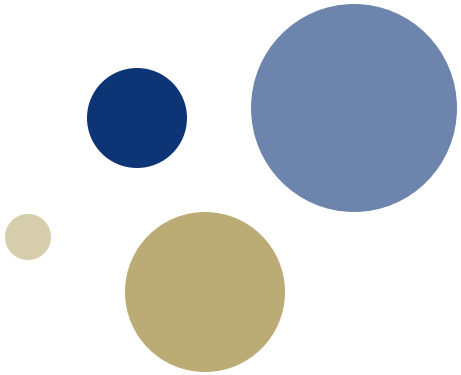
NTNU

Kunnskap for en bedre verden



Private Set Intersection from Key Exchange

NKS 25/10/2024

What is PSI?

- Private Set Intersection (PSI) is a type of Multi Party Computation performed between a *Sender* and a *Receiver*

- The sender and receiver have respective private sets X and Y.

- The goal of a PSI algorithm is for the receiver to learn the intersection of X and Y and nothing else.

- The receiver should also not learn anything about Y

Key Agreement

- There are many classes of algorithms developed for people to securely agree on secret keys: PKE, KEM, NIKE, KA

- Rosulek & Trieu [1] presents a scheme for PSI that is based on Key Agreement

- Consider algorithms KGen and KA

➢ KGen outputs public key pk and secret key sk

➢ KA(pk, sk) outputs shared key k

➢ If for two different runs KGen outputs pk^s, sk^s and pk^r, sk^r then $KA(pk^r, sk^s) = KA(pk^s, sk^r)$

Oblivious Key Value Store

- Polynomial interpolation is an algorithm that for a collection of points $\{v_i, k_i\}$ will output a polynomial f such that $f(v_i)=x_i$

- Oblivious Key-Value Stores is a generalization of this algorithm

$\underline{\text{Sender}(\mathsf{pp}, X)}$		$\underline{\text{Receiver}(\mathsf{pp}, Y)}$
$(\mathsf{pk}^{\mathsf{s}}, \mathsf{sk}^{\mathsf{s}}) := \mathsf{KGen}(\mathsf{pp})$		
	$\xrightarrow{\mathsf{pk}^{\mathsf{s}}}$	
		for $0 \le i \le n$:
		$(\mathsf{pk}^{\mathsf{r}}_i, \mathsf{sk}^{\mathsf{r}}_i) := \mathsf{KGen}(\mathsf{pp})$
		$\mathsf{f} = \mathsf{OKVS}\{y_i, \mathsf{pk}^{\mathsf{r}}_i\}_{i=0}^{n})$
	$\xleftarrow{\mathsf{f}}$	
for $0 \le i \le n$:		
$\mathsf{k}'_i = \mathsf{KA}(\mathsf{sk}^{\mathsf{s}}, \mathsf{f}(x_i))$		
$\mathsf{s}_i = \mathsf{H}(x_i, \mathsf{k}'_i)$		
$\mathsf{S}' = \mathsf{Sort}(\{\mathsf{s}_i\}_{i=0}^{n})$		
	$\xrightarrow{\mathsf{S}'}$	
		for $0 \le i \le n$:
		$\mathsf{k}_i := \mathsf{KA}(\mathsf{sk}^{\mathsf{r}}_i, \mathsf{pk}^{\mathsf{s}})$
		if $\mathsf{H}(y_i, \mathsf{k}_i) \in \mathsf{S}'$

Our work

- The realizes KA using Elliptic Curve Diffie-Hellman.
- Due to this being weak against quantum attacks we instead initialize it with KYBER

Citations

[1] Rosulek, Mike, and Ni Trieu. "Compact and malicious private set intersection for small sets." *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 2021.

[2] Garimella, Gayathri, et al. "Oblivious key-value stores and amplification for private set intersection." *Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16–20, 2021, Proceedings, Part II 41*. Springer International Publishing, 2021.