International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 2, Issue 5, May 2015)

Microblaze implementation of hb-2 crypto system with its cryptosystem with its authentication protocol

Sapna S
Digital Communication & Networking
Electronics &communication
PACE, Mangalore, India
sapna00765@gmail.com

Chandana B R
Digital Communication & Networking
Electronics &communication
PACE, Mangalore, India
Chandanaramya1@gmail.com

***Abstract*— Information technologies widely penetrate into people's day-to-day activity. This is one of the main trends of present-day society. An average man's life cannot be imagined without various gadgets. A lot of households use devices with an embedded operating system (besides usual personal computers), which can be connected to the Internet and can even be united into a wireless network. Everywhere people are surrounded by a variety of terminals, readers, sensors etc. Such expansion of smart technologies crucially raises data security problems. However, now it is impossible to suggest a cryptographic primitive that can be implemented in all types of target devices. We can tell that AES is a really strong algorithm with good performance. It is absolutely advisable to use AES in high-end devices, in a large variety of embedded systems or in some low-end devices (with several constraints). But it is impossible to use common cryptographic algorithms in specific devices with extremely constrained resources. The examples of such devices include:**

• RFIDs;

• Low-end smart cards (including wireless);

• Wireless sensors;

• Indicators, measuring devices, custom controllers etc.

The underlying principles and approaches to the design of algorithms intended for use in devices with extremely low resources are slightly different from the design criteria of commonly used cryptographic algorithms. This very specific field is covered by a branch of modern cryptography lightweight cryptography. Lightweight cryptography is a branch of the modern cryptography, which covers cryptographic algorithms intended for use in devices with low or extremely low resources.

***Index Terms*- cryptography, Hummingbird, cryptosystems, light weight cryptography, etc.**

I. Introduction

Modern cryptography concerns itself with the following four objectives:

1. Confidentiality (the information cannot be understood by anyone for whom it was unintended)
2. Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
3. Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)
4. Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information)

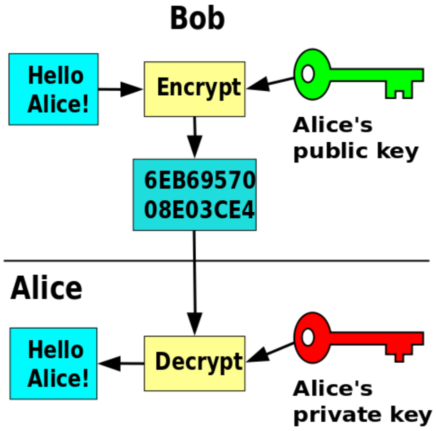

Figure 1: Illustration of cryptography

Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders.

1.1 Light-Weight Cryptography

There are several emerging areas in which highly constrained devices are interconnected, typically communicating wirelessly with one another, working in concert to accomplish some task. Examples of these areas include: sensor networks, healthcare, distributed control systems, the Internet of Things, cyber-physical systems, and the smart grid. Security and privacy can be very important in all of these areas. Because the majority of modern cryptographic algorithms were designed for desktop/server environments, many of these algorithms cannot be implemented in the devices used by these applications. When current algorithms can be engineered to fit into the limited resources of constrained environments, their performance is typically not acceptable. Therefore a new class of cryptography systems are designed for resource constrained devices and these systems are known as light-weight cryptosystems.

1.2 Humming Bird

Hummingbird is a recently proposed ultra-lightweight cryptographic algorithm targeted for low cost smart devices like RFID tags, smart cards, and wireless sensor nodes. It has a hybrid structure of block cipher and stream cipher and was developed with both lightweight software and lightweight hardware implementations for constrained devices in mind.

Moreover, Hummingbird has been shown to be resistant to the most common attacks to block ciphers and stream ciphers including birthday attack, differential and linear cryptanalysis, structure attacks, algebraic attacks, cube attacks, etc.

In practice, Hummingbird has been implemented across a wide range of different target platforms. Those implementations demonstrate that Hummingbird provides efficient and flexible software solutions for various embedded applications. However, the hardware performance of Hummingbird has not yet been investigated in detail.

II. Objectives

The following are the objectives of the project:

1. Study the design a HB-2 Cryptosystem and modify it based on DES cryptosystem
2. Create a RTL design of the proposed system
3. Simulate it using a test bench
4. Observe the implementation parameters.

III. Methologies

The project will be carried out in the following stages:

1. Further literature survey has to carried out to extract more ideas
2. A design plan should be created with an application
3. RTL Design of the proposed design should made
4. RTL verification should be done to make sure the design is working as decided
5. Next, speed, area, power and other parameters should be observed and tabulated.
6. Comparison of the parameters should be done.

IV. FPGA Implementation Flow

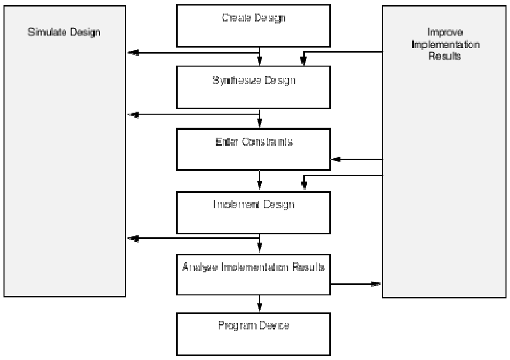

Figure 2: Design Flow

Implementation

After synthesis, you run design implementation, which converts the logical design into a physical file format that can be downloaded to the selected target device.

After synthesis, you run design implementation, which comprises the following steps:

1. **Translate** - merges the incoming net lists and constraints into a Xilinx design file.
2. **Map** - fits the design into the available resources on the target device, and optionally, places the design.
3. **Place and Route -** places and routes the design to the timing constraints.
4. **Generate Programming File -** creates a bit stream file that can be downloaded to the device.

Using the Project Navigator Design Goals and Strategies, you can modify process properties to control the implementation and optimization of the design.

V. Design Specification

Specification

The following are the design specifications of the main project:

1. A module for implementing the previously described logic needs to be developed using Verilog. Encryption, decryption and initialization all of these should be present as one module such that all of them can be implemented for FPGA.
2. The module should be made implementable on FPGA
3. A test-bench should be written to verify the functionality of the FPGA module

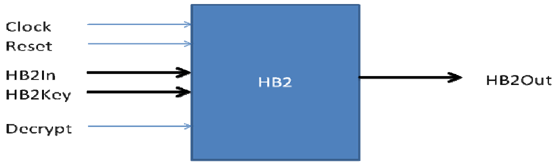

Figure 3: Top-level pin out diagram for the Hummingbird module

VI. Comparison & Results

Data Comparison

Table 1: Data Comparison Table.

Mode	*Input Data*	*Input Key*	*Output*	*Result*
Encryption	95F8A5E5DD31D900	**0101010101010101** **0101010101010101** **0101010101010101**	8000000000000000	PASS
Decryption	8000000000000000	**0202020202020202** **0101010101010101** **0101010101010101**	dbbc229fcfa9cc39	**FAIL**
Decryption	8000000000000000	**0101010101010101** **0101010101010101** **0101010101010101**	95F8A5E5DD31D900	PASS

Comparison of parameters with previous work

	Paper [1]	Our Design
Frequency	32.2 MHz	153.563 MHz
LUTs	1024	1276
Flip-flops	145	64
Slices	558	684
Power	Not done	34.06mW

Table 2: Comparison of parameters with previous work.

VII. Applications

Generally the light-weight cryptosystems are designed not be working as a standalone system. It is designed to be a part of the systems in which it is installed. In that light, we have the following applications for the Hummingbird-2 algorithm.

1. Hybrid firmware encryption

Hybrid firmware is a class of software which interacts closely with the hardware and responsible for their correct operation. These are generally proprietary for a system and require some amount of security to prevent reverse engineering and other piracy problems.

2. Wireless sensor networks

A wireless sensor network (WSN) are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

These nodes are limited in resources and Hummingbird-2 will be an excellent cryptography protocol to use here.

3. Challenge response protocols

In computer security, challenge-response authentication is a family of protocols in which one party presents a question ("challenge") and another party must provide a valid answer ("response") to be authenticated. The simplest example of a challenge-response protocol is password authentication, where the challenge is asking for the password and the valid response is the correct password. Clearly an adversary who can eavesdrop on a password authentication can then authenticate itself in the same way. One solution is to issue multiple passwords, each of them marked with an identifier.

4. Key-establishment protocols

In cryptography, a key-agreement protocol is a protocol whereby two or more parties can agree on a key in such a way that both influence the outcome. If properly done, this precludes undesired third parties from forcing a key choice on the agreeing parties. Protocols that are useful in practice also do not reveal to any eavesdropping party what key has been agreed upon.

Many key exchange systems have one party generate the key, and simply send that key to the other party -- the other party has no influence on the key. Using a key-agreement protocol avoids some of the key distribution problems associated with such systems.

5. Electronic bio-metric passports

A biometric passport, also known as an e-passport, ePassport or a digital passport, is a combined paper and electronic passport that contains biometric information that can be used to authenticate the identity of travelers. It uses contactless smart card technology, including a microprocessor chip (computer chip) and antenna (for both power to the chip and communication) embedded in the front or back cover, or center page, of the passport. Document and chip characteristics are documented in the International Civil Aviation Organization's (ICAO) Doc 9303. The passport's critical information is both printed on the data page of the passport and stored in the chip. Public Key Infrastructure (PKI) is used to authenticate the data stored electronically in the passport chip making it expensive and difficult to forge when all security mechanisms are fully and correctly implemented.

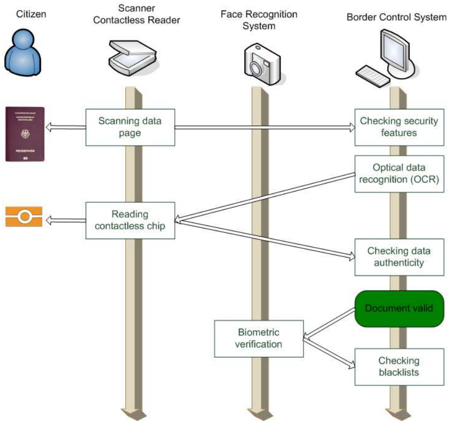

Fig 8.1 Electronics passport reading process

6. Contactless payment

Contactless payment systems are credit cards and debit cards, key fobs, smartcards or other devices that use radio-frequency identification for making secure payments. The embedded chip and antenna enable consumers to wave their card or fob over a reader at the point of sale.

Fig 8.2 Contactless payment

7. Supply chain management

A supply chain attack is a cryptographic attack where a product, typically a device that performs encryption or secure transactions, is tampered with during manufacture or while it is still in the supply chain by persons with physical access. The tampering may, for example, install a root-kit or hardware-based spying components.

8. MANETS

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Ad hoc is Latin and means "for this purpose".

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

Vehicular Ad hoc Networks (VANETs) are used for communication between vehicles and roadside equipment. Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents.

Smart Phone Ad hoc Networks (SPANs) leverage the existing hardware (primarily Bluetooth and Wi-Fi) in commercially available smart phones to create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. SPANs differ from traditional hub and spoke networks, such as Wi-Fi Direct, in that they support multi-hop relays and there is no notion of a group leader so peers can join and leave at will without destroying the network.

Internet based mobile ad hoc networks (iMANETs) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. For example, multiple sub-MANETs may be connected in a classic Hub-Spoke VPN to create a geographically distributed MANET. In such type of networks normal ad hoc routing algorithms don't apply directly. One implementation of this is Persistent System's Cloud Relay.

Military / Tactical MANETs are used by military units with emphasis on security, range, and integration with existing systems. Common waveforms include the US Army's SRW, Harris's ANW2 and HNW, Persistent Systems' Wave Relay, Trellisware's TSM and Silvus Technologies' StreamCaster.

A mobile ad-hoc network (MANET) is an ad-hoc network but an ad-hoc network is not necessarily a MANET.

9. Home automation

Home automation is the residential extension of building automation. It is automation of the home, housework or household activity. Home automation may include centralized control of lighting, HVAC (heating, ventilation and air conditioning), appliances, security locks of gates and doors and other systems, to provide improved convenience, comfort, energy efficiency and security. Home automation for the elderly and disabled can provide increased quality of life for persons who might otherwise require caregivers or institutional care.

ZigBee is enabling technology of Home automation which designates an emerging practice of increased automation of intelligent appliances and household applications. ZigBee has many advantages of high availability, low power consumption, low cost which ideal for residential setting. But, security features in ZigBee networks which required a number of keys, consisting of master keys, network keys, link keys and don't offer various services depended on users. This paper proposes an application of attributed-based cryptography for security in ZigBee networks. The proposal offers various services in ZigBee networks using attributes, and reduces the number of keys which is useful in automation where various electronic devices communicate each other.

10. Internet-of-Things

The Internet of Things (IoT) is the network of physical objects or "things" embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure.

Things, in the IoT, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, or field operation devices that assist fire-fighters in search and rescue. These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices. Current market examples include smart thermostat systems and washer/dryers that utilize Wi-Fi for remote monitoring.

All the above are some of the major applications for the utilization of the Hummingbird-2 cryptography algorithm.

CONCLUSION & FUTURE WORK

In this chapter we present a novel ultra-lightweight cryptographic algorithm, Hummingbird,

which is a combination of block cipher and stream cipher. The hybrid structure adopted in Hummingbird can provide the designed security with small block size which is expected to meet the stringent response time and power consumption requirements in a large variety of embedded applications. We show that Hummingbird seems to be resistant to the most common attacks to block ciphers and stream ciphers including birthday attacks, differential and linear cryptanalysis, structure attacks, algebraic attacks, cube attacks, etc. Efficient software implementations of Hummingbird on 4-, 8- and 16-bit microcontrollers have been investigated. In this work, we see its efficiency on FPGA Verilog implementation as well.

In this work, we have created as system that is common for both encryption and decryption which help reduce area and increase speed. It also helps achieve better power efficiency.

Future work

Further, the Hummingbird-2 algorithm can be tried out for the following:

1. Soft-processors such as Microblaze and Nios II which form an integral part of the FPGA systems
2. Implemented as an application on Embedded Linux and other RTOS systems.
3. Implemented for the Android and iOS system such that it can be used in mobile systems.

REFERENCES

[1] L. Sterpone, M. SonzaReorda and M. Violante, “Evaluating Different Solutions to Design Fault Tolerant Sytems with SRAM-based FPGAs,” *Journal of Electronic Testing: Theory and Applications*, vol. 23, pp. 47-54, 2007.

[2] K. Kyriakoulakos and D. Pnevmatikatos, “A Novel SRAM-Based FPGA Architecture for Efficient TMR Fault Tolerance Support,” *International Conference on Field Programmable Logic and Applications*, pp. 193-198, 2009.

[3] L. Sterpone and M. Violantem, “Analysis of the Robustness of the TMR Architecture in SRAM-Based FPGAs”, *IEEE Trans. Nucl. Sci.*, vol. 52, no. 5, pp. 1545-1549, Oct. 2005.

[4] E. Stott, P. Sedcole, and P. Y.K. Cheung, “Fault Tolerant Methods for Reliability in FPGAs,” *International Conference on Field Programmable Logic and Applications*, pp. 415-420, 2008.

[5] S. Ghosh, P. Ndai and K. Roy, “A Novel Low Overhead Fault Tolerant Kogge-Stone Adder using Adaptive Clocking,” *Design, Automation and Test*, pp. 366-371, 2008.

[6] M. Abramovici, C. Stroud, C. Hamiltion, S. Wijesuriya, and V. Verma, “Using Roving STARs for On-Line Testing and Diagnisis of FPGAs in Fault-Tolerant Applications,” *Test Conference*, pp. 973-982, 1999.

[7] T. Lynch and E. E. Swartzlander, “A Spanning Tree Carry Lookahead Adder,” *IEEE Transactions on Computers*, vol. 41, no. 8, pp. 931-939, Aug. 1992.

[8] J. Vundavalli, “Design and Analysis of wide bit adders for FPGA Implementation,”
MSEE Thesis, University of Texas at Tyler, May 2010.

[9] D. H. K. Hoe, C. Martinez, and J. Vundavalli, “Design and Characterization of Parallel Prefix Adders using FPGAs,” *IEEE 43rd Southeastern Symposium on System Theory*, pp. 170-174, March 2011.

[10]] R. Iris, D. Hammerstrom, J. Harlow, W. H. Joyner Jr., C. Lau, D. Marculescu, A. Orailoglu, M. Pedram, “Architectures for Silicon Nanoelectronics and Beyond,” *Computer*, vol. 40, no. 1, pp. 25-33, Jan. 2007.

[11] J. M. Emmert, C. Stroud, and M. Abramovici, “Online Fault Tolerance for FPGA Logic Blocks,” *IEEE Trans. on VLSI Systems*, vol. 15, no. 2, pp. 216-226, February 2007.

[12] M. Abramovici, J. M. Emmert, and C. Stroud, “Roving STARs: An Integrated Approach to On-Line Testing, Diagnosis, and Fault Tolerance for FPGAs,” *NASA/ DoD Workshop on Evolvable Hardware*, pp. 73-92, 2001.

[13] N. H. E. Weste and D. Harris, *CMOS VLSI Design*, Pearson-Addison-Wesley, Third edition, 2005.

[14] N. Banerjee, C. Augustine, K. Roy, “Fault-Tolerance with Graceful Degradation in Quality: A Design Methodology and its Application to Digital Signal Processing Systems,” *IEEE International Symposium on, Defect and Fault Tolerance of VLSI Systems*, pp. 323-331, 1-3 Oct. 2008.