Group Signature dengan Skema Secret Sharing

Mekanisme *(t,n)-Threshold* Group Signature Praktis

Agung Utama Putra
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
agungutama91@gmail.com

***Abstract*—Group signature adalah mekanisme yang memungkinkan seorang group member mendatangani sebuah pesan elektronik atas nama group. (t,n)-*threshold* group signature adalah mekanisme group signature yang mengharuskan minimum t dari n group member terlibat dalam pembuatan signature. Dalam tulisan ini diajukan mekanisme (t,n)-*threshold* group signature praktis menggunakan RSA dan skema secret sharing berbasis Lagrange interpolating polynomial. Analisis keamanan menunjukkan mekanisme ini memenuhi persyaratan keamanan group signature. Pekerjaan lebih lanjut dibutuhkan untuk meningkatkan keamanan mekanisme ini dengan tetap mempertahankan kepraktisannya.**

Keywords—digital signature; group signature; (t,n)-threshold group signature; RSA; secret sharing;

I. PENDAHULUAN

Group signature adalah mekanisme yang memungkinkan seorang anggota kelompok atau group member menandatangani sebuah pesan elektronik atas nama kelompoknya, tanpa mengungkap identitas penandatangan [1]. Group signature dapat digunakan dalam berbagai aplikasi seperti e-voting, e-bidding, e-cash, fingerprinting, dan sebagainya [2].

Berbagai mekanisme group signature telah diajukan dalam berbagai tulisan sejak pertama kali diperkenalkan oleh Chaum dan van Heyst [1] [3] [4]. Meskipun telah dibuktikan aman, mekanisme-mekanisme tersebut tidak efisien untuk sebuah group berukuran besar, karena ukuran group public keys dan signature yang proporsional dengan jumlah group member. Mekanisme lain yang berbasis pada logaritma diskrit [5], DSS [6], dan RSA [2] memiliki ukuran group public keys yang konstan sehingga lebih tepat digunakan untuk group berukuran besar.

Namun mekanisme-mekanisme yang disebutkan sebelumnya adalah untuk memungkinkan salah satu anggota kelompok membuat group signature, siapapun anggota tersebut. Untuk alasan keamanan, ada kalanya sebuah kebijakan dalam suatu organisasi mengharuskan suatu dokumen ditandatangani oleh beberapa individu. Untuk mengakomodir hal ini, Desmedt dan Frankel [7] memperkenalkan mekanisme (t,n)-*threshold* group signature yang berbasis pada beberapa konsep, salah satunya adalah secret sharing.

Secret sharing atau (t,n)-*threshold schemes* adalah mekanisme membagi suatu data rahasia ke dalam n buah bagian, dimana akan dibutuhkan minimum t buah bagian untuk dapat merekonstruksi data rahasia tersebut [8] [9]. Shamir mengajukan skema secret sharing yang berbasis pada Lagrange interpolating polynomial [9].

Skema secret sharing telah menjadi *building block* pada mekanisme (t,n)-*threshold* group signature yang telah diajukan [7] [10] [11]. Konsekuensi yang tidak dapat dihindari adalah peningkatan kompleksitas pada setiap prosedur dalam mekanisme group signature tersebut, termasuk prosedur verifikasi signature yang harus dilakukan penerima group signature, untuk tetap memenuhi persyaratan keamanan group signature. Referensi [2] mengajukan mekanisme group signature praktis berbasis RSA yang tetap memenuhi persyaratan keamanan group signature, namun mekanisme ini bukanlah mekanisme (t,n)-*threshold* group signature.

Dalam tulisan ini akan diajukan sebuah mekanisme (t,n)-*threshold* group signature yang praktis. Mekanisme group signature yang diajukan menggunakan RSA dan skema secret sharing berbasis Lagrange interpolating polynomial. Group public key dan signature dalam mekanisme ini akan berukuran konstan. Dalam tulisan ini juga akan ditunjukkan analisis keamanan mekanisme yang diajukan.

Bagian II mendeskrpisikan definisi-definisi dan asumsi-asumsi yang digunakan. Bagian III mengajukan mekanisme group signature yang dibuat. Bagian IV merupakan analisis keamanan mekanisme group signature yang diajukan. Bagian V mendeskripsikan pekerjaan yang masih harus dilakukan dalam meningkatkan keamanan mekanisme group signature yang diajukan. Bagian VI merupakan kesimpulan.

II. DEFINISI DAN ASUMSI

Pada bagian ini akan dijelaskan definisi-definisi dan asumsi-asumsi yang digunakan dalam mekanisme group signature.

A. Definisi

Terdapat setidaknya 2 (dua) pihak yang terlibat dalam mekanisme group signature: group manager (GM) dan group member, serta prosedur-prosedur sebagai berikut [1] [12] [2] [6]:

- **Setup**: algoritma yang menghasilkan parameter sistem, pasangan public key dan private key, dan sebagainya.
- **Join**: protokol antara group manager dan user sehingga user tersebut bergabung menjadi group member.
- **Sign**: algoritma yang menghasilkan group signature terhadap suatu pesan.
- **Verify**: algoritma yang melakukan verifikasi terhadap validitas suatu group signature.

B. *Asumsi*

Group manager (GM) bertugas sebagai pihak yang mengelola group member dan pelaksanaan prosedur-prosedur diatas (selain **Verify**). Oleh karena itu, GM harus diasumsikan dapat dipercaya sepenuhnya (totally trusted), dan komunikasi antara GM dengan group member harus dilakukan via saluran aman [1] [2].

Setiap group member U_i mendapatkan identitas keanggotaan x_i yang merupakan merupakan identitas user tersebut, dan *membership secret* y_i yang merupakan kunci milik member yang digunakan untuk membuat group signature. Diasumsikan untuk setiap 1 (satu) membership id, terdapat tepat 1 (satu) membership secret.

Fungsi hash kriptografi $H(m)$ adalah sebuah fungsi satu arah (*one-way function*). Fungsi hash kriptografi dapat menggunakan salah satu dari fungsi yang distandarisasi oleh NIST [13].

Group signature yang akan dibuat harus dilakukan oleh minimum t group member dari jumlah keseluruhan group member n dan $t \leq n$.

III. Mekanisme Group Signature

Mekanisme yang diusulkan dideskripsikan sebagai berikut:

A. *Setup*

GM memilih dua bilangan prima p dan q, dan menghitung $n = p \times q$ dan totient $\varphi(n) = (p-1) \times (q-1)$. GM kemudian memilih nilai e dimana $1 < e < \varphi(n)$ sehingga e dan $\varphi(n)$ coprime. Hitung d sehingga $d \times e \pmod{\varphi(n)} = 1$.

Group public key adalah (e, n). Group private key adalah d. Kemudian pilih fungsi hash kripografi $H(m)$ yang disetujui untuk digunakan. Terakhir, GM memilih bilangan prima r dimana $r > n$ dan $r > d$.

Group public key dan $H(m)$ dipublikasikan. Group private key d hanya disimpan selama group belum memiliki $t \leq n$ member, dan dimusnahkan setelahnya. Bilangan r dapat disimpan GM atau disertakan pada identitas anggota dan membership secret.

B. *Join*

Apabila group belum memiliki t member (group baru dibentuk), GM membuat suatu polinomial:

$$P(x) = a_0 + a_1 x + \cdots a_t x^{t-1} \pmod{r} \qquad (1)$$

Konstanta $a_o = d$, dan konstanta-konstanta $a_1, a_2, \ldots, a_t$ dipilih secara acak. $P(x)$ akan digunakan hingga $t \leq n$ member sudah bergabung.

Apabila group sudah memiliki *n* member, polinomial $P(x)$ diinterpolasi dengan bantuan t group member menggunakan Lagrange interpolating polynomial [14] dengan persamaan (2) dan (3) untuk merekonstruksi kembali persamaan (1).

$$P(x) = \sum_{i=1}^{t} P_i(x) \pmod{r} \qquad (2)$$

$$P_i(x) = y_i \prod_{\substack{j=1 \\ j \neq i}}^{t} \frac{x - x_j}{x_i - x_j} \pmod{r} \qquad (3)$$

Setelah $P(x)$ didapatkan, untuk setiap user yang akan bergabung GM memilih x_i yang dikaitkan dengan user tersebut secara unik, dengan $x_i \neq 0$. Kemudian dihitung $y_i = P(x_i)$ dengan persamaan (1).

Group member U_i menerima (x_i, y_i) via saluran aman. GM tidak menyimpan y_i maupun $P(x)$ setelah prosedur ini dilakukan.

C. *Sign*

GM menerima pesan m yang akan dibuatkan signature-nya serta t buah (x_i, y_i). GM merekonstruksi persamaan (1) dengan persamaan (2) dan (3) untuk mendapatkan group private key $d = P(0)$. GM kemudian membuat group signature σ untuk pesan m dengan $\sigma = H(m)^d \bmod n$.

Group signature disertakan bersama dengan pesan m. GM tidak menyimpan y_i maupun $P(x)$ setelah prosedur ini dilakukan.

D. *Verify*

Penerima pesan m memverifikasi group signature menggunakan public key yang dipublikasikan. Group signature σ untuk pesan m valid apabila $H(m) = \sigma^e \bmod n$.

IV. Analisis Keamanan

Karena berbasis pada RSA dengan skema secret sharing, mekanisme group signature yang dijelaskan memenuhi persyaratan keamanan group signature [1] [2] [6] [15] sebagai berikut.

A. *Correctness*

Group signature valid yang dihasilkan oleh prosedur **Sign** selalu diterima oleh prosedure **Verify**. Untuk itu perlu dibuktikan dua hal:

(a) bahwa untuk setiap m, e, d, dan $ed \equiv 1 \pmod{\varphi(pq)}$, $(m^e)^d \equiv m \pmod{pq}$ akan selalu terpenuhi; dan

(b) bahwa polinomial $P(x)$ dapat direkonstruksi jika dan hanya jika terdapat minimum t buah (x_i, y_i).

Poin (a) telah dibuktikan dalam tulisan asli tentang RSA pada [16]. Poin (b) telah dibuktikan dengan ekuivalennya: bahwa setiap t buah (x_i, y_i) akan selalu didapatkan $P(x)$ yang unik [9]. Karena kedua poin tersebut terpenuhi, maka dapat dipastikan bahwa setiap group signature valid selalu dapat diverifikasi dengan benar.

B. *Unforgeability*

Tidak satupun group member dapat membuat group signature yang valid seorang diri. Hal ini dimungkinkan karena setiap group member hanya mengetahui x_i dan y_i miliknya sendiri, dan polinomial $P(x)$ tidak akan dapat direkonstruksi apabila hanya ada kurang dari t buah (x_i, y_i) seperti diterangkan sebagai berikut.

Misal diasumsikan $t-1$ dari keseluruhan n buah (x_i, y_i) dan r diketahui oleh seorang penyerang. Untuk setiap kandidat private key d dengan diketahui $d \in [0, r)$, penyerang hanya dapat membuat satu dan hanya satu-satunya polinomial $P'(x)$ dengan orde $t-1$ sehingga $P'(0) = d$ dan $P'(x_i) = y_i$ untuk semua $t-1$ pasangan (x_i, y_i) yang sudah didapatkan. Dengan menginterpolasi semua kemungkinan polinomial, semua polinomial tersebut sama-sama mungkin merupakan polinomial yang benar, sehingga tidak ada informasi yang dapat disimpulkan oleh penyerang tersebut tentang private key d yang asli [9].

C. *Anonimity*

Diberikan sebuah group signature yang valid, tidak dimungkinkan untuk menentukan siapa saja group member yang melakukan signing oleh penerima group signature. Hal ini karena sebagaimana halnya dalam mekanisme klasik RSA, penerima pesan hanya mengetahui group public key. Sementara itu, group signature pesan m dibuat tetap menggunakan group private key, namun group private key tersebut dapat direkonstruksi dengan himpunan t group member yang manapun [9].

D. *Anonimity*

Diberikan beberapa group signature yang dibuat oleh himpunan group member yang sama atau berbeda, tidak mungkin mengkomputasi untuk menentukan bahwa group signature dibuat oleh himpunan t group member yang sama. Hal ini seperti yang didiskusikan sebelumnya. Group signature tetap dibuat menggunakan group private key yang sama, sehingga tidak ada informasi mengenai group member yang membuat signature.

V. PEKERJAAN LEBIH LANJUT

Mekanisme group signature yang diajukan dapat mengakomodir implementasi RSA yang sudah diadopsi oleh teknologi saat ini, tanpa memerlukan banyak perubahan pada mekanisme digital signature dengan RSA yang telah banyak digunakan. Namun, mekanisme group signature ini belum menjadi *secure* group signature karena masih ada 3 (tiga) persyaratan keamanan yang perlu dipenuhi [1] [2] [6] [15]:

- **Exculpability**: signature yang dibuat oleh suatu himpunan *t* group member tidak boleh dapat diatributkan ke himpunan *t* group member yang lain.
- **Traceability**: apabila terjadi sengketa terkait signature yang dibuat pada suatu pesan, GM harus memiliki metode untuk mengetahui semua t group member yang membuat signature pada pesan tersebut.
- **Coalition-resistance**: group member tidak boleh dapat berkolaborasi untuk membuat group signature yang valid tanpa sepengetahuan GM. GM harus dapat mengetahui siapa saja group member yang berkolaborasi.

Sebuah prosedur **Open** yang hanya bisa dilakukan oleh GM diperlukan untuk memenuhi persyaratan keamanan diatas [1] [12] [2] [6]. Prosedur ini belum didefinisikan secara formal dalam mekanisme ini.

Pada mekanisme yang diajukan pada tulisan ini, persyaratan keamanan diatas hanya terpenuhi apabila diasumsikan GM benar-benar *totally trusted* dan prosedur **Sign** hanya dapat dilakukan GM, sehingga GM dapat menyimpan log setiap kali prosedur **Sign** dilakukan. Memastikan hanya GM yang dapat melakukan prosedur **Sign** dapat dilakukan dengan cara bilangan prima r disimpan hanya oleh GM (tidak dibagikan ke group member). Namun hal ini bergantung pada asumsi bahwa nilai r cukup jauh lebih besar dari d dan n sehingga group member tidak dapat mengetahui nilai r dengan mudah.

Mekanisme yang diajukan juga belum mengakomodir penghapusan (*revoking*) keanggotaan seorang group member. Sebuah prosedur **Revoke** diperlukan untuk hal ini [17]. Prosedur ini belum didefinisikan secara formal dalam mekanisme ini.

Penulis mempertimbangkan realisasi prosedur **Open** dan **Revoke** dapat dilakukan kedepannya dengan mengadopsi metode yang digunakan pada [2], yaitu dengan menambahkan satu pihak Security Mediator (SEM) dalam mekanisme yang sudah dibuat.

VI. KESIMPULAN

Mekanisme (t, n)-*threshold* group signature yang diajukan cukup praktis dan sederhana dengan menggunakan RSA dan skema secret sharing berbasis Lagrange interpolating polynomial. Mekanisme ini memenuhi persyaratan keamanan group signature hingga batas tertentu, selama status *totally trusted* GM dapat dipertahankan dan GM dapat menyimpan log pesan yang ditandatangani. Pekerjaan lebih lanjut dibutuhkan untuk meningkatkan keamanan mekanisme yang telah dibuat, terutama realisasi prosedur **Open** dan **Revoke**.

REFERENSI

[1] D. Chaum dan E. van Heyst, "Group Signatures," dalam *Lecture Notes in Computer Science*, Springer-Verlag, 1991, pp. 257-265.

[2] S. Cui dan X. Cheng, "Practical Group Signatures from RSA," dalam *Proceedings of the 20th International Conference on Advanced Information Networking and Applications*, Vienna, 2006.

[3] L. Chen dan T. P. Pedersen, "New group signature schemes," dalam *Lecture Notes in Computer Science*, Springer-Verlag, 1994, pp. 171-181.

[4] J. Camenisch dan M. Stadler, "Efficient and generalized group," dalam *Lecture Notes in Computer Science*, Springer-Verlag, 1997, pp. 465-479.

[5] S. Rong-Hua, "An Efficient Secure Group Signature Scheme," dalam *IEEE TENCON*, 2002.

[6] D. Liu, X. Wang, L. Guo dan M. Huang, "An Efficient Scheme of Group Signature based on DSA," dalam *International Conference on Multimedia Information Networking and Security*, Hubei, 2009.

[7] Y. Desmedt dan Y. Frankel, "Shared generation of authenticators and signatures," dalam *Lecture Notes in Computer Science*, Springer-Verlag, 1991, pp. 457-469.

[8] G. R. Blakley, "Safeguarding cryptographic keys," *National Computer Conference,* pp. 313-317, 1979.

[9] A. Shamir, "How to Share a Secret," *Communications of the ACM,* vol. 22, no. 11, pp. 612-613, 1979.

[10] L. Harn, "Group-oriented (t,n) threshold digital signature scheme and digital multisignature," dalam *IEE Proceedings - Computers and Digital Techniques*, 1994.

[11] W. Tianqin, "a (t,n)-threshold group signature scheme based on compartmented secret sharing," dalam *International Conference on Web Information Systems and Mining*, 2010.

[12] S. Mohanty, B. Majhi dan V. Iyer, "A strong designated verifiable group signature scheme," dalam *International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s)*, Kottayam, 2013.

[13] FIPS 180-4, Secure Hash Standard, Gaithersburg: National Institute of Standards and Technology, 2015.

[14] R. Séroul, "Lagrange Interpolation," dalam *Programming for Mathematicians*, Berlin, Springer-Verlag, 2000, pp. 269-273.

[15] G. Ateniese dan G. Tsudik, "Some open issues and new directions in group signature schemes," dalam *Lecture Notes in Computer Science*, Springer-Verlag, 1999, p. 196–211.

[16] R. Rivest, A. Shamir dan a. L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM,* vol. 21, no. 2, pp. 120-126, 1978.

[17] J. Zhang dan Q. Geng, "On the Security of Group Signature Scheme and Designated Verifier Signature Scheme," dalam *International Conference on Networking, Architecture, and Storage*, Chongqing, 2008.