Pseudorandom Functions and Lattices

Abhishek Banerjee[1] Chris Peikert[1] Alon Rosen[2]

[1]Georgia Tech

[2]IDC Herzliya

CRYPTO 2011 Rump Session
16 Aug 2011

Pseudorandom Functions

- A family $\mathcal{F} = \{F : \{0,1\}^k \to \{0,1\}\}$ s.t. $(F \leftarrow \mathcal{F}) \overset{c}{\approx}$ rand function.

  Oodles of applications in symmetric cryptography.

Pseudorandom Functions

- A family $\mathcal{F} = \{F : \{0,1\}^k \to \{0,1\}\}$ s.t. $(F \leftarrow \mathcal{F}) \overset{c}{\approx}$ rand function.

  Oodles of applications in symmetric cryptography.

1. Goldreich-Goldwasser-Micali [GGM'84]
   - ✔ Based on any PRG

Pseudorandom Functions

- A family $\mathcal{F} = \{F : \{0,1\}^k \to \{0,1\}\}$ s.t. $(F \leftarrow \mathcal{F}) \stackrel{c}{\approx}$ rand function.

  Oodles of applications in symmetric cryptography.

1. Goldreich-Goldwasser-Micali [GGM'84]
   - ✔ Based on any PRG
   - ✗ Inherently sequential, depth $\geq k$ for k-bit inputs

Pseudorandom Functions

- A family $\mathcal{F} = \{F : \{0,1\}^k \to \{0,1\}\}$ s.t. $(F \leftarrow \mathcal{F}) \stackrel{c}{\approx}$ rand function.

  Oodles of applications in symmetric cryptography.

1. Goldreich-Goldwasser-Micali [GGM'84]
   - ✔ Based on any PRG
   - ✗ Inherently sequential, depth $\geq k$ for k-bit inputs

2. Naor-Reingold/Naor-Reingold-Rosen [NR'95,NR'97,NRR'00]
   - ✔ Based on "synthesizers" or number theory (DDH, factoring)
   - ✔ Low-depth: NC^2, NC^1 or even TC^0

Pseudorandom Functions

- A family $\mathcal{F} = \{F : \{0,1\}^k \to \{0,1\}\}$ s.t. $(F \leftarrow \mathcal{F}) \overset{c}{\approx}$ rand function.

  Oodles of applications in symmetric cryptography.

1. Goldreich-Goldwasser-Micali [GGM'84]
   - ✔ Based on any PRG
   - ✗ Inherently sequential, depth $\geq k$ for k-bit inputs

2. Naor-Reingold/Naor-Reingold-Rosen [NR'95,NR'97,NRR'00]
   - ✔ Based on "synthesizers" or number theory (DDH, factoring)
   - ✔ Low-depth: NC^2, NC^1 or even TC^0
   - ✗ Huge circuits that need mucho preprocessing
   - ✗ No "post-quantum" construction under standard assumptions

Our Results

1. Low-depth, (relatively) small-circuit PRFs from (ring-)LWE

Our Results

1. Low-depth, (relatively) small-circuit PRFs from (ring-)LWE
   - ⋆ Synthesizer-based PRF in NC^2 (or TC^1) *a la* [NR'95]
   - ⋆ Direct construction in NC^1 (or TC^0) analogous to [NR'97,NRR'00]

Our Results

1. Low-depth, (relatively) small-circuit PRFs from (ring-)LWE
   - Synthesizer-based PRF in NC^2 (or TC^1) *a la* [NR'95]
   - Direct construction in NC^1 (or TC^0) analogous to [NR'97,NRR'00]
2. Main technique: "derandomization" of LWE: deterministic errors

“Learning With Rounding” (LWR)

Learning With Errors (LWE)   [Regev’05]

- Distinguish pairs $(\mathbf{a}_i\ ,\ b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ from uniform
- Interpretation: errors e_i “wipe out” lsb’s of the inner products

"Learning With Rounding" (LWR)

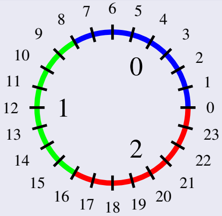
Learning With Errors (LWE) [Regev'05]

- Distinguish pairs $(\mathbf{a}_i\ ,\ b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ from uniform
- Interpretation: errors e_i "wipe out" lsb's of the inner products

Learning With Rounding (LWR) [This work]

- Let $q > p$ and define $\lfloor x \rceil_p = \lfloor (p/q) \cdot x \rceil \bmod p$.

  (Common in decryption to "remove noise.")



"Learning With Rounding" (LWR)

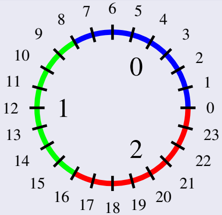
Learning With Errors (LWE) [Regev'05]

- Distinguish pairs $(\mathbf{a}_i\ ,\ b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ from uniform
- Interpretation: errors e_i "wipe out" lsb's of the inner products

Learning With Rounding (LWR) [This work]

- Let $q > p$ and define $\lfloor x \rceil_p = \lfloor (p/q) \cdot x \rceil \bmod p$.

  (Common in decryption to "remove noise.")



- LWR: distinguish pairs

$$\left(\mathbf{a}_i\ ,\ b_i = \lfloor \langle \mathbf{a}_i, \mathbf{s} \rangle \rceil_p\right) \in \mathbb{Z}_q^n \times \mathbb{Z}_p \quad \text{from uniform}$$

  Interpretation: "throw out" lsb's of the inner products

“Learning With Rounding” (LWR)

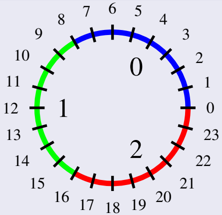
Learning With Errors (LWE) [Regev’05]

- Distinguish pairs $(\mathbf{a}_i \,,\, b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ from uniform
- Interpretation: errors e_i “wipe out” lsb’s of the inner products

Learning With Rounding (LWR) [This work]

- Let $q > p$ and define $\lfloor x \rceil_p = \lfloor (p/q) \cdot x \rceil \bmod p$.

  (Common in decryption to “remove noise.”)



- LWR: distinguish pairs

$$\left(\mathbf{a}_i \,,\, b_i = \lfloor \langle \mathbf{a}_i, \mathbf{s} \rangle \rceil_p\right) \in \mathbb{Z}_q^n \times \mathbb{Z}_p \quad \text{from uniform}$$

  Interpretation: “throw out” lsb’s of the inner products

- We prove LWE $\leq$ LWR for appropriate parameters

Synthesizer-Based PRF (*a la* [NR'95])

Synthesizer from LWR

- For random $\mathbf{a}_1, \mathbf{a}_2, \ldots$ and $\mathbf{s}_1, \mathbf{s}_2, \ldots$ (mod q),

$$\left(\lfloor \langle \mathbf{a}_i \; , \; \mathbf{s}_j \rangle \rceil_p \right)_{i,j} \stackrel{c}{\approx} \text{uniform mod } p$$

Synthesizer-Based PRF (*a la* [NR'95])

Synthesizer from LWR

- For random $\mathbf{a}_1, \mathbf{a}_2, \ldots$ and $\mathbf{s}_1, \mathbf{s}_2, \ldots \pmod q$,

$$\Big(\lfloor \langle \mathbf{a}_i \,,\, \mathbf{s}_j \rangle \rceil_p \Big)_{i,j} \overset{c}{\approx} \text{uniform mod } p$$

PRF on Domain $\{0,1\}^{k=2^d}$ (e.g. $d = 7$)

- (Public) moduli $q_d > q_{d-1} > \cdots > q_0$.
- Secret key is $2k$ square matrices $\mathbf{S}_{i,b} \in \mathbb{Z}_{q_d}^{n \times n}$ for $i \in [k]$, $b \in \{0,1\}$.

(Or ring elements $s_{i,b}$ using ring-LWR [LPR'10].)

Synthesizer-Based PRF (*a la* [NR'95])

Synthesizer from LWR

- For random $\mathbf{a}_1, \mathbf{a}_2, \ldots$ and $\mathbf{s}_1, \mathbf{s}_2, \ldots \pmod q$,

$$\left(\lfloor \langle \mathbf{a}_i \ , \ \mathbf{s}_j \rangle \rceil_p \right)_{i,j} \stackrel{c}{\approx} \text{uniform mod } p$$

PRF on Domain $\{0,1\}^{k=2^d}$ (e.g. $d = 7$)

- (Public) moduli $q_d > q_{d-1} > \cdots > q_0$.
- Secret key is $2k$ square matrices $\mathbf{S}_{i,b} \in \mathbb{Z}_{q_d}^{n \times n}$ for $i \in [k]$, $b \in \{0,1\}$.

  (Or ring elements $s_{i,b}$ using ring-LWR [LPR'10].)
- Depth $d = \lg k$ tree of LWR synthesizers:

$$F(x_1 \cdots x_8) =$$

$$\left\lfloor \left\lfloor \lfloor \mathbf{S}_{1,x_1} \cdot \mathbf{S}_{2,x_2} \rceil_{q_2} \cdot \lfloor \mathbf{S}_{3,x_3} \cdot \mathbf{S}_{4,x_4} \rceil_{q_2} \right\rceil_{q_1} \cdot \left\lfloor \lfloor \mathbf{S}_{5,x_5} \cdot \mathbf{S}_{6,x_6} \rceil_{q_2} \cdot \lfloor \mathbf{S}_{7,x_7} \cdot \mathbf{S}_{8,x_8} \rceil_{q_2} \right\rceil_{q_1} \right\rceil_{q_0}$$

Shallower: A Direct Construction

- Public moduli $q > p$.
- Secret key is ring elements $a, s_1, \ldots, s_k$ modulo q

Shallower: A Direct Construction

- Public moduli $q > p$.
- Secret key is ring elements $a, s_1, \ldots, s_k$ modulo q
- "Rounded subset-product" function:

$$F(x_1 \cdots x_k) = \left\lfloor a \cdot \prod_{i=1}^{k} s_i^{x_i} \bmod q \right\rceil_p .$$

- Very efficient evaluation in TC^0, by reduction to subset-sum

Shallower: A Direct Construction

- Public moduli $q > p$.
- Secret key is ring elements $a, s_1, \ldots, s_k$ modulo q
- "Rounded subset-product" function:

$$F(x_1 \cdots x_k) = \left\lfloor a \cdot \prod_{i=1}^{k} s_i^{x_i} \bmod q \right\rceil_p .$$

- Very efficient evaluation in TC^0, by reduction to subset-sum

Details: ePrint report #2011/401