論文の内容の要旨

# GENERALIZED ANALYSIS METHODS FOR EFFICIENCY OF REPRESENTATIONS FOR SCALAR MULTIPLICATION

（スカラー乗法における数値表現の効率性の一般的な解析方法）

氏名　　スッパキットパイサーン　　ウォラポン

In this thesis, we propose algorithms to speed up the scalar multiplication, one of the bottleneck operations in elliptic curve cryptography, and introduce methods to analyse algorithms for scalar multiplications. To reduce a computation time of the operation, the method that we interest in this work is to change the representation of a scalar, that is to represent a positive integer using other representations than the binary representation with digit set {0,1}. Many representations such as the binary representation with digit set {-1, 0, 1} are redundant, i.e. there are many ways to represent a scalar in the representation. The computation time of scalar multiplication strongly depends on how we represent the scalar. For example, the Hamming weight is important factor to speed up the operation on the binary representation. Then, conversion algorithms to find the way to represent a positive integer for faster scalar multiplication are studied in many works, such as work by Müller, which propose a conversion algorithm for binary representation with digit set {0, ±1, ±3, ... , ±(2*h* + 1) } for any natural number *h*. We are also interested in an efficiency of each conversion on scalar multiplication. For binary representation, we use *average joint Hamming density* to evaluate the conversion, and *minimal average joint Hamming density* is devised to find the efficiency of each representation given an optimal conversion. By Müller, it is known that the average joint Hamming density of binary representation with digit set {0, ±1, ±3, ... ,±(2h + 1)} is 1/(*h* + 2).

Most of the works on improving the number representation on scalar multiplication are based on the mathematical construction of the representations. The construction helps them to devise the algorithm with fast conversion time and output expansions with minimal weight. Also, the minimal average joint Hamming density can be calculated from the construction. However, finding the mathematical construction of many representations are not trivial, and are still not attained. The optimal conversions with their average efficiency are still open problems. These include many representations practically

used in scalar multiplication. The problem is harder when we consider multi-scalar multiplication, which is the crucial operation in elliptic curve signature verification. This operation depends on the expansion of more than one scalar. To find the optimal conversion, we have to take all scalars involved in the operation into account. In this case, the mathematical construction becomes more complicated, and has not been found in most cases even for the binary representation with digit set {0, ±1, ±3}.

In our approach, we do not consider the mathematical constructions, but propose the optimal conversions directly from the structure of each representation based on dynamic programming scheme. Thus, we are able to obtain the optimal conversions based on dynamic programming scheme for many classes of representations whose optimal conversions have not been proposed. These include *r*-radix representation, which is the representation with base more than 2 used for speeding up pairing-based cryptography. Also, we can find the optimal conversions for scalar-multiplication using a double-base chain, the representation simultaneously using two bases. The outputs of our optimal conversions improve the results of the previous works by 3.2 - 11.3% in less than a second for 192 to 448-bit inputs with Java implementation on a personal computer. Moreover, we find the optimal conversions for multi-scalar multiplication, and solve the open problem proposed by Solinas in 2001.

From our optimal conversions, we construct Markov chains automatically. Then, we find the efficiency of each representation from its stationary distribution of the Markov chains. This enables us to find the minimal average Hamming density automatically. Although the number of states in the Markov chains is generally infinite, we propose many methods to reduce the number of states. The most important technique is that we define the similarity between the states, and consider the similar state as one state. Using the methods, the finiteness of Markov chain with the existence of stationary distribution is proven in a class of representation whose digit set be a finite set such that there exists a natural number $\Lambda$ where digit set $D_S \subseteq \{0, \pm1, \dots, \pm\Lambda\}$ and $\{0, \pm1, \pm\Lambda\} \subseteq D_S$. The class covers most of representations practically used in scalar multiplication such as the representation which digit set are {0, ±1} and {0, ±1, ±3}. One of the most notable results from this method is the minimal average joint Hamming weight of multi-scalar multiplication when two scalars are considered and digit set is {0, ±1, ±3}. We can show that the value is 0.3575. This improves the best upper bound 0.3616 proposed by Dahmen, Okeya, and Takagi in 2007. As we have found the minimal average joint Hamming weight of many representations, we can analyze the trend of the value on each digit set. In addition to the trend in binary representation found by Müller, we have discovered a relationship between digit set and minimal average joint Hamming weight in *r*-radix representation for scalar multiplication. For multi-scalar multiplication with two integers, we found the minimal average joint Hamming weight of the representation when the digit set is a subset of {0, ±1, ±3}. As a result, we discover a number of representations which have a small difference in the computation time of multi-scalar multiplication, but have a large advantage in the pre-computation step over representations proposed in previous works.

From the average joint Hamming weight, we explore more properties of the automatically-constructed finite state machine. We can find how minimal Hamming weight of all positive integers span when it is expanded in each representation. We show that these representations are always normal, and we use this fact with the spanning deviation to propose an effective countermeasure of side channel attacks.