# Combining PRIDE and PKA for the Use in Embedded Systems

Christopher Robert Philabaum

Response to Dr. Tolga Yalçin

INF501, Dr. Igor Steinmacher

October 11, 2018

## Introduction

The field, study, and practical uses of Internet of Things (IoT) devices have grown considerably over the past few years. From smartwatches, to thermostats, and now even smart cars, IoT devices are becoming more ubiquitous. One of the biggest hurdles when it comes to IoTs is that of security. Each device can have varying degrees of limited compute resources at hand, and this limits the potential amount of security any given device can use to protect itself from attacks. One of the most widely used ciphers, AES, is usually considered a fast, lightweight block cipher that can be found even on chip credit cards that protect one's financial transactions. "Fast" and "lightweight" are relative terms when compared to older, broken ciphers like DES; when it comes to embedded systems, however, AES is still too large and slow of a cipher when used on the likes of 8-bit or 16-bit microcontrollers or microprocessors.

On October 5th, 2018, Dr. Yalçin presented his work associated with Albrecht, et al. [1] to everyone in the INF501 course. His research explores and understudied aspect of truly fast, lightweight ciphers that can both be secure and still used effectively and efficiently on embedded systems. In relation, the work I've done with Dr. Bertrand Cambou, Dr. Bilal Habib, and Duane Booher provides a lightweight key exchange mechanism that can be implemented for embedded systems (PKA) [2]. I believe that many of the fine optimizations and methodologies used in designing and implementing PRIDE can be similarly applied when implementing PKA for an embedded system.

## PRIDE and the Linear Layer

The job of a cipher algorithm is to put basically encrypt (and decrypt) messages, to hide the message from those that are not meant to read it. There are two main types of ciphers: stream ciphers and block ciphers. Stream ciphers operate on a per character level by encrypt each character independently from one another; block ciphers work by a given "block size", where instead a fixed size of characters is encrypted or decrypted at once (aka. *metacharacters*).

While there are many designs and methodologies to block ciphers, the more modern approach uses what are known as substitution-permutation networks (SPNs). Dr. Yalçin noted in his talk that most research has been placed on the substitution (confusion or *non-linear layer*) phase, whereas there hasn't been much in the way of permutation (diffusion or *linear layer*) phase. More specifically, while there are certainly "specialized linear layer constructions" in the wild, there are little in the name of "generalized linear layer constructions".

*WIP: explain the basic designs and optimizations used for PRIDE.*

## PKA and Public-Key Infrastructures

While cybersystems must worry about actively hiding messages from outside parties, there lies another problem: securely transmitting keys to be used in said ciphers. A public-key infrastructure is a system designed to transmit encryption keys either over a secure or insecure channel. These keys can then be used to encrypt messages back-and-forth, either independently deriving new keys from what was communicated or directly with the keys themselves. The latter of the two is the approach I studied under Dr. Cambou. Similarly to Dr. Yalçin, we placed our focus on creating a system that could be properly used on embedded systems without concern of constraints. "Public-Key Exchange scheme that is Addressable" is such a system that allows for two parties to independently derive the same private key from a provided public key while minimizing resources.

*WIP: Compare some design compares to PRIDE, in particular the idea of using bitslicing to make PKA more efficient.*

## Conclusion and Thoughts

Optimization, namely in the context of computer science and algorithms, has always been one of my favorite problems to fixate over. To me, it's akin to solving a puzzle, beating a game, or like a challenge to overcome. This is what caught my eye most about Dr. Yalçin's presentation. Not only was his presentation focused on a topic I've only started to accustom to (cryptography), but rather the optimization of it. Normally, one wouldn't think that cryptography would need to be well-optimized, and that all research would only focus on the pure strength and security of the algorithms designed. With the increasing amount of low-power systems, however, more care must be considered when designing new ciphers to be used not today, but in the next decade. By learning from the design principles of PRIDE, I plan to apply them toward my research on PKA or whatever new cybersystems may come my way.

## References

[1] M. R. Albrecht, B. . Driessen, E. B. Kavun, G. . Leander, C. . Paar and T. . Yalcin, "Block Ciphers – Focus on the Linear Layer (feat. PRIDE )," , 2014. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-662-44371-2_4. [Accessed 11 10 2018].

[2] E. B. Kavun, G. . Leander and T. . Yalcind, "A reconfigurable architecture for searching optimal software code to implement block cipher permutation matrices," , 2013. [Online]. Available: https://doi.org/10.1109/reconfig.2013.6732263. [Accessed 11 10 2018].

[3] B. Habib, B. Cambou, D. Booher and C. Philabaum, "Public Key Exchange scheme that is Addressable (PKA)," in *IEEE Conference on Communications and Network Security*, Las Vegas, United States, 2017.