Encryption scheme of information in CUDA applicable to RTGS systems

By Miguel Angel López Mendoza
Agenda

1. High Performance on Payment Systems
2. Characteristics of our new Payment System (SPEI-2)
3. Encryption mechanism implemented
4. Why GPU-accelerated?
5. Why AES-CTR?
6. Next steps for SPEI-2
7. Banco de México, ready to face the future!
A payment system is any system used to settle financial transactions between its participant banking institutions.

In Mexico, we have a Nationwide Payment System known as SPEI® (Sistema de Pagos Electrónicos Interbancarios) or Interbank Electronic Payment System, based mainly on a DNS scheme (Deferred Net Settlement), executed every 3 seconds.

SPEI was completely developed by personnel of Bank of Mexico.

Now, we are currently working on the design and prototyping stages of our completely new Hybrid Payment System (SPEI-2). This new system will have the ability to process payments on an RTGS scheme (Real-Time Gross Settlement) additionally to the DNS scheme of its antecessor.
Characteristics of our new Payment System (SPEI-2)

The three main requirements of the design of SPEI-2 are: high level of security, high throughput, and high availability.

A first goal to achieve in the inception and prototyping stages was the security mechanisms and how to accelerate them, focused on the encryption of information as our first approach (which is one of the most cpu-demanding process in the actual version of SPEI).

Our design is based on symmetric keys, which are delivered through a PKI (Public Key Infrastructure) during the login process, so that we ensure the system is protected against a man in the middle attack intended to obtain the symmetric keys.
Encryption mechanism implemented

The starting point is the login process in which the delivery of the encryption parameters are sent to participants.

Once the participant has completed the login process every subsequent message to be sent from the client to the server and vice versa is divided into 16-Byte blocks (AES128), and padded with zeros if necessary. For each block a different counter is assigned (it is incremented for every block), and only once nounce per message is assigned.
Encryption mechanism implemented

The next step is the AES block encryption process, that is applied to the concatenation of the nounce with each of the counters, so that, generating the encryption blocks.

Finally all of the 16 Bytes of the message are encrypted or decrypted by xor-ing them with its corresponding encryption blocks.
Why GPU-accelerated?

It is evident that the execution process of the AES-CTR algorithm to generate all of the encryption/decryption blocks can be executed in a parallelized fashion using the power of the GPUs.
Why AES-CTR?

We have chosen AES-CTR among others algorithms like AES-CBC (Cipher Block Chaining) or AES-ECB (Electronic Codebook) due to the possibility to parallelize the encryption process by independent blocks, in which of course, the high level of security holds.
Next steps for SPEI-2

Encryption of information, is not the only process we expect to accelerate through GPU computing.

The following processes will be accelerated too among the most important:

- Electronic signature verification
- Net settlement (acceleration of the knapsack problem)
- Fraud detection

Approximately 60% of the main processes of SPEI-2 will be accelerated through GPU computing.
Banco de México, ready to face the future!

The nationwide system SPEI-2 will be able to process a very high volume of operations, specifically **more than 100M operations per hour**, which is ten times the calculated **maximum burst of demanded operations, under the next 15 years** and around **1000 times** the payments processing power of the actual version of SPEI.

Based on the projection of the demand for electronic payments in Mexico over the following 15 years including new business models, the analysis of our parallelization model, and the results of the prototypes finished at this moment, we are sure that using the processing power of **GPUs allows us to reach the performance requirements**, and at a considerably less cost than just using the processing power of CPUs.