Digital Signatures using Elliptic Curve with Extended Galois Fields

Jolan Philippe
Northern Arizona University, SICCS
Flagstaff, AZ. USA
jp2589@nau.edu

Abstract

The interesting algebraic structures provide beautiful properties which can be applied to cryptography science. We present in this paper how the Galois Fields can be applied to generate a digital signature (DSA) easily. We cover in this paper, all the necessary aspects to thoroughly understand the strengths of DSA created from elliptic curve cyclic based on extended Galois Fields.

1 Introduction

In the real world, we use to sign a paper document to ensure its authenticity. In computer science, the same approach is used to certify the integrity, the authentication and non-repudiation of data such as documents, messages, or identification. Digital signatures are gaining in importance around the world, and are now considered as the same legal level with handwritten ones. Nowadays, sensitive data (e.g., all the banking information, including transactions) are transmitted through networks. For this reason, the data must be secured, and be protected from malicious attacks. There exist different encryption techniques, more or less reliable, to hide the content of the messages [7, 13, 15]. Cryptography has been used during History, especially on message transmissions during conflict periods [19]. The encrypted messages passing is based on a key approach, that is used to create a cipher from plain text. Depending on the technique, the key can be symmetrical or asymmetrical. In other words, the key to encrypt the data is not necessarily the same one to decrypt. Digital signatures are based on the second approach. A user has a pair of two related keys. The first one, the private key, is used to encrypt data, while the second one, the public key, is used to decrypt data. In the context of DSA, the private key is used to sign the data, and the public key is used to check the authenticity of the signature. The finite field arithmetic is often used to manipulate signatures. The finite fields are cyclic groups of integers [6, 14], that is a field which contains a finite number of elements. The combination of arithmetic tools and cryptography makes robust signatures for exchanged messages.

To contribute to this field of study, we propose a new approach to create a digital signature, based on an extension of the prime Galois Fields. This paper is presented as follow.

Section 2 presents the strong Galois Field algebra, based on prime numbers. The elliptic curves geometry is described in Section 3. We cover the digital signature theory and its application using elliptic curves with Extended Galois Field in Section 4. Section 5 gives an overview of other ways to create and verify the digital signature. Finally, Section 6 concludes the paper and present future works.

2 Galois Fields

2.1 Finite Fields

An algebraic structure on a set S is defined by its collection of finite operations. There exist three types of carrier sets.

The groups are defined by the operator $\bullet$ such as:

- the operator respects closure property: $\forall a\ b \in S,\ a \bullet b$ is also in S
- $\bullet$ is associative: $\forall a\ b\ c \in S,\ a \bullet (b \bullet c) = (a \bullet b) \bullet c$;
- there exists an identity element $\iota_\bullet$: $\forall a \in S, a \bullet \iota_\bullet = \iota_\bullet \bullet a = a$
- all elements have an inverse: $\forall a \in S, \exists a^{-1}, a \bullet a^{-1} = \iota_\bullet$

If $\bullet$ respects commutativity, the group is called an abelian group. The operator $\bullet$ used to be written with $\oplus$. The dual operator $\ominus$ is then defined such that $a \ominus b = a \oplus b^{-1}$

The rings are defined with the same properties. In addition to $\oplus$ and $\ominus$, a ring has a closed, and associative operator $\otimes$ paired with its neutral element $\iota_\otimes$. In the definition of the rings, $\oplus$ and $\otimes$ are distributive, that is:

- $a \oplus (b \otimes c) = (a \oplus b) \otimes (a \oplus c)$;
- $a \otimes (b \oplus c) = (a \times b) \oplus (a \times c)$.

The fields extend the rings with the commutative property of $\otimes$ and an operator $\oslash$ such that

- $a \otimes a^{-1} = \iota_\otimes$;
- $a^{-1} = \iota_\otimes \oslash a$;
- $a \oslash b = a \otimes b^{-1}$.

The Galois fields are fields defined with a prime number p of positive natural number and are written $G\mathcal{F}_p$. The operators for ring sets are defined by:

- $a \oplus b = a + b\ mod\ p$ with $\iota_\oplus = 0$;

– $a \ominus b = a - b \ mod \ p$ with $\iota_{\ominus} = 0$;

– $a \otimes b = a * b \ mod \ p$ with $\iota_{\otimes} = 1$.

The inverse operator of $\otimes$, $\oslash$, is defined such that $a \oslash b \equiv a * b^{-1} \ mod \ p$ with b^{-1} the number which gives the following result: $b^{-1} * b \equiv b * b^{-1} \equiv 1 \ mod \ p$

2.2 Extended Galois Field

The extended Galois fields are defined with two parameters: (i) a prime number p,(ii) and an integer m. $G\mathcal{F}_{p^m}$ defines a field containing p^m elements. An interesting extension of the Galois fields are presented with $p = 2$ and are written with polynomials $A_{(x)} = \sum_{i=m-1}^{0} a_i * x^i; a_i \in G\mathcal{F}_2 = \{0, 1\}$. The polynomial A is then written $A = (a_{m-1}, ..., a_i, ..., a_0)$

Example 1
With $p = 2$ *and* $m = 3$ *(*$G\mathcal{F}_{2^3}$*),* $A_{(x)} = a_2x^2 + a_1x^1 + a_0$

Binary	*000*	*001*	*010*	*011*	*100*	*101*	*110*	*111*
Polynomials	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1

We can notice that, for $p = 2$, the operators $\oplus$ and $\ominus$ are equivalent. It means $a \ominus b = a \oplus b$ that is $a + a \equiv a - a \ mod \ p = 0$.

From the definition of the extended Galois Field, we have the following results:

Result 1 (Addition)
$\forall p \in \mathbb{P}, \ m \in \mathbb{N}, \ A_{(x)} \ B_{(x)} \ C_{(x)} \in G\mathcal{F}_{p^m}, \ A_{(x)} \oplus B_{(x)} = C_{(x)} = \sum_{i=0}^{m} c_i * x^i$
with $c_i \equiv a_i + b_i \ mod \ p$

Result 2 (Subtraction)
$\forall p \in \mathbb{P}, \ m \in \mathbb{N}, \ A_{(x)} \ B_{(x)} \ C_{(x)} \in G\mathcal{F}_{p^m}, \ A_{(x)} \ominus B_{(x)} = C_{(x)} = \sum_{i=0}^{m} c_i * x^i$
with $c_i \equiv a_i - b_i \ mod \ p$

Result 3 (Equivalence)
$\forall m \in \mathbb{N}, \ A_{(x)} \ B_{(x)} \in G\mathcal{F}_{2^m}, \ A_{(x)} \oplus B_{(x)} = A_{(x)} \ominus B_{(x)}$

For each extended Galois Field $G\mathcal{F}_{m^p}$, an irreducible polynomial $P_{(x)}$ is defined from AES [1, 16]. This polynomial is defined on $G\mathcal{F}_{p^m+1}$. Using $P_{(x)}$, we can now define the multiplication, the inverse and the division operations.

Result 4 (Multiplication)
$\forall p \in \mathbb{P}, \ m \in \mathbb{N}, \ A_{(x)} \ B_{(x)} \ C_{(x)} \in G\mathcal{F}_{p^m} \ P_{(x)} \in G\mathcal{F}_{p^m+1},$
$C_{(x)} = A_{(x)} \otimes B_{(x)} \equiv A_{(x)} * B_{(x)} \ mod \ P_{(x)}$

Result 5 (Inverse)
$\forall p \in \mathbb{P}, \ m \in \mathbb{N}, \ A_{(x)} \in G\mathcal{F}_{p^m} \ P_{(x)} \in G\mathcal{F}_{p^m+1}, \ A_{(x)} \otimes A_{(x)}^{-1} \equiv 1 \ mod \ P_{(x)}$

Result 6 (Division)
$\forall p \in \mathbb{P}, \ m \in \mathbb{N}, \ A_{(x)} \ B_{(x)} \ C_{(x)} \in G\mathcal{F}_{p^m} \ P_{(x)} \in G\mathcal{F}_{p^m+1},$
$C_{(x)} = A_{(x)} \oslash B_{(x)} \equiv A_{(x)} * B_{(x)}^{-1} \ mod \ P_{(x)}$

Example 2
With $p = 2$ and $m = 3$ $(G\mathcal{F}_{2^3})$, $P_{(x)} = x^3 + x + 1$.
Let's define $A_{(x)} = x^2 + x + 1$ and $B_{(x)} = x^2 + 1$.

$$\begin{aligned} A_{(x)} \otimes B_{(x)} \quad = \quad A_{(x)} * B_{(x)} \quad &\equiv \quad (x^2 + x + 1) * (x^2 + 1) \ mod \ P_{(x)} \\ &\equiv \quad (x^2 + x + 1) * (x^2 + 1) \ mod \ P_{(x)} \\ &\equiv \quad x^4 + x^3 + x^2 + x^2 + x + 1 \ mod \ P_{(x)} \\ &\equiv \quad x^4 + x^3 + x + 1 \ mod \ P_{(x)} \\ &\equiv \quad (x^3 + x + 1)(x + 1) + (x^2 + x) \ mod \ P_{(x)} \\ &= \quad x^2 + x \end{aligned}$$

3 Elliptic Curves

Definition 1 (Elliptic Curve (EC))
In mathematics, an elliptic curve is a plane and symmetric algebraic curve defined by an equation of the form $y^2 = x^3 + a.x + b$ with x y a $b \in \mathbb{Z}$. The Figure below presents an example of an elliptic curve.

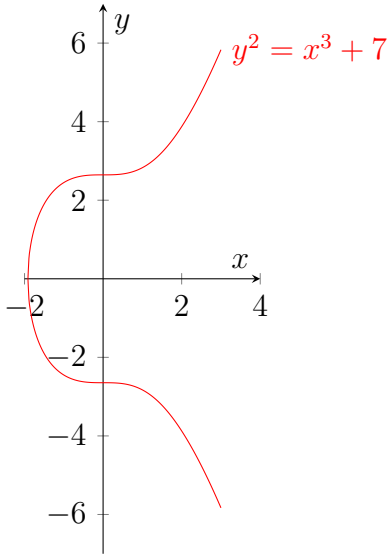

Figure 1: Example of an elliptic curve defined by $y^2 = x^3 + 7$

3.1 Elliptic Curves using cyclic finite groups

Definition 2 (Elliptic Curve Cyclic (ECC))
Considering a value $m \in \mathbb{Z}$ with $m > 3$, we can define a cyclic group from the EC equation: $y^2 = x^3 + a.x + b$ curve defined by an equation of the form $y^2 \equiv x^3 + a.x + b \ mod \ m$ with x y a $b \in \mathbb{Z}$. In other words, the ECC group based on the modular group $\mathbb{Z}_m$ is the set of all pairs (x, y) verifying $y^2 \equiv x^3 + a.x + b \ mod \ m$.

Definition 3 (Operator • for ECC)
Considering a cyclic group G defined by $y^2 \equiv x^3 + a.x + b \ mod \ m$. We can set $\bullet$, a binary operator such that:

- $\bullet$ *is closed:* $\forall a \ b \in G, (a \bullet b) \in G$
- $\bullet$ *is associative:* $\forall a \ b \ c \in G, a \bullet (b \bullet c) = (a \bullet b) \bullet c$
- $\bullet$ *is commutative:* $\forall a \ b \in G, a \bullet b = a \bullet b$
- $\bullet$ *has a neutral element $\iota_\bullet$:* $\forall a \in G, a \bullet \iota_\bullet = \iota_\bullet \bullet a = a$
- *There exists an inverse for every element of G:* $\forall a \in G, \exists a^{-1}, a \bullet a^{-1} = a^{-1} \bullet a = \iota_\bullet$

$\bullet$ is then defined, for every element $A(x_A, y_A)$ and $B(x_B, y_B)$ of ECC, by $A \bullet B = C(x_C, y_C)$ with $x_C = s^2 - x_A - x_B \ mod \ m$ and $y_C = s(x_A - x_C) - y_A \ mod \ m$. The value of s depends on the equality of A and B.

- if $A = B$, $s = (y_B - y_A)(x_B - x_A)^{-1} \ mod \ m$
- $s = (3x_A^2 + a)(2y_A) \ mod \ m$ otherwise $(A \neq B)$

From a primitive element P, we can start a cyclic group G. We can enumerate all the elements of the group from P. Because $\bullet$ is closed, for every element $Q \in G$, $P \bullet Q \in G$. A enumeration of the elements would be $P; 2P; 3P; ...; qP$ with q the number of elements in G.

Example 3
A primitive element for E : $y^2 \equiv x^3 + a.x + b \ mod \ m$: $A(5, 1)$.
By calculation of the elements in E, we obtain $q = 19$

Result 7
For a group on a elliptic curve E, defined from the primitive P and containing q elements, $P \bullet qP = \iota_\bullet$.

3.2 Elliptic Curves using extended Galois Fields

In the same way, we can define the elliptic curves using Galois Fields.

Definition 4 (Elliptic Curve Cyclic groups with $G\mathcal{F}_p m$)
Using $G\mathcal{F}_p m$, the elliptic curve is not symmetric anymore. A group G is defined by all $X \ Y \in G\mathcal{F}_p m$ which respects $Y^2 + XY \equiv X^3 + a.X^2 + b \ mod \ P_{(x)}$ with $P_{(x)}$ an irreducible polynomial for $G\mathcal{F}_p m$.

The operator $\bullet$ is defined, for every element $A(x_A, y_A)$ and $B(B_{(x)}, B_{(y)})$ of ECC, by $A \bullet B = C(x_C, y_C)$ with

- if $A = B$,
  $s \equiv x_A + y_A(x_A)^{-1} \ mod \ P_{(x)}$
  $x_C \equiv s^2 + s + a \ mod \ P_{(x)}$
  $y_C \equiv s(x_A + x_C) + x_C + y_A \ mod \ P_{(x)}$

– if $A \neq B$,
$s \equiv (y_B + y_A)(x_B + x_A)^{-1}\ mod\ P_{(x)}$
$x_C \equiv s^2 + s + x_A + x_B + a\ mod\ P_{(x)}$
$y_C \equiv s(x_A + x_C) + x_C + y_A\ mod\ P_{(x)}$

Here again, from a primitive element P, we can start a cyclic group G. We can enumerate all the elements of the group from P. However, the elements in G are defined by polynomials. The list of the polynomials can be generated from $g = x$, a generator from the group. To get the next polynomial of a polynomial q, we calculate $q.g\ mod\ P_{(x)}$.

Result 8
Every polynomials in a cyclic group $G\mathcal{F}_{p^m}$ defined with the irreducible polynomial $P_{(x)}$, and generated with g, can be expressed by g^n with n an integer included between 0 and $p^m - 2$.

Result 9
Because $G\mathcal{F}_{p^m}$ is a cyclic group of 2^m elements, the inverse of a polynomial g^n is a polynomial $g^{n'}$ with $n' = p^m - 1$

Example 4
Let's consider the group $G\mathcal{F}_{2^4}$, with the generator $g = x$ and $P_{(x)} = x^4 + x + 1$. We set the elliptic curve E over $G\mathcal{F}_{2^4}$ defined by all pairs (x, y) respecting $Y^2 + xy \equiv x^3 + g^4.x^2 + 1\ mod\ P_{(x)}$.
The number q of elements on E is equal to 15, and the inverse of g^x is equal to $g^{-x} = g^{(2^m-1)-x} = g^{15-x}$

4 Digital Signature

4.1 Protection by Identification

Because of privacy, the content of sent data must be hidden. Encryption techniques have been designed to protect the content of data however. The messages are exchanged from a machine to another one, and are encrypted using keys. Each user has a set of two related keys: a public key, and a private key. The public key is, as indicated by its name, public and can be widely shared. The private key is only known by its owner. The sender uses the receiver's public key to encrypt its message, and the receivers use his private key to decrypt.

However, the messages are usually exchanged on open networks environment. This aspect of communication leads to possibility of security problems. A famous example is the "man-in-the-middle" attack. While communication is initialized between two users, a third malicious user, can intercept the communication and alter its content. The receiver thinks he is receiving a message from the sender while he is actually receiving it from someone else.

The ensure the identity of the sender and the content of the message is correct, digital signatures have been established. The receiver doesn't need to know how the signature has been encrypted but how to decrypt it, to be sure that the message has not been corrupted.

Assuming that each user has a pair of public and private key, a digital signature is generated as following:

1. The sender generates a signature depending on the content of the message and the private key and his private key. The use of hash function on the message content to generate the signature is used during the generation. More ephemeral values, higher is the security of the signature. The advantage of using ephemeral is that, from the same message, you get different signatures. In the same way, the chosen values used to sign the message must be high to increase the complexity of a possible decryption. Basically, the private key of the sender is signing the message transmitter, and the hash function the message content.

2. The receiver receives the message, and using the public key of the sender, he must be able to ensure the correctness of the message. If a hash function has been used during the encryption, the same one must be used during the decryption. For this reason, the hash function must be a part of the public key.

There exists several ways to generate a digital signature. The two most factors of the generation are: (i) the used algebra or arithmetic technique; and (ii) the hash function to sign the content of the message. We present below a way to generate digital signature using elliptic curve theory and more precisely using extended Galois fields applied to elliptic curve theory.

4.2 DSA with ECC

4.2.1 Generation

An Elliptic Curve can be used to generate a digital signature. The approach works because of the cyclic aspect of a group generated from an elliptic curve. From a group, defined by elliptic curve equation $E : y^2 \equiv x^3+a.x+b[m]$, and a primitive $A = (x_A, y_A)$, a set of q points can be generated. To generate a private key, the sender picks one of these numbers, defined by B, such as there exists $d \in \{1..q-1\}$ which verifies $B = dA$. This pair of coordinates are the "private" base of the signature. The ephemeral aspect of the signature is represented by a number $k_E \in \{1..q-1\}$ in order to get $R = k_E A = (x_R, y_R)$. To create the final signature, we also need to introduce a message-related part, using a hash function h. These three aspects are combined into a value S such as, for a specific message M, $S \equiv (h(M)+d.x_R)k_E^{-1}\ mod\ q$. k_E^{-1} is defined such as $k_E^{-1}.k_E \equiv 1\ mod\ q$. The message transmitter will share the following values with the receiver: $(m,\ a,\ b,\ q,\ A,\ B,\ h)$. The signature is now fitted as $(x_R,\ S)$.

4.2.2 Verification

The receiver of the message has now all the keys to verify the correctness of the signature. Because x_R is used to generate S, it is possible to retrieve the value of x_R by inversion. Considering W the inverse of S modulo q, that is $W.S \equiv 1\ mod\ q$, we can "eliminate" the variables around X_r in the calculation of S. The primitive element A and the resulting value B from the private key are known. It appears that $R = W.h(M).A + W.r.B\ mod\ q$ then we the receiver can defined $P = (W.h(M)\ mod\ q)A + (W.r\ mod\ q)B = (x_P, y_P)$. The proof is provided below. Because he doesn't know R, can test the equality $P = R$. However, he knows x_R thus he can perform the test $x_P = x_R$. If the equality is true, then the signature of the message can be considered correct.

4.2.3 Proof

$$
\begin{aligned}
S &\equiv (h(M) + d.r)k_E^{-1} \ mod \ q \\
k_E S &\equiv (h(M) + d.r) \ mod \ q \\
k_E &\equiv (h(M) + d.r)S^{-1} \ mod \ q \\
k_E &\equiv (h(M) + d.r)W \ mod \ q \\
k_E &\equiv W.h(M) + W.d.r \ mod \ q \\
k_E.A &= (W.h(M) + W.d.r \ mod \ q).A \\
k_E.A &= (W.h(M) \ mod \ q).A + (W.d.r \ mod \ q).A \\
k_E.A &= (W.h(M) \ mod \ q).A + (W.r \ mod \ q).d.A \\
k_E.A &= (W.h(M) \ mod \ q).A + (W.r \ mod \ q)B \qquad \square
\end{aligned}
$$

4.3 DSA with ECC using Extended Galois Field

4.3.1 Generation

The exact same approach can be used with Extend Galois field. According to the elliptic curve using Galois fields definition, the equation of the curve is $E : y^2 + xy \equiv x^3 + a.x^2 + b \ mod \ P_{(x)}$ and gets a primitive element A. x,y and $P_{(x)}$ are depending on the used extended Galois field $G\mathcal{F}_{p^m}$. A point B can be created using the private key d such that $d \in \{1..q-1\}$ with q the number of different points on E from the primitive A. An ephemeral number $k_E \in \{1..q-1\}$ is used to set $R = k_E A = (x_R, y_R)$. Because we are handling values on an extended Galois field, x_R is defined by a polynomial $R_{(x)}$ represented with a binary number. By base conversion, we get r, such that $x_{R\ 2} \rightarrow_{10} r$. As previously, S can be defined for a specific message M, by $S \equiv (h(M) + d.x_R)k_E^{-1} \ mod \ q$. Finally, the signature of the message is $(x_R,\ S)$. and $(a,\ b,\ P_{(x)},\ A,\ B,\ h)$ will be shared with the receiver.

4.3.2 Verification and Proof

The verification of the signature and the proof of correctness of the verification are exactly the same ones than the digital signature using ECC.

5 Related Work

Hash functions One of the important aspect of the signature security is the hash function used to generate the signature. Different Secure Hash Algorithm (SHA) have been designed through the years. Important properties must be set.

1. The function must be defined for each entry;
2. The returned values must have the same size, independently of the entry;
3. To be secured, collisions not be able to happen. That is, two different entries can return the same result.

The most recent works on SHA have been organized in a programming contest. The goal of the competition was to design a more secure hash function than the existing ones. The

National Institute of Standards and Technology (NIST) used the approach to create the standard SHA-3 [12, 22].

Digital signatures There exists other way to generate a digital signature. For example, [10] presents a signature produced using RSA [11]. In 1984, Taher Elgamal designated a signature based on cyclic groups and discrete logarithms [8]. The NIST has also its own standard for signature generation based on big numbers [17]. Other generators are based on large numbers. Using smart cards [9], Schnorr designated a very secure digital signature on [20, 21].

Cryptography The encryption of the message, to hide its content, can be performed using algorithms such as DES [5] or AES [3]. The second one is a completely public algorithm, very often used as a standard for encryption. For example, Contiki [2, 4], the Open Source OS for Internet of Things (IoT), implements it, and its correctness [18] has been ensured using formal methods by French teams.

6 Conclusion

We have presented how to protect a message based on a signature approach. From the Galois fields theory, combined with the elliptic curves, it is possible to create a strong signature. The complexity and the security of the signature have not been discussed in this paper but the study of how robust is the digital can be made as future work.

References

[1] Announcing approval of Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard (AES). 11 2001.

[2] John Barton and Erik Jung. *Distributed, Embedded Sensor and Actuator Platforms*, pages 105–129. Springer US, Boston, MA, 2008.

[3] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanalysis of the full aes. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology – ASIACRYPT 2011*, pages 344–371, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[4] L. Bruno, M. Franceschinis, C. Pastrone, R. Tomasi, and M. Spirito. 6lowdtn: Ipv6-enabled delay-tolerant wsns for contiki. In *2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, pages 1–6, June 2011.

[5] D. Coppersmith. The data encryption standard (des) and its strength against attacks. *IBM Journal of Research and Development*, 38(3):243–250, May 1994.

[6] Desoky and Ashikhmin. Cryptography software system using galois field arithmetic. In *2006 IEEE Information Assurance Workshop*, pages 386–387, June 2006.

[7] Whitfield Diffie and Martin E. Hellman. Exhaustive cryptanalysis of the NBS Data Encryption Standard. 10(6):74–84, June 1977.

[8] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In George Robert Blakley and David Chaum, editors, *Advances in Cryptology*, pages 10–18, Berlin, Heidelberg, 1985. Springer Berlin Heidelberg.

[9] G. Jaspher, W. Kathrine, E. Kirubakaran, and Parul Prakash. Smart card based remote user authentication schemes: A survey. *Procedia Engineering*, 38:1318 – 1326, 2012. INTERNATIONAL CONFERENCE ON MODELLING OPTIMIZATION AND COMPUTING.

[10] Burt Kaliski. RSA digital signature scheme. In *Encyclopedia of Cryptography and Security, 2nd Ed.*, pages 1061–1064. 2011.

[11] Stefan Katzenbeisser. *Recent Advances in RSA Cryptography*, volume 3. 01 2001.

[12] J. Kelsey, S. Change, R. Perlner, Information Technology Laboratory (National Institute of Standards, and Technology). *SHA-3 Derived Functions: CSHAKE, KMAC, TupleHash and ParallelHash*. NIST special publication; NIST special pub; NIST SP. U.S. Department of Commerce, National Institute of Standards and Technology, 2016.

[13] L. Lan. The aes encryption and decryption realization based on fpga. In *2011 Seventh International Conference on Computational Intelligence and Security*, pages 603–607, Dec 2011.

[14] Phil Lucht. Galois fields and cyclic codes, 08 2013.

[15] National Bureau of Standards. *Data Encryption Standard*. U. S. Department of Commerce, Washington, DC, USA, January 1977.

[16] Harris Nover and M K. Algebraic cryptanalysis of aes: an overview. 2004.

[17] National Institute of Standards, Technology (U.S.), Information Technology Laboratory (National Institute of Standards, and Technology). *Digital Signature Standard (DSS)*. Federal information processing standards publication. U.S. Department of Commerce, Technology Administration, Information Technology Laboratory, National Institute of Standards and Technology, 2000.

[18] Alexandre Peyrard, Nikolai Kosmatov, Simon Duquennoy, and Shahid Raza. Towards Formal Verification of Contiki: Analysis of the AES–CCM* Modules with Frama-C. In *RED-IOT 2018 - Workshop on Recent advances in secure management of data and resources in the IoT*, Madrid, Spain, February 2018.

[19] Klaus Schmeh. The east german encryption machine T-310 and the algorithm it used. *Cryptologia*, 30(3):251–257, 2006.

[20] C. P. Schnorr. Efficient identification and signatures for smart cards. In Gilles Brassard, editor, *Advances in Cryptology — CRYPTO' 89 Proceedings*, pages 239–252, New York, NY, 1990. Springer New York.

[21] C. P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161–174, Jan 1991.

[22] N.I.N.I.S. Technology. *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions: FiPS PUB 202*. CreateSpace Independent Publishing Platform, 2015.