**[Insert title here]**

*version 0.2 (updated 5/9/16)*

**Introduction**

*Purpose*

**Overall Description**

**Specific Requirements**

**System Design**

**Experiments/Trials**

**Results/Conclusion**

**Design Considerations**

GPUs are suited for computations that will run on large data sets simultaneously in parallel. This will involve arithmetic on large data sets (matrices) where the same operation will be performed across each element at the same time. To meet this requirement, data needed to be structured in vectors which the GPU can manipulate. One vector represented recently extracted secret elements

Data structures and types – Moving data between the host device and the remote device (GPGPU in this case) can cause a performance hit if not utilized correctly. Due to this limitation, the sets of data transferred between devices are large and and infrequent.

**Glossary**

CUDA – parallel computing platform and application programming interface developed by NVIDIA. Allows developers to use GPGPUs. This platform

GPGPU – General purpose graphics processing unit

Kernel – code specifically ran on the GPGPU. The code will always represent an application to be executed across many threads.

TV-OTS – Time Valid One Time Signature

Notes

TVOTS for Time Critical Multicast Data Auth.

Introduction:

TV OTS is lightwieght

*The nature of time-critical messages implies two basic re-*

*quirements on the authentication scheme: 1) efficient algorithms*

*to minimize computational cost, and 2) the ability to avoid*

*packet buffering so that the data can be processed instantly*

*upon being available. Additional desirable properties for mul-*

*ticast authentication are 3) small communication overhead, 4)*

*tolerance to packet loss, and 5) resistance to malicious attacks*

RSA is computationally expensive on these machines.

*Another type of signature, which*

*is much more computationally efficient than regular public*

*key signatures, is the one-time signature (OTS) [11]–[13].*

*OTS is based on nothing more than one-way hash functions*

*and supports buffer-free signing and authentication. However,*

*there exist two drawbacks that prevent OTS from being widely*

*employed in practice: first, the signature size is much larger*

*than common public key signatures; second, the “one-timed-*

*ness” requires repeated distributions of public keys.*

Background and Models:

TVOTS is designed to work in a UDP type environment

*Network model*

Assuming nodes which packets travel through can be malicious, so a “multicast tree” must be established as follows:

-the Sender does not know the message until it is ready

-The desired end-to-end delay on each packet is short and upper bound to **SIGMA**

*refers to the time taken for a packet to be transmitted across a network from source to destination*

**-A sender time stamp is embedded into each packet so the R can check if the received packet has expired.**

-The Sender signs the message as soon as it appears.

-The sending rate of the messages from Sender is dynamic but upperbound by **LAMBDA\_M**

-Packets are transmitted using UDP/IP, no feedback is used.

*Security Goal*

To create to secruity property which Reciever can verify the fact that the received data is from Sender. Reciever should also be able to detect that the given packet was not from Adversary.

*Attack Model*

The goal of the Adversary is to either pose as Sender or to modify a packet sent by Sender.

-The Adversary has full control over the network. Adversary can selectively eavesdrop, capture, resend, delay, and alter packets.

-Adversary has a fast network.

-**Computation power** **of Adversary is limited but unbounded, Adversary has more powerful hardware than Sender and Receiver.**

-**Adversary can compromise any number of Rs and learn the secrets Receiver knows.**

*Assumptions*

-Receiver has access from a trusted key server which Receiver can obtain Sender's key to verify Sender.

-We assume there there is a synchronized time system for both Receiver and Sender can loosely synchronize.

TVOTS model:

TVOTS tries to balance the amount of bits being signed with public keys (due to the computational expense) and Block Base / Auth. Delay (due to requiring packet buffering) to create a fast and reliable scheme.

*For example, according to Figure 3(a)*

*the resultant signature size of signing 40 bits is only 14 of that of*

*encoding 160 bits. Intuitively, we improve the efficiency of OTS*

*by signing the first l-bit of the hash of the message. However,*

*this gives rise to the following security problem: Adv can*

*make use of the signature generated by S over some message*

*msg as a valid signature for other (malicious) message msg ,*

*as long as msg is a l-bit partial collision hash of msg, i.e.*

*H l (msg ) = H l (msg), where H l (·) = trunc l (H(·)), trunc l*

*denotes a function that truncates the input to the first l bits,*

*and H is a secure hash function. As a result, Adv can “legally”*

*sign msg even if he does not know the private key and cannot generate the signature by him or herself.*

***l- in this case is the collision length, This can determine the difficulty of Adversary's calculation. To prevent this attack, create an l which is larger than sigma.***

Private and public keys are associated with a given time period.

*The time by which R can accept the message is t R = T Adv +*

*S*

*t 0 − . After that time R will stop verifying any message.*

*Therefore, S must sign the message before T Adv + t S 0 − − σ*

*(recall that σ is the desired upper bound on the end-to-end*

*delay between S and R), i.e. t S 1 < T Adv + t S 0 − − σ. Hence,*

*the duration of the signature period will be*

*T Δ = t S 1 − t S 0 < T Adv − − σ*

*(1)*

*Because T Adv increases exponentially with l, we can make*

*T Δ long enough by simply choosing a relatively large l (refer*

*, our TV-OTS schemes*

*to Figure 4(a)). Since T Adv*

*can tolerate a very large synchronization error (e.g. several minutes)*

Security Primatives for TVOTS:

TVHORS scheme:

Security analysis for TVHORS:

Experimental Results:

Conclustion:

---------------------------------

The rising need for a smart grid comes from the aging technologies used. TV OTS comes as an authenication scheme to protect time critical data while remaining lightwieght in a multicast manner. However, under a set of given parameters, an attacker can {guess given identities from a pool of secrets, being able to extract data}. This project tries to explore those parameters to see if this attacks can be done in real time.

Cuda Reference Manual Notes:

http://docs.nvidia.com/cuda/cuda-c-best-practices-guide/index.html#axzz48DItyRxH

What should be ran on the GPU -

GPUs are suited for computations that will run on large data sets simultaneously in parallel. This will involve arithmetic on large data sets (matrices) where the same operation will be performed across each element at the same time.

To use CUDA, data values must be transferred from the host to the device along the PCI Express (PCIe) bus. These transfers are costly in terms of performance and should be minimized. (See [Data Transfer Between Host and Device](http://docs.nvidia.com/cuda/cuda-c-best-practices-guide/index.html" \l "data-transfer-between-host-and-device).) This cost has several ramifications:

* The complexity of operations should justify the cost of moving data to and from the device. Code that transfers data for brief use by a small number of threads will see little or no performance benefit. The ideal scenario is one in which many threads perform a substantial amount of work.

Data should be kept on the device as long as possible. Because transfers should be minimized, programs that run multiple kernels on the same data should favor leaving the data on the device between kernel calls, rather than transferring intermediate results to the host and then sending them back to the device for subsequent calculations.

//Notes on timing for the CUDA kernels

When using CPU timers, it is critical to remember that many CUDA API functions are asynchronous; that is, they return control back to the calling CPU thread prior to completing their work. All kernel launches are asynchronous, as are memory-copy functions with the Async suffix on their names. Therefore, to accurately measure the elapsed time for a particular call or sequence of CUDA calls, it is necessary to synchronize the CPU thread with the GPU by calling cudaDeviceSynchronize() immediately before starting and stopping the CPU timer. cudaDeviceSynchronize()blocks the calling CPU thread until all CUDA calls previously issued by the thread are completed.

//Notes on the balance between transfer of data and excution of code:

Concurrent copy and execute demonstrates how to overlap kernel execution with asynchronous data transfer. This technique could be used when the data dependency is such that the data can be broken into chunks and transferred in multiple stages, launching multiple kernels to operate on each chunk as it arrives. Sequential copy and execute and Staged concurrent copy and execute demonstrate this. They produce equivalent results. The first segment shows the reference sequential implementation, which transfers and operates on an array of N floats (where N is assumed to be evenly divisible by nThreads).

//The create of local variables in a thread on the GPU

Local memory is so named because its scope is local to the thread, not because of its physical location. In fact, local memory is off-chip. Hence, access to local memory is as expensive as access to global memory. In other words, the term local in the name does not imply faster access.

So use global variables whenever possible.

//Heuristics for Thread and Block calculation

The number of threads per block should be a multiple of 32 threads, because this provides optimal computing efficiency and facilitates coalescing.

The dimension and size of blocks per grid and the dimension and size of threads per block are both important factors. The multidimensional aspect of these parameters allows easier mapping of multidimensional problems to CUDA and does not play a role in performance. As a result, this section discusses size but not dimension.

Choosing the execution configuration parameters should be done in tandem; however, there are certain heuristics that apply to each parameter individually. When choosing the first execution configuration parameter-the number of blocks per grid, or grid size - the primary concern is keeping the entire GPU busy. The number of blocks in a grid should be larger than the number of multiprocessors so that all multiprocessors have at least one block to execute.

There are many such factors involved in selecting block size, and inevitably some experimentation is required. However, a few rules of thumb should be followed:

* Threads per block should be a multiple of warp size to avoid wasting computation on under-populated warps and to facilitate coalescing.
* A minimum of 64 threads per block should be used, and only if there are multiple concurrent blocks per multiprocessor.
* Between 128 and 256 threads per block is a better choice and a good initial range for experimentation with different block sizes.
* Use several (3 to 4) smaller thread blocks rather than one large thread block per multiprocessor if latency affects performance. This is particularly beneficial to kernels that frequently call \_\_syncthreads().

[http://docs.nvidia.com/cuda/cuda-c-best-practices-guide/index.html#axzz48vkOgrS8](http://docs.nvidia.com/cuda/cuda-c-best-practices-guide/index.html" \l "axzz48vkOgrS8) Section 10.5