Authenticated Key Exchange from Ring Learning with Errors

Jiang Zhang Zhenfeng Zhang Jintai Ding
Michael Snook Özgür Dagdelen

DIMACS Workshop on the Mathematics of Post-Quantum Cryptography

January 16, 2015

Learning with Errors [2006, Regev]

$$\underbrace{\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}}_{\vec{b}} = \underbrace{\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix}}_{\vec{s}} + \underbrace{\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix}}_{\vec{e}}$$

- Approximate system over $\mathbb{Z}_q$
- Hard to find $\vec{s}$ from $A, \vec{b}$.
- Hard to tell if $\vec{s}$ even exists
- Reduction to lattice approximation problems

Ring LWE

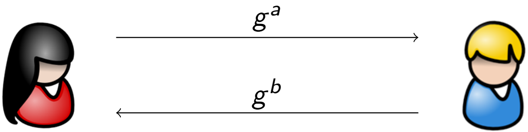
Definition

Let n be a power of 2, $q \equiv 1 \pmod{2n}$ prime. Define the ring

$$R_q = \frac{\mathbb{Z}_q[x]}{(x^n + 1)}.$$

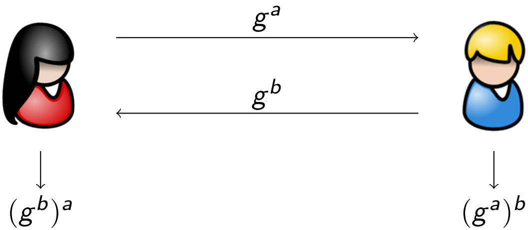
- Again, $b = as + e$ hard to find s
- Hard to distinguish from uniform b
- Approximation problems on *ideal* lattices
- More efficient than standard LWE

Diffie-Hellman Key Exchange



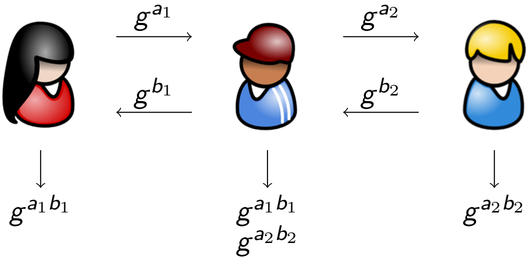
- Public g generates finite group

Diffie-Hellman Key Exchange



- Public g generates finite group
- Since $(g^a)^b = (g^b)^a = g^{ab}$, key is shared
- Security based on discrete logarithm

Man-in-the-Middle Attack



What Key Exchange Needs

- Shared key

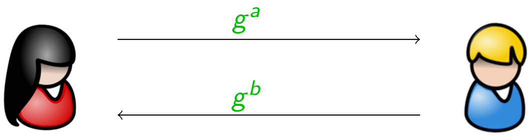
What Key Exchange Needs

- Shared key
- Authentication of each party—long term keys

What Key Exchange Needs

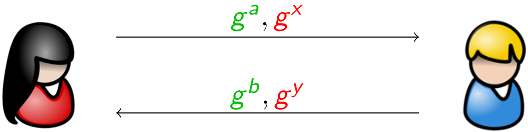
- Shared key
- Authentication of each party—long term keys
- Forward security—single-time keys

HMQV Protocol



- Static keys a, b; tied to each party's identity.

HMQV Protocol



- Static keys a, b; tied to each party's identity.
- Ephemeral keys x, y: forward security.

HMQV Protocol

$$\xrightarrow{g^a,\ g^x}$$

$$\xleftarrow{g^b,\ g^y}$$

$$\underbrace{\left(g^y (g^b)^e\right)^{x+da}}_{\sigma_A} \qquad\qquad \underbrace{\left(g^x (g^a)^d\right)^{y+eb}}_{\sigma_B}$$

- Static keys a, b; tied to each party's identity.
- Ephemeral keys x, y: forward security.
- Publicly derivable computations d, e.

HMQV Protocol

$$\xrightarrow{g^a,\ g^x}$$

$$\xleftarrow{g^b,\ g^y}$$

$$\underbrace{(g^y(g^b)^e)^{x+da}}_{\sigma_A} = g^{(y+eb)(x+da)} = \underbrace{(g^x(g^a)^d)^{y+eb}}_{\sigma_B}$$

- Static keys a, b; tied to each party's identity.
- Ephemeral keys x, y: forward security.
- Publicly derivable computations d, e.
- Shared key is $K = H(\sigma_A) = H(\sigma_B)$

The Post-Quantum World

- DH, HMQV Rely on hardness of discrete logarithm: vulnerable to quantum algorithms
- Ding's original Goal: create an analogue to DH based off hard lattice problems

Diffie-Hellman from Ideal Lattices

$$\xrightarrow{\quad p_A = as_A + 2e_A \quad}$$

$$\xleftarrow{\quad p_B = as_B + 2e_B \quad}$$

- Public $a \in R_q$. Acts like generator g in DH.

Diffie-Hellman from Ideal Lattices

$$\xrightarrow{p_A = as_A + 2e_A}$$

$$\xleftarrow{p_B = as_B + 2e_B}$$

$$k_A = s_A p_B \qquad\qquad k_B = p_A s_B$$

- Public $a \in R_q$. Acts like generator g in DH.

Diffie-Hellman from Ideal Lattices

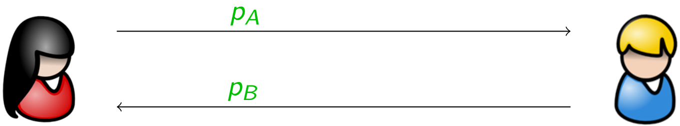
$$\xrightarrow{p_A = as_A + 2e_A}$$

$$\xleftarrow{p_B = as_B + 2e_B}$$

$$k_A = s_A p_B \quad \approx \quad k_B = p_A s_B$$

- Public $a \in R_q$. Acts like generator g in DH.
- Each side's key is only *approximately* equal to the other.
- Difference is even—same low bits.
- No authentication—MitM

HMQV from Ideal Lattices



- p_A, p_B as above. Public, static keys for authentication

HMQV from Ideal Lattices

$$p_A, x_A = ar_A + 2f_A \longrightarrow$$

$$\longleftarrow p_B, y_B = ar_B + 2f_B$$

- p_A, p_B as above. Public, static keys for authentication
- x_A, y_B same form. Forward secrecy.

HMQV from Ideal Lattices

$$\xrightarrow{p_A,\ x_A = ar_A + 2f_A}$$

$$\xleftarrow{p_B,\ y_B = ar_B + 2f_B}$$

$$\downarrow \qquad\qquad \downarrow$$

$$k_A = (p_B d + y_B)(s_A c + r_A) + 2dg_A \qquad k_B = (p_A c + x_A)(s_B d + r_B) + 2cg_B$$

- p_A, p_B as above. Public, static keys for authentication
- x_A, y_B same form. Forward secrecy.
- c, d publicly derivable; g_A, g_B random, small.

Key Derivation

Obtaining shared secret from approximate shared secret:

$$\begin{aligned}
k_A &= (k_A^{(0)}, k_A^{(1)}, \ldots, k_A^{(n-1)}) \\
k_B &= (k_B^{(0)}, k_B^{(1)}, \ldots, k_B^{(n-1)}) \\
\tilde{g} &= (g^{(0)}, g^{(1)}, \ldots, g^{(n-1)}) \\
k_A - k_B &= 2\tilde{g} \\
k_A &\equiv k_B \pmod 2
\end{aligned}$$

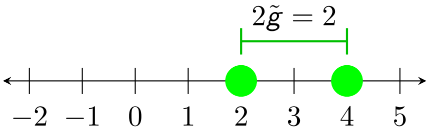
Key Derivation

Obtaining shared secret from approximate shared secret:

$$k_A = (k_A^{(0)}, k_A^{(1)}, \dots, k_A^{(n-1)})$$
$$k_B = (k_B^{(0)}, k_B^{(1)}, \dots, k_B^{(n-1)})$$
$$\tilde{g} = (g^{(0)}, g^{(1)}, \dots, g^{(n-1)})$$
$$k_A - k_B = 2\tilde{g}$$
$$k_A \equiv k_B \pmod{2}$$

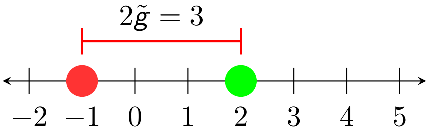
- Each $k_A^{(j)} = k_B^{(j)} + 2g^{(j)}$.
- Each $g^{(j)}$ is small ($|g^{(j)}| < \frac{q}{8}$).
- Matching coefficients differ by small multiple of 2
- Take each coefficient mod 2, get n bit secret

Wrap-around Illustrated



- Difference 2, both even.

Wrap-around Illustrated



- Difference 2, both even.
- But wait! If $q = 5$, $\mathbb{Z}_q = \{-2, -1, 0, 1, 2\}$.
- 4 becomes -1, now parities disagree!

Compensating for Wrap-Around

- Recall: $|g^{(j)}| < \frac{q}{8}$
- Define $E = \{-\lfloor \frac{q}{4} \rfloor, \ldots, \lfloor \frac{q}{4} \rceil\}$. Middle half of $\mathbb{Z}_q$.
- If $k_B^{(j)} \in E$, no wrap-around occurs; $k_A^{(j)} \equiv k_B^{(j)}$.
- If $k_B^{(j)} \notin E$, then $k_B^{(j)} + \frac{q-1}{2} \in E$
- If $k_B^{(j)} \notin E$, $k_A^{(j)} + \frac{q-1}{2} \equiv k_B^{(j)} + \frac{q-1}{2}$.

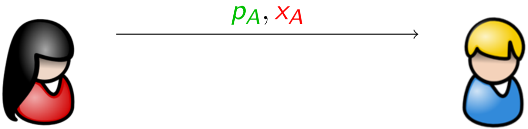
Wrap-around Defeated

Define $w_B^{(j)} = \begin{cases} 0 & k_B^{(j)} \in E, \\ 1 & k_B^{(j)} \notin E. \end{cases}$ Then $k_B^{(j)} + w_B^{(j)} \frac{q-1}{2} \in E$.

Also, $k_B^{(j)} + w_B^{(j)} \frac{q-1}{2} \equiv k_A^{(j)} + w_B^{(j)} \frac{q-1}{2} \pmod 2$.

- $k_B^{(j)} + w_B^{(j)} \frac{q-1}{2} \bmod q \bmod 2 = k_A^{(j)} + w_B^{(j)} \frac{q-1}{2} \bmod q \bmod 2$.
- Wrap-around correction $w_B = (w_B^{(0)}, w_B^{(1)}, \ldots, w_B^{(n-1)})$
- $\sigma_B = k_B + w_B \frac{q-1}{2} \bmod 2$.
- $\sigma_A = k_A + w_B \frac{q-1}{2} \bmod 2$.

HMQV from Ideal Lattices—Corrected



HMQV from Ideal Lattices—Corrected

$$\xrightarrow{\quad p_A,\, x_A \quad}$$

$$\downarrow$$

$$k_B$$

HMQV from Ideal Lattices—Corrected

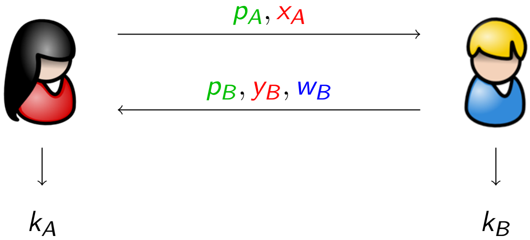
$$\xrightarrow{p_A,\, x_A}$$

$$\xleftarrow{p_B,\, y_B,\, w_B}$$

$$\downarrow$$

$$k_B$$

HMQV from Ideal Lattices—Corrected



HMQV from Ideal Lattices—Corrected

$$\xrightarrow{p_A,\ x_A}$$

$$\xleftarrow{p_B,\ y_B,\ w_B}$$

$$\begin{array}{ccccc} \downarrow & & & & \downarrow \\ k_A & \longrightarrow & \sigma_A = \sigma_B & \longleftarrow & k_B \end{array}$$

HMQV from Ideal Lattices—Corrected

$$\xrightarrow{p_A,\ x_A}$$

$$\xleftarrow{p_B,\ y_B,\ w_B}$$

$$\begin{tikzcd} k_A \arrow[r] & \sigma_A = \sigma_B \arrow[d, "H"] & k_B \arrow[l] \\ & \text{Key} & \end{tikzcd}$$

Thank You