

The Search for the Anti-Bit

Ulrich Kaiser, Bob Luckin

Tixaltix GmbH, Freising, Germany
{ d-kaiser@ti.com, bob@ti.com }

Abstract Drawing parallels to the field of anti-matter in modern physics the existence of anti-bits is postulated. The theory of bit and anti-bit pairs is developed and related experiments are designed that make use of high-speed bit stream collisions. Several circuits and a measurement system approach are described. Stream ciphers play an important role for the generation of the arbitrary high-speed bit streams. Therefore, new developments during the eSTREAM project are also discussed. Due to the difficult calibrations needed significant results are not expected until the spring of 2007 at the earliest.

Introduction

Very often, significant advances in scientific knowledge in a given field of research can be made simply by drawing parallels from other, more established domains. This axiom, sometimes known as the Law of Similarity, is more widely recognized in some fields than others, but the principle is as true of computing as it is of any other scientific discipline. It has been widely documented by Bonewits [1], Hardy [2], and other researchers, and leads us to some interesting discoveries.

Let us consider the domain of physics / natural philosophy as an example; more specifically the realm of particle physics. The concept of anti-matter is well-known to the modern physicist. It is of course tied to the general philosophical concept of opposing dualities, which can be exemplified as: “for every Yin there must be an opposing Yang”. Thus the existence of matter implies the existence of anti-matter, a tenet subsequently verified by experimental observation (see appendix A).

Applying this principle to the discipline of computing leads us to the inevitable and obvious concept of the anti-bit. The anti-bit is the complement to the ‘elementary particle’ of computer science, the bit [5]. The existence of the anti-bit has yet to be proven experimentally, and several international research teams [5-8] at MIT, CERN and TU Garching are hunting for it - the problem is essentially one of detection.

Conditions for the Search

What conditions might produce anti-bits, and how can they be observed and identified ? From the Law of Similarity, we can deduce the following properties relating to bits and anti-bits:

1. A collision between a bit and an anti-bit should result in the annihilation of both.
2. Such a collision will result in the release of a certain amount of energy in some form.
3. There will be a corresponding perturbation in the local information field adjacent to the collision.

Unfortunately, these properties only relate to the destruction of the elusive anti-bit, and do not provide any clue regarding the conditions under which one could be formed. Where and when might we expect to find anti-bits occurring in detectable quantities ? Clearly the most likely time for this is just after they have been created, before they have had time to decay or be annihilated by a collision with a bit. Similarly, we should look in the area immediately proximate to that in which the creation takes place. What is needed then, is to

identify likely processes which should lead to the formation of anti-bits, and base our search upon these, to maximize the chances of detection.

Although the properties of the bit/anti-bit pair mentioned above do not provide us with a clue as to possible means of creating anti-bits, not all is lost. We can draw once again from the discipline of physics to give us help. It is known that whilst anti-matter is destroyed by collision (with matter), it can also be created by collision – under suitable conditions of high energy. We deduce that the same property should hold true for the anti-bit. Clearly one process which should lead to the creation of anti-bits is the high energy collision of datastreams, and this is where we should start our search.

Hardware for the Search and related Experiments

The block diagram of the unit that is responsible for the generation of the high-speed bit stream is depicted in figure 1. Data generated by means of Stream Cipher primitives is parallel-loaded into the SN65LVDS151 Serializer [9] input latches on the first rising edge of the MCLK, which is following a rising edge of the clock SCLK. SCLK is derived from MCLK by means of a clock divider with a factor of ten, and is also responsible for the internal clocking inside every Stream Cipher block. The data is sent out serially from the internal shift registers to output BS on the rising edges of MCLK. Data from input DI<0>, respectively StreamCipher<0>, is shifted out first. The maximum clock frequency for MCLK is 200 MHz, minimum is 50 MHz. (The most important thing to note about all of this is BS.)

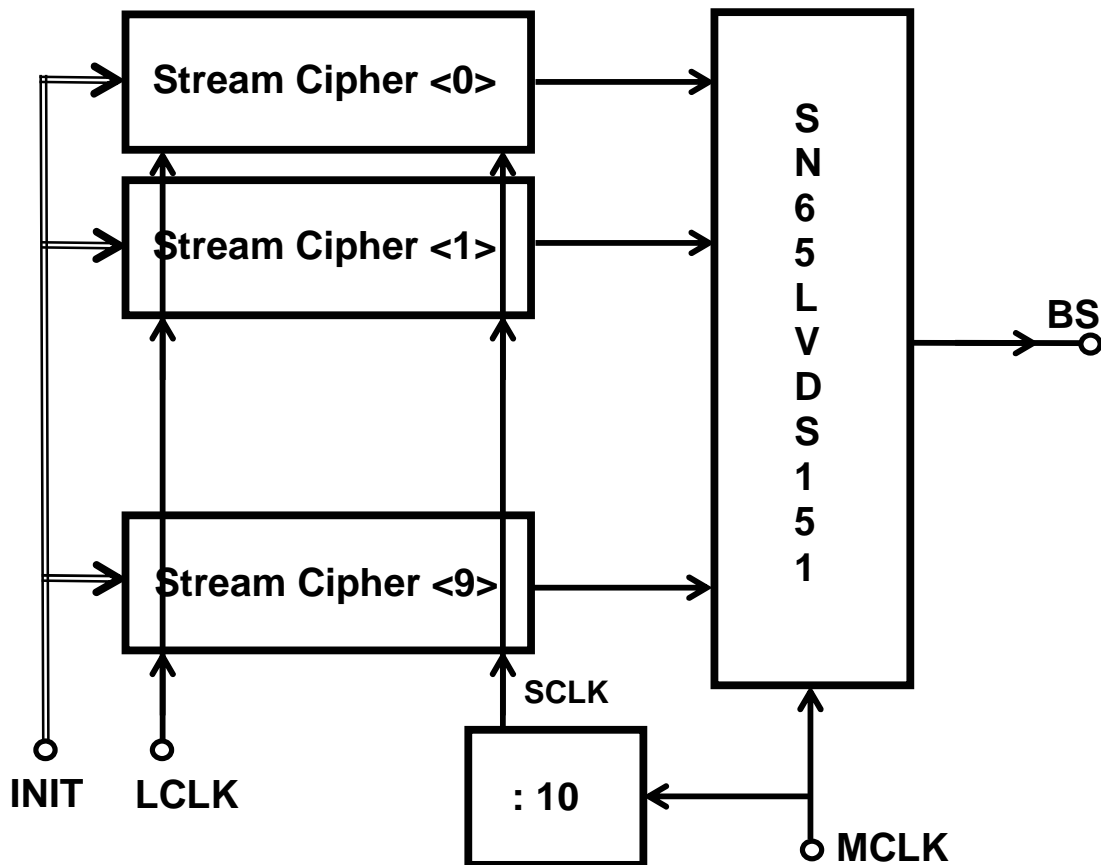


Figure 1 Block Diagram of the high-speed bit stream generation unit (BSG)

The different Stream Ciphers are loaded at the beginning of each experiment via the data bus INIT and supporting clock LCLK. The data loaded consists of initialization vectors, cryptographic keys and configuration data. The StreamCipher(s) chosen must support an output data rate of 5 to 20 Mhz. They are realized by means of FPGA designs to allow them to be exchanged easily. (Note: for the sake of clarity, other necessary signals of this unit have been omitted in the diagram.)

In order to give the bit stream the highest energy possible a special circuit (HSBD) was designed in high-speed Advanced Schottky TTL technology. This bit driver is able to amplify input signals of 200 MHz without problems and drives up to 4.1 Amperes at the output (push-pull stage) at ambient temperature. Figure 2 shows the schematic diagram of this high-speed driver which consists of Schottky-Transistors to fulfill the requirement of sufficient drive strength at high speed. The Schottky-NPN at the input node and the Schottky-Diode at the output node are countermeasures with respect to Electro-Static Discharge (ESD) strikes.

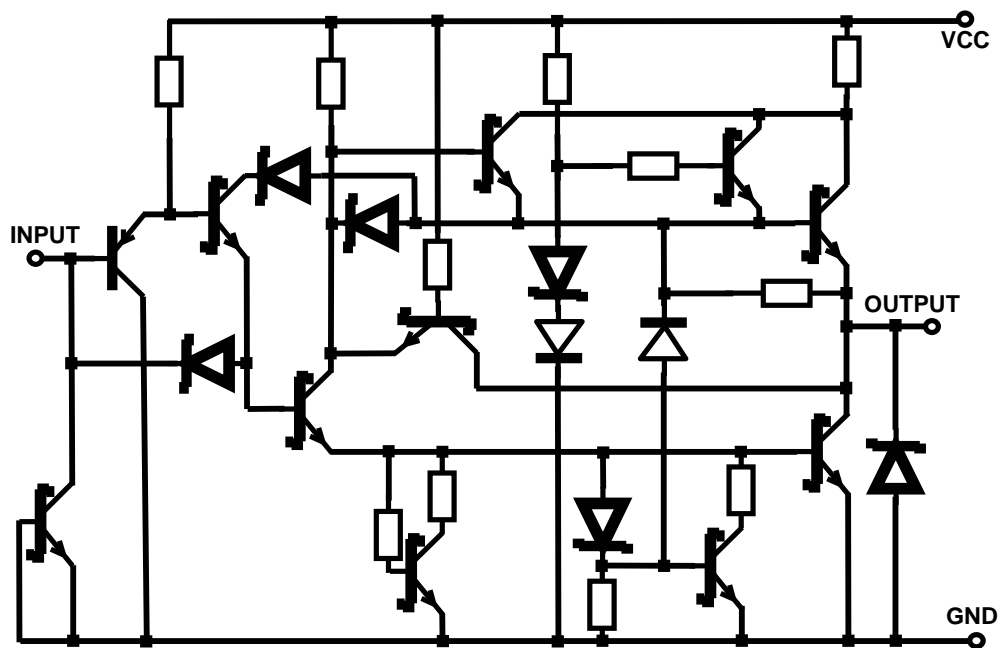


Figure 2 Schematic Diagram of the high-speed bit driver (HSBD)

The 3D Detection Sensor (DS) is illustrated in figure 3. The sensor consists of a semiconductor in cubical form, six electrodes (red) and three sensor pairs (dark blue). The donut-shaped electrodes (red) are used to apply six stimulating bit streams to the cube. Three sensor pairs are located in the middle of the donut electrodes. Each sensor pair is connected to one of the three sensor amplifiers. (Note: for the sake of clarity, the GND connections have been omitted in the drawing; all six corners are connected to ground potential.)

The semiconductor material should be chosen so that maximum sensitivity can be achieved. First experiments make use of GaInSb crystals of different sizes, because the wavelength of the bit/anti-bit pair (see appendix B) has yet to be determined with precision. The electrodes are prepared with gold and normal gold bond wires as found in current semiconductor packaging technology. The sensors are built by means of arsenic implants and gold contacts as well.

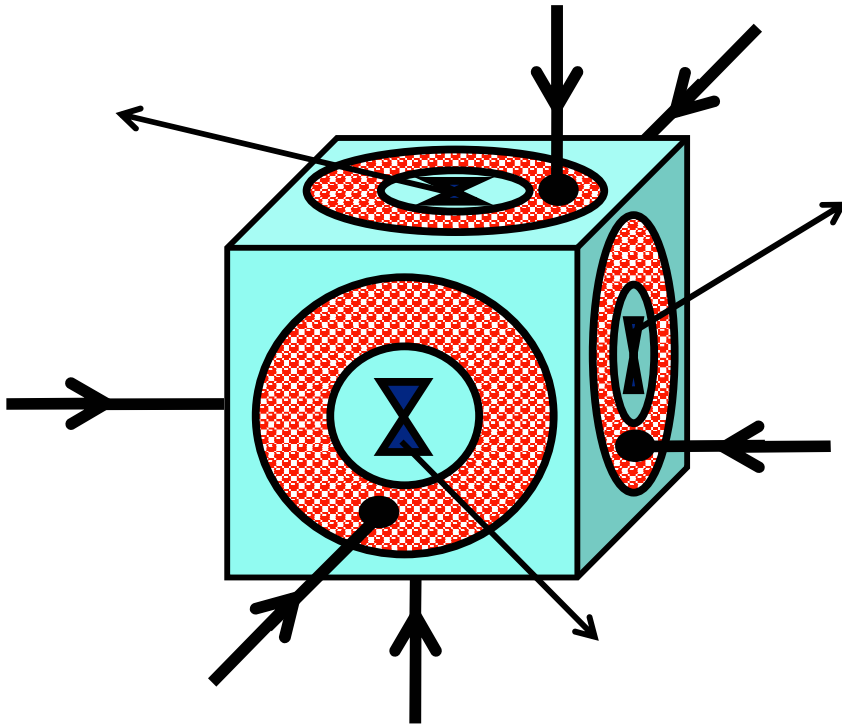


Figure 3 Drawing of the 3D detection sensor (DS)

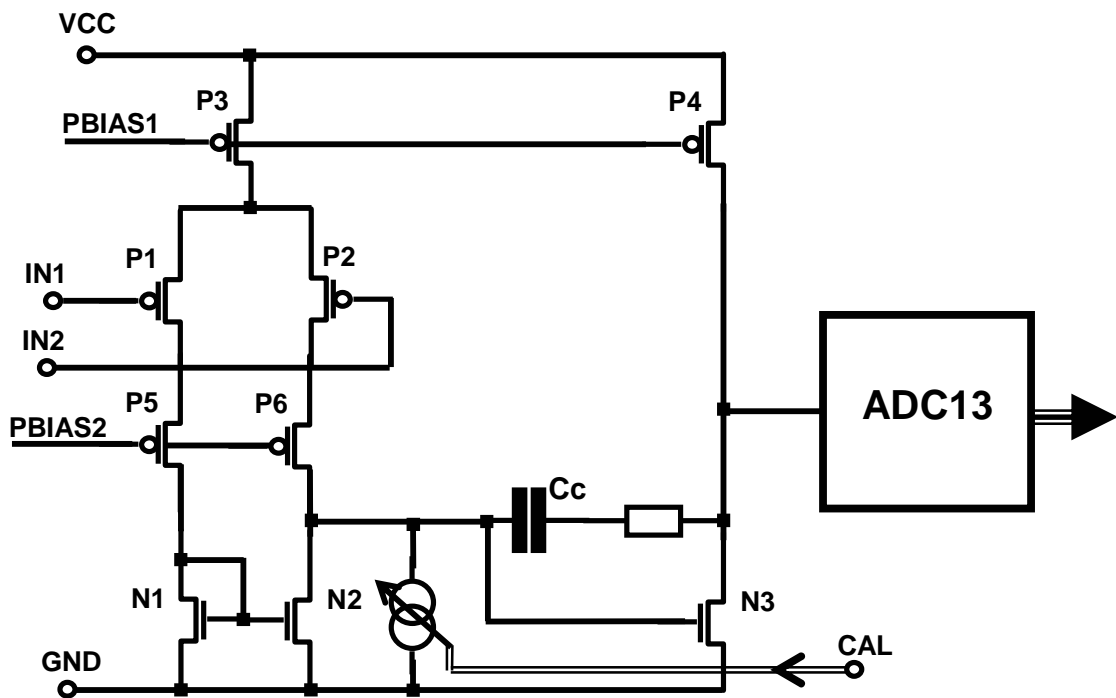


Figure 4 Diagram of one channel of the 3D sensor amplifier with digital output (SA)

Figure 4 shows one channel of the three channel (i.e. 3D) sensor amplifier with the related Analog-Digital-Converter (ADC). The amplifier consists of a differential amplifier stage with PMOS input transistors in order to support low-noise operation [10]. The input CAL is prepared for the calibration of the circuit by means of an external digitally controlled current source. The ADC is a converter with a 13-bit resolution; however, at 10MHz input frequency only 11.2 bits accuracy can be guaranteed [11].

Figure 5 presents the system containing six bit stream generators (BSG), three sensor amplifiers (SA), three sensor pairs (marked blue), one detector (marked red) and one cubicle chamber (marked green, transparent) for noise shielding with respect to the outer environment. Thus the system allows both 3D experiments and 3D measurements. The coordinates are marked with x, y, and z respectively. A separate workstation is connected to this system to enable the initialization of the stream ciphers, calibration of the sensor amplifiers, starting and stopping of the three main clocks MCLKx, MCLKy, and MCLKz, and the collection of measurement data from the sensor amplifiers. (Note: supporting signals are not shown here, for clarity; the same holds for power supplies, ground connections, the main oscillator and the main control unit.)

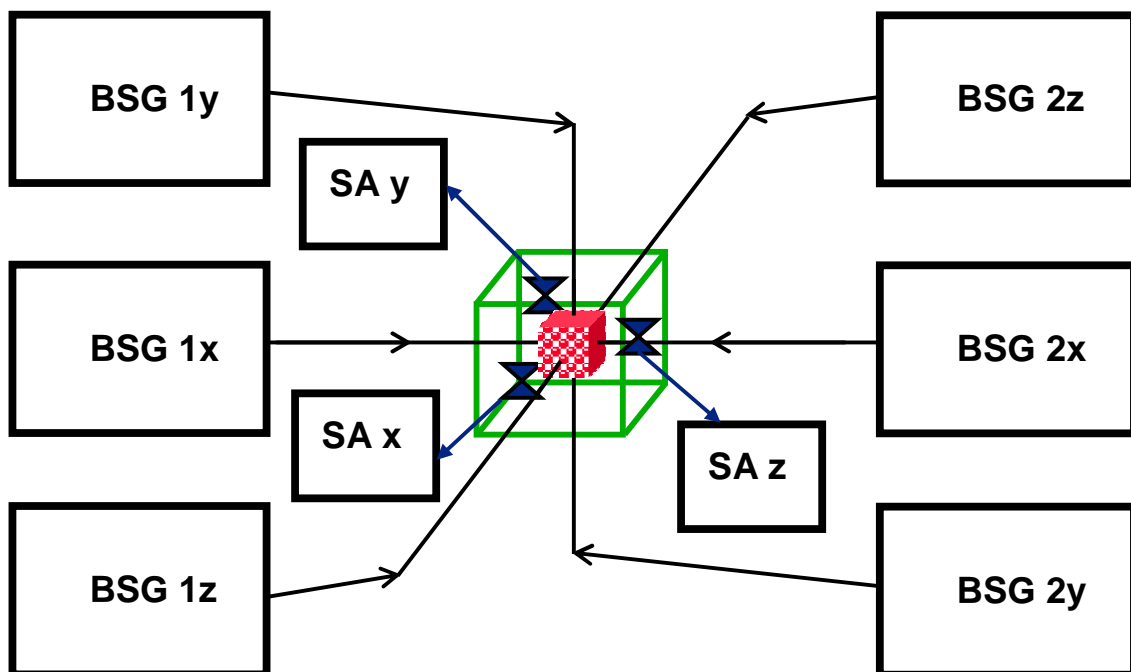


Figure 5 System overview

The system makes use of stream ciphers as opposed to random number generators because of the fact that not every random number generator is suitable for building a good stream cipher, but a good stream cipher can work as a good random number generator with its data input 'clamped' to a constant value.

One option is to take a proven block cipher in counter mode and run it as a stream cipher, e.g. AES in counter mode, called AES-CTR. Another possibility is the choice of RC4, a well-known Stream Cipher because of its application in internet protocols. Additionally, there are many more stream ciphers in the field now as a result of the eSTREAM competition [12], started at the end of 2004 following the workshop SASC 2004. This makes the choice very difficult, but allows us to design and conduct numerous experiments.

Table 1 lists some of the stream ciphers that are under discussion as part of the eSTREAM project. Trivium was designed for high-speed hardware and is therefore a good candidate for the pool of ciphers to choose from. The same holds for Grain, Phelix, and Hermes8 [13]. Other candidates are more suited for software applications. A faster version of Salsa - Salsa8 - is also under development.

However, the security evaluation for these ciphers have not yet been completed. But more important for the application described here is the need for 20 Mbps data rate when implemented as an FPGA design so that the serializer (fig. 1) is fed without any interruption.

Table 1 Stream Ciphers and their properties

Name	Throughput	Initialization speed	Security
AES-CTR	medium	medium	Ok
Trivium	high	high	Evaluation
Grain	high	medium	Evaluation
Salsa20	medium	medium	Ok
RC4	high	medium	Ok
Hermes8	medium	medium	Evaluation
ABC	high	low	Evaluation
Phelix	high	high	Evaluation

The application of a 3D digital filtering process followed by an adaptive 2D projection results in a sequence of images located in close proximity to the collision point. Analysis of these images will allow us to determine the presence (or lack thereof) of anti-bits in the event under examination. In essence, collisions which result in creation of bit/anti-bit pairs should appear as sources in the vector field, whereas the corresponding annihilations will be recognizable as field drains.

Results

We anticipate initial publication of results and related conclusions in the spring of 2007. We will commence with a series of calibration runs; hence we don't expect to achieve significant results immediately. Brin [14] has shown that as we continue to make further runs on a regular basis we can expect a steadily improving performance curve from the equipment, and we believe that it will be providing us with trenchant data approximately one year after commissioning is complete, say April 1st.

Whilst we fully expect our experiments to provide conclusive positive identification of anti-bits as a result of the high-energy collision of data streams, we realise the possibility that the data gathered during the next year may not bear out our hopes. In the unlikely event that this should occur, it will not of course be possible to conclude that anti-bits do not exist; although in such a case we may be required to modify our line of reasoning with respect to processes liable to cause the creation of these data particles.

Conclusions

We derived the theoretical background for the assumption of the existence of anti-bits and described their properties. The experiments regarding the detection of anti-bits were discussed, and suitable detector hardware and experimental setup were presented.

We close with an observation from the well-known movie "My Fair Lady" [15], based on a work by Shaw [16]. In one of the musical sequences Eliza Dolittle's father expresses his firm belief in "a little bit of luck". We expect with confidence the exact opposite: "a little anti-bit of luck".

Acknowledgments

This work is funded in part by the National Science Foundation (NSF) Grant CCR-97.04.01, the NSF Information Technology Research (ITR) Award No. CCR-00.04.01, and the European ESPRIT Program on Multidisciplinary Information Science Transfer (E-MIST) 89-4-1.

Special thanks go to the initiators and organizers of the eSTREAM project, and also the organizers of SKEW 2005 and SASC 2006 conferences.

References

- [1] P. E. I. Bonewits, *Real Magic: An Introductory Treatise on the Basic Principles of Yellow Magic*, Weiser Books, 1989
- [2] L. Hardy, *Master of the Five Magics*, Del Rey, 1985
- [3] Mende, Simon, *Physik – Gleichungen und Tabellen*, Fachbuch Verlag Leipzig, 1982
- [4] P. Davis, *Die Urkraft*, Rasch & Roehrig, 1986
- [5] Luckin, Gardner, Hawkes, et al., *Theory of Anti-Bit Existence and Behavior*, International Conference on Computer Science, ICCS, Los Angeles, April 1999
- [6] Gardner, Hawkes, Hagman, et al., *Detection Probabilities of Anti-Bits*, *Letters to Computer International*, June 2000
- [7] Dubois, Voigt, Spruengli, *Characterization and Analysis of Anti-Bits*, International Conference on Computer Science, ICCS, Genf, April 2001
- [8] Dietmayer, Hoffmann, Kaiser, Zimmermann, *Detection of Anti-Bits – Algorithms and Performability on Probabilistic Networks*, *IEEE Transactions on Computers*, April 2003
- [9] *Serializer-Transmitter SN65LVDS151*, Data Sheet slls444a.pdf, Texas Instruments, December 2000
- [10] Allen, Holberg, *CMOS Analog Circuit Design*, publ. by Holt/Rinehart/Winston, New York 1987
- [11] ADS5444, Data Sheet, Texas Instruments, 2005, <http://focus.ti.com/lit/ds/symlink/ads5444.pdf>
- [12] ECRYPT Stream Cipher Project, <http://www.ecrypt.eu.org/stream>
- [13] Tim Good et al., *Review of Stream Cipher Candidates from a Low Resource Perspective*, <http://www.ecrypt.eu.org/stream/papers/2006/016.pdf>
- [14] D. Brin, *The Practice Effect*, Bantam Books, Spectra Series, 1984 and 1994
- [15] A. J. Lerner (screenplay/lyrics), F. Loewe (lyrics), G. B. Shaw (play *Pygmalion*), Warner Bros., 1964
- [16] G. B. Shaw, *Pygmalion* (play 1912, movie 1938)

Appendix

A) For every existing proton, neutron, electron and neutrino there also exists a related anti-particle [3]. While some hadrons consist of three quarks, e.g. the proton consists of two u-quarks and one d-quark, other hadrons such as pion and kaon have one quark and one antiquark each, e.g. the positive pion one u-quark and one d-antiquark. There is even a neutral anti-kaon, containing an s-quark and a d-antiquark. The quark theory, developed from 1963 onwards, could be first verified in 1969 by means of a series of historical experiments at the linear accelerator collider SLAC in Stanford [4]. But then in 1977 the so-called ypsilon which consists of a b-quark and a b-antiquark was found.

B) Quantum mechanics offers the concept of wave-particle duality [4] which resolves the competing theories of light proposed by Huygens and Newton in the 1600s. Through the work of Einstein, de Broglie and many others, it is now established that all objects have both particle nature and wave nature.