Imperial College London

NTRU in Quaternion Algebras of Bounded Discriminant

Cong Ling & **Andrew Mendelsohn**

August 16, 2023

Imperial College London

NTRU

Let $\mathcal{R} = \mathbb{Z}[x]/f(x)\mathbb{Z}[x]$ be a polynomial ring, $\deg(f) = n$, $q \geq 2$.

NTRU Assumption

Let $g, f \in \mathcal{R}$ be 'short' and f invertible mod q.
Given $h := f^{-1} \cdot g \bmod q$, it is hard to recover g and f.

NTRU

Let $\mathcal{R} = \mathbb{Z}[x]/f(x)\mathbb{Z}[x]$ be a polynomial ring, $\deg(f) = n$, $q \geq 2$.

NTRU Assumption

Let $g, f \in \mathcal{R}$ be 'short' and f invertible mod q.
Given $h := f^{-1} \cdot g \bmod q$, it is hard to recover g and f.

A lattice problem:

$$\mathcal{L}_{h,q} := \{(x, y) \in \mathcal{R}^2 : xh - y \equiv 0 \bmod q\}$$

NTRU Assumption: it is hard to find short vectors in $\mathcal{L}_{h,q}$ (wrt. the Euclidean norm).

NTRU

Let $\mathcal{R} = \mathbb{Z}[x]/f(x)\mathbb{Z}[x]$ be a polynomial ring, $\deg(f) = n$, $q \geq 2$.

NTRU Assumption

Let $g, f \in \mathcal{R}$ be 'short' and f invertible mod q.
Given $h := f^{-1} \cdot g \bmod q$, it is hard to recover g and f.

A lattice problem:

$$\mathcal{L}_{h,q} := \{(x, y) \in \mathcal{R}^2 : xh - y \equiv 0 \bmod q\}$$

NTRU Assumption: it is hard to find short vectors in $\mathcal{L}_{h,q}$ (wrt. the Euclidean norm).

Reasons for assuming: [FPMS22], [PMS21], ... and time.

What about different $\mathcal{R}$?

Some NTRU Variants

NTRU as matrices: suppose $f(x) = x^n + 1$, n a power of two.
Fix basis $\{1, x, ..., x^{n-1}\}$, write $fh - g = 0 \bmod q$ as

$$\begin{pmatrix} f_0 & -f_{n-1} & \dots & -f_1 \\ f_1 & f_0 & \dots & -f_2 \\ \vdots & \vdots & \ddots & \vdots \\ f_{n-1} & f_{n-2} & \dots & f_0 \end{pmatrix} \begin{pmatrix} h_0 \\ h_1 \\ \vdots \\ h_{n-1} \end{pmatrix} - \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{n-1} \end{pmatrix} = \mathbf{0} \bmod q$$

Some NTRU Variants

NTRU as matrices: suppose $f(x) = x^n + 1$, n a power of two. Fix basis $\{1, x, ..., x^{n-1}\}$, write $fh - g = 0 \bmod q$ as

$$\begin{pmatrix} f_0 & -f_{n-1} & \cdots & -f_1 \\ f_1 & f_0 & \cdots & -f_2 \\ \vdots & \vdots & \ddots & \vdots \\ f_{n-1} & f_{n-2} & \cdots & f_0 \end{pmatrix} \begin{pmatrix} h_0 \\ h_1 \\ \vdots \\ h_{n-1} \end{pmatrix} - \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{n-1} \end{pmatrix} = \mathbf{0} \bmod q$$

[CG05],[CPSWX19],[CKKS19]: $f(x) = x^n + 1$. $\mathbf{Fh} = \mathbf{g} \in \mathcal{R}_q^k$.

$$\mathcal{L}_{\mathbf{h},q} = \{(\mathbf{F}, \mathbf{g}) \in \mathcal{R}^{k \times (k+1)} : \mathbf{Fh} - \mathbf{g} = \mathbf{0} \bmod q\}$$

$$\begin{pmatrix} f_{0,0} & f_{0,1} & \cdots & f_{0,k-1} \\ f_{1,0} & f_{1,1} & \cdots & f_{1,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ f_{k-1,0} & f_{k-1,1} & \cdots & f_{k-1,k-1} \end{pmatrix} \begin{pmatrix} h_0 \\ h_1 \\ \vdots \\ h_{n-1} \end{pmatrix} - \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{n-1} \end{pmatrix} = \mathbf{0} \bmod q$$

An NTRU PKE Scheme

Setup

$q \gg p : \gcd(q,p) = 1$. Message $m \in \mathcal{R}_p$. $h := f^{-1}g \bmod q$.

KeyGen: $(pk, sk) = (h, (f, g))$ where f is invertible mod q and $f \equiv 1 \bmod p$.

Encrypt m: $e, t \leftarrow \mathcal{R}_q$. Set $c = p \cdot (h \cdot t + e) + m \bmod q$

Decrypt c: compute $m \bmod p = (f \cdot c \bmod q) \bmod p$.

Correctness: works if $\|pgt + pfe + fm\|_\infty < \frac{q}{2}$

An NTRU PKE Scheme

Setup

$q \gg p : \gcd(q, p) = 1$. Message $m \in \mathcal{R}_p$. $h := f^{-1}g \bmod q$.

KeyGen: $(pk, sk) = (h, (f, g))$ where f is invertible mod q and $f \equiv 1 \bmod p$.

Encrypt m: $e, t \leftarrow \mathcal{R}_q$. Set $c = p \cdot (h \cdot t + e) + m \bmod q$

Decrypt c: compute $m \bmod p = (f \cdot c \bmod q) \bmod p$.

Correctness: works if $\|pgt + pfe + fm\|_\infty < \frac{q}{2}$

We don't need $ab = ba$ for decryption (except $pf = fp$).
So one could run this over many noncommutative rings.

Quaternion Algebras

Setup

$n = 2^r$, ℓ an odd prime: $\ell \equiv 1 \bmod n$ and $\ell \not\equiv 1 \bmod 2n$.
$K := \mathbb{Q}(\zeta_n)$ and $L := \mathbb{Q}(\zeta_n, \sqrt{\ell})$. $\theta \in \mathrm{Gal}(L/K)$ nontrivial.

Quaternion Algebras

Setup

$n = 2^r$, ℓ an odd prime: $\ell \equiv 1 \bmod n$ and $\ell \not\equiv 1 \bmod 2n$.
$K := \mathbb{Q}(\zeta_n)$ and $L := \mathbb{Q}(\zeta_n, \sqrt{\ell})$. $\theta \in \mathrm{Gal}(L/K)$ nontrivial.

Quaternion algebra:

$$\mathcal{A} = L \oplus uL,$$

with $u^2 = \zeta_n$, and $xu = u\theta(x)$ for all $x \in L$.

Quaternion Algebras

Setup

$n = 2^r$, ℓ an odd prime: $\ell \equiv 1 \bmod n$ and $\ell \not\equiv 1 \bmod 2n$.
$K := \mathbb{Q}(\zeta_n)$ and $L := \mathbb{Q}(\zeta_n, \sqrt{\ell})$. $\theta \in \mathrm{Gal}(L/K)$ nontrivial.

Quaternion algebra:

$$\mathcal{A} = L \oplus uL,$$

with $u^2 = \zeta_n$, and $xu = u\theta(x)$ for all $x \in L$.

Orders: subrings which are full-rank lattices; e.g. 'natural' order:

$$\Lambda := \mathcal{O}_L \oplus u\mathcal{O}_L$$

Λ is a maximal order in $\mathcal{A}$.

$$\Lambda_q := \Lambda / q\Lambda = \mathcal{O}_L / q\mathcal{O}_L \oplus u\mathcal{O}_L / q\mathcal{O}_L$$

Imperial College London

NTRU in Cyclic Algebras: CNTRU

$n = 2^r$, ℓ an odd prime: $\ell \equiv 1 \bmod n$ and $\ell \not\equiv 1 \bmod 2n$.
$K := \mathbb{Q}(\zeta_n)$, $L := \mathbb{Q}(\zeta_n, \sqrt{\ell})$, $\theta \in \mathrm{Gal}(L/K)$. $\Lambda := \mathcal{O}_L \oplus u\mathcal{O}_L$.

CNTRU Assumption

Let g, $f \in \Lambda$ be 'short' and $f \bmod q\Lambda$ invertible.
Given $h := f^{-1} \cdot g \bmod q\Lambda$, it is hard to recover g and f.

NTRU in Cyclic Algebras: CNTRU

$n = 2^r$, ℓ an odd prime: $\ell \equiv 1 \bmod n$ and $\ell \not\equiv 1 \bmod 2n$.
$K := \mathbb{Q}(\zeta_n)$, $L := \mathbb{Q}(\zeta_n, \sqrt{\ell})$, $\theta \in \mathrm{Gal}(L/K)$. $\Lambda := \mathcal{O}_L \oplus u\mathcal{O}_L$.

CNTRU Assumption

Let g, $f \in \Lambda$ be 'short' and $f \bmod q\Lambda$ invertible.
Given $h := f^{-1} \cdot g \bmod q\Lambda$, it is hard to recover g and f.

A lattice problem:

$$\mathcal{L}_{h,q} := \{(x, y) \in \Lambda^2 : xh - y \equiv 0 \bmod q\Lambda\}$$

CNTRU Assumption: it is hard to find short vectors in $\mathcal{L}_{h,q}$ (wrt. the Euclidean norm, for some embedding $\Lambda \hookrightarrow \mathbb{R}^{2n}$).

NTRU in Cyclic Algebras: CNTRU

$n = 2^r$, ℓ an odd prime: $\ell \equiv 1 \bmod n$ and $\ell \not\equiv 1 \bmod 2n$.
$K := \mathbb{Q}(\zeta_n)$, $L := \mathbb{Q}(\zeta_n, \sqrt{\ell})$, $\theta \in \mathrm{Gal}(L/K)$. $\Lambda := \mathcal{O}_L \oplus u\mathcal{O}_L$.

CNTRU Assumption

Let $g, f \in \Lambda$ be 'short' and $f \bmod q\Lambda$ invertible.
Given $h := f^{-1} \cdot g \bmod q\Lambda$, it is hard to recover g and f.

A lattice problem:

$$\mathcal{L}_{h,q} := \{(x, y) \in \Lambda^2 : xh - y \equiv 0 \bmod q\Lambda\}$$

CNTRU Assumption: it is hard to find short vectors in $\mathcal{L}_{h,q}$ (wrt. the Euclidean norm, for some embedding $\Lambda \hookrightarrow \mathbb{R}^{2n}$).

We change the above PKE scheme to obtain IND-CPA security from **Cyclic LWE**.

Cyclic LWE: a structured LWE problem

$L_{\mathbb{R}} = L \otimes_{\mathbb{Q}} \mathbb{R}$.

Ψ = a family of error distributions over $L_{\mathbb{R}} \oplus uL_{\mathbb{R}}$.

CLWE distribution

For error distribution $\psi \in \Psi$, $q \geq 2$, and secret $s \in \Lambda_q$, a sample from the CLWE distribution $\Pi_{q,s,\psi}$ is obtained by sampling $e \leftarrow \psi$, $a \leftarrow \Lambda_q$ uniformly at random, and outputting

$$(a, b) = (a, as + e \bmod q\Lambda) \in \Lambda_q \times (L_{\mathbb{R}} \oplus uL_{\mathbb{R}})/q\Lambda$$

Cyclic LWE: a structured LWE problem

$L_{\mathbb{R}} = L \otimes_{\mathbb{Q}} \mathbb{R}$.
Ψ = a family of error distributions over $L_{\mathbb{R}} \oplus uL_{\mathbb{R}}$.

CLWE distribution

For error distribution $\psi \in \Psi$, $q \geq 2$, and secret $s \in \Lambda_q$, a sample from the CLWE distribution $\Pi_{q,s,\psi}$ is obtained by sampling $e \leftarrow \psi$, $a \leftarrow \Lambda_q$ uniformly at random, and outputting

$$(a, b) = (a, as + e \bmod q\Lambda) \in \Lambda_q \times (L_{\mathbb{R}} \oplus uL_{\mathbb{R}})/q\Lambda$$

Search CLWE: recover s from a collection of independent samples for any $s \in \Lambda_q$ and $\psi \in \Psi$.
Decision CLWE: given independent samples from $\Pi_{q,s,\psi}$ for random (s, ψ) or uniform samples, decide which is the case whp.

Cyclic LWE: a structured LWE problem

$L_{\mathbb{R}} = L \otimes_{\mathbb{Q}} \mathbb{R}$.
Ψ = a family of error distributions over $L_{\mathbb{R}} \oplus uL_{\mathbb{R}}$.

CLWE distribution

For error distribution $\psi \in \Psi$, $q \geq 2$, and secret $s \in \Lambda_q$, a sample from the CLWE distribution $\Pi_{q,s,\psi}$ is obtained by sampling $e \leftarrow \psi$, $a \leftarrow \Lambda_q$ uniformly at random, and outputting

$$(a, b) = (a, as + e \bmod q\Lambda) \in \Lambda_q \times (L_{\mathbb{R}} \oplus uL_{\mathbb{R}})/q\Lambda$$

Search CLWE: recover s from a collection of independent samples for any $s \in \Lambda_q$ and $\psi \in \Psi$.
Decision CLWE: given independent samples from $\Pi_{q,s,\psi}$ for random (s, ψ) or uniform samples, decide which is the case whp.

[GMLV22]: a reduction from SIVP on ideal lattices in Λ to search CLWE, and a (restricted) search-to-decision reduction.

Cyclic NTRU: a structured problem

Write $f = f_0 + uf_1$, $h = h_0 + uh_1 \in \mathcal{O}_L + u\mathcal{O}_L$. Then

$$f \cdot h = f_0 h_0 + \zeta_n \theta(f_1) h_1 + u\big(f_1 h_0 + \theta(f_0) h_1\big)$$

Cyclic NTRU: a structured problem

Write $f = f_0 + uf_1$, $h = h_0 + uh_1 \in \mathcal{O}_L + u\mathcal{O}_L$. Then

$$f \cdot h = f_0 h_0 + \zeta_n \theta(f_1) h_1 + u\big(f_1 h_0 + \theta(f_0) h_1\big)$$

So with L-basis $\{1, u\}$ of Λ, write $f \cdot h - g = 0 \bmod q\Lambda$ as

$$\begin{pmatrix} f_0 & \gamma\theta(f_1) \\ f_1 & \theta(f_0) \end{pmatrix} \begin{pmatrix} h_0 \\ h_1 \end{pmatrix} - \begin{pmatrix} g_0 \\ g_1 \end{pmatrix} = \mathbf{0} \bmod q\Lambda$$

Cyclic NTRU: a structured problem

Write $f = f_0 + uf_1$, $h = h_0 + uh_1 \in \mathcal{O}_L + u\mathcal{O}_L$. Then

$$f \cdot h = f_0 h_0 + \zeta_n \theta(f_1) h_1 + u\big(f_1 h_0 + \theta(f_0) h_1\big)$$

So with L-basis $\{1, u\}$ of Λ, write $f \cdot h - g = 0 \bmod q\Lambda$ as

$$\begin{pmatrix} f_0 & \gamma\theta(f_1) \\ f_1 & \theta(f_0) \end{pmatrix} \begin{pmatrix} h_0 \\ h_1 \end{pmatrix} - \begin{pmatrix} g_0 \\ g_1 \end{pmatrix} = \mathbf{0} \bmod q\Lambda$$

Compare to [CPSWX19],[CKKS19] in rank 2:

$$\begin{pmatrix} f_0 & f_2 \\ f_1 & f_3 \end{pmatrix} \begin{pmatrix} h_0 \\ h_1 \end{pmatrix} - \begin{pmatrix} g_0 \\ g_1 \end{pmatrix} = \mathbf{0} \bmod q\Lambda$$

Imperial College London

Contributions, and Why?

Contributions

1. Uniformity of CNTRU public keys (requires results on q-ary lattices from maximal orders in quaternion algebras)
2. IND-CPA secure CNTRU PKE, assuming CLWE (requires bounded ℓ)
3. Extra CNTRU cryptographic functionality: KEM, signatures

Contributions, and Why?

Contributions

1. Uniformity of CNTRU public keys (requires results on q-ary lattices from maximal orders in quaternion algebras)
2. IND-CPA secure CNTRU PKE, assuming CLWE (requires bounded ℓ)
3. Extra CNTRU cryptographic functionality: KEM, signatures

Motivations

1. [CKKS19] has no security proof. [CPSWX19] proves uniformity of public keys for partially split q - but recommends fully split q for efficiency. We prove uniformity of public keys for fully split q.
2. To understand cryptographic properties in CDAs - and of CLWE.
3. Quaternions algebras offer a natural generalisation of number fields.

CNTRU PKE

Trace form: $x = x_0 + ux_1 \in \Lambda$.

$$\mathrm{Tr}(x) := \mathrm{Tr}_{K/\mathbb{Q}}\left(\mathrm{trace}\begin{pmatrix} x_0 & \gamma\theta(x_1) \\ x_1 & \theta(x_0) \end{pmatrix}\right)$$

Then

$$\Lambda^\vee = \{x \in \mathcal{A} : \ \mathrm{Tr}(x\Lambda) \subset \mathbb{Z}\}$$

CNTRU PKE

Trace form: $x = x_0 + ux_1 \in \Lambda$.

$$\mathrm{Tr}(x) := \mathrm{Tr}_{K/\mathbb{Q}}\left(\mathrm{trace}\begin{pmatrix} x_0 & \gamma\theta(x_1) \\ x_1 & \theta(x_0) \end{pmatrix}\right)$$

Then

$$\Lambda^\vee = \{x \in \mathcal{A} : \ \mathrm{Tr}(x\Lambda) \subset \mathbb{Z}\}$$

$D_{\Lambda,\sigma}$ = discrete Gaussian. D_σ = Gaussian over $L^2_{\mathbb{R}}$. $p \in \Lambda_q^\times$.
$\chi := \lfloor D_\sigma \rceil_{\Lambda^\vee}$, where $\lfloor \cdot \rceil_{\Lambda^\vee}$ is a discretisation.

CNTRU PKE

Trace form: $x = x_0 + ux_1 \in \Lambda$.

$$\mathrm{Tr}(x) := \mathrm{Tr}_{K/\mathbb{Q}}\left(\mathrm{trace}\begin{pmatrix} x_0 & \gamma\theta(x_1) \\ x_1 & \theta(x_0) \end{pmatrix}\right)$$

Then

$$\Lambda^\vee = \{x \in \mathcal{A} : \ \mathrm{Tr}(x\Lambda) \subset \mathbb{Z}\}$$

$D_{\Lambda,\sigma}$ = discrete Gaussian. D_σ = Gaussian over $L^2_{\mathbb{R}}$. $p \in \Lambda_q^\times$.
$\chi := \lfloor D_\sigma \rceil_{\Lambda^\vee}$, where $\lfloor \cdot \rceil_{\Lambda^\vee}$ is a discretisation.

KeyGen: Sample $f', g \leftarrow D_{\Lambda,\sigma}$. Set $f := p \cdot f' + 1$; if $f \bmod q \notin \Lambda_q^\times$, resample. If $g \bmod q \notin \Lambda_q^\times$, resample. Return $sk = (f, g)$ and $pk = h = f^{-1}pg \in \Lambda_q^\times$.

Encryption: Given $m \in \Lambda_p^\vee$, sample $s, e \hookleftarrow \chi$ and return $c = hs + pe + m \in \Lambda_q^\vee$.

Decryption: Given c and secret key f, compute $(f \cdot c \bmod q) \bmod p$.

IND-CPA Security

IND-CPA: let $\mathcal{A}$ be a IND-CPA attack algorithm. Follow [SS11]: Use $\mathcal{A}$ to construct algorithm $\mathcal{B}$ against (a variant of) CLWE.

IND-CPA Security

IND-CPA: let $\mathcal{A}$ be a IND-CPA attack algorithm. Follow [SS11]: Use $\mathcal{A}$ to construct algorithm $\mathcal{B}$ against (a variant of) CLWE.

1. $\mathcal{B}$ has LWE sample $(a, c') = (a, as + e) \in \Lambda_q^{\times} \times \Lambda_q^{\vee}$.
2. $\mathcal{B}$ runs $\mathcal{A}$ with $pk = h = p \cdot a \in \Lambda_q$.
3. $\mathcal{A}$ outputs messages $m_0, m_1 \in \Lambda_p^{\vee}$, then $\mathcal{B}$ $b \hookleftarrow U(\{0,1\})$, computes $c = p \cdot c' + m_b$, and sends c to $\mathcal{A}$.
   So $\mathcal{A}$ has $(pa, pc' + m_b) = (h, hs + pe + m_b)$.
4. $\mathcal{A}$ guesses b' for b. If $b' = b$, $\mathcal{B}$ outputs 1. Else, $\mathcal{B}$ outputs 0.

Bounded ℓ

The proof of IND-CPA security requires h be uniform. We prove:

Let $\epsilon > 0$, q be a completely split prime, $p \in \mathcal{Z}(\Lambda_q^\times)$, and

$$\sigma \geq 4n^{3/2}\sqrt[4]{\ell}\sqrt{2\ln(32nq)}q^{\frac{1}{2}+2\epsilon}.$$

Let $y_i \in \Lambda_q$ and $z_i = -y_i p^{-1} \bmod q$ for $i = 1, 2$, and $D^\times_{\sigma,z_i}$ denote $D_{\Lambda,\sigma}$ restricted by rejection to $\Lambda_q^\times + z_i$. Then

$$\Delta\left(\frac{y_1 + pD^\times_{\sigma,z_1}}{y_2 + pD^\times_{\sigma,z_2}} \bmod q, U\left(\Lambda_q^\times\right)\right) \leq 2^{22n}q^{-8n\epsilon}.$$

Bounded ℓ

The proof of IND-CPA security requires h be uniform. We prove:

Let $\epsilon > 0$, q be a completely split prime, $p \in \mathcal{Z}(\Lambda_q^\times)$, and

$$\sigma \geq 4n^{3/2}\sqrt[4]{\ell}\sqrt{2\ln(32nq)}q^{\frac{1}{2}+2\epsilon}.$$

Let $y_i \in \Lambda_q$ and $z_i = -y_i p^{-1} \bmod q$ for $i = 1, 2$, and $D^\times_{\sigma,z_i}$ denote $D_{\Lambda,\sigma}$ restricted by rejection to $\Lambda_q^\times + z_i$. Then

$$\Delta\left(\frac{y_1 + pD^\times_{\sigma,z_1}}{y_2 + pD^\times_{\sigma,z_2}} \bmod q, U\left(\Lambda_q^\times\right)\right) \leq 2^{22n}q^{-8n\epsilon}.$$

$$\mathrm{disc}(\Lambda/\mathbb{Z}) := \left\{\det\left(\mathrm{Tr}\left(x_i x_j\right)\right)_{i,j=1}^{nd^2} \mid (x_1, \ldots, x_{nd^2}) \in \Lambda^{nd^2}\right\}$$

$$\mathrm{disc}(\Lambda/\mathbb{Z}) \leq (n\sqrt{\ell})^{4n}$$

Let $\mathcal{I}$ be an ideal of Λ. Then

$$\lambda_1(\mathcal{I}) \leq (nd^2)^{1/2} N_{\mathcal{A}/\mathbb{Q}}(\mathcal{I})^{1/nd^2}\,\mathrm{disc}(\Lambda/\mathbb{Z})^{1/2nd^2}.$$

Thankyou for Listening! And Future Work

- Trapdoor basis of CNTRU lattice
- Higher index CDAs?

Imperial College London

References

[PMS21]: Pellet-Mary, Stehle. On the hardness of the NTRU problem. Asiacrypt '21.

[FPMS22]: Felderhoff, Pellet-Mary, Stehle. On Module Unique-SVP and NTRU. Asiacrypt '22.

[DW21]: Ducas, van Woerden. NTRU Fatigue: How Stretched is Overstretched? Asiacrypt '21.

[CG05]: Coglianese, Goi. MaTRU: A New NTRU-Based Cryptosystem. Indocrypt '05.

[CPSWX19]: Chuengsatiansup, Prest, Stehle, Wallet, Xagawa. ModFalcon. Asia CCS '20.

[CKKS19]: Cheon, Kim, Kim, Son. A New Trapdoor over Module-NTRU Lattice and its Application to ID-based Encryption. Eprint archive 2019/1468.

[GMLV22]: Grover, M., Ling, Vehkalahti. Noncommutative Ring Learning With Errors From Cyclic Algebras. J. of Cryptology 35.

[SS11]: Stehle, Steinfeld. Making NTRU as Secure as Worst-Case Problems over Ideal Lattices. Eurocrypt '11.