

Overview

- NICE (New Ideal Coset Encryption) is a public-key cryptosystem whose security is based on factoring $q^2 p$ (p, q distinct primes).
- Quadratic decryption time, allowing for fast signature generation.
- Makes use of the relationship between ideals in a non-maximal and the maximal order of a quadratic number field.
  - Original NICE: imaginary quadratic orders (Takagi & Paulus, J. Cryptology **13**, 2000).
  - REAL-NICE: adaptation to real quadratic orders.

Outline

- Mathematical Preliminaries (don't let them scare you!)
- Original NICE
- REAL-NICE
- Our Findings

Overview

- NICE (New Ideal Coset Encryption) is a public-key cryptosystem whose security is based on factoring q^2p (p, q distinct primes).
- Quadratic decryption time, allowing for fast signature generation.
- Makes use of the relationship between ideals in a non-maximal and the maximal order of a quadratic number field.
  - Original NICE: imaginary quadratic orders (Takagi & Paulus, J. Cryptology **13**, 2000).
  - REAL-NICE: adaptation to real quadratic orders.

Outline

- Mathematical Preliminaries (don't let them scare you!)
- Original NICE
- REAL-NICE
- Our Findings

Overview

- NICE (New Ideal Coset Encryption) is a public-key cryptosystem whose security is based on factoring $q^2 p$ (p, q distinct primes).
- Quadratic decryption time, allowing for fast signature generation.
- Makes use of the relationship between ideals in a non-maximal and the maximal order of a quadratic number field.
  - Original NICE: imaginary quadratic orders (Takagi & Paulus, J. Cryptology **13**, 2000).
  - REAL-NICE: adaptation to real quadratic orders.

Outline

- Mathematical Preliminaries (don't let them scare you!)
- Original NICE
- REAL-NICE
- Our Findings

Overview

- NICE (New Ideal Coset Encryption) is a public-key cryptosystem whose security is based on factoring q^2p (p, q distinct primes).
- Quadratic decryption time, allowing for fast signature generation.
- Makes use of the relationship between ideals in a non-maximal and the maximal order of a quadratic number field.
  - Original NICE: imaginary quadratic orders (Takagi & Paulus, J. Cryptology **13**, 2000).
  - REAL-NICE: adaptation to real quadratic orders.

Outline

- Mathematical Preliminaries (don't let them scare you!)
- Original NICE
- REAL-NICE
- Our Findings

Overview

- NICE (New Ideal Coset Encryption) is a public-key cryptosystem whose security is based on factoring $q^2 p$ (p, q distinct primes).
- Quadratic decryption time, allowing for fast signature generation.
- Makes use of the relationship between ideals in a non-maximal and the maximal order of a quadratic number field.
  - Original NICE: imaginary quadratic orders (Takagi & Paulus, J. Cryptology **13**, 2000).
  - REAL-NICE: adaptation to real quadratic orders.

Outline

- Mathematical Preliminaries (don't let them scare you!)
- Original NICE
- REAL-NICE
- Our Findings

Quadratic Orders and Ideals

$\Delta_1 \in \mathbb{Z}$ with $\Delta_1 \equiv 1 \pmod 4$, $\qquad \Delta_f = f^2\Delta_1$ with $f \in \mathbb{Z}$

Quadratic order of **conductor** f: $\mathcal{O}_{\Delta_f} = \mathbb{Z} \oplus \mathbb{Z}\, f\, \dfrac{\Delta_1 + \sqrt{\Delta_1}}{2}$

Properties:

- $\mathcal{O}_{\Delta_f}$ is **imaginary** if $\Delta_f < 0$ and **real** if $\Delta_f > 0$
- $\mathcal{O}_{\Delta_f} \subseteq \mathcal{O}_{\Delta_1}$; $\mathcal{O}_{\Delta_1}$ is the **maximal** order

An $\mathcal{O}_{\Delta_f}$-**ideal** is a subset $\mathfrak{a} = (N, B)$ of $\mathcal{O}_{\Delta_f}$ characterized by two integers $N = N(\mathfrak{a})$ (the **norm** of $\mathfrak{a}$) and $B = B(\mathfrak{a})$ such that

- $N > 0$ is unique, B is unique modulo $2N$
- $B^2 \equiv \Delta_f \pmod{4N}$
- $\gcd(N, B, (\Delta_f - B^2)/4N) = 1$

An $\mathcal{O}_{\Delta_f}$-ideal $\mathfrak{a}$ with $N(\mathfrak{a}) < \sqrt{|\Delta_f|}/2$ is **reduced**

Quadratic Orders and Ideals

$\Delta_1 \in \mathbb{Z}$ with $\Delta_1 \equiv 1 \pmod 4$, $\qquad \Delta_f = f^2\Delta_1$ with $f \in \mathbb{Z}$

Quadratic order of **conductor** f: $\mathcal{O}_{\Delta_f} = \mathbb{Z} \oplus \mathbb{Z}\, f\, \dfrac{\Delta_1 + \sqrt{\Delta_1}}{2}$

Properties:

- $\mathcal{O}_{\Delta_f}$ is **imaginary** if $\Delta_f < 0$ and **real** if $\Delta_f > 0$
- $\mathcal{O}_{\Delta_f} \subseteq \mathcal{O}_{\Delta_1}$; $\mathcal{O}_{\Delta_1}$ is the **maximal** order

An $\mathcal{O}_{\Delta_f}$-**ideal** is a subset $\mathfrak{a} = (N, B)$ of $\mathcal{O}_{\Delta_f}$ characterized by two integers $N = N(\mathfrak{a})$ (the **norm** of $\mathfrak{a}$) and $B = B(\mathfrak{a})$ such that

- $N > 0$ is unique, B is unique modulo $2N$
- $B^2 \equiv \Delta_f \pmod{4N}$
- $\gcd(N, B, (\Delta_f - B^2)/4N) = 1$

An $\mathcal{O}_{\Delta_f}$-ideal $\mathfrak{a}$ with $N(\mathfrak{a}) < \sqrt{|\Delta_f|}/2$ is **reduced**

Quadratic Orders and Ideals

$\Delta_1 \in \mathbb{Z}$ with $\Delta_1 \equiv 1 \pmod 4$, $\quad \Delta_f = f^2\Delta_1$ with $f \in \mathbb{Z}$

Quadratic order of **conductor** f: $\mathcal{O}_{\Delta_f} = \mathbb{Z} \oplus \mathbb{Z} f \frac{\Delta_1 + \sqrt{\Delta_1}}{2}$

Properties:

- $\mathcal{O}_{\Delta_f}$ is **imaginary** if $\Delta_f < 0$ and **real** if $\Delta_f > 0$
- $\mathcal{O}_{\Delta_f} \subseteq \mathcal{O}_{\Delta_1}$; $\mathcal{O}_{\Delta_1}$ is the **maximal** order

An $\mathcal{O}_{\Delta_f}$**-ideal** is a subset $\mathfrak{a} = (N, B)$ of $\mathcal{O}_{\Delta_f}$ characterized by two integers $N = N(\mathfrak{a})$ (the **norm** of $\mathfrak{a}$) and $B = B(\mathfrak{a})$ such that

- $N > 0$ is unique, B is unique modulo $2N$
- $B^2 \equiv \Delta_f \pmod{4N}$
- $\gcd(N, B, (\Delta_f - B^2)/4N) = 1$

An $\mathcal{O}_{\Delta_f}$-ideal $\mathfrak{a}$ with $N(\mathfrak{a}) < \sqrt{|\Delta_f|}/2$ is **reduced**

Quadratic Orders and Ideals

$\Delta_1 \in \mathbb{Z}$ with $\Delta_1 \equiv 1 \pmod 4$, $\quad \Delta_f = f^2\Delta_1$ with $f \in \mathbb{Z}$

Quadratic order of **conductor** f: $\mathcal{O}_{\Delta_f} = \mathbb{Z} \oplus \mathbb{Z}\, f\, \dfrac{\Delta_1 + \sqrt{\Delta_1}}{2}$

Properties:

- $\mathcal{O}_{\Delta_f}$ is **imaginary** if $\Delta_f < 0$ and **real** if $\Delta_f > 0$
- $\mathcal{O}_{\Delta_f} \subseteq \mathcal{O}_{\Delta_1}$; $\mathcal{O}_{\Delta_1}$ is the **maximal** order

An $\mathcal{O}_{\Delta_f}$-**ideal** is a subset $\mathfrak{a} = (N, B)$ of $\mathcal{O}_{\Delta_f}$ characterized by two integers $N = N(\mathfrak{a})$ (the **norm** of $\mathfrak{a}$) and $B = B(\mathfrak{a})$ such that

- $N > 0$ is unique, B is unique modulo $2N$
- $B^2 \equiv \Delta_f \pmod{4N}$
- $\gcd(N, B, (\Delta_f - B^2)/4N) = 1$

An $\mathcal{O}_{\Delta_f}$-ideal $\mathfrak{a}$ with $N(\mathfrak{a}) < \sqrt{|\Delta_f|}/2$ is **reduced**

Quadratic Orders and Ideals

$\Delta_1 \in \mathbb{Z}$ with $\Delta_1 \equiv 1 \pmod 4$, $\quad \Delta_f = f^2\Delta_1$ with $f \in \mathbb{Z}$

Quadratic order of **conductor** f: $\mathcal{O}_{\Delta_f} = \mathbb{Z} \oplus \mathbb{Z} f \dfrac{\Delta_1 + \sqrt{\Delta_1}}{2}$

Properties:

- $\mathcal{O}_{\Delta_f}$ is **imaginary** if $\Delta_f < 0$ and **real** if $\Delta_f > 0$
- $\mathcal{O}_{\Delta_f} \subseteq \mathcal{O}_{\Delta_1}$; $\mathcal{O}_{\Delta_1}$ is the **maximal** order

An $\mathcal{O}_{\Delta_f}$**-ideal** is a subset $\mathfrak{a} = (N, B)$ of $\mathcal{O}_{\Delta_f}$ characterized by two integers $N = N(\mathfrak{a})$ (the **norm** of $\mathfrak{a}$) and $B = B(\mathfrak{a})$ such that

- $N > 0$ is unique, B is unique modulo $2N$
- $B^2 \equiv \Delta_f \pmod{4N}$
- $\gcd(N, B, (\Delta_f - B^2)/4N) = 1$

An $\mathcal{O}_{\Delta_f}$-ideal $\mathfrak{a}$ with $N(\mathfrak{a}) < \sqrt{|\Delta_f|}/2$ is **reduced**

Quadratic Orders and Ideals

$\Delta_1 \in \mathbb{Z}$ with $\Delta_1 \equiv 1 \pmod 4$, $\quad \Delta_f = f^2 \Delta_1$ with $f \in \mathbb{Z}$

Quadratic order of **conductor** f: $\mathcal{O}_{\Delta_f} = \mathbb{Z} \oplus \mathbb{Z} f \dfrac{\Delta_1 + \sqrt{\Delta_1}}{2}$

Properties:

- $\mathcal{O}_{\Delta_f}$ is **imaginary** if $\Delta_f < 0$ and **real** if $\Delta_f > 0$
- $\mathcal{O}_{\Delta_f} \subseteq \mathcal{O}_{\Delta_1}$; $\mathcal{O}_{\Delta_1}$ is the **maximal** order

An $\mathcal{O}_{\Delta_f}$**-ideal** is a subset $\mathfrak{a} = (N, B)$ of $\mathcal{O}_{\Delta_f}$ characterized by two integers $N = N(\mathfrak{a})$ (the **norm** of $\mathfrak{a}$) and $B = B(\mathfrak{a})$ such that

- $N > 0$ is unique, B is unique modulo $2N$
- $B^2 \equiv \Delta_f \pmod{4N}$
- $\gcd(N, B, (\Delta_f - B^2)/4N) = 1$

An $\mathcal{O}_{\Delta_f}$-ideal $\mathfrak{a}$ with $N(\mathfrak{a}) < \sqrt{|\Delta_f|}/2$ is **reduced**

Ideal Equivalence

Ideal Equivalence: $\mathfrak{a} \sim \mathfrak{b} \iff \alpha\mathfrak{a} = \beta\mathfrak{b}$ for some $\alpha, \beta \in \mathcal{O}_{\Delta_f} \setminus \{0\}$

Ideal class group of $\mathcal{O}_{\Delta_f}$: $Cl(\mathcal{O}_{\Delta_f}) = \{\text{set of equivalence classes}\}$

Properties:

- Finite Abelian group;
- The identity is the **principal class** containing $\mathcal{O}_{\Delta_f}$;
- Efficient arithmetic;
- Given any $\mathcal{O}_{\Delta_f}$-ideal $\mathfrak{a}$, it is efficient to compute a reduced ideal $\rho_{\Delta_f}(\mathfrak{a}) \sim \mathfrak{a}$;
- If N is an upper bound on the number of reduced ideals in each ideal class, then $N \cdot \#Cl(\mathcal{O}_{\Delta_f}) \approx \sqrt{|\Delta_f|}$
- If $\mathcal{O}_{\Delta_f}$ is imaginary, then $N = 1$ and $\#Cl(\mathcal{O}_{\Delta_f}) \approx \sqrt{|\Delta_f|}$;
- If $\mathcal{O}_{\Delta_f}$ is real, then
  - usually $Cl(\mathcal{O}_{\Delta_f})$ is very small and $N \approx \sqrt{\Delta_f}$;
  - for certain very special choices of Δ_1, we have N small and $\#Cl(\mathcal{O}_{\Delta_1})$ small.

Ideal Equivalence

Ideal Equivalence: $\mathfrak{a} \sim \mathfrak{b} \iff \alpha\mathfrak{a} = \beta\mathfrak{b}$ for some $\alpha, \beta \in \mathcal{O}_{\Delta_f} \setminus \{0\}$

Ideal class group of $\mathcal{O}_{\Delta_f}$: $Cl(\mathcal{O}_{\Delta_f}) = \{\text{set of equivalence classes}\}$

Properties:

- Finite Abelian group;
- The identity is the **principal class** containing $\mathcal{O}_{\Delta_f}$;
- Efficient arithmetic;
- Given any $\mathcal{O}_{\Delta_f}$-ideal $\mathfrak{a}$, it is efficient to compute a reduced ideal $\rho_{\Delta_f}(\mathfrak{a}) \sim \mathfrak{a}$;
- If N is an upper bound on the number of reduced ideals in each ideal class, then $N \cdot \#Cl(\mathcal{O}_{\Delta_f}) \approx \sqrt{|\Delta_f|}$
- If $\mathcal{O}_{\Delta_f}$ is imaginary, then $N = 1$ and $\#Cl(\mathcal{O}_{\Delta_f}) \approx \sqrt{|\Delta_f|}$;
- If $\mathcal{O}_{\Delta_f}$ is real, then
  - usually $Cl(\mathcal{O}_{\Delta_f})$ is very small and $N \approx \sqrt{\Delta_f}$;
  - for certain very special choices of Δ_1, we have N small and $\#Cl(\mathcal{O}_{\Delta_1})$ small.

Ideal Equivalence

Ideal Equivalence: $\mathfrak{a} \sim \mathfrak{b} \iff \alpha\mathfrak{a} = \beta\mathfrak{b}$ for some $\alpha, \beta \in \mathcal{O}_{\Delta_f} \setminus \{0\}$

Ideal class group of $\mathcal{O}_{\Delta_f}$: $Cl(\mathcal{O}_{\Delta_f}) = \{\text{set of equivalence classes}\}$

Properties:

- Finite Abelian group;
- The identity is the **principal class** containing $\mathcal{O}_{\Delta_f}$;
- Efficient arithmetic;
- Given any $\mathcal{O}_{\Delta_f}$-ideal $\mathfrak{a}$, it is efficient to compute a reduced ideal $\rho_{\Delta_f}(\mathfrak{a}) \sim \mathfrak{a}$;
- If N is an upper bound on the number of reduced ideals in each ideal class, then $N \cdot \#Cl(\mathcal{O}_{\Delta_f}) \approx \sqrt{|\Delta_f|}$
- If $\mathcal{O}_{\Delta_f}$ is imaginary, then $N = 1$ and $\#Cl(\mathcal{O}_{\Delta_f}) \approx \sqrt{|\Delta_f|}$;
- If $\mathcal{O}_{\Delta_f}$ is real, then
  - usually $Cl(\mathcal{O}_{\Delta_f})$ is very small and $N \approx \sqrt{\Delta_f}$;
  - for certain very special choices of Δ_1, we have N small and $\#Cl(\mathcal{O}_{\Delta_1})$ small.

Ideal Equivalence

Ideal Equivalence: $\mathfrak{a} \sim \mathfrak{b} \iff \alpha\mathfrak{a} = \beta\mathfrak{b}$ for some $\alpha, \beta \in \mathcal{O}_{\Delta_f} \setminus \{0\}$

Ideal class group of $\mathcal{O}_{\Delta_f}$: $Cl(\mathcal{O}_{\Delta_f}) = \{$set of equivalence classes$\}$

Properties:

- Finite Abelian group;
- The identity is the **principal class** containing $\mathcal{O}_{\Delta_f}$;
- Efficient arithmetic;
- Given any $\mathcal{O}_{\Delta_f}$-ideal $\mathfrak{a}$, it is efficient to compute a reduced ideal $\rho_{\Delta_f}(\mathfrak{a}) \sim \mathfrak{a}$;
- If N is an upper bound on the number of reduced ideals in each ideal class, then $N \cdot \#Cl(\mathcal{O}_{\Delta_f}) \approx \sqrt{|\Delta_f|}$
- If $\mathcal{O}_{\Delta_f}$ is imaginary, then $N = 1$ and $\#Cl(\mathcal{O}_{\Delta_f}) \approx \sqrt{|\Delta_f|}$;
- If $\mathcal{O}_{\Delta_f}$ is real, then
  - usually $Cl(\mathcal{O}_{\Delta_f})$ is very small and $N \approx \sqrt{\Delta_f}$;
  - for certain very special choices of Δ_1, we have N small and $\#Cl(\mathcal{O}_{\Delta_1})$ small.

Ideal Equivalence

Ideal Equivalence: $\mathfrak{a} \sim \mathfrak{b} \iff \alpha\mathfrak{a} = \beta\mathfrak{b}$ for some $\alpha, \beta \in \mathcal{O}_{\Delta_f} \setminus \{0\}$

Ideal class group of $\mathcal{O}_{\Delta_f}$: $Cl(\mathcal{O}_{\Delta_f}) = \{\text{set of equivalence classes}\}$

Properties:

- Finite Abelian group;
- The identity is the **principal class** containing $\mathcal{O}_{\Delta_f}$;
- Efficient arithmetic;
- Given any $\mathcal{O}_{\Delta_f}$-ideal $\mathfrak{a}$, it is efficient to compute a reduced ideal $\rho_{\Delta_f}(\mathfrak{a}) \sim \mathfrak{a}$;
- If N is an upper bound on the number of reduced ideals in each ideal class, then $N \cdot \#Cl(\mathcal{O}_{\Delta_f}) \approx \sqrt{|\Delta_f|}$
- If $\mathcal{O}_{\Delta_f}$ is imaginary, then $N = 1$ and $\#Cl(\mathcal{O}_{\Delta_f}) \approx \sqrt{|\Delta_f|}$;
- If $\mathcal{O}_{\Delta_f}$ is real, then
  - usually $Cl(\mathcal{O}_{\Delta_f})$ is very small and $N \approx \sqrt{\Delta_f}$;
  - for certain very special choices of Δ_1, we have N small and $\#Cl(\mathcal{O}_{\Delta_1})$ small.

Ideal Equivalence

Ideal Equivalence: $\mathfrak{a} \sim \mathfrak{b} \iff \alpha\mathfrak{a} = \beta\mathfrak{b}$ for some $\alpha, \beta \in \mathcal{O}_{\Delta_f} \setminus \{0\}$

Ideal class group of $\mathcal{O}_{\Delta_f}$: $Cl(\mathcal{O}_{\Delta_f}) = \{\text{set of equivalence classes}\}$

Properties:

- Finite Abelian group;
- The identity is the **principal class** containing $\mathcal{O}_{\Delta_f}$;
- Efficient arithmetic;
- Given any $\mathcal{O}_{\Delta_f}$-ideal $\mathfrak{a}$, it is efficient to compute a reduced ideal $\rho_{\Delta_f}(\mathfrak{a}) \sim \mathfrak{a}$;
- If N is an upper bound on the number of reduced ideals in each ideal class, then $N \cdot \#Cl(\mathcal{O}_{\Delta_f}) \approx \sqrt{|\Delta_f|}$
- If $\mathcal{O}_{\Delta_f}$ is imaginary, then $N = 1$ and $\#Cl(\mathcal{O}_{\Delta_f}) \approx \sqrt{|\Delta_f|}$;
- If $\mathcal{O}_{\Delta_f}$ is real, then
  - usually $Cl(\mathcal{O}_{\Delta_f})$ is very small and $N \approx \sqrt{\Delta_f}$;
  - for certain very special choices of Δ_1, we have N small and $\#Cl(\mathcal{O}_{\Delta_1})$ small.

Ideal Equivalence

Ideal Equivalence: $\mathfrak{a} \sim \mathfrak{b} \iff \alpha\mathfrak{a} = \beta\mathfrak{b}$ for some $\alpha, \beta \in \mathcal{O}_{\Delta_f} \setminus \{0\}$

Ideal class group of $\mathcal{O}_{\Delta_f}$: $Cl(\mathcal{O}_{\Delta_f}) = \{\text{set of equivalence classes}\}$

Properties:

- Finite Abelian group;
- The identity is the **principal class** containing $\mathcal{O}_{\Delta_f}$;
- Efficient arithmetic;
- Given any $\mathcal{O}_{\Delta_f}$-ideal $\mathfrak{a}$, it is efficient to compute a reduced ideal $\rho_{\Delta_f}(\mathfrak{a}) \sim \mathfrak{a}$;
- If N is an upper bound on the number of reduced ideals in each ideal class, then $N \cdot \#Cl(\mathcal{O}_{\Delta_f}) \approx \sqrt{|\Delta_f|}$
- If $\mathcal{O}_{\Delta_f}$ is imaginary, then $N = 1$ and $\#Cl(\mathcal{O}_{\Delta_f}) \approx \sqrt{|\Delta_f|}$;
- If $\mathcal{O}_{\Delta_f}$ is real, then
  - usually $Cl(\mathcal{O}_{\Delta_f})$ is very small and $N \approx \sqrt{\Delta_f}$;
  - for certain very special choices of Δ_1, we have N small and $\#Cl(\mathcal{O}_{\Delta_1})$ small.

$\mathcal{O}_{\Delta_1}$-Ideals and $\mathcal{O}_{\Delta_f}$-Ideals

There is a one-to-one correspondence

$$\begin{array}{rcl} \phi : \{\mathcal{O}_{\Delta_1}\text{-ideals}\} & \longleftrightarrow & \{\mathcal{O}_{\Delta_f}\text{-ideals}\} \\ \mathfrak{A} & \rightarrow & \mathfrak{a} = \phi(\mathfrak{A}) \\ \mathfrak{A} = \phi^{-1}(\mathfrak{a}) & \leftarrow & \mathfrak{a} \end{array}$$

Properties:

- ϕ and ϕ^{-1} are compatible with ideal multiplication
- ϕ and ϕ^{-1} preserve the N coefficient of any ideal
- ϕ preserves reducedness, but ϕ^{-1} doesn't
- ϕ^{-1} preserves ideal equivalence, but ϕ doesn't
- ϕ and ϕ^{-1} are efficiently computable if f is known
- ϕ and ϕ^{-1} are intractable to compute if f is unknown

ϕ^{-1} is the trap-door one-way function underlying NICE and REAL-NICE, with trap-door information f a prime

$\mathcal{O}_{\Delta_1}$-Ideals and $\mathcal{O}_{\Delta_f}$-Ideals

There is a one-to-one correspondence

$$\begin{array}{rcl} \phi : \{\mathcal{O}_{\Delta_1}\text{-ideals}\} & \longleftrightarrow & \{\mathcal{O}_{\Delta_f}\text{-ideals}\} \\ \mathfrak{A} & \rightarrow & \mathfrak{a} = \phi(\mathfrak{A}) \\ \mathfrak{A} = \phi^{-1}(\mathfrak{a}) & \leftarrow & \mathfrak{a} \end{array}$$

Properties:

- ϕ and ϕ^{-1} are compatible with ideal multiplication
- ϕ and ϕ^{-1} preserve the N coefficient of any ideal
- ϕ preserves reducedness, but ϕ^{-1} doesn't
- ϕ^{-1} preserves ideal equivalence, but ϕ doesn't
- ϕ and ϕ^{-1} are efficiently computable if f is known
- ϕ and ϕ^{-1} are intractable to compute if f is unknown

ϕ^{-1} is the trap-door one-way function underlying NICE and REAL-NICE, with trap-door information f a prime

$\mathcal{O}_{\Delta_1}$-Ideals and $\mathcal{O}_{\Delta_f}$-Ideals

There is a one-to-one correspondence

$$\begin{array}{rcl} \phi : \{\mathcal{O}_{\Delta_1}\text{-ideals}\} & \longleftrightarrow & \{\mathcal{O}_{\Delta_f}\text{-ideals}\} \\ \mathfrak{A} & \rightarrow & \mathfrak{a} = \phi(\mathfrak{A}) \\ \mathfrak{A} = \phi^{-1}(\mathfrak{a}) & \leftarrow & \mathfrak{a} \end{array}$$

Properties:

- ϕ and ϕ^{-1} are compatible with ideal multiplication
- ϕ and ϕ^{-1} preserve the N coefficient of any ideal
- ϕ preserves reducedness, but ϕ^{-1} doesn't
- ϕ^{-1} preserves ideal equivalence, but ϕ doesn't
- ϕ and ϕ^{-1} are efficiently computable if f is known
- ϕ and ϕ^{-1} are intractable to compute if f is unknown

ϕ^{-1} is the trap-door one-way function underlying NICE and REAL-NICE, with trap-door information f a prime

$\mathcal{O}_{\Delta_1}$-Ideals and $\mathcal{O}_{\Delta_f}$-Ideals

There is a one-to-one correspondence

$$\begin{array}{rcl} \phi : \{\mathcal{O}_{\Delta_1}\text{-ideals}\} & \longleftrightarrow & \{\mathcal{O}_{\Delta_f}\text{-ideals}\} \\ \mathfrak{A} & \rightarrow & \mathfrak{a} = \phi(\mathfrak{A}) \\ \mathfrak{A} = \phi^{-1}(\mathfrak{a}) & \leftarrow & \mathfrak{a} \end{array}$$

Properties:

- ϕ and ϕ^{-1} are compatible with ideal multiplication
- ϕ and ϕ^{-1} preserve the N coefficient of any ideal
- ϕ preserves reducedness, but ϕ^{-1} doesn't
- ϕ^{-1} preserves ideal equivalence, but ϕ doesn't
- ϕ and ϕ^{-1} are efficiently computable if f is known
- ϕ and ϕ^{-1} are intractable to compute if f is unknown

ϕ^{-1} is the trap-door one-way function underlying NICE and REAL-NICE, with trap-door information f a prime

Original NICE, Keys and Messages

Private Key: Large distinct primes p, q with $p \equiv 3 \pmod 4$

Public Key: $(\Delta_q, k, n, \mathfrak{p})$ where

- $\Delta_q = q^2 \Delta_1$ with $\Delta_1 = -p$
- $k =$ bit length of $\sqrt{|\Delta_1|/4}$
- $n =$ bit length of $q - (\Delta_1/q)$
- $\mathfrak{p}$ is a randomly chosen $\mathcal{O}_{\Delta_q}$-ideal so that $\phi^{-1}(\mathfrak{p})$ is principal in $\mathcal{O}_{\Delta_1}$

Messages are bit strings of length k of the form

$$\overline{m} = m \underbrace{000 \cdots 000}_{t \text{ zeros}}$$

where m is the plaintext and t is chosen sufficiently large to foil the chosen ciphertext attack of Jaulmes & Joux (EUROCRYPT 2000)

Original NICE, Keys and Messages

Private Key: Large distinct primes p, q with $p \equiv 3 \pmod 4$

Public Key: $(\Delta_q, k, n, \mathfrak{p})$ where

- $\Delta_q = q^2 \Delta_1$ with $\Delta_1 = -p$
- $k =$ bit length of $\sqrt{|\Delta_1|}/4$
- $n =$ bit length of $q - (\Delta_1/q)$
- $\mathfrak{p}$ is a randomly chosen $\mathcal{O}_{\Delta_q}$-ideal so that $\phi^{-1}(\mathfrak{p})$ is principal in $\mathcal{O}_{\Delta_1}$

Messages are bit strings of length k of the form

$$\overline{m} = m\,\underbrace{000\cdots000}_{t \text{ zeros}}$$

where m is the plaintext and t is chosen sufficiently large to foil the chosen ciphertext attack of Jaulmes & Joux (EUROCRYPT 2000)

Original NICE, Keys and Messages

Private Key: Large distinct primes p, q with $p \equiv 3 \pmod 4$

Public Key: $(\Delta_q, k, n, \mathfrak{p})$ where

- $\Delta_q = q^2 \Delta_1$ with $\Delta_1 = -p$
- $k =$ bit length of $\sqrt{|\Delta_1|}/4$
- $n =$ bit length of $q - (\Delta_1/q)$
- $\mathfrak{p}$ is a randomly chosen $\mathcal{O}_{\Delta_q}$-ideal so that $\phi^{-1}(\mathfrak{p})$ is principal in $\mathcal{O}_{\Delta_1}$

Messages are bit strings of length k of the form

$$\overline{m} = m \underbrace{000 \cdots 000}_{t \text{ zeros}}$$

where m is the plaintext and t is chosen sufficiently large to foil the chosen ciphertext attack of Jaulmes & Joux (EUROCRYPT 2000)

Original NICE, Keys and Messages

Private Key: Large distinct primes p, q with $p \equiv 3 \pmod 4$

Public Key: $(\Delta_q, k, n, \mathfrak{p})$ where

- $\Delta_q = q^2 \Delta_1$ with $\Delta_1 = -p$
- $k =$ bit length of $\sqrt{|\Delta_1|}/4$
- $n =$ bit length of $q - (\Delta_1/q)$
- $\mathfrak{p}$ is a randomly chosen $\mathcal{O}_{\Delta_q}$-ideal so that $\phi^{-1}(\mathfrak{p})$ is principal in $\mathcal{O}_{\Delta_1}$

Messages are bit strings of length k of the form

$$\overline{m} = m \underbrace{000 \cdots 000}_{t \text{ zeros}}$$

where m is the plaintext and t is chosen sufficiently large to foil the chosen ciphertext attack of Jaulmes & Joux (EUROCRYPT 2000)

Original NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, \mathfrak{p})$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \ldots, 2^{n-1}\}$
- The ciphertext is the reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{M} = \rho_{\Delta_1}(\phi^{-1}(\mathfrak{c}))$ $\quad * * *$ Note that $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ $* * *$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

Theorem

With probability at least $P_t = 1 - 2^{-2^t/k}$, we have $l = N(\mathfrak{m}) \leq \overline{m} + 2^t$. This implies the following:

- *$\phi^{-1}(\mathfrak{m})$ is reduced, so $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$, and hence $N(\mathfrak{M}) = N(\mathfrak{m}) = l$.*
- *The $k - t$ high order bits of $\overline{m}$ and $N(\mathfrak{M}) = l$ are identical, and hence make up m. So NICE is correct with probability at least P_t.*

Original NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, \mathfrak{p})$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \ldots, 2^{n-1}\}$
- The ciphertext is the reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{M} = \rho_{\Delta_1}(\phi^{-1}(\mathfrak{c}))$ $\quad * * *$ Note that $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ $* * *$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

Theorem

With probability at least $P_t = 1 - 2^{-2^t/k}$, we have $l = N(\mathfrak{m}) \leq \overline{m} + 2^t$. This implies the following:

- *$\phi^{-1}(\mathfrak{m})$ is reduced, so $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$, and hence $N(\mathfrak{M}) = N(\mathfrak{m}) = l$.*
- *The $k - t$ high order bits of $\overline{m}$ and $N(\mathfrak{M}) = l$ are identical, and hence make up m. So NICE is correct with probability at least P_t.*

Original NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, \mathfrak{p})$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \ldots, 2^{n-1}\}$
- The ciphertext is the reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{M} = \rho_{\Delta_1}(\phi^{-1}(\mathfrak{c}))$ $\quad * * *$ Note that $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ $* * *$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

Theorem

With probability at least $P_t = 1 - 2^{-2^t/k}$, we have $l = N(\mathfrak{m}) \leq \overline{m} + 2^t$. This implies the following:

- $\phi^{-1}(\mathfrak{m})$ *is reduced, so* $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$, *and hence* $N(\mathfrak{M}) = N(\mathfrak{m}) = l$.
- *The $k - t$ high order bits of $\overline{m}$ and $N(\mathfrak{M}) = l$ are identical, and hence make up m. So NICE is correct with probability at least P_t.*

Original NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, \mathfrak{p})$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \ldots, 2^{n-1}\}$
- The ciphertext is the reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{M} = \rho_{\Delta_1}(\phi^{-1}(\mathfrak{c}))$ $\quad * * *$ Note that $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ $* * *$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

Theorem

With probability at least $P_t = 1 - 2^{-2^t/k}$, we have $l = N(\mathfrak{m}) \le \overline{m} + 2^t$. This implies the following:

- *$\phi^{-1}(\mathfrak{m})$ is reduced, so $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$, and hence $N(\mathfrak{M}) = N(\mathfrak{m}) = l$.*
- *The $k - t$ high order bits of $\overline{m}$ and $N(\mathfrak{M}) = l$ are identical, and hence make up m. So NICE is correct with probability at least P_t.*

Original NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, \mathfrak{p})$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \ldots, 2^{n-1}\}$
- The ciphertext is the reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{M} = \rho_{\Delta_1}(\phi^{-1}(\mathfrak{c}))$ $\quad$ $* * *$ Note that $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ $* * *$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

Theorem

With probability at least $P_t = 1 - 2^{-2^t/k}$, we have $l = N(\mathfrak{m}) \leq \overline{m} + 2^t$. This implies the following:

- $\phi^{-1}(\mathfrak{m})$ *is reduced, so* $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$*, and hence* $N(\mathfrak{M}) = N(\mathfrak{m}) = l$*.*
- *The* $k - t$ *high order bits of* $\overline{m}$ *and* $N(\mathfrak{M}) = l$ *are identical, and hence make up* m*. So NICE is correct with probability at least* P_t*.*

Original NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, \mathfrak{p})$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \ldots, 2^{n-1}\}$
- The ciphertext is the reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{M} = \rho_{\Delta_1}(\phi^{-1}(\mathfrak{c}))$ $\quad * * *$ Note that $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ $* * *$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

Theorem

With probability at least $P_t = 1 - 2^{-2^t/k}$, we have $l = N(\mathfrak{m}) \le \overline{m} + 2^t$. This implies the following:

- $\phi^{-1}(\mathfrak{m})$ *is reduced, so* $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$, *and hence* $N(\mathfrak{M}) = N(\mathfrak{m}) = l$.
- *The* $k - t$ *high order bits of* $\overline{m}$ *and* $N(\mathfrak{M}) = l$ *are identical, and hence make up* m. *So NICE is correct with probability at least* P_t.

Original NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, \mathfrak{p})$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \ldots, 2^{n-1}\}$
- The ciphertext is the reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{M} = \rho_{\Delta_1}(\phi^{-1}(\mathfrak{c}))$ $\quad * * *$ Note that $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ $* * *$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

Theorem

With probability at least $P_t = 1 - 2^{-2^t/k}$, we have $l = N(\mathfrak{m}) \leq \overline{m} + 2^t$. This implies the following:

- $\phi^{-1}(\mathfrak{m})$ *is reduced, so* $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$*, and hence* $N(\mathfrak{M}) = N(\mathfrak{m}) = l$.
- *The* $k - t$ *high order bits of* $\overline{m}$ *and* $N(\mathfrak{M}) = l$ *are identical, and hence make up* m. *So NICE is correct with probability at least* P_t.

Original NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, \mathfrak{p})$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \ldots, 2^{n-1}\}$
- The ciphertext is the reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{M} = \rho_{\Delta_1}(\phi^{-1}(\mathfrak{c}))$ $\quad * * *$ Note that $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ $* * *$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

Theorem

With probability at least $P_t = 1 - 2^{-2^t/k}$, we have $l = N(\mathfrak{m}) \leq \overline{m} + 2^t$. This implies the following:

- *$\phi^{-1}(\mathfrak{m})$ is reduced, so $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$, and hence $N(\mathfrak{M}) = N(\mathfrak{m}) = l$.*
- *The $k - t$ high order bits of $\overline{m}$ and $N(\mathfrak{M}) = l$ are identical, and hence make up m. So NICE is correct with probability at least P_t.*

Original NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, \mathfrak{p})$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \ldots, 2^{n-1}\}$
- The ciphertext is the reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{M} = \rho_{\Delta_1}(\phi^{-1}(\mathfrak{c}))$ $\quad * * *$ Note that $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ $* * *$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

Theorem

With probability at least $P_t = 1 - 2^{-2^t/k}$, we have $l = N(\mathfrak{m}) \leq \overline{m} + 2^t$. This implies the following:

- *$\phi^{-1}(\mathfrak{m})$ is reduced, so $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$, and hence $N(\mathfrak{M}) = N(\mathfrak{m}) = l$.*
- *The $k - t$ high order bits of $\overline{m}$ and $N(\mathfrak{M}) = l$ are identical, and hence make up m. So NICE is correct with probability at least P_t.*

Original NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, \mathfrak{p})$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \ldots, 2^{n-1}\}$
- The ciphertext is the reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{M} = \rho_{\Delta_1}(\phi^{-1}(\mathfrak{c}))$ $\quad * * *$ Note that $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ $* * *$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

Theorem

With probability at least $P_t = 1 - 2^{-2^t/k}$, we have $l = N(\mathfrak{m}) \leq \overline{m} + 2^t$. This implies the following:

- $\phi^{-1}(\mathfrak{m})$ *is reduced, so* $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$*, and hence* $N(\mathfrak{M}) = N(\mathfrak{m}) = l$.
- *The* $k - t$ *high order bits of* $\overline{m}$ *and* $N(\mathfrak{M}) = l$ *are identical, and hence make up* m*. So NICE is correct with probability at least* P_t.

Original NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, \mathfrak{p})$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \ldots, 2^{n-1}\}$
- The ciphertext is the reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{M} = \rho_{\Delta_1}(\phi^{-1}(\mathfrak{c}))$ $\quad * * *$ Note that $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ $* * *$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

Theorem

With probability at least $P_t = 1 - 2^{-2^t/k}$, we have $l = N(\mathfrak{m}) \leq \overline{m} + 2^t$.

This implies the following:

- $\phi^{-1}(\mathfrak{m})$ *is reduced, so* $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$*, and hence* $N(\mathfrak{M}) = N(\mathfrak{m}) = l$.
- *The* $k - t$ *high order bits of* $\overline{m}$ *and* $N(\mathfrak{M}) = l$ *are identical, and hence make up* m*. So NICE is correct with probability at least* P_t.

Original NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, \mathfrak{p})$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \dots, 2^{n-1}\}$
- The ciphertext is the reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{M} = \rho_{\Delta_1}(\phi^{-1}(\mathfrak{c}))$ $* * *$ Note that $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ $* * *$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

Theorem

With probability at least $P_t = 1 - 2^{-2^t/k}$, we have $l = N(\mathfrak{m}) \leq \overline{m} + 2^t$. This implies the following:

- $\phi^{-1}(\mathfrak{m})$ *is reduced, so* $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$, *and hence* $N(\mathfrak{M}) = N(\mathfrak{m}) = l$.
- *The $k - t$ high order bits of $\overline{m}$ and $N(\mathfrak{M}) = l$ are identical, and hence make up m. So NICE is correct with probability at least P_t.*

Original NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, \mathfrak{p})$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \ldots, 2^{n-1}\}$
- The ciphertext is the reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{M} = \rho_{\Delta_1}(\phi^{-1}(\mathfrak{c}))$ $* * *$ Note that $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ $* * *$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

Theorem

With probability at least $P_t = 1 - 2^{-2^t/k}$, we have $l = N(\mathfrak{m}) \leq \overline{m} + 2^t$. This implies the following:

- $\phi^{-1}(\mathfrak{m})$ *is reduced, so* $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$, *and hence* $N(\mathfrak{M}) = N(\mathfrak{m}) = l$.
- *The* $k - t$ *high order bits of* $\overline{m}$ *and* $N(\mathfrak{M}) = l$ *are identical, and hence make up* m. *So NICE is correct with probability at least* P_t.

Security

Theorem

Assume that there exists an algorithm **A** *that computes for any* $\mathcal{O}_{\Delta_q}$*-ideal* $\mathfrak{a}$ *the* $\mathcal{O}_{\Delta_1}$*-ideal* $\mathfrak{A} = \phi^{-1}(\mathfrak{a})$ *without knowledge of* q*. By using* **A** *as an oracle,* Δ_q *can be factored in random polynomial time. The number of required queries to the oracle is polynomially bounded in* $\log(\Delta_q)$*.*

Other Observations:

- The number of $\mathcal{O}_{\Delta_q}$-ideal classes of the form $[\mathfrak{m}\mathfrak{p}^r]$, and hence the size of the ciphertext space, is $2^{n-1} \approx q$
- NICE was extended to provide IND-CCA2 security in the random oracle model, using standard techniques (NICE-X, Buchmann, Sakurai & Takagi, ICISC 2001)

Security

Theorem

Assume that there exists an algorithm **A** *that computes for any $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{a}$ the $\mathcal{O}_{\Delta_1}$-ideal $\mathfrak{A} = \phi^{-1}(\mathfrak{a})$ without knowledge of q. By using* **A** *as an oracle, Δ_q can be factored in random polynomial time. The number of required queries to the oracle is polynomially bounded in $\log(\Delta_q)$.*

Other Observations:

- The number of $\mathcal{O}_{\Delta_q}$-ideal classes of the form $[\mathfrak{m}\mathfrak{p}^r]$, and hence the size of the ciphertext space, is $2^{n-1} \approx q$
- NICE was extended to provide IND-CCA2 security in the random oracle model, using standard techniques (NICE-X, Buchmann, Sakurai & Takagi, ICISC 2001)

Theorem

Assume that there exists an algorithm **A** *that computes for any* $\mathcal{O}_{\Delta_q}$*-ideal* $\mathfrak{a}$ *the* $\mathcal{O}_{\Delta_1}$*-ideal* $\mathfrak{A} = \phi^{-1}(\mathfrak{a})$ *without knowledge of* q*. By using* **A** *as an oracle,* Δ_q *can be factored in random polynomial time. The number of required queries to the oracle is polynomially bounded in* $\log(\Delta_q)$*.*

Other Observations:

- The number of $\mathcal{O}_{\Delta_q}$-ideal classes of the form $[\mathfrak{m}\mathfrak{p}^r]$, and hence the size of the ciphertext space, is $2^{n-1} \approx q$
- NICE was extended to provide IND-CCA2 security in the random oracle model, using standard techniques (NICE-X, Buchmann, Sakurai & Takagi, ICISC 2001)

Extending NICE to Real Quadratic Orders

Obstacles:

- The number of ideal classes of the form $[\mathfrak{m}\mathfrak{p}^r]$ can be very small, yielding a potentially far too small ciphertext space.
- Ideal classes don't have unique reduced representatives, so we can no longer infer $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$ from $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ after decryption.

Solution:

- Instead of hiding the message $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m}$ in some random ideal class $[\mathfrak{m}\mathfrak{p}^r]$, it is instead hidden in the cycle of reduced ideals in its own ideal class. Each such cycle must therefore be large ($\approx q$)
- The decrypter now needs to locate a specific reduced $\mathcal{O}_{\Delta_1}$-ideal $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ in the cycle of reduced ideals in its own class. Each such cycle must therefore be small ($\approx \log(\Delta_1)$)

Extending NICE to Real Quadratic Orders

Obstacles:

- The number of ideal classes of the form $[\mathfrak{m}\mathfrak{p}^r]$ can be very small, yielding a potentially far too small ciphertext space.
- Ideal classes don't have unique reduced representatives, so we can no longer infer $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$ from $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ after decryption.

Solution:

- Instead of hiding the message $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m}$ in some random ideal class $[\mathfrak{m}\mathfrak{p}^r]$, it is instead hidden in the cycle of reduced ideals in its own ideal class. Each such cycle must therefore be large ($\approx q$)
- The decrypter now needs to locate a specific reduced $\mathcal{O}_{\Delta_1}$-ideal $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ in the cycle of reduced ideals in its own class. Each such cycle must therefore be small ($\approx \log(\Delta_1)$)

Extending NICE to Real Quadratic Orders

Obstacles:

- The number of ideal classes of the form $[\mathfrak{m}\mathfrak{p}^r]$ can be very small, yielding a potentially far too small ciphertext space.
- Ideal classes don't have unique reduced representatives, so we can no longer infer $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$ from $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ after decryption.

Solution:

- Instead of hiding the message $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m}$ in some random ideal class $[\mathfrak{m}\mathfrak{p}^r]$, it is instead hidden in the cycle of reduced ideals in its own ideal class. Each such cycle must therefore be large ($\approx q$)
- The decrypter now needs to locate a specific reduced $\mathcal{O}_{\Delta_1}$-ideal $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ in the cycle of reduced ideals in its own class. Each such cycle must therefore be small ($\approx \log(\Delta_1)$)

Extending NICE to Real Quadratic Orders

Obstacles:

- The number of ideal classes of the form $[\mathfrak{m}\mathfrak{p}^r]$ can be very small, yielding a potentially far too small ciphertext space.
- Ideal classes don't have unique reduced representatives, so we can no longer infer $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$ from $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ after decryption.

Solution:

- Instead of hiding the message $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m}$ in some random ideal class $[\mathfrak{m}\mathfrak{p}^r]$, it is instead hidden in the cycle of reduced ideals in its own ideal class. Each such cycle must therefore be large ($\approx q$)
- The decrypter now needs to locate a specific reduced $\mathcal{O}_{\Delta_1}$-ideal $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ in the cycle of reduced ideals in its own class. Each such cycle must therefore be small ($\approx \log(\Delta_1)$)

Obstacles:

- The number of ideal classes of the form $[\mathfrak{m}\mathfrak{p}^r]$ can be very small, yielding a potentially far too small ciphertext space.
- Ideal classes don't have unique reduced representatives, so we can no longer infer $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$ from $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ after decryption.

Solution:

- Instead of hiding the message $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m}$ in some random ideal class $[\mathfrak{m}\mathfrak{p}^r]$, it is instead hidden in the cycle of reduced ideals in its own ideal class. Each such cycle must therefore be large ($\approx q$)
- The decrypter now needs to locate a specific reduced $\mathcal{O}_{\Delta_1}$-ideal $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ in the cycle of reduced ideals in its own class. Each such cycle must therefore be small ($\approx \log(\Delta_1)$)

Extending NICE to Real Quadratic Orders

Obstacles:

- The number of ideal classes of the form $[\mathfrak{m}\mathfrak{p}^r]$ can be very small, yielding a potentially far too small ciphertext space.
- Ideal classes don't have unique reduced representatives, so we can no longer infer $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$ from $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ after decryption.

Solution:

- Instead of hiding the message $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m}$ in some random ideal class $[\mathfrak{m}\mathfrak{p}^r]$, it is instead hidden in the cycle of reduced ideals in its own ideal class. Each such cycle must therefore be large ($\approx q$)
- The decrypter now needs to locate a specific reduced $\mathcal{O}_{\Delta_1}$-ideal $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ in the cycle of reduced ideals in its own class. Each such cycle must therefore be small ($\approx \log(\Delta_1)$)

Extending NICE to Real Quadratic Orders

Obstacles:

- The number of ideal classes of the form $[\mathfrak{m}\mathfrak{p}^r]$ can be very small, yielding a potentially far too small ciphertext space.
- Ideal classes don't have unique reduced representatives, so we can no longer infer $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$ from $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ after decryption.

Solution:

- Instead of hiding the message $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m}$ in some random ideal class $[\mathfrak{m}\mathfrak{p}^r]$, it is instead hidden in the cycle of reduced ideals in its own ideal class. Each such cycle must therefore be large ($\approx q$)
- The decrypter now needs to locate a specific reduced $\mathcal{O}_{\Delta_1}$-ideal $\mathfrak{M} \sim \phi^{-1}(\mathfrak{m})$ in the cycle of reduced ideals in its own class. Each such cycle must therefore be small ($\approx \log(\Delta_1)$)

REAL-NICE, Keys and Messages

Private Key: Large distinct primes p, q with $p \equiv 1 \pmod 4$

Public Key: $(\Delta_q, k, n, (\mathfrak{p}))$ where

- $\Delta_q = q^2 \Delta_1$ with $\Delta_1 = p$
- $k =$ bit length of $\sqrt{\Delta_1}/4$
- $n =$ bit length of $q - (\Delta_1/q)$
- $\mathfrak{p}$ is a randomly chosen $\mathcal{O}_{\Delta_q}$-ideal so that $\phi^{-1}(\mathfrak{p})$ is principal; inclusion of $\mathfrak{p}$ in the public key is optional

Messages are bit strings of length k the form

$$\overline{m} = 1\underbrace{000\cdots000}_{u-1 \text{ zeros}}m\underbrace{000\cdots000}_{t \text{ zeros}}$$

- m is the plaintext
- t is as in the original NICE
- u is large enough that with high probability P_u, every $\mathcal{O}_{\Delta_1}$-ideal class contains at most one reduced ideal $\mathfrak{A}$ with $N(\mathfrak{A}) = 100\cdots000\,X$

REAL-NICE, Keys and Messages

Private Key: Large distinct primes p, q with $p \equiv 1 \pmod 4$

Public Key: $(\Delta_q, k, n, (\mathfrak{p}))$ where

- $\Delta_q = q^2 \Delta_1$ with $\Delta_1 = p$
- $k =$ bit length of $\sqrt{\Delta_1}/4$
- $n =$ bit length of $q - (\Delta_1/q)$
- $\mathfrak{p}$ is a randomly chosen $\mathcal{O}_{\Delta_q}$-ideal so that $\phi^{-1}(\mathfrak{p})$ is principal; inclusion of $\mathfrak{p}$ in the public key is optional

Messages are bit strings of length k the form

$$\overline{m} = 1\underbrace{000\cdots000}_{u-1 \text{ zeros}}m\underbrace{000\cdots000}_{t \text{ zeros}}$$

- m is the plaintext
- t is as in the original NICE
- u is large enough that with high probability P_u, every $\mathcal{O}_{\Delta_1}$-ideal class contains at most one reduced ideal $\mathfrak{A}$ with $N(\mathfrak{A}) = 100\cdots000\,X$

REAL-NICE, Keys and Messages

Private Key: Large distinct primes p, q with $p \equiv 1 \pmod 4$

Public Key: $(\Delta_q, k, n, (\mathfrak{p}))$ where

- $\Delta_q = q^2\Delta_1$ with $\Delta_1 = p$
- $k =$ bit length of $\sqrt{\Delta_1}/4$
- $n =$ bit length of $q - (\Delta_1/q)$
- $\mathfrak{p}$ is a randomly chosen $\mathcal{O}_{\Delta_q}$-ideal so that $\phi^{-1}(\mathfrak{p})$ is principal; inclusion of $\mathfrak{p}$ in the public key is optional

Messages are bit strings of length k the form

$$\overline{m} = 1\underbrace{000\cdots000}_{u-1 \text{ zeros}}m\underbrace{000\cdots000}_{t \text{ zeros}}$$

- m is the plaintext
- t is as in the original NICE
- u is large enough that with high probability P_u, every $\mathcal{O}_{\Delta_1}$-ideal class contains at most one reduced ideal $\mathfrak{A}$ with $N(\mathfrak{A}) = 100\cdots000X$

REAL-NICE, Keys and Messages

Private Key: Large distinct primes p, q with $p \equiv 1 \pmod 4$

Public Key: $(\Delta_q, k, n, (\mathfrak{p}))$ where

- $\Delta_q = q^2 \Delta_1$ with $\Delta_1 = p$
- $k =$ bit length of $\sqrt{\Delta_1}/4$
- $n =$ bit length of $q - (\Delta_1/q)$
- $\mathfrak{p}$ is a randomly chosen $\mathcal{O}_{\Delta_q}$-ideal so that $\phi^{-1}(\mathfrak{p})$ is principal; inclusion of $\mathfrak{p}$ in the public key is optional

Messages are bit strings of length k the form

$$\overline{m} = 1\,\underbrace{000\cdots000}_{u-1 \text{ zeros}}m\underbrace{000\cdots000}_{t \text{ zeros}}$$

- m is the plaintext
- t is as in the original NICE
- u is large enough that with high probability P_u, every $\mathcal{O}_{\Delta_1}$-ideal class contains at most one reduced ideal $\mathfrak{A}$ with $N(\mathfrak{A}) = 100\cdots000\,X$

REAL-NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, (\mathfrak{p}))$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \ldots, 2^{n-1}\}$
- If the public key does not include $\mathfrak{p}$, generate a randomly chosen $\mathcal{O}_{\Delta_q}$-ideal so that $\phi^{-1}(\mathfrak{p})$ is principal
- The ciphertext is a reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{C} = \phi^{-1}(\mathfrak{c})$ $\quad * * *$ Note that $\mathfrak{C} \sim \phi^{-1}(\mathfrak{m})$ $* * *$
- Search through the cycle of reduced ideals equivalent to $\mathfrak{C}$ until an ideal $\mathfrak{M}$ is found such that $N(\mathfrak{M}) = 100 \cdots 000\, X$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

REAL-NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, (\mathfrak{p}))$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \ldots, 2^{n-1}\}$
- If the public key does not include $\mathfrak{p}$, generate a randomly chosen $\mathcal{O}_{\Delta_q}$-ideal so that $\phi^{-1}(\mathfrak{p})$ is principal
- The ciphertext is a reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{C} = \phi^{-1}(\mathfrak{c})$ $\quad$ $***$ Note that $\mathfrak{C} \sim \phi^{-1}(\mathfrak{m})$ $***$
- Search through the cycle of reduced ideals equivalent to $\mathfrak{C}$ until an ideal $\mathfrak{M}$ is found such that $N(\mathfrak{M}) = 100 \cdots 000\, X$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

REAL-NICE, Encryption & Decryption

To encrypt $\overline{m}$ with public key $(\Delta_q, k, n, (\mathfrak{p}))$:

- Find the smallest prime $l > \overline{m}$ so that Δ_q is a square modulo l
- Solve $b^2 \equiv \Delta_q \pmod{4l}$ and set $\mathfrak{m}$ to be the $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{m} = (l, b)$
- Generate random $r \in_R \{1, 2, \ldots, 2^{n-1}\}$
- If the public key does not include $\mathfrak{p}$, generate a randomly chosen $\mathcal{O}_{\Delta_q}$-ideal so that $\phi^{-1}(\mathfrak{p})$ is principal
- The ciphertext is a reduced $\mathcal{O}_{\Delta_q}$-ideal $\mathfrak{c} = \rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$

To decrypt $\mathfrak{c}$ with private key (p, q):

- Compute $\mathfrak{C} = \phi^{-1}(\mathfrak{c})$ $\quad * * *$ Note that $\mathfrak{C} \sim \phi^{-1}(\mathfrak{m})$ $* * *$
- Search through the cycle of reduced ideals equivalent to $\mathfrak{C}$ until an ideal $\mathfrak{M}$ is found such that $N(\mathfrak{M}) = 100 \cdots 000\, X$
- m is the $k - t$ high order bits of $N(\mathfrak{M})$

Correctness and Security

Theorem

With probability at least $P_u = (1 - 2^{-u})^N$, we have $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$. Here, N is an upper bound on the number of reduced ideals in any $\mathcal{O}_{\Delta_1}$-ideal class. So REAL-NICE is correct with probability at least $\min\{P_t, P_u\}$.

Choice of Parameters:

- As before, breaking REAL-NICE leads to a factorization of Δ_q in random polynomial time. Choose p and q accordingly.
- Choosing $\mathfrak{p}$ properly ensures that the ciphertext ideals $\rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$, $r = 1, 2, \ldots$ are all distinct (choice depends on bit length of Δ_q only).
- Choosing $q \pm 1$ to have a large prime factor ensures with high probability that each $\mathcal{O}_{\Delta_q}$-ideal class contains a large number of reduced ideals.
- Choosing $p = \Delta_1$ to be a **Schinzel sleeper** ensures with high probability that each $\mathcal{O}_{\Delta_1}$-ideal class contains a small number of reduced ideals $N < \kappa \log(\Delta_1)$ with κ explicitly computable.

Correctness and Security

Theorem

With probability at least $P_u = (1 - 2^{-u})^N$, we have $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$. Here, N is an upper bound on the number of reduced ideals in any $\mathcal{O}_{\Delta_1}$-ideal class. So REAL-NICE is correct with probability at least $\min\{P_t, P_u\}$.

Choice of Parameters:

- As before, breaking REAL-NICE leads to a factorization of Δ_q in random polynomial time. Choose p and q accordingly.
- Choosing $\mathfrak{p}$ properly ensures that the ciphertext ideals $\rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$, $r = 1, 2, \ldots$ are all distinct (choice depends on bit length of Δ_q only).
- Choosing $q \pm 1$ to have a large prime factor ensures with high probability that each $\mathcal{O}_{\Delta_q}$-ideal class contains a large number of reduced ideals.
- Choosing $p = \Delta_1$ to be a **Schinzel sleeper** ensures with high probability that each $\mathcal{O}_{\Delta_1}$-ideal class contains a small number of reduced ideals $N < \kappa \log(\Delta_1)$ with κ explicitly computable.

Correctness and Security

Theorem

With probability at least $P_u = (1 - 2^{-u})^N$, we have $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$. Here, N is an upper bound on the number of reduced ideals in any $\mathcal{O}_{\Delta_1}$-ideal class. So REAL-NICE is correct with probability at least $\min\{P_t, P_u\}$.

Choice of Parameters:

- As before, breaking REAL-NICE leads to a factorization of Δ_q in random polynomial time. Choose p and q accordingly.
- Choosing $\mathfrak{p}$ properly ensures that the ciphertext ideals $\rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$, $r = 1, 2, \ldots$ are all distinct (choice depends on bit length of Δ_q only).
- Choosing $q \pm 1$ to have a large prime factor ensures with high probability that each $\mathcal{O}_{\Delta_q}$-ideal class contains a large number of reduced ideals.
- Choosing $p = \Delta_1$ to be a **Schinzel sleeper** ensures with high probability that each $\mathcal{O}_{\Delta_1}$-ideal class contains a small number of reduced ideals $N < \kappa \log(\Delta_1)$ with κ explicitly computable.

Correctness and Security

Theorem

With probability at least $P_u = (1 - 2^{-u})^N$*, we have* $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$*. Here,* N *is an upper bound on the number of reduced ideals in any* $\mathcal{O}_{\Delta_1}$*-ideal class. So REAL-NICE is correct with probability at least* $\min\{P_t, P_u\}$*.*

Choice of Parameters:

- As before, breaking REAL-NICE leads to a factorization of Δ_q in random polynomial time. Choose p and q accordingly.
- Choosing $\mathfrak{p}$ properly ensures that the ciphertext ideals $\rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$, $r = 1, 2, \ldots$ are all distinct (choice depends on bit length of Δ_q only).
- Choosing $q \pm 1$ to have a large prime factor ensures with high probability that each $\mathcal{O}_{\Delta_q}$-ideal class contains a large number of reduced ideals.
- Choosing $p = \Delta_1$ to be a **Schinzel sleeper** ensures with high probability that each $\mathcal{O}_{\Delta_1}$-ideal class contains a small number of reduced ideals $N < \kappa \log(\Delta_1)$ with κ explicitly computable.

Correctness and Security

Theorem

With probability at least $P_u = (1 - 2^{-u})^N$, we have $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$. Here, N is an upper bound on the number of reduced ideals in any $\mathcal{O}_{\Delta_1}$-ideal class. So REAL-NICE is correct with probability at least $\min\{P_t, P_u\}$.

Choice of Parameters:

- As before, breaking REAL-NICE leads to a factorization of Δ_q in random polynomial time. Choose p and q accordingly.
- Choosing $\mathfrak{p}$ properly ensures that the ciphertext ideals $\rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$, $r = 1, 2, \ldots$ are all distinct (choice depends on bit length of Δ_q only).
- Choosing $q \pm 1$ to have a large prime factor ensures with high probability that each $\mathcal{O}_{\Delta_q}$-ideal class contains a large number of reduced ideals.
- Choosing $p = \Delta_1$ to be a **Schinzel sleeper** ensures with high probability that each $\mathcal{O}_{\Delta_1}$-ideal class contains a small number of reduced ideals $N < \kappa \log(\Delta_1)$ with κ explicitly computable.

Correctness and Security

Theorem

With probability at least $P_u = (1 - 2^{-u})^N$, we have $\mathfrak{M} = \phi^{-1}(\mathfrak{m})$. Here, N is an upper bound on the number of reduced ideals in any $\mathcal{O}_{\Delta_1}$-ideal class. So REAL-NICE is correct with probability at least $\min\{P_t, P_u\}$.

Choice of Parameters:

- As before, breaking REAL-NICE leads to a factorization of Δ_q in random polynomial time. Choose p and q accordingly.
- Choosing $\mathfrak{p}$ properly ensures that the ciphertext ideals $\rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$, $r = 1, 2, \ldots$ are all distinct (choice depends on bit length of Δ_q only).
- Choosing $q \pm 1$ to have a large prime factor ensures with high probability that each $\mathcal{O}_{\Delta_q}$-ideal class contains a large number of reduced ideals.
- Choosing $p = \Delta_1$ to be a **Schinzel sleeper** ensures with high probability that each $\mathcal{O}_{\Delta_1}$-ideal class contains a small number of reduced ideals $N < \kappa \log(\Delta_1)$ with κ explicitly computable.

Summary of Numerical Results

Comparative Implementation of all five NIST levels of security of

- REAL-NICE with small public key and NICE — prototypes, using NTL
- OpenSSL RSA — highly optimized

Results:

- NICE outperforms REAL-NICE at all five NIST levels for both encryption and decryption; more so for decryption.
  - Generation of a new ideal $\mathfrak{p}$ for each message slows down encryption of REAL-NICE over NICE, but allows for a smaller public key in REAL-NICE.
  - Search through the cycle of reduced ideals equivalent to the decryption ideal. $\mathfrak{M}$ slows down decryption of REAL-NICE over NICE.
- NICE and REAL-NICE outperform RSA in decryption at all five NIST levels.
- NICE and REAL-NICE outperform RSA in overall performance at the two highest NIST levels.

Summary of Numerical Results

Comparative Implementation of all five NIST levels of security of

- REAL-NICE with small public key and NICE — prototypes, using NTL
- OpenSSL RSA — highly optimized

Results:

- NICE outperforms REAL-NICE at all five NIST levels for both encryption and decryption; more so for decryption.
  - Generation of a new ideal $\mathfrak{p}$ for each message slows down encryption of REAL-NICE over NICE, but allows for a smaller public key in REAL-NICE.
  - Search through the cycle of reduced ideals equivalent to the decryption ideal. $\mathfrak{M}$ slows down decryption of REAL-NICE over NICE.
- NICE and REAL-NICE outperform RSA in decryption at all five NIST levels.
- NICE and REAL-NICE outperform RSA in overall performance at the two highest NIST levels.

Summary of Numerical Results

Comparative Implementation of all five NIST levels of security of

- REAL-NICE with small public key and NICE — prototypes, using NTL
- OpenSSL RSA — highly optimized

Results:

- NICE outperforms REAL-NICE at all five NIST levels for both encryption and decryption; more so for decryption.
  - Generation of a new ideal $\mathfrak{p}$ for each message slows down encryption of REAL-NICE over NICE, but allows for a smaller public key in REAL-NICE.
  - Search through the cycle of reduced ideals equivalent to the decryption ideal. $\mathfrak{M}$ slows down decryption of REAL-NICE over NICE.
- NICE and REAL-NICE outperform RSA in decryption at all five NIST levels.
- NICE and REAL-NICE outperform RSA in overall performance at the two highest NIST levels.

Summary of Numerical Results

Comparative Implementation of all five NIST levels of security of

- REAL-NICE with small public key and NICE — prototypes, using NTL
- OpenSSL RSA — highly optimized

Results:

- NICE outperforms REAL-NICE at all five NIST levels for both encryption and decryption; more so for decryption.
  - Generation of a new ideal $\mathfrak{p}$ for each message slows down encryption of REAL-NICE over NICE, but allows for a smaller public key in REAL-NICE.
  - Search through the cycle of reduced ideals equivalent to the decryption ideal. $\mathfrak{M}$ slows down decryption of REAL-NICE over NICE.
- NICE and REAL-NICE outperform RSA in decryption at all five NIST levels.
- NICE and REAL-NICE outperform RSA in overall performance at the two highest NIST levels.

Summary of Numerical Results

Comparative Implementation of all five NIST levels of security of

- REAL-NICE with small public key and NICE — prototypes, using NTL
- OpenSSL RSA — highly optimized

Results:

- NICE outperforms REAL-NICE at all five NIST levels for both encryption and decryption; more so for decryption.
  - Generation of a new ideal $\mathfrak{p}$ for each message slows down encryption of REAL-NICE over NICE, but allows for a smaller public key in REAL-NICE.
  - Search through the cycle of reduced ideals equivalent to the decryption ideal. $\mathfrak{M}$ slows down decryption of REAL-NICE over NICE.
- NICE and REAL-NICE outperform RSA in decryption at all five NIST levels.
- NICE and REAL-NICE outperform RSA in overall performance at the two highest NIST levels.

Summary of Numerical Results

Comparative Implementation of all five NIST levels of security of

- REAL-NICE with small public key and NICE — prototypes, using NTL
- OpenSSL RSA — highly optimized

Results:

- NICE outperforms REAL-NICE at all five NIST levels for both encryption and decryption; more so for decryption.
  - Generation of a new ideal $\mathfrak{p}$ for each message slows down encryption of REAL-NICE over NICE, but allows for a smaller public key in REAL-NICE.
  - Search through the cycle of reduced ideals equivalent to the decryption ideal. $\mathfrak{M}$ slows down decryption of REAL-NICE over NICE.
- NICE and REAL-NICE outperform RSA in decryption at all five NIST levels.
- NICE and REAL-NICE outperform RSA in overall performance at the two highest NIST levels.

Further Work

- Security proof for REAL-NICE — IND-CCA2 security in the random oracle model, as for NICE?
- Security of choosing Δ_1 to be a Schinzel sleeper?
- Comparison to q^2p RSA (Takagi, CRYPTO 1998) – faster decryption
- Better Implementation
- Integer multiple side step encryption for REAL-NICE:
  - Not applicable to the imaginary setting.
  - Successfully used for real hyperelliptic curves.
  - Instead of computing $\rho_{\Delta_q}(\mathfrak{mp}^r)$ using square & multiply, choose a random number r of square steps and replace the (quadratic complexity) multiply steps by (linear complexity) reduction steps.
  - Preliminary computations show that IMS-REAL-NICE outperforms REAL-NICE even under the most conservative analysis, using provable results on reduced ideals.
  - Much better performance under heuristic assumptions on the behaviour of reduced ideals, but requires careful security analysis.

Further Work

- Security proof for REAL-NICE — IND-CCA2 security in the random oracle model, as for NICE?
- Security of choosing Δ_1 to be a Schinzel sleeper?
- Comparison to q^2p RSA (Takagi, CRYPTO 1998) – faster decryption
- Better Implementation
- Integer multiple side step encryption for REAL-NICE:
  - Not applicable to the imaginary setting.
  - Successfully used for real hyperelliptic curves.
  - Instead of computing $\rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$ using square & multiply, choose a random number r of square steps and replace the (quadratic complexity) multiply steps by (linear complexity) reduction steps.
  - Preliminary computations show that IMS-REAL-NICE outperforms REAL-NICE even under the most conservative analysis, using provable results on reduced ideals.
  - Much better performance under heuristic assumptions on the behaviour of reduced ideals, but requires careful security analysis.

Further Work

- Security proof for REAL-NICE — IND-CCA2 security in the random oracle model, as for NICE?
- Security of choosing Δ_1 to be a Schinzel sleeper?
- Comparison to q^2p RSA (Takagi, CRYPTO 1998) – faster decryption
- Better Implementation
- Integer multiple side step encryption for REAL-NICE:
  - Not applicable to the imaginary setting.
  - Successfully used for real hyperelliptic curves.
  - Instead of computing $\rho_{\Delta_q}(\mathfrak{mp}^r)$ using square & multiply, choose a random number r of square steps and replace the (quadratic complexity) multiply steps by (linear complexity) reduction steps.
  - Preliminary computations show that IMS-REAL-NICE outperforms REAL-NICE even under the most conservative analysis, using provable results on reduced ideals.
  - Much better performance under heuristic assumptions on the behaviour of reduced ideals, but requires careful security analysis.

Further Work

- Security proof for REAL-NICE — IND-CCA2 security in the random oracle model, as for NICE?
- Security of choosing Δ_1 to be a Schinzel sleeper?
- Comparison to q^2p RSA (Takagi, CRYPTO 1998) – faster decryption
- Better Implementation
- Integer multiple side step encryption for REAL-NICE:
  - Not applicable to the imaginary setting.
  - Successfully used for real hyperelliptic curves.
  - Instead of computing $\rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$ using square & multiply, choose a random number r of square steps and replace the (quadratic complexity) multiply steps by (linear complexity) reduction steps.
  - Preliminary computations show that IMS-REAL-NICE outperforms REAL-NICE even under the most conservative analysis, using provable results on reduced ideals.
  - Much better performance under heuristic assumptions on the behaviour of reduced ideals, but requires careful security analysis.

Further Work

- Security proof for REAL-NICE — IND-CCA2 security in the random oracle model, as for NICE?
- Security of choosing Δ_1 to be a Schinzel sleeper?
- Comparison to q^2p RSA (Takagi, CRYPTO 1998) – faster decryption
- Better Implementation
- Integer multiple side step encryption for REAL-NICE:
  - Not applicable to the imaginary setting.
  - Successfully used for real hyperelliptic curves.
  - Instead of computing $\rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$ using square & multiply, choose a random number r of square steps and replace the (quadratic complexity) multiply steps by (linear complexity) reduction steps.
  - Preliminary computations show that IMS-REAL-NICE outperforms REAL-NICE even under the most conservative analysis, using provable results on reduced ideals.
  - Much better performance under heuristic assumptions on the behaviour of reduced ideals, but requires careful security analysis.

Further Work

- Security proof for REAL-NICE — IND-CCA2 security in the random oracle model, as for NICE?
- Security of choosing Δ_1 to be a Schinzel sleeper?
- Comparison to q^2p RSA (Takagi, CRYPTO 1998) – faster decryption
- Better Implementation
- Integer multiple side step encryption for REAL-NICE:
  - Not applicable to the imaginary setting.
  - Successfully used for real hyperelliptic curves.
  - Instead of computing $\rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$ using square & multiply, choose a random number r of square steps and replace the (quadratic complexity) multiply steps by (linear complexity) reduction steps.
  - Preliminary computations show that IMS-REAL-NICE outperforms REAL-NICE even under the most conservative analysis, using provable results on reduced ideals.
  - Much better performance under heuristic assumptions on the behaviour of reduced ideals, but requires careful security analysis.

Further Work

- Security proof for REAL-NICE — IND-CCA2 security in the random oracle model, as for NICE?
- Security of choosing Δ_1 to be a Schinzel sleeper?
- Comparison to $q^2 p$ RSA (Takagi, CRYPTO 1998) – faster decryption
- Better Implementation
- Integer multiple side step encryption for REAL-NICE:
  - Not applicable to the imaginary setting.
  - Successfully used for real hyperelliptic curves.
  - Instead of computing $\rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$ using square & multiply, choose a random number r of square steps and replace the (quadratic complexity) multiply steps by (linear complexity) reduction steps.
  - Preliminary computations show that IMS-REAL-NICE outperforms REAL-NICE even under the most conservative analysis, using provable results on reduced ideals.
  - Much better performance under heuristic assumptions on the behaviour of reduced ideals, but requires careful security analysis.

Further Work

- Security proof for REAL-NICE — IND-CCA2 security in the random oracle model, as for NICE?
- Security of choosing Δ_1 to be a Schinzel sleeper?
- Comparison to $q^2 p$ RSA (Takagi, CRYPTO 1998) – faster decryption
- Better Implementation
- Integer multiple side step encryption for REAL-NICE:
  - Not applicable to the imaginary setting.
  - Successfully used for real hyperelliptic curves.
  - Instead of computing $\rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$ using square & multiply, choose a random number r of square steps and replace the (quadratic complexity) multiply steps by (linear complexity) reduction steps.
  - Preliminary computations show that IMS-REAL-NICE outperforms REAL-NICE even under the most conservative analysis, using provable results on reduced ideals.
  - Much better performance under heuristic assumptions on the behaviour of reduced ideals, but requires careful security analysis.

Further Work

- Security proof for REAL-NICE — IND-CCA2 security in the random oracle model, as for NICE?
- Security of choosing Δ_1 to be a Schinzel sleeper?
- Comparison to $q^2 p$ RSA (Takagi, CRYPTO 1998) – faster decryption
- Better Implementation
- Integer multiple side step encryption for REAL-NICE:
  - Not applicable to the imaginary setting.
  - Successfully used for real hyperelliptic curves.
  - Instead of computing $\rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$ using square & multiply, choose a random number r of square steps and replace the (quadratic complexity) multiply steps by (linear complexity) reduction steps.
  - Preliminary computations show that IMS-REAL-NICE outperforms REAL-NICE even under the most conservative analysis, using provable results on reduced ideals.
  - Much better performance under heuristic assumptions on the behaviour of reduced ideals, but requires careful security analysis.

Further Work

- Security proof for REAL-NICE — IND-CCA2 security in the random oracle model, as for NICE?
- Security of choosing Δ_1 to be a Schinzel sleeper?
- Comparison to q^2p RSA (Takagi, CRYPTO 1998) – faster decryption
- Better Implementation
- Integer multiple side step encryption for REAL-NICE:
  - Not applicable to the imaginary setting.
  - Successfully used for real hyperelliptic curves.
  - Instead of computing $\rho_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$ using square & multiply, choose a random number r of square steps and replace the (quadratic complexity) multiply steps by (linear complexity) reduction steps.
  - Preliminary computations show that IMS-REAL-NICE outperforms REAL-NICE even under the most conservative analysis, using provable results on reduced ideals.
  - Much better performance under heuristic assumptions on the behaviour of reduced ideals, but requires careful security analysis.