CLAIMS

What is claimed is:

1. A method of communication between functional blocks in a system-on-chip, the method comprising:

exchanging a respective public key between a first functional block and a second functional block in the system-on-chip for a communication therebetween, the first functional block being a transmitter of the communication and the second function block being a receiver of the communication;

generating, at the first functional block, a first code based on the public key of the second functional block;

generating, at the second functional block, a second code based on the public key of the first functional block;

obfuscating, at the first functional block, an address associated with the communication based on the first code to produce an obfuscated address;

transmitting, at the first functional block, the obfuscated address to the second functional block via an interconnect communication infrastructure in the system-on-chip;

receiving, at the second functional block, the obfuscated address from the first functional block via the interconnect communication infrastructure; and

deobfuscating, at the second functional block, the obfuscated address received based on the second code to produce a deobfuscated address associated with the communication;

wherein said obfuscating, at the first functional block, the address associated with the communication comprises:

generating a first random sequence based on the first code; and

obfuscating the address based on the first random sequence to produce the obfuscated address, and

wherein said deobfuscating, at the second functional block, the obfuscated address comprises:

generating a second random sequence based on the second code; and

deobfuscating the address based on the second random sequence to produce the deobfuscated address associated with the communication.

2. The method according to claim 1, further comprising:

generating, at each of the first functional block and the second functional block, a respective secret key for the communication; and

generating, at each of the first functional block and the second functional block, the respective public key based on the respective secret key.

3. The method according to claim 1,

wherein said generating, at the first functional block, the first code comprises generating a new first code periodically based on a first time interval, and

wherein said generating, at the second functional block, the second code comprises generating a new second code periodically based on a second time interval.

4. The method according to claim 1,

wherein said generating the first random sequence comprises generating the first random sequence based on a first stochastic function, the first stochastic function being synchronized based on a first input clock signal and initialized by the first code functioning as a seed to the first stochastic function, and

wherein said generating the second random sequence comprises generating the second random sequence based on a second stochastic function, the second stochastic function being synchronized based on a second input clock signal and initialized by the second code functioning as a seed to the second stochastic function.

5. The method according to claim 4,

wherein the first stochastic function is configured to generate the first random sequence and the second stochastic function is configured to generate the second random sequence in a manner that is time-dependent, deterministic and cyclic, and

wherein the first and second input clock signals are based on a common clock source.

6. The method according to claim 1 , wherein said obfuscating, at the first functional block, the address associated with the communication is completed within a communication latency time.

7. The method according to claim 1, further comprising:

encoding, at the first functional block, the obfuscated address to produce an encoded address; and

decoding, at the second functional block, the encoded address to produce the obfuscated address,

wherein said transmitting, at the first functional block, the obfuscated address to the second functional block comprises transmitting the encoded address including the obfuscated address to the second functional block, and

wherein said receiving, at the second functional clock, the obfuscated address from the first functional block comprises receiving the encoded address including the obfuscated address from the first functional block.

8. The method according to claim 7,

wherein said encoding, at the first functional block, the obfuscated address comprises encoding the obfuscated address based on a first substitution- permutation network comprising a substitution box function and a permutation box function, and

wherein said decoding, at the second functional block, the encoded address to produce the obfuscated address comprises decoding the encoded address based on a second substitution-permutation network comprises an inverse substitution box function and an inverse permutation box function.

9. The method according to claim 8,

wherein said encoding, at the first functional block, the obfuscated address is selectively enabled, and

wherein said decoding, at the second functional block, the encoded address is selectively enabled.

10. A system-on-chip comprising:

a first functional block; and

a second functional block communicatively coupled to the first functional block via an interconnect communication infrastructure,

wherein the first functional block comprises an address encoder, the address encoder comprising:

a first public key generator configured to exchange a public key with the second functional block for a communication between the first functional block and the second functional block, the first functional block being a transmitter of the communication and the second function block being a receiver of the communication;

a first code generator configured to generate a first code based on the public key of the second functional block;

an address obfuscator configured to obfuscate an address associated with the communication based on the first code to produce an obfuscated address; and

an address transmitter configured to transmit the obfuscated address to the second functional block via the interconnect communication infrastructure in the system-on-chip,

wherein the second functional block comprises an address decoder, the address decoder comprising:

a second public key generator configured to exchange a public key with the first functional block for the communication;

a second code generator configured to generate a second code based on the public key of the first functional block;

an address receiver configured to receive the obfuscated address from the first functional block via the interconnect communication infrastructure; and

an address deobfuscator configured to deobfuscate the obfuscated address received based on the second code to produce a deobfuscated address associated with the communication;

wherein the address obfuscator is configured to:

generate a first random sequence based on the first code; and

obfuscate the address based on the first random sequence to produce the obfuscated address, and

wherein the address deobfuscator is configured to:

generate a second random sequence based on the second code; and deobfuscate the address based on the second random sequence to produce the deobfuscated address associated with the communication.

11. The system-on-chip according to claim 10,

wherein the address encoder further comprises a first secret key generator configured to generate a secret key of the first functional block for the communication,

wherein the address decoder further comprises a second secret key generator configured to generate a secret key of the second functional block for the communication,

wherein the first public key generator is configured to generate the public key of the first functional block based on the secret key of the first functional block, and

wherein the second public key generator is configured to generate the public key of the second functional block based on the secret key of the second functional block.

12. The system-on-chip according to claim 10,

wherein the first code generator is configured to generate a new first code periodically based on a first time interval; and

wherein the second code generator is configured to generate a new second code periodically based on a second time interval.

13. The system-on-chip according to claim 10,

wherein said generate the first random sequence comprises generating the first random sequence based on a first stochastic function, the first stochastic function

being synchronized based on a first input clock signal and initialized by the first code functioning as a seed to the first stochastic function, and

wherein said generate the second random sequence comprises generating the second random sequence based on a second stochastic function, the second stochastic function being synchronized based on a second input clock signal and initialized by the second code functioning as a seed to the second stochastic function.

14. The system-on-chip according to claim 13,

wherein the first stochastic function is configured to generate the first random sequence and the second stochastic function is configured to generate the second random sequence in a manner that is time-dependent, deterministic and cyclic; and

wherein the first and second input clock signals are based on a common clock source.

15. The system-on-chip according to claim 10, wherein

the address obfuscator is configured to obfuscate the address associated with the communication within a communication latency time.

16. The system-on-chip according to claim 10,

wherein the address encoder further comprises an encoder configured to encode the obfuscated address to produce an encoded address,

wherein the address decoder further comprises a decoder configured to decode the encoded address to produce the obfuscated address,

wherein the address transmitter is configured to transmit the encoded address including the obfuscated address to the second functional block, and wherein the address receiver is configured to receive the encoded address including the obfuscated address from the first functional block.

17. The system-on-chip according to claim 16,

wherein the encoder is configured to encode the obfuscated address based on a first substitution-permutation network comprising a substitution box function and a permutation box function; and

wherein the decoder is configured to decode the encoded address based on a second substitution-permutation network comprises an inverse substitution box function and an inverse permutation box function.

18. A method of forming a system-on-chip, the method comprising:

forming a first functional block on a substrate; and

forming a second functional block on the substrate, the second functional block being communicatively coupled to the first functional block via an interconnect communication infrastructure,

wherein the first functional block comprises an address encoder, the address encoder comprising:

a first public key generator configured to exchange a public key with the second functional block for a communication between the first functional block and the second functional block, the first functional block being a transmitter of the communication and the second function block being a receiver of the communication;

a first code generator configured to generate a first code based on the public key of the second functional block;

an address obfuscator configured to obfuscate an address associated with the communication based on the first code to produce an obfuscated address; and

an address transmitter configured to transmit the obfuscated address to the second functional block via an interconnect communication infrastructure in the system-on-chip,

wherein the second functional block comprises an address decoder, the address decoder comprising:

a second public key generator configured to exchange a public key with the first functional block for the communication;

a second code generator configured to generate a second code based on the public key of the first functional block;

an address receiver configured to receive the obfuscated address from the first functional block via the interconnect communication infrastructure; and

an address deobfuscator configured to deobfuscate the obfuscated address received based on the second code to produce a deobfuscated address associated with the communication;

wherein the address obfuscator is configured to:

generate a first random sequence based on the first code; and

obfuscate the address based on the first random sequence to produce the obfuscated address, and

wherein the address deobfuscator is configured to:

generate a second random sequence based on the second code; and deobfuscate the address based on the second random sequence to produce the deobfuscated address associated with the communication.