論 文 内 容 の 要 旨

博士論文題目

Lightweight Physical Layer Encryption Methods for IoT Sensor Transceivers
(IoT センサートランシーバー向け物理層軽量暗号化手法)

氏　名　Hoang Dai Long

本論文では、モノのインターネット（IoT）センサートランシーバー向け低コスト低消費電力物理層暗号化（PLE）を提案し回路を開発した。PLE は、送受信機のセキュリティを強化する新たな暗号化手法である。従来の PLE 方法では実行する回路のコストと消費電力が多く、電力と計算リソースが限られている IoT センサートランシーバーに適用できない。本研究は、IoT センサー向けに 2 つの物理層暗号化方法を提案する。提案手法は、ハードウェア回路のコストと消費電力を削減し、かつ、システムのパフォーマンスを低下させないことを目指す。

第 1 の手法は、サインビット暗号化である。本手法では、変調されたシンボルのサインビットのみを暗号化する。提案手法の性能を評価するために、IEEE 802.11ah 規格に従って Matlab でシミュレーションを行った。結果、従来の方法ではビットエラーレート（BER）とパケットエラーレート（PER）のパフォーマンスが約 3 dB 低下するのに対し、提案手法では BER と PER のパフォーマンスが低下しないことを示した。提案手法は、XOR 演算のみを使用するため、回路が低コストかつ低消費電力である。しかし、本手法ではサインビットのみを暗号化するためシステムのセキュリティがまだ高くない。

そこで第 2 の手法として、共同変調方式暗号化（JEM）を提案した。JEM 手法では、変調されたシンボルのすべてのビットを暗号する。このため、システムのセキュリティが高い。本手法は、変調方式のマップと暗号化の二つ機能を一つのブロックにマージする。提案する JEM には次の利点がある。1) JEM を使用したシステムは BER と PER のパフォーマンスが低下しない。2) JEM を使用した送受信機は物理層暗号化を全く使用しない送受信機と比べ、ハードウェア回路の面積と消費電力がわずかしか増加しない。3) JEM のハードウェア回路は、従来型 PLE 手法回路の 1/40 で済む。

以上のように、本論文は、新たな JEM 手法と、CORDIC に基づく従来型 PLE 暗号化手法のハードウェア回路を開発し、回路の面積と消費電力を比較評価した。

氏　名	Hoang Dai Long

（論文審査結果の要旨）（Ａ４　１枚　１、２００字程度）

本論文では、モノのインターネット（IoT）センサートランシーバー向け低コスト低消費電力物理層暗号化（PLE）を提案し回路を開発した。PLE は、送受信機のセキュリティを強化する新たな暗号化手法である。従来の PLE 方法では実行する回路のコストと消費電力が多く、電力と計算リソースが限られている IoT センサートランシーバーに適用できない。本研究は、IoT センサー向けに２つの物理層暗号化方法を提案する。提案手法は、ハードウェア回路のコストと消費電力を削減し、かつ、システムのパフォーマンスを低下させないことを目指す。

第１の手法は、サインビット暗号化である。本手法では、変調されたシンボルのサインビットのみを暗号化する。提案手法の性能を評価するために、IEEE 802.11ah 規格に従って Matlab でシミュレーションを行った。結果、従来の方法ではビットエラーレート（BER）とパケットエラーレート（PER）のパフォーマンスが約 3 dB 低下するのに対し、提案手法では BER と PER のパフォーマンスが低下しないことを示した。提案手法は、XOR 演算のみを使用するため、回路が低コストかつ低消費電力である。しかし、本手法ではサインビットのみを暗号化するためシステムのセキュリティがまだ高くない。

そこで第２の手法として、共同変調方式暗号化（JEM）を提案した。JEM 手法では、変調されたシンボルのすべてのビットを暗号する。このため、システムのセキュリティが高い。本手法は、変調方式のマップと暗号化の二つ機能を一つのブロックにマージする。提案する JEM には次の利点がある。1) JEM を使用したシステムは BER と PER のパフォーマンスが低下しない。2) JEM を使用した送受信機は物理層暗号化を全く使用しない送受信機と比べ、ハードウェア回路の面積と消費電力がわずかしか増加しない。3) JEM のハードウェア回路は、従来型 PLE 手法回路の 1/40 で済む。

以上のように、本論文は、新たな JEM 手法と、CORDIC に基づく従来型 PLE 暗号化手法のハードウェア回路を開発し、回路の面積と消費電力を比較評価した。

以上、本論文は学術上、実際上寄与するところが少なくない。よって、本論文は博士(工学)の学位論文として価値あるものと認める。