Indian Institute of Technology Delhi

COL 759 - Cryptography

Assignment 4

Garv Nagori, Naman Agarwal
2021CS10549, 2021CS10555

Contents

§1 Question 1

§1.1 Part a)

> **Claim 1.1 —** If there exists a p.p.t. algorithm A that breaks the collision-resistance property of this hash function family with non negligible probability ϵ, then there exists a p.p.t. algorithm B that breaks the discrete log assumption with non-negligible probability ϵ'.

Reduction for Discrete Log Challenger

Challenger $\mathcal{C}$		**Reduction** $\mathcal{B}$		**Adversary** $\mathcal{A}$
$(q, g, .) \leftarrow G(1^\lambda)$				
$a \leftarrow \mathbb{Z}_q$	$\xrightarrow{(q\ ,\ g\ ,\ A = g^a\ )}$	Sample $(\lambda - 1)\alpha_i \leftarrow\$\ \mathbb{Z}_q$ s.t. $g^{\alpha_i} \neq A$		
		Key k = random permutation of A andα_i		
			$\xrightarrow{k}$	
	$\xleftarrow{a}$	Compute a as shown below	$\xleftarrow[\text{x' } = (x'_0,\ x'_1\ ,\ ...)]{\text{x } = (x_0,\ x_1\ ,\ ...)}$	

To get a , we will check if the coefficient of A in both are different. If yes, we can calculate "a" using equality of hash functions $\sum_{i=1}^{n} \alpha_i \cdot x_i = \sum_{i=1}^{n} \alpha_i \cdot x_i'$ with the only unknown term being a.
We know that there has to be atleast 2 seperate indices for which $x_i \neq x_i'$ for x and x' to be a collision. Also the probability of winning depends on the coefficients for A being different so the probability of breaking discrete log challenger is $\epsilon' = \epsilon/n$

§1.2 Part b)

Given hash function $h_{N,e,z} : \mathbb{Z}_N^* \times \mathbb{Z}_e \to \mathbb{Z}_N^*$ where $h_{N,e,z}(a, b) = a^e \cdot z^b$ mod N.

> **Claim 1.2 —** If a polynomial time adversary $\mathcal{A}$ breaks CRHF game for this hash function with non-negligible probability then there exists a reduction $\mathcal{B}$ which break can RSA with non-negligible probability.

Reduction

RSA challenger $\mathcal{C}$		**Reduction** $\mathcal{B}$		**Adversary** $\mathcal{A}$
	$\xrightarrow{(\text{N , e , } x^e\ )}$		$\xrightarrow{(\text{N , e , } x^e\ )}$	
	$\xleftarrow{\text{x}}$	Compute x as shown below	$\xleftarrow[(a_2,\ b_2)]{(a_1,\ b_1)}$	

We know that

$$h(N, e, x^e, a_1, b_1) = h(N, e, x^e, a_2, b_2)$$
$$a_1^e \cdot x^{eb_1} = a_2^e \cdot x^{eb_2}$$

Now we can say that given e co prime to ϕ(n) if $a^e = b^e$ mod N then a = b mod N.
We know there exists d such that $e \cdot d = 1$ mod $\phi(n)$ and raising both sides to d we get a = b mod N.

So we can say $a_1 \cdot x^{b_1} = a_2 \cdot x^{b_2}$
Since a_1 and a_2 are coprime to N, we can calculate their inverses using Extended Euclidean Algorithm and hence compute $x^{b_1 - b_2}$.
Given $b_1, b_2 \in \mathbb{Z}_e$, $b_1 - b_2$ is coprime to e.
Again using extended euclidean algorithm we can calculate A,B such that
$Ae + B(b_1 - b_2) = \gcd\ (\ e, (b_1 - b_2)\ ) = 1$.
Doing $(x^e)^A \cdot (x^{b_1 - b_2})^B = x^1$ we calculate x and break RSA challenger.

§2 Acknowledgements

We have used the style file from here[1] to typeset and the style file from here[2] for cryptographic games and protocols to produce this document.

[1]https://github.com/vEnhance/dotfiles/blob/main/texmf/tex/latex/evan/evan.sty
[2]https://github.com/arnomi/cryptocode