Dronecrypt - An Efficient Cryptographic Framework for Small Aerial Drones

Muslum Ozgur Ozmen  
Oregon State University  
Corvallis, Oregon, USA  
ozmenmu@oregonstate.edu

Attila A. Yavuz  
Oregon State University  
Corvallis, Oregon, USA  
attila.yavuz@oregonstate.edu

Abstract—Aerial drones are becoming an integral part of application domains including but not limited to, military operations, package delivery, construction, monitoring and search/rescue operations. It is critical to ensure the cyber security of networked drone systems in these applications. Standard cryptographic services can be deployed to provide basic security services; however, they have been shown to be inefficient in terms of energy and time consumption, especially for small aerial drones with resource-limited processors. Therefore, there is a significant need for a highly efficient cryptographic framework that can meet the requirements of small aerial drones.

We propose an improved cryptographic framework for small aerial drones, which offers significant energy efficiency and speed advantages over standard cryptographic techniques. (i) We create to the best of our knowledge the first highly optimized public key infrastructure (PKI) based framework for small aerial drones, which provides energy efficient techniques by harnessing special pre-computation methods and optimized elliptic curves. (ii) We also integrate recent light-weight symmetric primitives into our PKI techniques to provide a full-fledged cryptographic framework. (iii) We implemented standard counterparts and our proposed techniques on an actual small aerial drone (Crazyflie 2.0), and provided an in-depth energy analysis. Our experiments showed that our improved cryptographic framework achieves up to 35× lower energy consumption than its standard counterpart.

I. INTRODUCTION

Aerial drones are emerging mobile cyber-physical systems with potential applications such as military operations, package delivery, reconnaissance, environmental monitoring and disaster recovery/response [1], [2], [3], [4]. Due to the significant financial and strategic value involved, aerial drones are expected to be exclusively targeted by attackers. These attacks are especially critical for military networks where some sensitive information can be extracted. For instance, in 4th December 2011, a US drone (RQ-170 Sentinel) was captured by Iranian forces. A strong theory that explains how it was captured supposes that the navigation system of the drone was attacked [4], [5]. Another incident is the keylogging attack that targeted a US drone fleet in September 2011 [4]. This attack can cause the exposure of the control station and potentially result in the full control on the drone.

Therefore, it is critical to ensure the cyber security of aerial drone systems. In particular, the basic security services such as confidentiality, authentication, and integrity must be provided to refrain from mentioned attacks. These services are mainly guaranteed via fundamental cryptographic techniques such as symmetric ciphers and PKI. Symmetric key cryptography is highly preferred due to its efficiency and well-analyzed security. However, public key primitives can also be highly useful for certain drone applications. For instance, public key cryptography offers scalability, public verifiability, and non-repudiation that are critical for large and distributed drone networks (e.g., military operations, search and rescue).

There are various standard cryptographic techniques, but the majority of them may not meet the needs of aerial drones. Energy and bandwidth constraints pose critical limitations towards the deployment of standard cryptographic techniques on small aerial drones [6]. In the following, we outline recent cryptographic techniques that are considered for aerial drones and highlight some obstacles against practical deployments.

A. Related Work

Initial approaches to secure the aerial drones include implementation of well-known protocols (e.g., RSA and AES) on FPGAs [7], [8]. However, they showed that standard techniques take a lot of computation time and consume high amount of energy on small aerial drones that are further confirmed by our experiments (see Section V).

Seo et al. [9] proposed a security framework that implemented some symmetric ciphers with white-box cryptography to mitigate the impacts of drone capture attacks [9]. However, the insecurity of this line of research has been later shown in [10]. Won et. al. proposed Certificateless Signcrytion based protocols for mid-size aerial drones (e.g., AR.Drone 2.0) in [11]. This protocol reduces the communication overhead by eliminating certificates, but requires several exponentiations and therefore introduces heavy overhead, which might not be practical for resource-limited small aerial drones. Moreover, aerial drones are expected to be an integral part of Internet of Things (IoT), which vastly relies on PKI technology. Certificateless protocols cannot be seamlessly integrated into existing PKI-based IoT systems without significant alterations.

One may observe that the following issues that should be addressed towards a practical deployment of cryptographic techniques on small aerial drones (i) The existing standard primitives and cryptographic protocols are inefficient in terms of energy/time consumption for small aerial drones that operates with resource-limited microprocessors (see Figure 1). (ii) The existing cryptographic protocols for aerial drones only focus on a few specific primitives but do not offer a comprehensive framework that harbors a variety of light-weight symmetric and asymmetric primitives. (iii) To the best of our knowledge, there is no open-source framework, even for some standard cryptographic primitives, which offers a detailed energy assessment.
B. Our Contribution

Towards the practical adoption of cryptographic techniques to resource-limited small aerial drones, we propose an improved cryptographic framework by harnessing various cryptographic primitives and optimizations, which provides significantly lower delay and energy consumption for small aerial drones, compared to the deployment of standard cryptographic techniques. We further outline our contributions as follows:

- **An Efficient Framework with Algorithmic Improvements**: Our goal is to reduce the computation and communication overhead of standard cryptographic primitives to minimize their energy consumption for small aerial drones. Therefore, we exploit synergies among special pre-computation techniques and elliptic curves (EC), which not only offer the most compact key/signature sizes among available alternatives, but also significantly reduce the computational cost of EC scalar multiplication.

  We develop (to the best of our knowledge) the first real-world implementation of Boyko-Peinado-Venkatesan (BPV) pre-computation technique on FourQ curve. BPV technique reduces the cost of an EC scalar multiplication to only a few EC additions with only a small constant-size storage overhead. Remark that FourQ curve is one of the most addition friendly curves (even with a better efficiency than that of Curve25519), and therefore our integration further enhances the efficiency of BPV. We then instantiate BPV-FourQ-Schnorr and BPV-FourQ-ECIES as our improved digital signature and integrated encryption schemes, which significantly outperform their standard counterparts. Moreover, we also integrate some of the recent lightweight symmetric primitives into our improved PKI suite to create a full-fledged cryptographic framework.

- **In-depth Energy Analysis**: The energy consumption of standard Elliptic Curve Cryptography (ECC) based primitives have not been investigated thoroughly for recently emerging small aerial drones. In this paper, we implemented both standard ECC techniques and our proposed cryptographic framework and presented a detailed energy consumption analysis. As demonstrated in Figure 1, for different cryptographic primitives, our experiments showed that proposed improvements enable up to 35× less energy consumption compared to the standard techniques for small aerial drones (see Section V). Similar performance gains were observed for the lightweight ciphers over the standard symmetric primitives.

- **Open-Source Framework**: While isolated implementation results were reported for particular cryptographic primitives such as RSA and AES [7], [8], to the best of our knowledge, no comprehensive open-source cryptographic framework is available for small aerial drones. Towards meeting this need, we fully implemented our standard and improved cryptographic frameworks. We will open-source both to enable a broad test and potential adoption at

  https://github.com/ozgurozmen/Dronecrypt

**Limitations**: The main limitation of our proposed framework is the increased private key size, that is inherited from the BPV pre-computation technique. More specifically, our improved PKI primitives require the sender to store a private key of 64 KB. However, this increased private key size translates into significant improvements on computational time and energy consumption. Considering the storage capabilities of small aerial drones, we believe this is a desirable trade-off for security-critical applications. On the other hand, if the drone is highly memory-limited and cannot tolerate such storage, standard cryptographic primitives should be preferred.

![Fig. 1: The performance comparison of the proposed and standard cryptographic frameworks.](image-url)
II. PRELIMINARIES

TABLE I: Notation followed to describe schemes.

| $F_q$       | Finite Field |
| $\mathcal{G}$ | Generator Group Point |
| $n$         | Order of Group |
| $(y, Y)$    | Private/Public key pair |
| $\Gamma$   | BPV Precomputation Table |
| $m$         | Message |
| $\zeta_k$  | IND-CPA Encryption via key $k$ |
| $\zeta^e_k$ | IND-CPA Decryption via key $k$ |
| $\times$    | Elliptic Curve Scalar Multiplication (Ecal) |
| $KDF$       | Key Derivation Function |

Elliptic Curve (EC) points are shown in bold

BPV Pre-computation Technique: We use BPV generator [12], which reduces the computational cost of an Emul to a few EC additions with the expense of a table storage. The BPV generator is a tuple of two algorithms (Offline, Online) defined in Algorithm 1.

Algorithm 1 Boyko-Peinado-Venkatesan (BPV) Generator

$$(\Gamma, v, k, F_q, \mathcal{G}, n) \leftarrow \text{BPV.Offline}(\mathbb{1}^\kappa)$$;
1: Set the EC system-wide parameters $\text{params} \leftarrow (F_q, \mathcal{G}, n)$;
2: Generate BPV parameters $(v, k)$, where $k$ and $v$ are the number of pairs to be pre-computed and the number of elements to be randomly selected out $k$ pairs, respectively, for $2 < v < k$.
3: $r_i^k \leftarrow \mathbb{Z}_n^v$, $R_i^k \leftarrow r_i^k \times \mathcal{G}$, $i = 0, \ldots, k - 1$.
4: Set pre-computation table $\Gamma = \{r_i^k, R_i^k\}_{i=0}^{k-1}$.

$$(r, R) \leftarrow \text{BPV.Offline}(\Gamma, v, k, F_q, \mathcal{G}, n)$$;
1: Generate a random set $S \subset [0, k - 1]$, where $|S| = v$.
2: $r \leftarrow \sum_{i \in S} r_i^k \mod n$, $R \leftarrow \sum_{i \in S} R_i^k$.

FourQ Curve: FourQ is a high-security, high-performance elliptic curve that is proposed by Costello et. al [13]. FourQ synergizes some well-known EC optimizations to offer high-speed EC scalar multiplication and EC addition while preserving 128-bit security.

Standard Techniques: Our standard cryptographic framework consists of broadly standardized techniques.

We select secp256k1 curve to implement our standard public key cryptography services, such as EC DH [15], ECDSA [16], and ECIES [17]. Secp256k1 is a NIST recommended curve [18], which is frequently used in practice. We implemented a key exchange, a digital signature and an integrated scheme to secure a variety of applications. We also implemented some of the most well-known symmetric key cryptography techniques such as AES as the block cipher [19], AES-GCM as the authenticated encryption [20] and HMAC with SHA-256 for MAC. Note that, an open-source implementation and in-depth energy analysis of such standard cryptographic framework for small aerial drones are not currently available (to the best of our knowledge).

III. PROPOSED FRAMEWORK

A. Low Cost PKC Primitives

One may consider adopting traditional pre-computation methods to reduce the computation overhead of cryptographic techniques. However, traditional online/offline pre-computation methods require linear storage. Thus, they may not be feasible for small aerial drones equipped with lightweight microcontrollers. In addition, once the pre-computed tokens are depleted, they must be regenerated. It is shown that the regeneration cost of these pre-computation techniques may incur even more cost than following the original protocol [21].

We propose an integrated approach that only requires small-constant storage overhead and highly optimized EC addition operations as opposed to a full EC scalar multiplication. To achieve this objective, we present an instantiation of BPV on FourQ curve, which is ideal for BPV due to its very fast EC additions. With BPV, we reduce EC scalar multiplication operations of our target schemes/protocols to only a few EC addition operations. The integration of FourQ into BPV amplifies the performance gain as it is an addition efficient curve. As it will be showcased in Section V, this strategy enables almost $35 \times$ more efficient operations compared to the standard schemes (with standard curves such as secp256k1). The storage cost of such an energy efficiency gain is only a constant-size storage of 64KB (for parameters $v = 16, k = 1024$, see Section II) keying material. With the current capabilities of low-end processors, even on the small aerial drones (such as Crazyflie 2.0 [6]), it is feasible to store such a private key. We then use BPV-FourQ to instantiate three main cryptographic schemes, which creates the following efficient digital signature, key exchange, and integrated encryption suite:

(i) We integrate our optimized BPV-FourQ into Schnorr signature scheme to gain computational efficiency. This transformation is presented in Algorithm 2.

Algorithm 2 BPV-FourQ-Schnorr Signature

$$(\Gamma, v, Y) \leftarrow \text{BPV-FourQ-Schnorr.Ky}(\mathbb{1}^\kappa)$$;
1: Generate parameters and BPV table as $$(\Gamma, v, k, F_q, \mathcal{G}, n) \leftarrow \text{BPV.Offline}(\mathbb{1}^\kappa)$.
2: Generate private/public key pair $(y \leftarrow \mathbb{Z}_n^v, Y \leftarrow y \times \mathcal{G})$

$$(s, e) \leftarrow \text{BPV-FourQ-Schnorr.Sig}(m, y, \Gamma)$$;
1: $(r, R) \leftarrow \text{BPV.Offline}(\Gamma, v, k, F_q, \mathcal{G}, n)$
2: $e \leftarrow H(m||R)$, $s \leftarrow (r - e \cdot y) \mod n$ where $H$ is a full domain cryptographic hash function $H : \{0, 1\}^* \rightarrow \mathbb{Z}_n^v$.

$$(b \leftarrow \text{BPV-FourQ-Schnorr.Ver}(m, (s, e), Y)$$;
1: $R' \leftarrow e \times Y + s \times \mathcal{G}$
2: If $e = H(m||R')$ then set $b = 1$ as valid, else $b = 0$.

(ii) Similarly, we instantiate ECDH with BPV-FourQ. In the ECDH variant, each node first derives its private/public key pair with an EC scalar multiplication, and then one more EC scalar multiplication is performed in order to obtain the shared key [15]. We adopt BPV protocol so that each node derives its private/public key pair with only EC additions. This decreases the computation time and energy consumption of the protocol by almost $1.5 \times$, in the expense of storing a 64KB table. Moreover, it is almost $28 \times$ more efficient than its standard counterpart (ECDH on secp256k1, see Section V).

(iii) In ECIES protocol, node 1 first derives the shared secret by generating an ephemeral private/public key pair and then
computing the shared secret using node 2’s public key [17]. Then, she generates encryption and MAC keys from this shared secret with a pre-determined key derivation function. We adopt BPV to ECIES by transforming the first EC scalar multiplication (where the ephemeral private/public key pair is generated) to EC additions, as depicted in Algorithm 3.

Algorithm 3 BPV-FourQ-ECIES Encryption

\begin{align*}
(\Gamma, y, Y) & \leftarrow BPV\text{-}FourQ\text{-}ECIES.(Kg(1^k)):
\end{align*}

1. Generate parameters and BPV table as 
   
   \begin{align*}
   (\Gamma, v, k, F_q, G, n) & \leftarrow BPV\text{-}Offline(1^k).
   
   \end{align*}

2. Generate private/public key pair \( (y, Z_n, Y) \leftarrow y \times G \)

\begin{align*}
(c, d, R) & \leftarrow BPV\text{-}FourQ\text{-}ECIES.(Enc(m, \Gamma, \Gamma)):
\end{align*}

1. \( (r, R) \leftarrow BPV\text{-}Online(\Gamma, v, k, F_q, G, n) \)
2. Generate shared secret as \( T \leftarrow r \times Y \)
3. \( (k_{enc}, k_{MAC}) \leftarrow KDF(T) \)
4. \( c \leftarrow k_{enc}(m) \)
5. \( d \leftarrow MAC_{k_{MAC}}(c) \)

\begin{align*}
(m & \leftarrow BPV\text{-}FourQ\text{-}ECIES.(Dec(y, \langle c, d, R \rangle)):
\end{align*}

1. \( T' \leftarrow y \times R \mod p \)
2. \( (k_{enc}, k_{MAC}) \leftarrow KDF(T') \)
3. If \( d \neq MAC_{k_{MAC}}(c) \) return INVALID
4. \( m \leftarrow Dec(k_{enc}(c)) \)

B. Low Cost Symmetric Key Primitives

We integrate light-weight ciphers and symmetric authentication mechanisms into our framework. Specifically, we use CHACHA20 as a very fast stream cipher [22], CHACHA-POLY as the authenticated encryption and POLY1305 as the MAC protocol [23]. These schemes provide faster and energy-efficient encryption/authentication while still offering high-security guarantees [24]. Our experiments confirmed that the adoption of these light-weight ciphers offer significant improvements in terms of computation time and energy consumption. For instance, these light-weight symmetric techniques enable up-to 7× improvement over standard symmetric ciphers (e.g., AES) for small aerial drones (see Section V).

IV. SECURITY OF THE PROPOSED FRAMEWORK

The security of our improved PKC suite depends on the improvement techniques (BPV pre-computation technique and FourQ curve), since the underlying schemes (Schnorr, ECDH and ECIES) are all well-studied and standardized. BPV technique takes advantage of the random walks on Cayley graphs over Abelian groups and it relies on the hardness of hidden subset sum problem. Boyko et al. show that any attack to BPV technique would require solving non-linear lattice problems [12]. BPV technique in elliptic curve based schemes (as adopted in our proposed framework) were later investigated in [25], with an integration to ECDSA. This integration relies on the affine hidden subset sum problem. Since the BPV technique is used in our schemes without any modification, it inherits its security guarantees presented in [12], [25]. As discussed in Section II, FourQ is a special elliptic curve that combines multiple optimizations to enable fast operations. While offering high computational efficiency, FourQ still preserves 128-bit security level that is the same with standardized secp256k1 curve [13].

The security of the light-weight ciphers and symmetric authentication mechanisms are studied in [24]. Their security is equivalent to their well-known standard counterparts such as AES. Moreover, we used CHACHA20, that is the 20 round CHACHA scheme to ensure its security [24]. Therefore, the security of our proposed framework is well-analyzed and comparable to the standard framework.

V. PERFORMANCE EVALUATION

A. Experimental Setup and Evaluation Metrics

We worked on Crazyflie 2.0 (Figure 2) due to its open-source software and hardware [6]. Crazyflie 2.0 has two microcontrollers: (i) An STM32F405 microcontroller as the main controller that runs all the flight control codes. Both cryptographic frameworks were implemented on this microcontroller due to its capabilities. (ii) An ultra-light-weight nRF51822 microcontroller is responsible for the communication (radio) and power management.

STM32F405 is equipped with an ARM Cortex M-4 architecture and operates at 168 MHz. It is a 32-bit microcontroller with a 192 KB SRAM and 1MB flash memory. Although STM32F405 is a resourceful processor, it has very low power consumption. It operates at 3.3V and takes 40mA of current while operating at 168 MHz. Our evaluation metrics include computation time, storage, communication bandwidth, and energy consumption. We measured the energy consumption with the formula \( E = V \times I \times t \), where \( V = 3.3V \), \( I = 40mA \) [26] and \( t \) is the computation time based on the clock cycles. Moreover, we connected an ammeter between the device and the battery to double check the current taken by the processor and observed insignificant difference with 40mA, while running at 168 MHz.

We used the following libraries in our implementations. (i) All symmetric primitives are implemented using WolfCrypt [27]. (ii) We implemented all standard public key services using microECC [28] as it is a light-weight and open-source library that supports various NIST recommended curves. (iii) All optimized public key primitives are implemented with open-source Microsoft FourQ library [13]. We selected BPV parameters as \( v = 16 \) and \( k = 1024 \), which sets the size of \( 1 \) as 64KB, that can be easily stored in STM32F405. We note that all libraries used for both standard and optimized frameworks are open-source, therefore they can be easily integrated to various aerial drones.

B. Performance Evaluation and Comparison

Experimental evaluation and comparison of the standard framework and our proposed framework are presented in Tables II and III, for public key and symmetric cryptography, respectively.
Although energy consumption is critical for small aerial drones, computation time also has some crucial effects on the adoption of cryptographic protocols in practice. For instance, there are time-critical applications that need frequent data transmission (e.g., camera mounted on an aerial drone for video surveillance - 24 frames per second are necessary). Cryptographic primitives used to secure such applications should meet this demand by offering high-speed operations. Therefore, we believe CPU Time improvements depicted in Tables II and III are also critical for small aerial drones.

Below, we present the comparison between the standard framework and our proposed framework, with an application to use-cases for small aerial drones.

- **Digital Signature and Broadcast Authentication**: Digital signatures are commonly used for broadcast authentication and key certification purposes. Drones may be used in scenarios where the drone needs to broadcast its sensor data, such as GPS data for location, photo frames for monitoring networks for the management and distribution of symmetric keys. That is, it might not be always possible to assume pre-installed symmetric keys for all drones in all applications as the controller/server may change for different purposes and use-cases. Therefore, an efficient key exchange protocol is useful to be deployed on drones.

A key exchange protocol is also essential for aerial drone networks for the management and distribution of symmetric keys. That is, it might not be always possible to assume pre-installed symmetric keys for all drones in all applications as the controller/server may change for different purposes and use-cases. Therefore, an efficient key exchange protocol is useful to be deployed on drones.

Our optimized framework with algorithmic improvements achieves significantly lower energy consumption and faster encryption/key exchange than that of the standard framework. BPV-FourQ-ECIES is $27.70 \times$ more energy efficient than standard ECIES protocol. BPV-FourQ-ECDH also improved its standard counterpart by 27.68 $×$. Besides the energy efficiency, our optimized protocols offer fast computation that is important for time-critical applications.

- **Light-weight Symmetric Primitives**: Symmetric key cryptography can be used for various use-cases on drones, due to their low energy consumption. For instance, securing the command and control channel is the minimum requirement for a safe operation of any aerial drone system. This channel can be easily secured via symmetric key primitives. We suggest using an authenticated symmetric encryption to secure this communication channel. Moreover, when a single aerial drone reports its sensor data to one or a few base stations, symmetric key primitives can be preferred over public key schemes.
Although the energy consumption of symmetric primitives is minimal compared to PKC, it is still useful to optimize their energy consumption as their use with high message throughputs might be much higher. For example, 100 messages per second are necessary to have a stable flight, which means 100 encryption/authentication operations per second [6]. When authenticated encryption schemes are used to secure this channel as suggested, our proposed framework offers 6.95× lower energy consumption. Our proposed framework still achieves 3.84× and 4.11× lower energy consumption for sole encryption and authentication, respectively. Therefore, our proposed framework offers significant energy improvement over its standard counterpart for symmetric key primitives.

**Discussions:** We would like to note that our experiments are performed on the drone processor while none of the flight control codes were active. When these codes are active, this would potentially increase the run-time of both frameworks. However, since the impact of such a slow-down would be similar, we believe the improvements of our framework will remain. More importantly, the message throughput that both framework can support will decrease. Considering that the standard framework is already struggling meeting with the requirements of time-critical use-cases with current configurations, it will suffer more from this decrease in throughput. Therefore, we believe that, in a real-life deployment, the benefits of our improved framework would even increase and our framework can meet the needs of stringent requirements of real-time applications.

**VI. CONCLUSION**

In this paper, to the best our knowledge, we proposed the first open-source low energy cryptographic framework tailored for small aerial drones with an in-depth energy consumption analysis. Our framework integrates various algorithmic optimizations to improve the performance of standard PKC techniques, all supported with light-weight symmetric ciphers. We have implemented and deployed our optimized framework on Crazyflie 2.0, and compared its performance with the standard techniques. Our experiments confirmed that our improved framework offers up to 35× higher speed and better energy efficiency compared with its standard counterpart. Therefore, our improved framework can meet some of the stringent energy and delay requirements of aerial drone networks with only a small impact on the battery life and end-to-end delay. We will open-source our cryptographic framework for public testing, improvement and adoption purposes.

**REFERENCES**


