Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices

Chris Peikert   Alon Rosen

Presented By
Rachit Garg
CS14B050

IIT Madras

Motivation

1. Collision-resistant hash functions are one of the most widely-employed cryptographic primitives.
2. Usually faster heuristic constructions such as MD5 and SHA-1 are employed. [cryptanalysis possible? [WYY05],[WY05]]
3. Paper proposes a practical hash function with rigorous security guarantees.

Definitions

- **Collision resistant functions**: A function family $\{f_a\}, a \in A$ is said to be collision-resistant if given a uniformly chosen $a \in A$, it is infeasible to find elements $x_1 \neq x_2$ so that $f_a(x_1) = f_a(x_2)$.

Definitions

- **Collision resistant functions**: A function family $\{f_a\}, a \in A$ is said to be collision-resistant if given a uniformly chosen $a \in A$, it is infeasible to find elements $x_1 \neq x_2$ so that $f_a(x_1) = f_a(x_2)$.
- **Generalized Knapsacks**: For a ring R, key $a = (a_1, ..., a_m) \in R^m$, and input $x = (x_1, ..., x_m)$.
  $f_a(x) = \sum_{i=1}^{m} a_i x_i$.

Definitions

- **Collision resistant functions**: A function family $\{f_a\}, a \in A$ is said to be collision-resistant if given a uniformly chosen $a \in A$, it is infeasible to find elements $x_1 \neq x_2$ so that $f_a(x_1) = f_a(x_2)$.
- **Generalized Knapsacks**: For a ring R, key $a = (a_1, ..., a_m) \in R^m$, and input $x = (x_1, ..., x_m)$.
  $f_a(x) = \sum_{i=1}^{m} a_i x_i$.
- **Cyclic Lattices**: A lattice is said to be cyclic if for any vector $x \in$, its cyclic rotation also belongs to . The cyclic rotation of $x = (x_0, ..., x_{n1})^T \in R^n$ is defined as $(x_{n-1}, x_0, ..., x_{n-2})^T$.

Micciancio's Result

- Micciancio suggested a specific choice of the ring R and a large subset S(for the input) for which inverting the function (for random a, x) is at least as hard as solving certain worst-case problems on cyclic lattices [Mic02].
- Here, for a different choice of $S \subset R$, the generalized knapsack function can enjoy even stronger cryptographic properties.

Micciancio's Result

- Micciancio suggested a specific choice of the ring R and a large subset S(for the input) for which inverting the function (for random a, x) is at least as hard as solving certain worst-case problems on cyclic lattices [Mic02].
- Here, for a different choice of $S \subset R$, the generalized knapsack function can enjoy even stronger cryptographic properties.
- **Generalized Knapsacks**: For a ring R, key $a = (a_1, ..., a_m) \in R^m$, and input $x = (x_1, ..., x_m)$.
  $f_a(x) = \sum_{i=1}^{m} a_i x_i$. $x_i \in S$

Paper Idea

- Formulated a reduction showing that for cyclic lattices of prime dimension n, the short independent vectors problem SIVP reduces to (a slight variant of) the shortest vector problem SVP with only a factor of 2 loss in approximation factor.
- Note that factor of loss in approximation is not trivial and the prime dimension constraint is not restricting.

Paper Idea

- Formulated a reduction showing that for cyclic lattices of prime dimension n, the short independent vectors problem SIVP reduces to (a slight variant of) the shortest vector problem SVP with only a factor of 2 loss in approximation factor.
- Note that factor of loss in approximation is not trivial and the prime dimension constraint is not restricting.
- Showed a worst case to average case reduction, where the worst case problem was SVP with an approximation factor up to $\tilde{O}(n)$.

Papers Results

- The choice of ring admits very efficient implementations of the knapsack function: using a Fast Fourier Transform algorithm. The resulting time complexity of the function is $O(mn\ .\ \mathrm{poly}(\log n))$, with key size $O(mn \log n)$.

Papers Results

- The choice of ring admits very efficient implementations of the knapsack function: using a Fast Fourier Transform algorithm. The resulting time complexity of the function is $O(mn \,.\, \text{poly}(\log n))$, with key size $O(mn \log n)$.

	Security	**Efficiency**	**Lattice Class**	**Assumption**	**Approx. Factor**
Ajtai	CRHF	$O(n^2)$	General	SVP etc.	poly(n)
Cai, Nerurkar	CRHF	$O(n^2)$	General	SVP etc.	$n^{4+\epsilon}$
Micciancio	OWF	$\tilde{O}(n)$	Cyclic	GDD	$n^{1+\epsilon}$
Micciancio, Regev	CRHF	$O(n^2)$	General	SVP etc.	$\tilde{O}(n)$
This work	CRHF	$\tilde{O}(n)$	Cyclic	SVP etc.	$\tilde{O}(n)$

Table: Comparison of results in lattice-based cryptographic functions with worst-case to average case security reductions, to date. Efficiency means the key size and computation time, as a function of the lattice dimension n. Security denotes the functions main cryptographic property.

Some More Definitions

Cyclotomic Subspace

$$H_\Phi = \{x \in \mathbb{R}^n : \Phi(\alpha) \text{ divides } x(\alpha) \in \mathbb{R}[\alpha]\}.$$

Some More Definitions

Cyclotomic Subspace

$$H_\Phi = \{x \in \mathbb{R}^n : \Phi(\alpha) \text{ divides } x(\alpha) \in \mathbb{R}[\alpha]\}.$$

SubSIVP

The cyclotomic (generalized) short independent vectors problem, $SubSIVP_\gamma^\zeta$, given an n-dimensional full-rank cyclic lattice basis B and an integer polynomial $\Phi(\alpha) \neq 0 \bmod (\alpha^n - 1)$ that divides $\alpha^n - 1$, asks for a set of $dim(H_\Phi)$ linearly independent (sub)lattice vectors $S \subset \mathcal{L}(B) \cap H_\Phi$ such that $||S|| \leq \gamma(n)\zeta(\mathcal{L}(B) \cap H_\Phi)$.

Some More Definitions

SubSVP

The cyclotomic (generalized) short vectors problem, $SubSVP_{\gamma}^{\zeta}$, given an n-dimensional full-rank cyclic lattice basis B and an integer polynomial $\Phi(\alpha) \neq 0 \bmod (\alpha^n - 1)$ that divides $\alpha^n - 1$, asks for a (sub)lattice vector $c \in \mathcal{L}(B) \cap H_{\Phi}$ such that $||c|| \leq \gamma(n)\zeta(\mathcal{L}(B) \cap H_{\Phi})$.

Some More Definitions

SubSVP

The cyclotomic (generalized) short vectors problem, $SubSVP_{\gamma}^{\zeta}$, given an n-dimensional full-rank cyclic lattice basis B and an integer polynomial $\Phi(\alpha) \neq 0 \bmod (\alpha^n - 1)$ that divides $\alpha^n - 1$, asks for a (sub)lattice vector $c \in \mathcal{L}(B) \cap H_{\Phi}$ such that $||c|| \leq \gamma(n)\zeta(\mathcal{L}(B) \cap H_{\Phi})$.

SubIncSVP

The cyclotomic (generalized) short vectors problem, $SubIncSVP_{\gamma}^{\zeta}$, given an n-dimensional full-rank cyclic lattice basis B and an integer polynomial $\Phi(\alpha) \neq 0 \bmod (\alpha^n - 1)$ that divides $\alpha^n - 1$, and a nonzero (sub)lattice vector $c \in \mathcal{L}(B) \cap H_{\Phi}$ such that $||c|| > \gamma(n)\zeta(\mathcal{L}(B) \cap H_{\Phi})$, asks for a non-zero (sub)lattice vector $c' \in \mathcal{L}(B) \cap H_{\Phi}$ such that $||c'|| \leq ||c||/2$.

Intuition

The divisors of $(\alpha^n - 1)$ in $\mathbb{Z}[\alpha]$ correspond to special cyclotomic linear subspaces of $\mathbb{R}^n$. These subspaces admit a natural partitioning into complementary pairs of orthogonal subspaces. Even more importantly, the subspaces are closed under cyclic rotation of vector coordinates, and under certain other conditions, these rotations are linearly independent. These facts imply a new connection between the SIVP and SVP problems in cyclic lattices.

Lemma H_Φ is closed under rotation, thats if $c \in H_\Phi$, then $rot(c) \in H_\Phi$.
Proof:

$$rot(c) = \alpha \cdot c(\alpha) \bmod (\alpha^n - 1)$$
$$(\alpha^n - 1) | rot(c) - \alpha \cdot c(\alpha)$$
$$\Phi(\alpha) | rot(c) - \alpha \cdot c(\alpha)$$
$$\Phi(\alpha) | rot(c)$$

Lemmas

Lemma H_Φ is closed under rotation, thats if $c \in H_\Phi$, then $rot(c) \in H_\Phi$.
Proof:

$$rot(c) = \alpha \cdot c(\alpha) \text{ mod } (\alpha^n - 1)$$
$$(\alpha^n - 1) | rot(c) - \alpha \cdot c(\alpha)$$
$$\Phi(\alpha) | rot(c) - \alpha \cdot c(\alpha)$$
$$\Phi(\alpha) | rot(c)$$

Lemma Let $c \in \mathbb{Z}^n$, and suppose $\Phi(\alpha) \in \mathbb{Z}[\alpha]$ divides $(\alpha^n - 1)$ and is coprime to $c(\alpha)$. Then $c, rot(c)...., rot^{deg(\Phi)-1}(c)$ are linearly independent.

Lemmas

Lemma H_Φ is closed under rotation, thats if $c \in H_\Phi$, then $rot(c) \in H_\Phi$.
Proof:

$$rot(c) = \alpha \cdot c(\alpha) \bmod (\alpha^n - 1)$$
$$(\alpha^n - 1) | rot(c) - \alpha \cdot c(\alpha)$$
$$\Phi(\alpha) | rot(c) - \alpha \cdot c(\alpha)$$
$$\Phi(\alpha) | rot(c)$$

Lemma Let $c \in \mathbb{Z}^n$, and suppose $\Phi(\alpha) \in \mathbb{Z}[\alpha]$ divides $(\alpha^n - 1)$ and is coprime to $c(\alpha)$. Then $c, rot(c) \ldots, rot^{deg(\Phi)-1}(c)$ are linearly independent.

Lemma Let $a, b \in \mathbb{R}^n$ with $a(\alpha) \cdot b(\alpha) = 0 \bmod (\alpha^n - 1)$. Then $\langle a, b \rangle = 0$.

Lemmas

Lemma H_Φ is closed under rotation, thats if $c \in H_\Phi$, then $rot(c) \in H_\Phi$.
Proof:

$$rot(c) = \alpha \cdot c(\alpha) \bmod (\alpha^n - 1)$$
$$(\alpha^n - 1) | rot(c) - \alpha \cdot c(\alpha)$$
$$\Phi(\alpha) | rot(c) - \alpha \cdot c(\alpha)$$
$$\Phi(\alpha) | rot(c)$$

Lemma Let $c \in \mathbb{Z}^n$, and suppose $\Phi(\alpha) \in \mathbb{Z}[\alpha]$ divides $(\alpha^n - 1)$ and is coprime to $c(\alpha)$. Then $c, rot(c)...., rot^{deg(\Phi)-1}(c)$ are linearly independent.
Lemma Let $a, b \in \mathbb{R}^n$ with $a(\alpha) \cdot b(\alpha) = 0 \bmod (\alpha^n - 1)$. Then $\langle a, b \rangle = 0$.
Lemma H_Φ is a linear subspace of $\mathbb{R}^n$ of dimension $n - deg(\Phi)$.

Reductions

Proposition For any $\zeta, \gamma(n)$, there is a deterministic, polynomial-time sublattice-preserving reduction from $SubSVP^{\zeta}_{\gamma}$ to $SubIncSVP^{\zeta}_{\gamma}$.

Proposition For any $\zeta, \gamma(n)$, there is a deterministic, polynomial-time sublattice-preserving reduction from $SubSVP_\gamma^\zeta$ to $SubIncSVP_\gamma^\zeta$.
Informal Proof:
Given an instance of $(B, \Phi(\alpha))$, iteratively reduce the length of c by invoking oracle for $SubIncSVP_\gamma^\zeta$ on $(B, \Phi(\alpha), c)$. If oracle fails we have solved $SubSVP_\gamma^\zeta$. (Note it is easy to show that the iterative process lasts poly number of times).

Reductions

Proposition For any $\zeta, \gamma(n)$, there is a deterministic, polynomial-time sublattice-preserving reduction from $SubSIVP_\gamma^\zeta$ to $SubSVP_\gamma^\zeta$ which makes one oracle call where $\Phi(\alpha) = (\alpha^n - 1)/\Phi_k(\alpha)$ for some $k|n$.

Reductions

Proposition For any $\zeta, \gamma(n)$, there is a deterministic, polynomial-time lattice-preserving reduction from $SIVP_{\max(n, 2\gamma)}$ on a cyclic lattice of prime dimension to $SubSVP_{\gamma}^{\lambda_1}$ which makes one oracle call where $\Phi(\alpha) = \Phi_1(\alpha) = \alpha - 1$.

Proposition For any $\zeta, \gamma(n)$, there is a deterministic, polynomial-time lattice-preserving reduction from $SIVP_{\max(n,2\gamma)}$ on a cyclic lattice of prime dimension to $SubSVP_{\gamma}^{\lambda_1}$ which makes one oracle call where $\Phi(\alpha) = \Phi_1(\alpha) = \alpha - 1$.

Intuition:

The main idea behind the proof is as follows: first, we use the *SubSVP* oracle to find a short vector in $\mathcal{L}(B) \cap H_{\Phi_1}$, then rotate it to yield $n-1$ linearly independent vectors. For the nth vector, we take the shortest vector in $\mathcal{L}(B) \cap H_{\Phi_n}$, which can be found efficiently; furthermore, it is an n-approximation to the shortest vector in $L(B) \setminus H_{\Phi_1}$.

$\mathbf{s}_i = \mathbf{b}_i \otimes (1, 1, ...) = (s_i, s_i....s_i) \in \mathcal{L}(B)$. Let $g = gcd(s_1, s_2....s_n)$.
Output $\mathbf{g} = (g, g....g)$ as the shortest vector.

Reductions

Proposition For any $\gamma(n)$, there is a deterministic, polynomial-time lattice-preserving reduction from $SVP_{\max(n,\gamma)}$ on a cyclic lattice of prime dimension to $SubSVP_{\gamma}^{\lambda_1}$ which makes one oracle call where $\Phi(\alpha) = \Phi_1(\alpha) = \alpha - 1$.

Idea:

The idea is same as in the previous reduction where we used the oracle to solve $SIVP$. To use the oracle to solve SVP, output minimum of norm of c, and the norm of the n^{th} vector as chosen before.

Finding Collisions

Generalized Compact Knapsacks: For any ring R, subset $S \subset R$ and integer $m \geq 1$, the generalized function family $H(R, S, m) = \{f_a : S^m \rightarrow R\}_{a \in R^m}$ is defined by:

$$f_a(x) = \sum_{i=1}^{m} x_i \cdot a_i$$

Observation: f_A is linear:

$$f_A(X) + f_A(X') = f_A(X + X')$$

For random key A, to find a collision with X' it suffices to find a non-zero $X \in S^m$ such that $f_A(X) = 0$, and $||X||_\infty$ is small.(So that the bound on $||X||_\infty$ is still satisfied).

Finding Collisions

$$f_a(x) = \sum_{i=1}^{m} x_i(\alpha) \cdot a_i(\alpha) mod(\alpha^n - 1)$$

We define $X = (x_1, x_2 ... x_m)$ as follows, for any q that is a divisor of n:

$$x_1(\alpha) = \frac{\alpha^n - 1}{\alpha^q - 1}$$
$$x_j(\alpha) = 0 | j \neq 1$$

Now $f_A(X) = 0$ if $a_1(\alpha)$ is divisible by $a^q - 1$, note that this happens with probability $1/p^q$. Over a uniform choice of A, so we have found a specific $X \neq 0$, such that $f_A(X) \neq 0$ with non-negligible probability.

Removing Collisions

The fact enabling this attack is that $(\alpha^n - 1)$ is not irreducible in $\mathbb{Z}_p[\alpha]$. So it easy to find $x(\alpha)$ with small coefficients such that $a(\alpha)x(\alpha) = 0 \bmod (\alpha^n - 1)$ and for each divisor of $(\alpha^n - 1)$ either $x(\alpha) = 0$ or $a(\alpha) = 0$.

Removing Collisions

The fact enabling this attack is that $(\alpha^n - 1)$ is not irreducible in $\mathbb{Z}_p[\alpha]$. So it easy to find $x(\alpha)$ with small coefficients such that $a(\alpha)x(\alpha) = 0 \bmod (\alpha^n - 1)$ and for each divisor of $(\alpha^n - 1)$ either $x(\alpha) = 0$ or $a(\alpha) = 0$.

To prevent this we enforce an algebraic constraint on X, informally we require every $x_i(\alpha)$ to be divisible over $\mathbb{Z}[\alpha]$ by $\frac{\alpha^n - 1}{\Phi_k(\alpha)}$ for some fixed k dividing n. Now essentially the evaluation is performed mod $\Phi_k(\alpha)$. And hence we show a reduction.

$$S_{D,\Phi} = \{x \in \mathbb{Z}_p^n : ||x||_\infty \leq D \text{ and } \Phi(\alpha) \text{ divides } x_{\mathbb{Z}}(\alpha) \text{ in } \mathbb{Z}[\alpha]\}$$

The main reduction

We reduce from $SubIncSVP_{\gamma}^{\eta_\epsilon}$ to collision function $H(\mathbb{Z}_{p(n)}, S_{D(n),\Phi}, m(n))$. Note that this is a worst case to average case reduction on cyclic lattices. Here we try to show three main properties:

1. Sampling an average instance.
2. Outputting a new vector and showing that it belongs in $\mathcal{L}(B) \cap H$.
3. It has a norm smaller than half the norm of input vector in *SubIncSVP*, with non negligible probability.

The algorithm

1. For $i = 1$ to m,
   - Generate uniform $\mathbf{v}_i \in \mathcal{L}(B) \cap H \cap P(Rot^d(\mathbf{c}))$. [MG02]
   - Generate noise $\mathbf{y}_i \in H$, according to $D_{H,s}$ for $s = 2||c||/\gamma(n)$. Let $y_i' = y_i \bmod P(B)$.
   - Choose b_i (as described below) so that $Rot^n(\mathbf{c}) \cdot \mathbf{b} = \mathbf{v_i} + \mathbf{y_i'}$, and let $\mathbf{a_i} = \lfloor \mathbf{b_i} \cdot p \rceil$

The algorithm

1. For $i = 1$ to m,
   - Generate uniform $\mathbf{v}_i \in \mathcal{L}(B) \cap H \cap P(Rot^d(\mathbf{c}))$. [MG02]
   - Generate noise $\mathbf{y}_i \in H$, according to $D_{H,s}$ for $s = 2||c||/\gamma(n)$. Let $y_i' = y_i \bmod P(B)$.
   - Choose b_i so that $Rot^n(\mathbf{c}) \cdot \mathbf{b} = \mathbf{v_i} + \mathbf{y_i'}$, and let $\mathbf{a_i} = \lfloor \mathbf{b_i} \cdot p \rceil$
2. Pass A to collision finding oracle, and get collission pairs X, X', let $Z = X - X'$, such that $||Z||_\infty \le 2D$ and $\Phi(\alpha)$ divides every $z_i(\alpha)$.
3. Output

$$c' = \sum_{i=1}^{m} (\mathbf{v_i} + \mathbf{y_i'} - \mathbf{y_i}) \otimes \mathbf{z_i} - \mathbf{c} \otimes \frac{\sum_{i=1}^{m} \mathbf{a_i} \otimes \mathbf{z_i}}{p}$$

Correctness

1. It is uniform because for choosing b we sample the latter half uniformly from I^{n-d}. And the former half is chosen such that $(I_{d\times d})^{-1}(v_i + y_i' - w)$, where $w = Rot^n(c) \cdot (0, 0, ...(b_i)_d, .., (b_i)_n)^T$. Since y' is statistically uniform from our choice of c such that the spread in the guassian is more than the smoothing parameter, and v is uniform. We have the former half is uniform, and since the latter half is already sampled uniformly we have that the $b_i's$ are uniform.

Correctness

1. Convolution of a lattice vector with an integer vector also lies in the lattice, hence the second property holds true. Note that the second term in the output vector is c convoluted with an integer vector due to a convolution z being congruent to zero mod p as we have constructed z from a collision.

Putting it together

Showed a reduction from *SubIncSVP* to generalized knapsack with a specific choice of ring. Showed a reduction from $SVP_{\max(n,\gamma)}$ to *SubSVP*, and *SubSVP* to *SubIncSVP*. Hence with appropriate parameters, the given choice of function is collision resistant assuming hardness of SVP, with gamma approximation on cyclic lattices.

References

Daniele Micciancio and Shafi Goldwasser, *Complexity of Lattice Problems: a cryptographic perspective*, The Kluwer International Series in Engineering and Computer Science, vol. 671, Kluwer Academic Publishers, 2002.

Daniele Micciancio, *Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions*, Proceedings of the 43rd Symposium on Foundations of Computer Science (Washington, DC, USA), FOCS '02, IEEE Computer Society, 2002, pp. 356–365.

Xiaoyun Wang and Hongbo Yu, *How to break md5 and other hash functions*, Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques (Berlin, Heidelberg), EUROCRYPT'05, Springer-Verlag, 2005, pp. 19–35.

Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, *Finding collisions in the full sha-1*, Proceedings of the 25th Annual International Conference on Advances in Cryptology (Berlin, Heidelberg), CRYPTO'05, Springer-Verlag, 2005, pp. 17–36.

The End