Protocolo de Autenticação para Sistemas RFID com Baixo Custo Computacional

Marcus V. C. Rodrigues, B. B. Albert e F. M. de Assis

***Resumo*— Este artigo apresenta um esquema de autenticação de baixo custo para sistemas RFID. A idéia é utilizar um protocolo de distribuição de chaves secretas em conjunto com um protocolo de autenticação que não envolve o passo de cifragem usualmente utilizado nos MACs convencionais. Ambos os protocolos compartilham uma família de funções hash universal.**

***Palavras-Chave*— RFID, Protocolo de Autenticação, Protocolo de Distribuição de Chaves Secretas, Funções Hash Universais, dispositivos de baixo custo, dispositivos baixa potência.**

***Abstract*— This paper presents a low cost authentication scheme for RFID systems. The main idea is using a key distribution protocol in ensemble with an encryption-free authentication protocol. Both protocols share a universal hash function family.**

***Keywords*— RFID, Authentication Protocol, Secret Keys Distribution Protocol, Universal Hash Functions, low-cost devices, low-power devices.**

I. Introdução

Sistemas de IDentificação por Rádio Frequência (RFID) são cada vez mais adotados por empresas ao redor do mundo. Essa tecnologia permite, entre outras coisas, a identificação e o rastreamento de objetos e de pessoas. Um sistema RFID consiste basicamente de um leitor e de uma etiqueta. O leitor, em geral, é responsável pela alimentação e leitura dos dados da etiqueta e em alguns casos pelo envio de dados para as etiquetas, [1]. As etiquetas são dispositivos que podem ser passivos, semi-passivos ou ativos [2]. Nosso esquema é direcionado as etiquetas passivas, isto é, não possuem alimentação própria, e consistem de um circuito digital acoplado a uma antena. As informações contidas na etiqueta são lidas pelo leitor através da reflexão do sinal de RF enviado pelo leitor. A variação da carga da antena da etiqueta de acordo com a informação nela contida permite que o leitor possa fazer a distinção do bit que está sendo lido.

Duas características importantes desses sistemas é que eles usam comunicação sem fio e têm uma acentuada limitação de energia (a etiqueta). A primeira característica leva invariavelmente a questões referentes a segurança e a privacidade na utilização desses esquemas, [3]. As limitações de custo para as etiquetas RFID e as diferentes exigências por segurança dos diversos usuários das etiquetas, leva ao desenvolvimento de soluções específicas para cada conjunto de necessidades de aplicação, [4] e [5]. Em várias aplicações, como sistemas de controle de acesso em eventos (como exemplo, campeonatos esportivos mundiais), o objetivo principal da etiqueta RFID não é a confidencialidade, mas a autenticidade e a integridade dos dados lidos. Nesse aspecto, os protocolos de autenticação desempenham um papel importante para o uso da tecnologia RFID. Autenticação significa que os dados trocados entre os integrantes do sistema RFID vem de dispositivos autorizados.

A quantidade de portas que uma etiqueta de um sistema RFID pode conter é determinada, principalmente, pelo baixo custo a que se propõe. Como consequência, a etiqueta possui uma limitada capacidade computacional. Como foi dito anteriormente, isso limita os esquemas de segurança que podem ser adotados. Considerando a questão de autenticação, vários protocolos foram sugeridos, alguns baseados na operação ou-exclusivo e na conjectura de dificuldade do problema de LPN (do inglês - *Learning Parity in the Presence of Noise*) como o chamado protocolo HB [6] e suas variantes [7] e [8], outros baseados nos códigos de autenticação de mensagens (MAC - do inglês *Message Authentication Code*) que utilizam funções hash [9] e [10], por exemplo.

Uma das características de todos os protocolos de autenticação é a suposição de uma chave secreta compartilhada entre os integrantes do sistema. Para uma segurança incondicional essa chave deve ser usada apenas uma vez para cada rodada do protocolo, [11], o que é uma dificuldade para tais sistemas.

O sistema proposto é composto de duas etapas. A primeira é responsável pela geração de uma chave secreta compartilhada entre Alice (transmissor) e Bob (receptor), permitindo que cada chave gerada seja utilizada uma única vez. A segunda etapa é um protocolo de autenticação baseado na proposta de [12] que, objetivando reduzir a complexidade do mesmo, não faz uso de cifragem, comumente utilizada nos MACs. Vale a pena salientar que a família de funções hash universal é compartilhada entre os dois protocolos com o objetivo de diminuir o número de portas que devem ser implementadas na etiqueta RFID.

O artigo está organizado da seguinte forma: na próxima seção são apresentadas as definições importantes para o entendimento do protocolo. Na Seção III é descrito o sistema proposto. Uma análise informal do protocolo é realizada na Seção IV. As conclusões e perspectivas do trabalho proposto estão na Seção V.

II. Embasamento Teórico

A. MAC

Os MACs são usados para verificar se uma mensagem foi realmente originada de uma determinada fonte, com alta

Marcus V. C. Rodrigues, B. B. Albert e F. M. de Assis¸, Departamento de Engenharia Elétrica, Universidade Estadual de Campina Grande, Campina Grande, Brasil, E-mails: marcus.rodrigues@ee.ufcg.edu.br, albert@dee.ufcg.edu.br, fmarcos@dee.ufcg.edu.br. Este trabalho foi parcialmente financiado pela Capes

probabilidade. O algoritmo básico do MAC é o seguinte:

1) Alice (transmissor) compartiha uma chave secreta K com Bob (receptor);
2) Alice usa sua chave K e sua mensagem M para gerar o MAC que é concatenado com a mensagem M a ser enviada para Bob;
3) Bob recebe a mensagem M mais o MAC enviados por Alice. Com sua chave K e a mensagem M ele calcula o MAC correspondente e compara com o MAC enviado por Alice, se forem iguais, então, com alta probabilidade, a mensagem M foi enviada por Alice. Além disso, também com alta probabilidade, a mensagem M não foi alterada ao longo do percurso entre Alice e Bob.

A segurança do MAC está baseada em três propriedades: (a) sem a chave K é difícil criar um MAC válido; (b) dada uma mensagem M e seu MAC correspondente é difícil criar uma nova mensagem M' que produza o mesmo MAC, ou mesmo qualquer outro MAC válido (propriedade a); (c) Para um determinado MAC válido é difícil achar uma mensagem M' que corresponda a esse MAC. Um MAC é similar ao processo de cifragem mas com uma diferença, não precisa ser um processo reversível. Por conta disso, a função de autenticação é menos vulnerável de ser quebrada que a cifragem. Vale salientar que o protocolo MAC descrito acima não fornece confidencialidade, pois a mensagem M é transmitida sem alteração. Nesse trabalho, estamos interessados na aplicação de funções hash universais nos códigos de autenticação. Na próxima subseção revisaremos as definições relevantes sobre funções hash universais.

B. Funções Hash Universais

Uma Função Hash Universal é um mapeamento de um conjunto finito A com tamanho a para um conjunto finito B de tamanho b, em que $a \geq b$, conforme seus primeiros idealizadores *Carter e Wegman* [13]. Neste momento serão definidas algumas notações para em seguida serem apresentadas duas definições de Funções Hash Universais utilizadas por *Nevelsteen e Preneel* em [14].

1) Notações: Seja $\{0,1\}^*$ a representação de todas as sequências binárias incluindo a sequência vazia. O conjunto $H = \{h : A \rightarrow B\}$ munido de alguma distribuição de probabilidade, é uma família de funções hash com domínio $A \subseteq \{0,1\}^*$ e contradomínio $B \subseteq \{0,1\}^*$, onde $a = |A|$ e $b = |B|$. O conjunto $C \subseteq \{0,1\}^*$ representa o conjunto finito de sequências de chaves. O símbolo h_K representa uma função hash escolhida de um conjunto de funções hash H segundo uma chave aleatória $K \in C$.

O elemento $M \in A$ representa uma sequência de mensagens que serão divididas em blocos $M = (m_1, \cdots, m_n)$, onde n é o número de blocos de mensagens com comprimento w. Do mesmo modo a chave K é particionada como $K = (K_1, \cdots, K_i, \cdots, K_n)$, onde cada bloco K_i possui comprimento w.

Será usado $H[n, w]$ para representar uma família de funções hash em que n é o numero de blocos de mensagens (ou blocos de chaves) e w é o número de bits por bloco.

Seja U_w o conjunto de inteiros não negativos menores que 2^w, e P_w o conjunto de polinômios sobre o corpo finito $GF(2)$ de grau menor que w. $GF(2^w)$ representa o corpo finito de 2^w elementos definidos por: $GF(2)[x]/p(x)$, em que $p(x)$ é um polinômio irredutível de grau w sobre $GF(2)$.

2) Propriedades: As propriedades de uma função hash são, [15]:

- **Tamanho arbitrário das mensagens** - $h(x)$ pode ser aplicado a mensagens x de quaisquer tamanhos.
- **Comprimento fixo da saída** - $h(x)$ produz um valor hash z de comprimento fixado.
- **Eficiência** - $h(x)$ é relativamente fácil de computar.
- **Resistência a pré-imagem** - Para uma dada saída z, é inviável encontrar algum x tal que $h(x) = z$, isto é $h(x)$ é via-única.
- **Resistência a segunda pré-imagem** - Dado x_1, e assim $h(x_1)$, é computacionalmente inviável encontrar algum x_2 tal que $h(x_1) = h(x_2)$.
- **Resistência à colisão** - É computacionalmente inviável encontrar algum par de entrada $x_1 \neq x_2$ tal que $h(x_1) = h(x_2)$.

3) Definições: Para uma dada função hash $h \in H$ e para um par de mensagens (M, M') onde $M \neq M'$, a função $\delta_h(M, M') = 1$ se $h(M) = h(M')$, e 0 se difere. Quando $\delta_h(M, M') = 1$ dizemos que as funções $h(M)$ e $h(M')$ **colidem**. Para um dado conjunto finito de funções hash H, $\delta_H(M, M')$ é definido como $\sum_{h \in H} \delta_h(M, M')$. Quando h é escolhida aleatoriamente de H e duas mensagens distintas M e M' são dadas como entrada, a probabilidade de colisão é dada por: $\delta_h(M, M')/|H|$.

Definição 1: O conjunto de funções hash $H = \{h : A \rightarrow B\}$ é dito ser **universal** se para todo $M, M' \in A$ em que $M \neq M'$,

$$|\{h \in H : h(M) = h(M')\}| = \delta_H(M, M') = \frac{|H|}{b} \qquad (1)$$

4) Família de Funções Hash NH e sua variação WH: Black e demais em [9] introduziram uma família de funções hash quase universal chamadas NH com o objetivo de aumentar a velocidade dos protocolos de autenticação existentes até então. A definição da função hash NH é dada a seguir.

Definição 2: Dado $M = (m_1, \cdots, m_i, \cdots, m_n)$ e $K = (k_1, \cdots, k_i, \cdots, k_n)$ em que m_i e $k_i \in U_w$, para qualquer $n \geq 2$ par, NH é definida como:

$$NH_K(M) = \left[\sum_{i=1}^{n/2} ((m_{2i-1} + k_{2i-1}) \bmod 2^w) \right. \\ \left. ((m_{2i} + k_{2i}) \bmod 2^w) \right] \bmod 2^{2w} \qquad (2)$$

Com o propósito de tornar possível a construção em hardware da função NH para dispositivos de ultra baixa potência (como o RFID), *Yuksel* [16] implementou diversas modificações na

função hash NH, obtendo três variantes: a função hash PH (NH polinomial), a PR (NH polinomial com redução) e a WH (NH polinomial ponderada com redução, do inglês - *Weighted NH-Polynomial with Reduction*). Por sua eficiência, será utilizado no protocolo proposto a função hash WH, cuja definição é vista a seguir.

Definição 3: Dado $M = (m_1, \cdots, m_i, \cdots, m_n)$ e $K = (k_1, \cdots, k_i, \cdots, k_n)$ em que m_i e $k_i \in GF(2^w)$, para qualquer $n \geq 2$ par, e um polinômio irredutível $p(x) \in GF(2^w)[x]$, WH é definida como:

$$WH_K(M) = \sum_{i=1}^{n/2} (m_{2i-1} + k_{2i-1})\,(m_{2i} + k_{2i})\, x^{\left(\frac{n}{2}-i\right)w} \,(\mathrm{mod} p)\,.$$

A seguir será provado que a família de funções hash WH é uma família de funções hash universal.

Teorema 1: Para algum $n \geqslant 2$ par e $w \geqslant 1$, $WH[n, w]$ é universal em n sequências de comprimento iguais.

Prova: Será utilizado a seguinte abreviação

$$(m_{2i-1} + k_{2i-1})\,(m_{2i} + k_{2i}) = mk_{2i},$$
$$\left(m'_{2i-1} + k_{2i-1}\right)\,(m'_{2i} + k_{2i}) = m'k_{2i}$$

e assim por diante. Seja M e M' membros distintos do domínio A com igual comprimento. Se deseja mostrar que

$$Pr[WH_k(M) = WH_k(M')] = 2^{-w}.$$

Expandindo os termos na expressão de probabilidade, obtem-se

$$Pr\left[\sum_{i=1}^{n/2} mk_{2i}\left(x^{\left(\frac{n}{2}-i\right)w}\right) = \sum_{i=1}^{n/2} m'k_{2i}\left(x^{\left(\frac{n}{2}-i\right)w}\right)(\mathrm{mod} p)\right] = 2^{-w}. \quad (3)$$

No cálculo da probabilidade é suposto escolhas uniformes de $K = (k_1, \cdots, k_i, \cdots, k_n)$ com cada $k_i \in GF(2^w)$ e que a aritmética é sobre $GF(2^w)$. Como M e M' são distintos então $m_i \neq m'_i$ para algum $1 \leqslant i \leqslant n$. Considere que $m_{2l} \neq m'_{2l}$. Para alguma escolha de $k_1, \cdots, k_{2l-2}, k_{2l}, \cdots, k_n$, tem-se

$$Pr_{k_{2l-1} \in GF(2^w)}\left[\sum_{i=1}^{n/2} mk_{2i}\left(x^{\left(\frac{n}{2}-i\right)w}\right) = \sum_{i=1}^{n/2} m'k_{2i}\left(x^{\left(\frac{n}{2}-i\right)w}\right)(\mathrm{mod} p)\right] = 2^{-w}. \quad (4)$$

satisfeita para todo $1 \leqslant l \leqslant \frac{n}{2}$ implica em (3).
Fazendo y e z como

$$y = \left[\sum_{i=1}^{l-1} m'k_{2i}x^{\left(\frac{n}{2}-i\right)w} - \sum_{i=1}^{l-1} mk_{2i}x^{\left(\frac{n}{2}-i\right)w}\right](\mathrm{mod} p)$$

e

$$z = \left[\sum_{i=l+1}^{n/2} m'k_{2i}x^{\left(\frac{n}{2}-i\right)w} - \sum_{i=l+1}^{n/2} mk_{2i}x^{\left(\frac{n}{2}-i\right)w}\right](\mathrm{mod} p)$$

A probabilidade (4) pode ser reescrita como

$$Pr_{k_{2l-1}}\left[x^{\left(\frac{n}{2}-l\right)w}\left[mk_{2l} - m'k_{2l}\right] = y + z\,(\mathrm{mod} p)\right] = 2^{-w}.$$

Como $x^{\left(\frac{n}{2}-l\right)w}$ é inversível em $GF(2^w)$, a equação na expressão de probabilidade pode ser reescrita como

$$k_{2l-1}(m_{2l} - m'_{2l}) + m_{2l-1}(m_{2l} + k_{2l}) - m'_{2l-1}(m'_{2l} + k_{2l}) = x^{-\left(\frac{n}{2}-l\right)w}(y+z)(\mathrm{mod} p)$$

Resolvendo a equação para k_{2l-1} , obtem-se

$$k_{2l-1} = (m_{2l} - m'_{2l})^{-1}\Big((x^{-\left(\frac{n}{2}-l\right)w}(y+z) - m_{2l-1}(m_{2l} + k_{2l}) + m'_{2l-1}(m'_{2l} + k_{2l}))(\mathrm{mod} p).$$

Note que $(m_{2l} - m'_{2l})$ é inversível pois no começo da prova assumiu-se que $m_{2l} \neq m'_{2l}$. Isso prova que para qualquer m_{2l}, m'_{2l} (com $m_{2l} \neq m'_{2l}$) e $y, z \in GF(2^w)$ existe exatamente um $k_{2l-1} \in GF(2^w)$ que provoca uma colisão. Portanto,

$$Pr[WH_k(M) = WH_k(M')] = 2^{-w}.$$

Os resultados obtidos com a função hash WH sobre a NH foram: redução de 59% no consumo de potência dinâmica, redução de 66% no consumo de potência de fuga, aumento de até 7,4 vezes a velocidade de execução do protocolo, e redução de 74% no número de portas lógicas.

III. Sistema Proposto

A suposição básica, em termos de segurança, que envolve os protocolos de autenticação é o compartilhamento de uma chave secreta entre os participantes do esquema. Nos esquemas de segurança incondicional essa chave compartilhada deve ser usada uma única vez de modo que uma nova chave deve ser gerada e compartilhada cada vez que o protocolo for utilizado. Em geral a condição de segurança incondicional pode ser relaxada para segurança computacional se um ou os dois critérios a seguir são encontrados: (a) O custo de quebrar o protocolo excede o valor da informação que está sendo trocada; (b) O tempo necessário para quebrar o protocolo excede o tempo de vida útil da informação. Assim, na prática a chave pode ser usada mais de uma vez desde que satisfaça um ou os dois critérios acima. De qualquer modo a mesma chave não poderá ser usada indefinidamente, sob pena de ter a segurança do protocolo comprometida. Isto impõe uma questão importante que é como distribuir a chave secreta entre os integrantes do sistema. Esse trabalho propõe inicialmente um protocolo de distribuição de chaves secretas para sistemas de baixo custo baseado no ruído inerente do canal de comunicação [17] e apresentado na subseção seguinte. A segunda parte do esquema proposto diz respeito ao protocolo de autenticação que procura evitar o uso da cifragem após a mensagem ser comprimida através de uma função hash como é realizado normalmente pelos protocolos MAC. O protocolo é baseado no artigo [12] e será mostrado na Subseção III-B.

A. Protocolo de Distribuição de Chaves Secretas

Essa subseção lida com a aquisição de uma chave secreta pelo leitor $\mathcal{R}$ e pela etiqueta $\mathcal{T}$ de um sistema RFID mesmo quando inicialmente eles não compartilhem da chave secreta e um espião passivo $\mathcal{E}$ está presente na comunicação. O protocolo de distribuição de chaves é baseado em um canal ruidoso.

A primeira parte do protocolo, chamada de fase de destilação, é baseado no artigo de *Gander* e *Maurer* [18] em que $\mathcal{R}$ e $\mathcal{T}$ tornam o sistema a seu favor em relação ao $\mathcal{E}$. Suponha que $\mathcal{R}$ envia uma sequência aleatória de n-bit para $\mathcal{T}$ em um canal ruidoso. Essa sequência também pode ser recebida por $\mathcal{E}$ através de um outro canal, também ruidoso, independente do primeiro canal. Considere que as variáveis aleatórias $R = \{R_0, R_1, \ldots, R_{n-1}\}$, $T = \{T_0, T_1, \ldots, T_{n-1}\}$ e $E = \{E_0, E_1, \ldots, E_{n-1}\}$ são atribuídas a $\mathcal{R}$, $\mathcal{T}$ e $\mathcal{E}$ respectivamente. A sequência R é gerada por uma fonte discreta sem memória e despolarizada. Os dois canais binários simétricos (BSC) independentes, com probabilidades de cruzamento $P_{T|R} = p_T$ e $P_{E|R} = p_E$ geram as sequências T e E respectivamente. Após esta fase inicial supomos que $\mathcal{R}$ e $\mathcal{T}$ podem se comunicar por um canal sem erros mas inseguro, ou seja, $\mathcal{E}$ ainda está presente. O protocolo dessa fase, para uma iteração, é o seguinte:

1) $\mathcal{R}$ e $\mathcal{T}$ agrupam seus bits em pares;
2) $\mathcal{R}$ e $\mathcal{T}$ anunciam seus bits de paridade de cada par no canal;
3) Se as paridades não combinam
   a) Então $\mathcal{R}$ e $\mathcal{T}$ descartam seus pares de bits.
4) Caso contrário
   a) Eles guardam o primeiro bit do par.

Observe que $\mathcal{E}$ tem conhecimento de todo o procedimento. A confiabilidade dos bits aumenta com o número de iterações a custa de um encolhimento no tamanho da sequência de bits. Esse fato é provado em [18].

A segunda parte do protocolo, fase de reconciliação, em que ao final do processo $\mathcal{R}$ e $\mathcal{T}$ compartilham uma chave secreta sobre a qual $\mathcal{E}$ tem uma informação parcial. A fase de reconciliação é baseda no protocolo introduzido por *Brassard* e *Savail* em [19] e modificado por *Chabanne* e *Fumaroli* em [17] e pelos autores desse trabalho em [20]. Após a primeira fase alguns erros ainda podem existir entre as sequências R e T de modo que o algoritmo mostrado a seguir é aplicado a estas sequências.

Sejam, n o comprimento das sequências a serem reconciliadas; k a largura de um bloco; n/k o número de blocos; σ uma permutação no conjunto de todas as bijeções de $\{0, 1, ..., n-1\}$; x_0 a sequência de $\mathcal{R}$ após a primeira fase; y_0 a sequência de $\mathcal{T}$ após a primeira fase. No i-ésimo passo:

1) $x_i = \sigma(x_{i-1})$ em $\mathcal{R}$.
   $y_i = \sigma(y_{i-1})$ em $\mathcal{T}$.
2) x_i é dividido em n/k blocos em $\mathcal{R}$,
   y_i é dividido em n/k blocos em $\mathcal{T}$.
3) $x_i(j)$ é o j-ésimo bloco da sequência x_i,
   $y_i(j)$ é o j-ésimo bloco da sequência y_i.
4) Verificação de paridade:
   a) Se a paridade de $x_i(j)$ for igual a paridade de $y_i(j)$, $\mathcal{R}$ e $\mathcal{T}$ continuam testando a paridade do próximo bloco ou passam para o próximo passo se todos os blocos já tiverem sido verificados.
   b) Se a paridade $x_i(j)$ não for igual a paridade de $y_i(j)$ é iniciado uma busca dicotômica para encontrar a posição l na qual $x_i(j)[l] \neq y_i(j)[l]$. Então $\mathcal{R}$ inverte seu $x_i(j)[l]$ bit para corrigir o erro.
5) Após p iterações sem encontrar erros de paridade o processo é encerrado.

A última parte do protocolo, a fase de amplificação de privacidade, usa os resultados de *Yüksel* [16], em que uma outra chave é gerada pela aplicação de uma função hash universal nas sequências de $\mathcal{R}$ e $\mathcal{T}$. Esse procedimento garante que $\mathcal{E}$ não tem quase nenhuma informação sobre a chave compartilhada. Para esse propósito foi escolhida a classe de funções hash universais WH-64, definida na Subseção II-B.4 por ser relativamente fácil de se implementar em dispositivos tais como uma etiqueta RFID.

B. Protocolo de autenticação

O protocolo de autenticação proposto foi desenvolvido inicialmente por *G. Tsudik* [12] e procura evitar a etapa de cifragem dos MACs que utilizam funções hash.

Na figura 1 é ilustrado o esquema proposto utilizando uma função hash $h(.)$ para autenticar a mensagem M (sem uso de cifragem) trocada entre as partes.

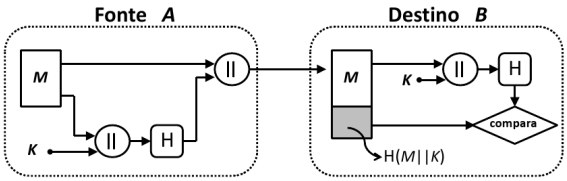

Fig. 1. Esquema de autenticação (sem cifragem) de mensagem com funções hash

Nesse esquema A calcula o valor hash sobre a concatenação de M e K, $H = h(M\|K)$, em que a operação $\|$ significa concatenação. A transmite a mensagem $M\|H$ para B. No receptor, B concatena a mensagem M com sua chave secreta compartilhada K e calcula o valor hash $H' = h(M\|K)$. Em seguida, H' é comparado com o valor hash H recebido de A para verificar a autencidade de M.

A família de funções hash utilizada é a mesma que a utilizada para a fase de amplicação de privacidade do protocolo de distribuição de chaves secretas, as chamadas funções hash WH definidas na Subseção II-B.4.

IV. Análise Informal

A análise do protocolo de distribuição de chaves foi realizada em [21] e não será repetida aqui. O protocolo de autenticação proposto tem algumas vantagens sobre os MACs que usam cifragem, como mostrado a seguir:

- Os softwares de cifragem, normalmente, são lentos. Mesmo que as quantidades de dados a serem cifradas sejam pequenas.

- Os custos de hardware para cifragem não são insignificantes.
- O hardware responsável por criptografia é otimizado para grandes quantidades de dados. Para pequenos blocos de dados, uma boa parte do tempo é gasto no *overhead* da inicialização do bloco de cifragem.
- Um algoritmo de criptografia pode ser protegido por uma patente.

Considerando o caso do sistema proposto, o protocolo de distribuição de chaves, Seção III-A, utiliza na fase de amplificação de privacidade a família de funções hash universal WH, a idéia é usar essa mesma função para implementar o protocolo de autenticação, que seria uma vantagem adicional em economia de portas e potência consumida na implementação de todo o sistema.

A confiança no sistema de autenticação reside em dois pontos básicos: no segredo da chave secreta compartilhada pelas partes legítimas e na dificuldade do invasor de achar uma mensagem M' tal que $h(M') = h(M||K)$ de tal modo que possa introduzir a mensagem M' no canal de comunicação de A e B fraudando assim o protocolo de autenticação. Supõe-se aqui que o invasor tem a capacidade de guardar e analisar as mensagens $M||h(M||K)$ bem como de inserir mensagens fraudulentas M' no sistema.

Conjectura 1: A família de funções hash universal WH tem a propriedade de resistência a pré-imagem.

Conjectura 2: A família de funções hash universal WH tem a propriedade de resistência a segunda pré-imagem.

Se essas conjecturas forem verdadeiras resta ao invasor o ataque de força bruta. Considerando uma chave de tamanho w o invasor deverá realizar em média 2^{w-1} operações para quebrar o protocolo, dado que ele conhece a função hash $h(.)$ que está sendo utilizada no momento. Como o número de funções hash WH é da ordem de 2^v, em que v é o tamanho da mensagem M tem-se então um esforço de 2^{w+v-1} operações em média para a quebra do protocolo, dado que o invasor não tem conhecimento da chave secreta K.

A chave secreta pode ser alterada regularmente através do protocolo de distribuição de chaves de modo a garantir sua confidência.

Percebe-se ainda esse esquema não oferece confidência da mensagem M. Na próxima seção são apresentas as conclusões e perspectivas de avanço do trabalho proposto.

V. CONCLUSÕES

Esse trabalho mostrou a possibilidade de implementação de serviços de segurança, em particular distribuição de chaves secretas e autenticação, para sistemas de baixo custo tais como RFID. Os protocolos fazem uso de uma mesma família de funções hash universal diminuindo assim os custos de implementação em termos de área e potência consumidas.

A segurança do protocolo de autenticação está baseado nas conjecturas 1 e 2 que precisam ser ainda formalmente estabelecidas. Cabe aqui uma pequena explicação, a escolha da família de funções hash WH não foi baseada nas conjecturas acima mas nas suas características de implementação em dispositivos de baixo custo tais como potência consumida e número de portas (área do circuito integrado). O número de vezes em que a chave secreta deve ser alterada para garantir sua confidência é um parâmetro que também precisa ser estudado com rigor.

Pretende-se, como próximo passo, a implementação do sistema proposto utilizando uma simulação da tecnologia RFID através de um sistema de desenvolvimento de rádio por software para se verificar sua viabilidade prática.

REFERÊNCIAS

[1] E. EPCglobal, "radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz-960 MHz version 1.0. 9," *URL:http://www.epcglobalinc.org/standards*, 2004-2008. [Online]. Available: http://www.epcglobalinc.org/standards

[2] E. Schuster, S. Allen, and D. Brock, *Global RFID: the value of the EPCglobal network for supply chain management*. Springer Verlag, 2007.

[3] A. Juels, "RFID security and privacy: A research survey," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, pp. 381–394, 2006.

[4] S. Spiekermann and S. Evdokimov, "Critical RFID Privacy-Enhancing Technologies," *Computing in Science and Engineering*, vol. 7, no. 2, pp. 56–62, 2009.

[5] M. Aigner and T. Burbridge, "The economic relevance of secure rfid solutions–a qualitative perspective (d. 4.1. 3)," 2007.

[6] N. Hopper and M. Blum, "Secure human identification protocols," *Advances in cryptology-ASIACRYPT 2001*, pp. 52–66, 2001.

[7] A. Juels and S. Weis, "Authenticating pervasive devices with human protocols," in *Advances in Cryptology–CRYPTO 2005*. Springer, 2005, pp. 293–308.

[8] B. Yoon, M. Sung, S. Yeon, H. Oh, Y. Kwon, C. Kim, and K. Kim, "HB-MP++ protocol: An ultra light-weight authentication protocol for RFID system," in *RFID, 2009 IEEE International Conference on*. IEEE, 2009, pp. 186–191.

[9] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, "UMAC: Fast and secure message authentication," in *Advances in Cryptology–CRYPTO*, vol. 99. Springer, 1999, pp. 216–233.

[10] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-hashing for message authentication," in *RFC*. Citeseer, 1997.

[11] C. E. Shannon, "Communication theory of secrecy systems," *Bell Systen Technicl Journal*, vol. 28, pp. 656–715, Oct. 1949.

[12] G. Tsudik, "Message authentication with one-way hash functions. ACM Comput," *Commun. Rev*, vol. 22, no. 5, pp. 29–38, 1992.

[13] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *JCSS*, vol. 18, pp. 143–154, 1979.

[14] W. Nevelsteen and B. Preneel, "Software performance of universal hash functions," in *Advances in CryptologyEUROCRYPT99*. Springer, 1999, pp. 24–41.

[15] C. Paar, J. Pelzl, and I. ebrary, *Understanding cryptography: a textbook for students and practitioners*. Springer, 2010.

[16] K. Yuksel, "Universal hashing for ultra-low-power cryptographic hardware applications [electronic resource]." Master's thesis, Worcester Polytechnic Institute, 2004. [Online]. Available: http://www.wpi.edu/Pubs/ETD/Available/etd-0428104-195331; http://worldcat.org/oclc/55848122

[17] H. Chabanne and G. Fumaroli, "Noisy cryptographic protocols for low-cost RFID tags," *IEEE Transactions on Information Theory*, vol. 52, no. 8, pp. 3562–3566, 2006.

[18] Gander and Maurer, "On the secret-key rate of binary random variables," in *ISIT: Proceedings IEEE International Symposium on Information Theory, sponsored by The Information Theory Society of The Institute of Electrical and Electronic Engineers*, 1994.

[19] G. Brassard and L. Salvail, "Secret key reconciliation by public discussion," *Lecture Notes in Computer Science*, vol. 765, pp. 410–423, 1994.

[20] F. M. A. B. Albert and M. Rodrigues, "Single shift-register for RFID tag secrecy," in *IEEE International Telecommunications Symposium - ITS2010*. SBrT, 2010.

[21] M. V. C. Rodrigues, "Segurança de Sistemas RFID com Modulação Aleatória," *Dissertação de Mestrado, DEE/UFCG*, 2010.