MO422-MC938 Algoritmos Criptográficos

Aula 1 - Visão Geral da Criptografia Moderna

Ricardo Dahab

Instituto de Computação
Universidade Estadual de Campinas

2s. 2018

Roteiro da aula

- Um pouco de História
- Criptografia Simétrica
  - Cifras de bloco e de fluxo
  - Algoritmos clássicos e modernos
- Resumo (Hash) Criptográfico
- Criptografia Assimétrica
  - RSA e ElGamal
  - Curvas Elípticas
  - Emparelhamentos Bilineares
  - Criptografia Pós-quântica
- Acordo e Distribuição de Chaves
  - Usando sistemas assimétricos
  - Criptografia Quântica (Distribuição quântica de chaves)
- Criptomania
- Desafios de hoje
- Cripto no Brasil e no mundo

Um pouco de História

$<$ **1970s.** Criptografia provê basicamente sigilo de comunicações: Meio diplomático e militar.

- Grande relevância na Segunda Guerra Mundial: Bletchley Park, Alan Turing, W.T. Tutte et al.
- COLOSSUS, o primeiro computador da era moderna.

1976. Novos paradigmas

- *New directions in Cryptography* (W. Diffie e M. Hellman).
- Criptografia de chave pública.
- Convergência notável: Criptografia pública na era da Internet.
- Esforços iniciaram-se no meio militar, na década de 1960.

Um pouco de História

- Hoje, técnicas criptográficas são maciçamente empregadas no comércio eletrônico e na prevenção de incidentes de segurança.
- Encriptação, assinaturas digitais e funções de autenticação criptográficas (hash) estão no cerne de praticamente todas comunicações e transações eletrônicas.
- Pesquisa na área historicamente embasada na estatística e álgebra linear.
- Hoje é multidisciplinar: Teoria dos Números, Teoria da Computação, Complexidade Computacional, Teoria dos Códigos e Reticulados, Computação e Física Quântica, Teoria da Informação Quântica, Métodos Formais, Álgebra.

Um pouco de História

1970s.

- Primeiro método padronizado para uso civil (DES).
- Várias propostas de sistemas de chaves públicas surgiram, baseadas na Teoria dos Números e Otimização Combinatória.

1980s.

- Consolidação do RSA (baseado na fatoração de inteiros). Alternativas relegadas ao segundo plano (eficiência, fragilidade).
- Surgimento dos sistemas baseados em curvas elípticas (ECC) (baseados no logaritmo discreto).
- Primeiras ameaças ao DES.
- Método de acordo de chaves baseado em efeitos quânticos.
- Primeiras funções de *hash* (resumo criptográfico).

Um pouco de História

1990s.

- Predominância clara do RSA.
- Primeiros dispositivos portáteis: aumento da popularidade dos ECC.
- Obsolescência do DES: advento do AES.
- Novas funções de resumo.
- Emparelhamentos bilineares ganham notoriedade: Criptografia baseada em identidades (IBE).
- Advento dos algoritmos quânticos de P. Shor (fatoração e logaritmo discreto em tempo polinomial).

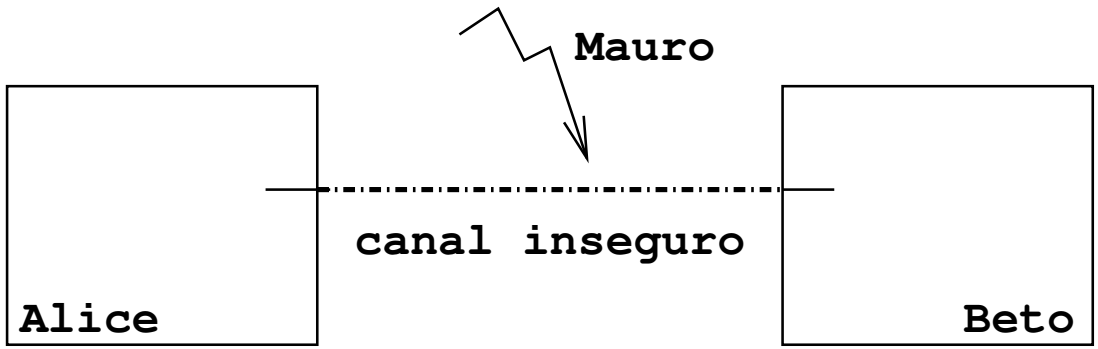
Um pouco de História

2000s

- Novos paradigmas de certificação de chaves públicas, impulsionados pelo advento de emparelhamentos.
- Novos protocolos baseados em emparelhamentos bilineares.
- Grande ênfase na demonstração formal da robustez de protocolos criptográficos.
- De volta ao passado: algoritmos pós-quânticos, baseados em códigos, reticulados, e outros.
- Ameaças sérias aos algoritmos de resumo: competição por novos em curso.
- Migração da criptografia para o hardware.

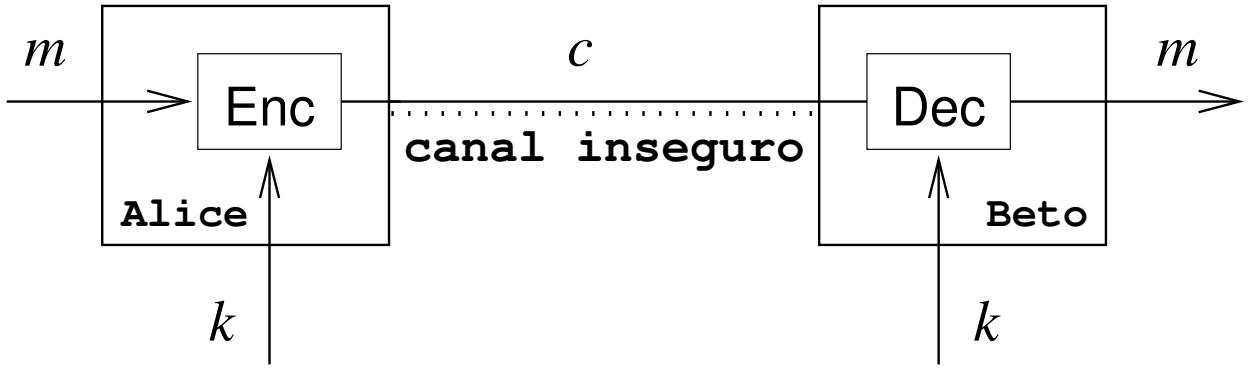
Modelo de comunicação

Alice, Beto e Mauro.



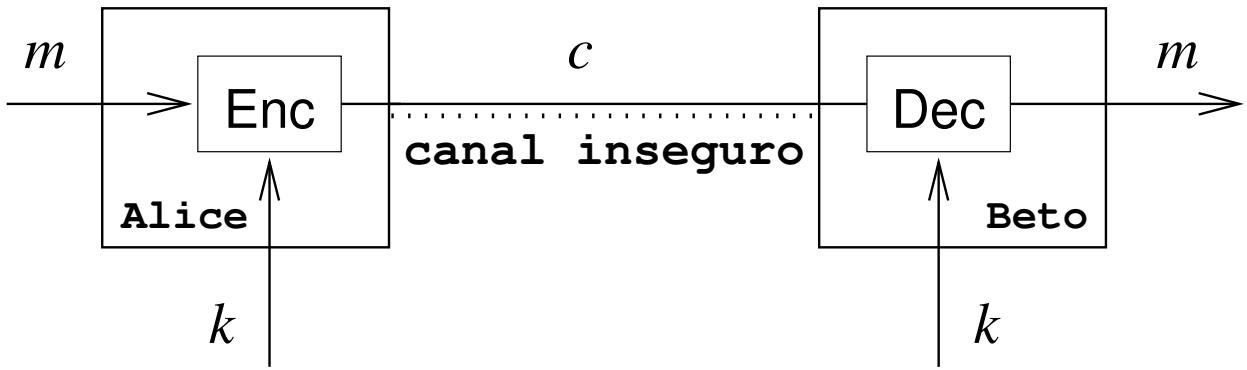
- Os métodos de Mauro vão desde a simples escuta (ataque passivo), até a modificação, repetição e injeção de mensagens com objetivos variados (ataque ativo).
- As técnicas criptográficas para prevenir tais ataques vêm de duas vertentes, a simétrica e a assimétrica, usadas isoladamente ou em conjunto.

Criptografia simétrica



- Alice e Beto desejam trocar mensagens m (*texto claro*) em sigilo;
- Alice aplica uma *função (ou algoritmo) de encriptação* $\textsc{Enc}_k(m)$, que transforma m numa *mensagem encriptada* ou *texto encriptado* c, sob a ação da *chave* k.
- Ao receber c, Beto aplica a função de *decriptação* $\textsc{Dec}_k(c)$, recuperando m.

Criptografia simétrica



- O objetivo é produzir um texto c que não guarde relação alguma com m.
- A inclusão da chave k no processo tem o objetivo de dar o poder de transformar c em m apenas a quem conhece k; isto é, prover sigilo na transmissão de m.

Criptografia simétrica

Cifras de bloco

- Chaves têm tamanho fixo e textos são cifrados em blocos de tamanho igual, segundo um método complexo repetidamente aplicado a cada bloco, com a mesma chave.

Cifras de fluxo

- Chaves têm tamanho arbitrário e seus bits são combinados um-a-um com os bits do texto claro, segundo um método simples, usualmente um ou-exclusivo.
- Se a chave for aleatória, de tamanho pelo menos igual ao do texto claro, e nunca antes usada para cifrar mensagens, temos o chamado *one-time pad*, de segurança perfeita.

Criptografia simétrica - premissas

- $\textsc{Enc}_{\cdot}(.)$ deve ser projetada de forma que seja muito difícil para Mauro calcular m a partir de c sem conhecimento de k, ainda que $\textsc{Enc}_{\cdot}(.)$ seja pública e Mauro tenha grande poder computacional.
- Dizemos que $\textsc{Enc}_k(.)$ deve ser uma função *de mão-única* para cada valor fixo de k; isto é, que $\textsc{Enc}_k(.)$ seja fácil de calcular, mas $\textsc{Enc}_k(.)^{-1}$, ou seja, $\textsc{Dec}_k(.)$, seja muito difícil de calcular sem o conhecimento da chave k.
- A quantidade de chaves possíveis deve ser muito grande, para evitar uma *busca exaustiva* de k.
- Alice e Beto têm que estabelecer a chave k em sigilo antes do seu uso. Essa dificuldade é recorrente. Veremos como essa dificuldade pode ser contornada.

Criptografia simétrica - simetria

- O adjetivo simétrico é bastante adequado. Tudo que um puder encriptar ou decriptar o outro também pode.
- Um benefício dessa simetria é a confiança que Alice e Beto têm de que estão trocando mensagens sigilosas um com o outro, e não com Mauro.
- Por outro lado, não é possível atribuir a um ou a outro a autoria de uma mensagem sem a ajuda de uma terceira parte confiável.
- Outras denominações são *sistemas de chaves secretas* e *sistemas de chaves simétricas*.

Alguns algoritmos simétricos modernos

- Data Encryption Standard (DES), 1977.
- Advanced Encryption Standard (AES), 2000.
- NIST (1997-1999): MARS, RC6, Serpent, Twofish.
- NESSIE (2003): MYSTY1, AES, Camellia (ISO 2005).
- CRYPTREC (2002): Camellia, SC2000, Hierocrypt-3, CIPHERUNICORN-A.
- ECRYPT (European Network of Excellence for Cryptology) 2004-2008: Kasumi (64-128), AES.
- Atualizar...

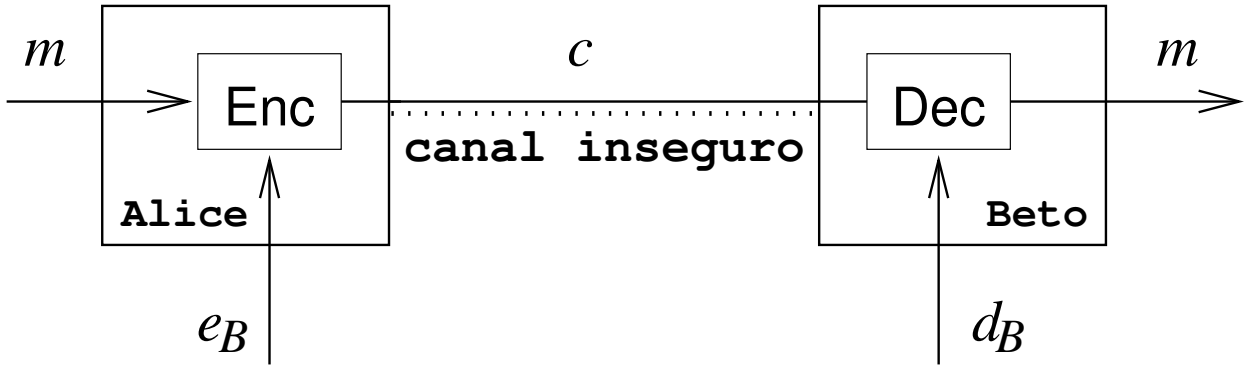
Funções de resumo criptográfico

Uma função de resumo criptográfico (hash)) é uma função $H : \{0,1\}^* \to \{0,1\}^n$ (*muitos-para-um*), satisfazendo:

- **Resistência ao cálculo de pré-imagens:** Dado um resumo r na imagem de H, é inviável (computacionalmente) encontrar qualquer m tal que $r = H(m)$.
- **Resistência ao cálculo de segunda pré-imagem:** Dado um resumo r na imagem de H, e m_1 tal que $r = H(m_1)$, é inviável encontrar $m_2 \neq m_1$ tal que $r = H(m_2)$.
- **Resistência a colisões:** Dado um resumo r, é inviável encontrar qualquer par $m_1 \neq m_2$ tais que $H(m_1) = H(m_2)$.

Algoritmos mais usados SHA-2, SHA-3. Novos padrões estão sendo definidos.
Muito úteis em assinaturas, códigos de autenticação, entre outros.

Criptografia assimétrica



- Alice aplica uma função de encriptação $\textsc{Enc}_{e_B}(m)$, que transforma m numa mensagem encriptada c, sob a ação da chave e_B.
- Beto então aplica a função de decriptação $\textsc{Dec}_{d_B}(c)$, recuperando m.
- No caso de mensagens de Beto para Alice, as chaves usadas são: e_A para encriptação e d_A para decriptação.

Criptografia Assimétrica

Note que:

- As chaves e_B, d_B são ambas de Beto.
- A primeira, e_B, é a chave pública de Beto, distribuída e utilizada livremente.
- A segunda, d_B, é de conhecimento exclusivo de Beto, sua chave privada. A chave e_B é utilizada para encriptação de mensagens para Beto e d_B para decriptação dessas mensagens.
- O mesmo se aplica para as chaves de Alice (e_A e d_A).

Consequências do modelo assimétrico

- Não é mais necessário um acordo prévio de chaves, já que cada usuário deve necessariamente gerar o seu próprio par de chaves.
- O número de chaves é $2n$ no caso assimétrico contra $n \times (n-1)/2$ chaves no caso simétrico.

Premissas do modelo assimétrico

- $\textsc{Enc}_{\cdot}(.)$ deve ser de mão-única para cada chave e_X, a menos que se conheça a chave d_X de decriptação.
- Obviamente, e_B e d_B são relacionadas, mas não deve ser possível calcular d_B a partir do conhecimento de e_B em tempo hábil; consequentemente, o número de possibilidades para d_B deve ser muito alto (centenas a milhares de bits)
- Alice tem a confiança de que a chave de encriptação é a chave e_B de Beto, contanto que a tenha obtido de forma confiável.

Criptografia assimétrica - assimetria

- A assimetria deste modelo é evidente: o poder na transmissão de mensagens de Alice para Beto é de Beto, o destinatário. Só Beto consegue decriptar mensagens, usando sua chave privada d_B.
- Outro subproduto marcante da assimetria é a possibilidade de que Beto possa *assinar* mensagens enviadas a Alice e outros.
- Imaginemos que existam funções $\textsc{Sign}_{d_B}(.))$ e $\textsc{Ver}_{e_B}(\cdot)$, com a propriedade de que $\textsc{Ver}_{e_B}(m, s)$ retorna 1 quando $s = \textsc{Sign}_{d_B}(m)$, e 0 caso contrário.
- Teremos em s o equivalente de uma assinatura digital de Beto em m, provendo assim irretratabilidade das mensagens assinadas por Beto.
- Criptografia assimétrica = de chave pública.

Alguns sistemas de chave pública populares

- RSA, 1978.
- ElGamal, 1984-1985.
- Rabin, 1979.
- Curvas Elípticas, Miller e Koblitz, 1985.
- DSA, 1991. Proposto por NIST.
- ECDSA, NIST (1999).
- IBE, 2000 (Criptografia Baseada em Identidades).
- Baseados em Códigos e Reticulados.

Breve histórico da criptografia de chave pública

- Conceito introduzido por Whitfield Diffie e Martin Hellman em 1976: Protocolo de acordo de chaves DH. (Logaritmo discreto módulo p).
- RSA: Rivest, Shamir Adleman, 1978. (Fatoração).
- ElGamal: (Assinatura digital), 1984-1985.(Logaritmo discreto módulo p.)
- Goverment Communications Headquarters (UK). (James Ellis, Clifford Cocks, Malcolm Williamson - primeiros inventores do RSA e do Protocolo DH, 1969-1974).

O RSA

Geração de Chaves:

1. Gere dois números primos aleatórios p e q (distintos)
2. Calcule $n = p \cdot q$
3. Calcule $\phi = (p-1) \cdot (q-1)$
4. Escolha um número e, $1 < e < \phi$, tal que $\text{mdc}(e, \phi) = 1$.
5. Calcule o (único) número d, $1 < d < \phi$, tal que $ed \equiv 1 \pmod{\phi}$.
6. Chave privada: d
7. Chave pública: e, n

O RSA

Algoritmo para encriptar

Para encriptar uma mensagem m para Alice, Beto faz o seguinte:

1. Obtem a chave pública (autêntica) de Alice e, n
2. Representa a mensagem m como um inteiro em $\{0, 1, 2, ...n-1\}$.
3. Calcula $c = m^e \mod n$
4. Envia o texto cifrado c para Alice.

O RSA

Algoritmo para decriptar:

Para recuperar o texto claro m a partir de c, Alice faz o seguinte:

1. Utiliza a chave privada d para calcular o texto claro m:

$$m = c^d \mod n$$

O RSA

- O RSA é baseado na dificuldade da fatoração de inteiros grandes (milhares de bits).
- A fatoração de n implica na imediata inversão da função $c = m^e \mod n$. Não se sabe se esses problemas são equivalentes.
- Melhores algoritmos para fatoração têm complexidade subexponencial.

Super-bonus: Usando-se a a chave privada sobre uma mensagem em claro m produz o equivalente de uma assinatura digital, verificável com a chave pública!!

Problema do logaritmo discreto

Agora uma fonte algébrica de sistemas de chave pública.

- Dado um grupo G, o número de elementos de $\mathbb{G}$ é a sua *ordem*. Se a ordem é finita, então $\mathbb{G}$ é um *grupo finito*.
- A *ordem de um elemento* $a \in \mathbb{G}$ é o menor inteiro positivo t tal que $ta = 0$. É um fato bem conhecido que a ordem de um elemento divide a ordem do grupo.
- Quando, para um grupo finito $\mathbb{G}$ de ordem n, existe um elemento α de ordem n, dizemos que $\mathbb{G}$ é *cíclico* e que α é um *gerador* de $\mathbb{G}$.

Definição

(Problema do logaritmo discreto-PLG) Dados elementos a, b de um grupo $(G, .)$, tais que $b = a^r$, o problema do logaritmo discreto é o de encontrar r conhecendo a e b apenas.

Logaritmo discreto em $\mathbb{Z}_7^*$

$p = 7$: um número primo

$\alpha = 3$: um gerador de $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

i	$3^i \mod 7$
0	1
1	3
2	2
3	6
4	4
5	5
6	1

$3^i \equiv 6 \pmod 7$; $\quad i = 3$

Problema do logaritmo discreto

- Para certos grupos finitos, o problema do logaritmo discreto é trivial, e.g. $(\mathbb{Z}_n, +)$.
- Em outros grupos, só se conhecem algoritmos subexponenciais, e.g. $(\mathbb{Z}_p^*, \times)$, p primo.
- Em outros ainda só se conhecem algoritmos exponenciais, e.g. o grupo de pontos de curvas elípticas sobre corpos finitos.
- O primeiro uso do PLG como base de um sistema criptográfico foi o protocolo de Diffie e Hellman para estabelecimento de chaves simétricas, em 1976.
- Seguiram-se o sistema de ElGamal (1984-85) e os baseados em curvas elípticas (1985).

Criptossistemas de Curvas Elípticas (ECC)

- Sistemas de chave pública propostos por Victor Miller e Neal Koblitz em 1985.
- Padrões: ANSI X9.62, IEEE P1363, FIPS 162-2, SEC 1-2, NIST
- Aplicações: cartões inteligentes, celulares, redes de sensores sem fio, etc.
- Companhias: Certicom, RSA Security, Cryptomathic, HITACHI.

Criptossistemas de Curvas Elípticas

A principal vantagem dos ECC é que utilizam chaves de comprimento menor com o mesmo nível de segurança oferecido por outros sistemas de chave pública (RSA, DSA).

ECC	RSA	AES
224	2048	-
256	3072	128
384	8192	192
512	15360	256

Nível de Segurança em bits

Emparelhamentos Bilineares

Definição

Sejam G_1 grupo aditivo, G_2 um grupo multiplicativo, ambos de ordem prima n. Seja α um gerador de G_1. Um emparelhamento bilinear é um mapeamento $\hat{e} : G_1 \times G_1 \to G_2$, tal que:

1. *(bilinearidade) Para todos $\beta, \gamma, \delta \in G_1$, $\hat{e}(\beta + \gamma, \delta) = \hat{e}(\beta, \delta)\hat{e}(\gamma, \delta)$ e $\hat{e}(\beta, \gamma + \delta) = \hat{e}(\beta, \gamma)\hat{e}(\beta, \delta)$;*
2. *(não-degeneração) $\hat{e}(\alpha, \alpha) \neq 1$;*
3. *(computabilidade) O mapeamento $\hat{e}$ é eficientemente computável.*

Consequência muito util:

$$\hat{e}(a\beta, b\gamma) = \hat{e}(\beta, \gamma)^{ab}, \text{para } a, b, \text{inteiros.} \quad (1)$$

Emparelhamentos Bilineares

- Emparelhamentos foram utilizados inicialmente para "atacar" uma certa classe de sistemas baseados em curvas elípticas.
- Posteriormente, descobriu-se que poderiam ser úteis também de forma construtiva, em esquemas de assinaturas, acordo de chaves, entre outras aplicações.
- Foi uma área de explosivo crescimento no fim da década de 1990 e início de 2000, com inúmeras novas aplicações e novas soluções elegantes para problemas antigos.

Emparelhamentos Bilineares

- O maior empecilho para seu emprego, inicialmente, foi a complexidade da sua implementação, ordens de magnitude maiores que outros sistemas para o mesmo fim.
- Emparelhamentos bilineares com utilidade criptográfica são poucos: bem conhecidos são os de Tate e Weil, construídos sobre grupos de pontos de curvas elípticas.
- Mas não são animais tão raros assim: o produto interno de dois vetores é um tipo de emparelhamento (mas não é util do ponto de vista criptográfico).

Pré-distribuição de chaves I (Diffie-Hellman)

Contexto inicial:

- Parâmetros públicos são: grupo $(G, .)$ e $\alpha \in G$ de ordem n.

Resultado: Chave de sessão k compartilhada por A e B.

1.	A:	$\texttt{sorteia}(r_A)$, inteiro em $\{0 \ldots n-1\}$;
		$x_A \leftarrow \alpha^{r_A}$;
		$\rightsquigarrow B$: (A, x_A);
	B:	$\texttt{sorteia}(r_B)$, inteiro em $\{0 \ldots n-1\}$;
		$x_B \leftarrow \alpha^{r_B}$;
		$\rightsquigarrow A$: (B, x_B);
2.	A:	$k = x_B^{r_A}$;
	B:	$k' = x_A^{r_B}$;

Emparelhamentos - exemplo de uso

- Alice, Beto e Carlos (C) querem estabelecer uma chave comum k.
- Com Diffie-Hellman clássico, duas rodadas são necessárias:
  [1.] $A \rightsquigarrow B : \alpha^{r_A}$, $B \rightsquigarrow C : \alpha^{r_B}$ e $C \rightsquigarrow A : \alpha^{r_C}$.
  [2.] $A \rightsquigarrow B : \alpha^{r_C r_A}$, $B \rightsquigarrow C : \alpha^{r_A r_B}$ e $C \rightsquigarrow A : \alpha^{r_B r_C}$.
- Após essas rodadas, os três calculam $k = \alpha^{r_A r_B r_C}$.
- É possível estabelecer a chave k com apenas uma rodada de mensagens?
- Sim, mas com emparelhamentos bilineares.

Pré-distribuição de chaves tripartite (Joux)

Contexto inicial: A, B, C usam um emparelhamento $\hat{e}$.
Resultado: Chave de sessão k compartilhada por A, B e C.

1.	A:	$\texttt{sorteia}(r_A)$, inteiro em $[0, n-1]$;
		$x_A \leftarrow r_A\alpha$;
		$\rightsquigarrow\{B, C\}$: (A, x_A);
	B:	$\texttt{sorteia}(r_B)$, inteiro em $[0, n-1]$;
		$x_B \leftarrow r_B\alpha$;
		$\rightsquigarrow\{A, C\}$: (B, x_B);
	C:	$\texttt{sorteia}(r_C)$, inteiro em $[0, n-1]$;
		$x_C \leftarrow r_C\alpha$;
		$\rightsquigarrow\{A, B\}$: (C, x_C);

Pré-distribuição de chaves tripartite (Joux)

Contexto inicial: A, B, C usam um emparelhamento $\hat{e}$.
Resultado: Chave de sessão k compartilhada por A, B e C.

2.	A:	$k \leftarrow \hat{e}(x_B, x_C)^{r_A}$;
	B:	$k \leftarrow \hat{e}(x_A, x_C)^{r_B}$;
	C:	$k \leftarrow \hat{e}(x_A, x_B)^{r_C}$.

Distribuição Quântica de Chaves

- Informação não é transformada mas enviada em claro por um canal onde não pode ser lida por um intruso de forma imperceptível. Isto é, em vez de esconder a informação, coíbe o acesso a ela.
- Início da década de 1970, S. Wiesner lançou idéias seminais sobre o uso de estados conjugados de partículas elementares para codificar e transmitir informação.
- Idéias formaram a base do trabalho de C. Bennett e G. Brassard (1984), o primeiro a descrever um protocolo completo para o acordo de uma chave (necessariamente!) aleatória, sem comunicação prévia entre as partes.

Distribuição Quântica de Chaves

- Os trabalhos de Wisner, Bennett e Brassard tornaram possível o sonho da cifra perfeita, o *one-time pad*:

  "Dado um texto t e uma chave k aleatória, de comprimento igual ao de t, o texto encriptado

  $$c = t \oplus k$$

  tem segredo perfeito, isto é, a divulgação de c não oferece informação alguma sobre t que já não fosse conhecida antes."

- Até hoje, essa distribuição quântica de chaves (*quantum key agreement*) é a única aplicação bem sucedida de técnicas quânticas em Criptografia, já com produtos comerciais.
- Não se conhecem métodos quânticos para encriptação e há outros resultados negativos.

Criptografia Pós-quântica

- A possibilidade do advento de computadores quânticos comerciais é uma ameaça concreta aos sistemas criptográficos baseados na fatoração de inteiros e no problema do logaritmo discreto.
- Para ambos os problemas, existem algoritmos quânticos que os resolvem em tempo polinomial (Shor, Grover).
- Alternativas tem sido buscadas ativamente pela comunidade de pesquisa criptográfica. Já há eventos totalmente dedicados ao tema.
- Velhas propostas: McEliece (1980s - códigos corretores de erros), Lamport-Diffie (1970s - Hash).
- Novas propostas: baseadas em reticulados, entre outras.

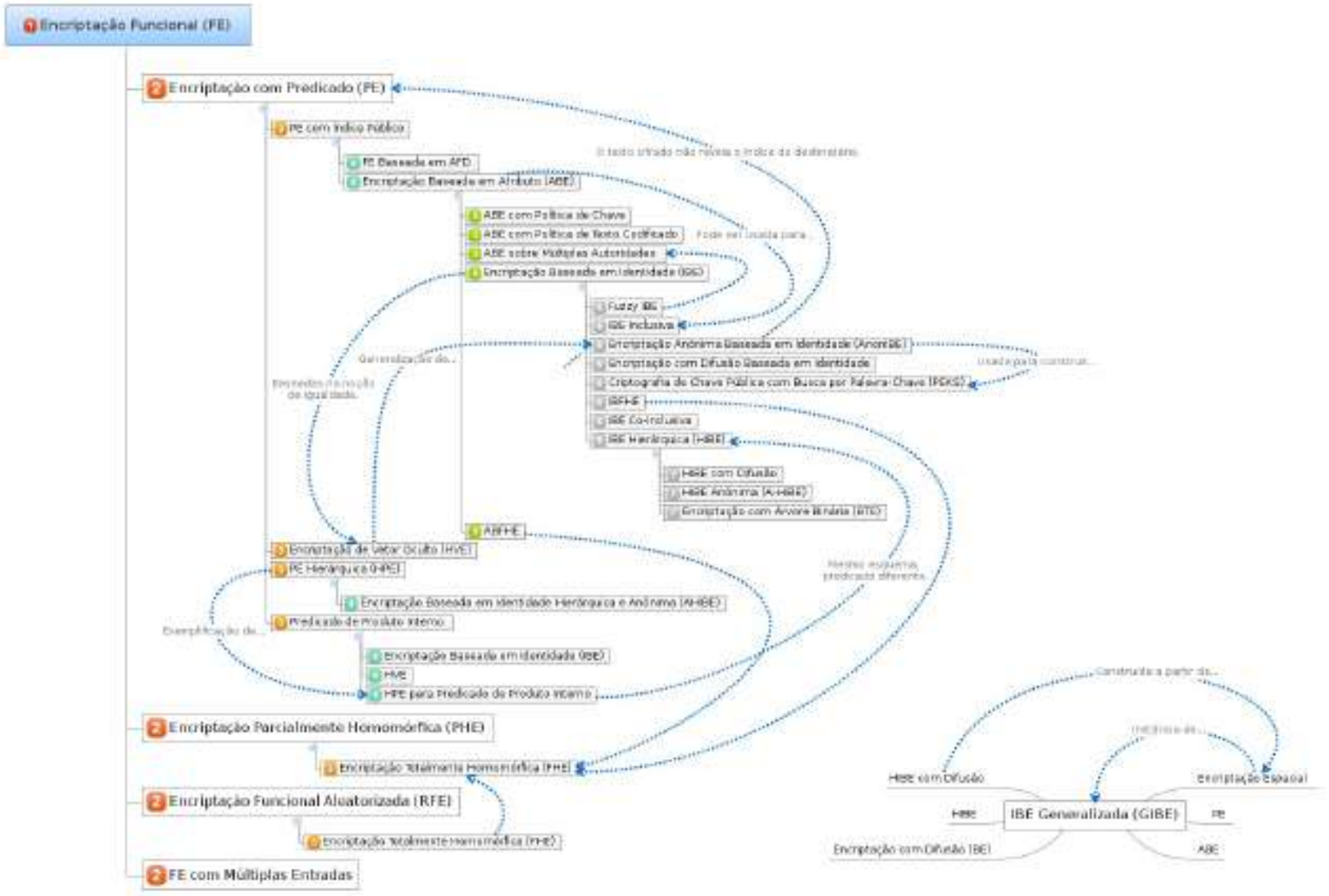
Criptomania

- Emparelhamentos possibilitaram a criação de muitas funcionalidades distintas da encriptação pura e simples.
- Na *Encriptação Funcional* o detentor da chave de decriptação sk_k, associada à palavra-chave k, é capaz de computar a funcionalidade $F(k, x)$ sobre a encriptação de x.
- Criptografia pós-quântica e desdobramentos $\rightarrow$ possibilitaram a concretização da encriptação (parcial, totalmente) homomórfica e muitos outros desdobramentos, teóricos e práticos.

Criptomania - Criptografia baseada em identidades

- Alternativa ao uso de certificados digitais. Proposta como esquema de assinaturas em 1984 por Adi Shamir.
- Ganhou impulso em 2001 com a primeira proposta prática de esquema de encriptação baseado em identidades, de Boneh e Franklin.
- Chaves públicas auto-identificáveis: `'Esta chave pertence a alice@alice.com'`.
- Chaves privadas são geradas em conjunto pelo usuário e um *gerador de chaves privadas–GCP*. Perda de independência das entidades.
- Outras informações na chave públicas (datas, etc).
- Há propostas alternativas.

Criptomania - Encriptação Funcional



Desafios de hoje

- **Computação ubíqua (Internet das Coisas):** dispositivos embutidos de baixo poder, comunicação sem fio, vulneráveis $\rightarrow$ Criptografia leve, baseada em ECC ou menos.
- **Redes adhoc:** ameaças à privacidade, dificuldade de autenticação, roaming. $\rightarrow$ Formas alternativas de identificação e autenticação.
- **Computação em nuvem:** ameaças ao sigilo e privacidade. $\rightarrow$ Computação com dados encriptados.
- **Ataques ao hardware:** Vazamento por canais secundários ou intrusão direta. $\rightarrow$ Métodos para uniformizar código e esconder perfis de execução.
- **Criptografia no mundo real:** Implementações mal-feitas são um grande problema. $\rightarrow$ Ferramentas, educação, conscientização.

Criptografia no Brasil

- Várias instituições têm grupos ativos de pesquisa em criptografia.
- Há muitas outras na área mais ampla de Segurança da Informação e Sistemas.
- Participação na SBC dentro da Comissão Especial de Segurança. Evento da área é o SBSeg, com parte do programa dedicado à Criptografia.
- Primeiro Latincrypt em 2010.
- CANS em 2013, PKC em 2018.

Criptografia no mundo

Veja o site da International Association for Cryptologic Research (www.iacr.org) para conferências e outros links internacionais de qualidade.

- CRYPTO. A mais tradicional
- EUROCRYPT
- ASIACRYPT Conference.
- CHES–Cryptographic Hardware Embedded Software. Voltada para cripto embarcada.
- PKC–Public Key Cryptography Workshop.
- FSE–Fast Software Encryption.
- TCC Theoretical Cryptography Conference.
- Africacrypt, Indocrypt, Latincrypt...

Visite o site do ePrint (Cryptology ePrint Archive) (eprint.iacr.org) também para artigos, outros eventos, etc.