講演番号: 75

CSK コードを用いた可視光通信用暗号の検討

Encryption technique for Visible Light Communication System by using CSK code

B-15

山本 貴寛　　北脇 孝太　　宮保 憲治
Takahiro Yamamoto　Kouta Kitawaki　Noriharu Miyaho
東京電機大学 情報環境学部
School of Information Environment, Tokyo Denki University

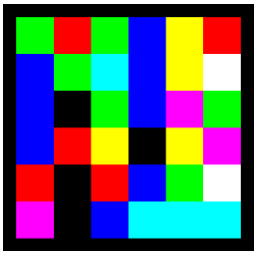
1 はじめに

近年ではスマートフォンが普及し，高精細なディスプレイやカメラが身近な存在となっている．

本稿ではそれらを利用したCSKコードによる可視光通信で利用可能な個人認証と暗号化を同時に行うことのできる符号化手法を提案する．

2 提案システムの概要

スマートフォンのディスプレイと Web カメラを用い，CSK コードによりパターン認証を可能とする可視光通信の原理を述べる．CSK コードは図 1 に示すように，n×n マスの正方形を使用し，マス毎に予め決められた色彩の中から任意の色彩を割り当てられるように画像パターンを構成できる．



マス数	36 マス
色数	8 色(3bit)
情報量	108bit

図 1. CSK コードを用いた画像パターンの例

利用者の認証と通信の暗号化を行う際に，SAS-2 (Simple And Secure password authentication protocol, Ver, 2)を用いた．この方式はワンタイムパスワードの一種であり，この方式を応用し，個人認証と情報送信を同時に行う手法を提案する．

3 通信方式の概要

SAS-2 方式は 3 回のハッシュ値生成と XOR，加算処理のみを用いるため高速性に適す．また，毎回新規に暗号鍵が生成されるため，セキュア性にも優れる．1:1 の認証が容易に実現可能であり，鍵の自動生成も，容易に可能とする特長を併せ持つ．

元来，SAS-2 では認証機能しか持ち合わせていないが，提案方式では，1 つの共有鍵に対して 1 つのパターン情報を割り当てることにより，認証と情報の送信を同時に行う事が可能となる．

4 暗号化処理のアルゴリズム

本方式では事前共有鍵として乱数のハッシュ値 $E(N_{(n,0)})$を共有する(n はパターン，0 は 0 番目の共有鍵の意味)．送信機は図 2 に示す演算処理を行って α, β を生成し，これを CSK に変調することで CSK コード画像の情報部を作成する．

$$\alpha = E(N_{(n,i+1)}) \oplus E(N_{(n,i)})$$
$$\beta = [E\{E(N_{(n,i+1)})\} + E(N_{(n,i)})] \oplus E(N_{(n,i)})$$

図 2. 送信機側の演算処理

受信機は上述した α, β を用い，図 3 に示す演算処理を行い，X を生成する．ここで，事前に共有した $E(N_{(n,i)})$と等しいことが検出されれば，受信した情報はパターン n であると判別することができる．

$$X = \beta \oplus [E\{\alpha \oplus E(N_{(n,i)})\} + E(N_{(n,i)})]$$

図 3. 受信機側の演算処理

通信が成功した場合，$(N_{(n,i+1)})$を新たな暗号鍵として送受信機のメモリ上に保存することにより、新たな暗号鍵の共有が同時に完了する．なお，ハッシュ値の生成には SHA-256 を用い実験検証を行った．

5 まとめ

CSK コードを用いた可視光通信において、ワンタイムパスワード形式の暗号化、個人認証と情報送信とを同時に行う暗号通信方式の提案を行った．今後は，最初の共有鍵を安全に共有できる方法に関し，実用的な方式を検討する必要がある．商用のサービスを目指し，今後も検討を加速する予定である．

参考文献

[1] T. Tsuji, A. Shimizu. “ A one-time password authentication method for low spec machines and on internet protocols,” IEICE Trans. Commun., vol. E87-B, no. 6, pp. 1594-1600, 2004.
[2] “ Short-Range Wireless Optical Communication Using Visible Light”, IEEE 802.15.7, 2011.